

Check Point™ VPN-1/FireWall-1® Administration Guide

Check Point 2000

Part No.: 700056
January 2000

CHECK POINT™
Software Technologies Ltd.



We Secure the Internet.

© 1999-2000 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Check Point, the Check Point logo, FireWall-1, FloodGate-1, INSPECT, IQ Engine, Open Security Extension, OPSEC, Provider-1, VPN-1 Accelerator Card, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 Appliance, VPN-1 SecuRemote, ConnectControl, and VPN-1 SecureServer are trademarks or registered trademarks of Check Point Software Technologies Ltd. Meta IP and User-to-Address Mapping are trademarks of MetalInfo, Inc., a wholly-owned subsidiary of Check Point Software Technologies, Inc. RealSecure is a trademark of Internet Security Systems, Inc. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

THIRD PARTIES:

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust's logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

Copyright © 1996-1998. Internet Security Systems, Inc. All Rights Reserved.

RealSecure, SAFESuite, Intranet Scanner, Internet Scanner, Firewall Scanner, and Web Scanner are trademarks or registered trademarks of Internet Security Systems, Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan.

Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Check Point Software Technologies Ltd.

International Headquarters:

3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@CheckPoint.com

U.S. Headquarters:

Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233

<http://www.checkpoint.com>

Please direct all comments regarding this publication to techwriters@checkpoint.com.

Contents

Preface	xxv	
Scope	xxv	
Who Should Use this User Guide	xxvi	
Summary of Contents	xxvi	
What Typographic Changes Mean	xxvii	
Shell Prompts in Command Examples	xxviii	
Network Topology Examples	xxviii	
1. Pre-Installation Configuration	1	
Definitions	1	
Overview	3	
VPN-1/FireWall-1 Architecture	3	
VPN-1/FireWall-1 Products	5	
Enterprise Products	5	
VPN-1/FireWall-1 Single Gateway Products	6	
VPN-1 Products	7	
VPN-1 Enterprise Products	7	
VPN-1 Single Gateway Products	8	
Add-On Products	8	
Example Configurations	9	
VPN-1/FireWall-1 Client/Server Model	13	
VPN-1/FireWall-1 Modules	13	
Client/Server	14	
		Client/Server Interaction 14
2. Installing and Configuring VPN-1/FireWall-1	17	
Before Installing VPN-1/FireWall-1	18	
Protecting the VPN-1/FireWall-1 Machine	18	
Routing	18	
IP Forwarding	18	
DNS	19	
IP Addresses	19	
VPN-1/FireWall-1 Component Configuration	19	
Connectivity	20	
Installation Procedure for a New Installation	20	
Upgrading to a New Version of VPN-1/FireWall-1	21	
Upgrading From a Version Before Version 4.0	21	
Backward Compatibility	21	
VPN-1/FireWall-1 Database	22	
Minimizing Downtime During Upgrades	22	
After Upgrading	23	
Which Components to Install	23	
Installing on Windows Platforms	24	
Minimum Installation Requirements	24	
Installing VPN-1/FireWall-1	25	
Uninstalling VPN-1/FireWall-1 (NT)	43	
Stopping VPN-1/FireWall-1 (NT)	43	
Reconfiguring VPN-1/FireWall-1 (NT)	44	

Installing on Unix Platforms	44	Modifying an Object from the Network Object Manager	100
Minimum Installation Requirements	44	Workstation Properties	102
Installing VPN-1/FireWall-1	45	Workstation Properties Window — General Tab	102
Configuring VPN-1/FireWall-1	51	Workstation Properties Window — Interfaces Tab	104
Uninstalling VPN-1/FireWall-1 (Unix)	57	Workstation Properties Window — VPN Tab	109
Installing the X/Motif GUI Client	58	Workstation Properties Window — Authentication Tab	110
After Installing VPN-1/FireWall-1	58	Workstation Properties Window — SNMP Tab	111
Reinstalling the Security Policy	58	Workstation Properties Window — Certificates tab	112
Obtaining Licenses	58	Workstation Properties Window — NAT (Network Address Translation) Tab	113
Installing Licenses	59	Workstation Properties Window — Account Unit Tab	114
Enabling Logging for FloodGate-1 and Third Party Products	61	Network Properties	115
Configuring VPN-1/FireWall-1	62	Network Properties Window — General Tab	115
Access Control	62	Network Properties Window — NAT (Address Translation) Tab	116
Concurrent Sessions	67	Domain Properties	117
Read Only Sessions	68	Domain Properties Window	117
Authenticating VPN-1/FireWall-1 Administrators	68	Router Properties	118
Distributed Configurations	69	Router Properties Window — General Tab	118
Configuring Centralized Logging	78	Router Properties Window — Interfaces Tab	120
Customer Log Module	78	Router Properties Window — SNMP Tab	127
▼ To direct logging to the Customer Log Module	79	Router Setup	128
Log Viewing and Management	82	Router Management	134
Frequently Asked Questions	83	Switch Object Properties	137
3. Graphical User Interface	87	Switch Properties Window — General Tab	138
Managing VPN-1/FireWall-1	87	Switch Properties Window — Interfaces Tab	139
The Check Point Policy Editor	88	Switch Properties Window — Address Translation Tab	139
Starting the Policy Editor	88	Switch Properties Window — SNMP Tab	139
Problems in Connecting to the Management Server	89	Switch Properties Window — Setup Tab	139
Displaying Policy Editor Windows	91	Switch Properties Window — VLANs Tab	140
Menus	92	Integrated FireWall Properties	141
VPN-1/FireWall-1 Toolbar	96	Integrated FireWalls window — General tab	142
Toolbar Buttons and Menu Commands	96	Integrated FireWalls Properties Window — Interfaces Tab	143
VPN-1/FireWall-1 Status Bar	96		
4. Network Objects	97		
Defining Network Objects	97		
Modifying an Object from the Policy Editor	98		

Integrated FireWalls Properties Window — SNMP Tab	143	Exporting Users from the VPN-1/FireWall-1 User Database	188
Integrated FireWalls Properties Window — NAT Tab	143	Configuring an LDAP Server for VPN-1/FireWall-1	189
Cisco PIX Firewall — Setup A Tab	143	Schema Checking	189
Cisco PIX FireWall — Setup B Tab	145	Troubleshooting	190
PIX Encryption Keys window	146	6. Services and Resources	191
Network Object Groups	147	Defining Services	192
Creating a Group	148	TCP Service Properties	194
Adding an Object to a Group	148	UDP Service Properties	196
Deleting an Object from a Group	149	RPC Service Properties	197
Logical Server Properties	149	ICMP Service Properties	199
Address Range Properties	150	User Defined (or “Other” or “Generic”) Service Properties	200
Address Range Properties Window — General Tab	150	User-Defined Service Properties Example	201
Address Range Properties Window — Address Translation Tab	151	Port Range	202
5. Managing Users	153	Service Groups	202
Overview	153	Resources	203
VPN-1/FireWall-1 Proprietary Users	153	Overview	203
Defining Users and Groups	153	Resource Windows	204
User Properties	156	Wild Cards	205
User Groups	165	URI Resources	205
User Database	166	SMTP Resources	215
Database Installation	167	SMTP Security Server	215
Generic User	167	FTP Resources	220
Overview	167	Resource Groups	222
Notes	169	List of Supported Services	224
External Users and Groups	169	TCP Services	224
Managing External Users	170	UDP Services	231
Managing External Groups	170	RPC Services	234
VPN-1/FireWall-1 LDAP Account Management	174	ICMP Services	235
Overview	174	Other IP Protocol Services	236
The LDAP Model	174		
Account Management Configuration	176		
LDAP Schema	182		
Proprietary Attributes	182		

7. Properties Setup 237

- Security Policy 238
- Services 242
- Log and Alert 243
- Access Lists 245
- SYNDefender 247
- Security Servers 248
- LDAP (Account Management) 249
- Authentication 252
- Encryption 253
- Connect Control 254
 - Server Load Balancing Parameters 254
- High Availability 255
- IP Pool NAT 256
- Desktop Security 257
- Traffic Control 258

8. Security Policy Rule Base 261

- Rule Base — Basic Concepts 261
- Editing a Policy 263
 - Adding a Rule 265
 - Modifying a Rule 266
- Copying, Cutting and Pasting Rules 277
- Deleting a Rule 277
- Completing the Rule Base 277
- Rule Authentication Properties 279
- Encryption Properties 280
- Interaction between Rule Base and Properties 281
- Implied Rules 282
- Masking Rules 283
 - Hiding Rules 283
 - Viewing Hidden Rules 283
 - Unhiding Hidden Rules 284
- Masks 285
- Querying the Rule Base 288
 - Example 288
 - Refining the Query 291
- Rule Base Queries window 295
- Rule Base Query window 296

Rule Base Query Clause window 297

- Disabling Rules 298
- Installing and Uninstalling the Security Policy 298
 - Verifying the Rule Base and Security Policy 298
 - Viewing the Inspection Script 299
 - Installing the Security Policy 300
 - Uninstalling the Security Policy 301
 - Inspection Code Loading 301
- Installing Access Lists 302
 - Importing Access Lists 302
 - Managing Imported Access Lists in the Rule Base 303
 - Verifying and Viewing Access Lists 304
- Installing Access Lists 305
- Default Security Policy 305
 - Overview 305
 - Default Security Policies 306
- Auxiliary Connections 307
- Established TCP Connections 308
 - Overview 308
 - Example 310

9. Time Objects 311

- Overview 311
- Time Object Windows 313
 - Time Object Properties Window — General Tab 313
 - Time Object Properties Window — Days Tab 314
- Time Object Groups 315
 - Creating a Group 315
 - Adding an Object to a Group 316
 - Deleting an Object from a Group 316

10. Server Objects 317

- Server Objects 317
 - Defining Server Objects 318
- UFP Servers 320
 - UFP Server Properties Window — General Tab 321
 - UFP Server Properties Window — Dictionary Tab 322

CVP Servers	322
CVP Server Properties Window — General Tab	322
CVP Manager	323
Overview	323
Configuration	324
Installation	325
CVP Manager Configuration File	325
Authenticated Communications (Control Channel)	327
Installation	329
RADIUS Servers	329
RADIUS Server Properties Window — General Tab	330
RADIUS Server Groups	331
Creating a RADIUS Server Group	331
Adding a Server to a RADIUS Server Group	331
Deleting a Server from a RADIUS Server Group	332
TACACS Servers	332
TACACS Server Properties Window — General Tab	332
AXENT Pathways Defender Servers	333
Defender Server Properties Windows—General Tab	333
Policy Servers	334
LDAP Account Units	334
LDAP Account Unit Properties Window — General Tab	335
LDAP Account Unit Properties Window — User Preferences Tab	337
LDAP Account Unit Properties Window — Encryption Tab	339

11.Security Servers and Content Security 341

Security Servers	341
Overview	341
Security Servers and the Rule Base	344
Interaction with OPSEC Products	354
Defining Security Servers	356
Security Server Configuration	357

Content Security	360
Resources and Security Servers	360
Web (HTTP)	363
Mail (SMTP)	365
FTP	365
CVP Inspection	365

12.System Status Viewer 369

Monitoring System Status	369
Starting the System Status Viewer	370
View	370
Displaying Object Properties	378
Displaying Objects	382
Updating Object Status	383
Options	384
Alerts	385
Menus	386
File Menu	386
View Menu	386
Window Menu	387
System Status Viewer Toolbar	388
Toolbar Buttons and Corresponding Menu Commands	388

13.Log Viewer 389

Viewing the Log	389
Starting the Log Viewer	390
Mode	391
Log Viewer Data	396
Hiding a Column	398
Changing a Column's Width	399
Navigation And Searching	400
Scrolling through the Log File	400
Navigating to a Specific Location in the Log File	400
Finding a Specific Record	401
Displaying Selected Entries	402
Selection Criteria	402
Log Viewer Options	418
Options window — General tab	418

Online Update	419	FTP port command	440
Log File Management	419	Generating Address Translation Rules Automatically	440
Opening a Different Log File	419	Overview	440
Starting A New Log File	419	Configuring Address Translation — Windows GUI	442
Deleting The Currently Displayed Log File	420	Overview	442
Printing and Saving Log Entries	420	Structure of an Address Translation Rule	442
Saving the Currently Displayed Log Entries	420	Address Translation Rule Base Example	443
Printing the Currently Displayed Log Entries	420	Defining Address Translation Rules	445
Miscellaneous Functions	420	Using the Address Translation Rules Editor	448
Redirecting Logging to Another Master	420	Address Translation Examples	457
Exporting Log Data to Another Application	420	Gateway with Two Interfaces	457
Stop Update	421	Gateway with Three Interfaces	460
Reload Log Data	421	Managing PIX Address Translation	464
Menus	421	Overview	465
File Menu	421	Using PIX in the Address Translation Rule Base	466
Edit Menu	422	PIX Address Translation Example	467
View Menu	422	Advanced Topics	470
Select Menu	423	Address Translation and Anti-Spoofing	470
Window Menu	423	Rule Base	475
Help Menu	424	Frequently Asked Questions	475
Log Viewer Toolbar	424	15.Authentication	481
Toolbar Buttons and their corresponding menu commands	424	Overview	481
14.Network Address Translation	425	VPN-1/FireWall-1 Authentication	481
Introduction	425	Three Kinds of Authentication	482
The Need for Address Translation	425	How A User Authenticates	483
Example	427	User Authentication	484
Configuring Address Translation	428	User Authentication — Overview	485
Translation Modes	428	User Authentication — Deployment	486
Hide Mode	429	Non-Transparent User Authentication	495
Statically Translating Addresses	432	User Authentication and the HTTP Security Server	497
Address Translation and Routing	435	Session Authentication	515
Configuring Routing on the Gateway	435	Session Authentication — Overview	515
IANA Recommendations	439	Session Authentication — Deployment	517
Supported Services	439	Client Authentication	526
New Services	439	Client Authentication — Overview	526
Restrictions	439	Client Authentication — Deployment	531

Single Sign On — Additional Features 542

Client Authentication — Examples 545

Encrypted Client Authentication 553

Client Authentication — Security
Considerations 553

Client Authentication — Additional Features 554

16.Active Network Management 557

VPN-1/FireWall-1 State Synchronization 557

Implementation 558

Timing Issues 560

Restrictions 561

Troubleshooting 562

High Availability 563

Overview 563

When Does a VPN/FireWall Module Become
Active? 565

Before Configuring High Availability 565

Installation 567

Synchronization 573

Using High Availability in Virtual Private
Networks 574

Commands 574

Additional Configuration Parameters 579

Server Load Balancing 581

The Need for Server Load Balancing 581

How Server Load Balancing Works 582

Load Balancing Algorithms 584

Logical Servers 584

Rule Base 586

Load Measuring 586

Connection Accounting 587

Active Connections 587

17.Routers and Embedded Systems 589

Overview 589

Routers and Blackboxes 590

Embedded Systems and Appliances 591

18.SNMP and Network Management Tools 593

Overview 593

VPN-1/FireWall-1 SNMP Agent (daemon) 593

FireWall-1 HP OpenView Extension 595

Installing the FireWall-1 HP OpenView
Extension 596

▼ To install the VPN-1/FireWall-1 HP OpenView
Extension (Solaris2) 596

▼ To install the VPN-1/FireWall-1 HP OpenView
Extension
(HP-UX) 596

Uninstalling the VPN-1/FireWall-1 HP OpenView
Extension 597

▼ To uninstall the VPN-1/FireWall-1 HP OpenView
Extension (Solaris2) 597

▼ To uninstall the VPN-1/FireWall-1 HP OpenView
Extension (HP-UX) 598

Viewing FireWalled Objects 598

VPN-1/FireWall-1 MIB Source 600

19.FAQ (Frequently Asked Questions) 605

Defining Objects and Services 605

Daemons 609

Security Servers 609

Logging 614

Security 616

Guidelines for Deploying SYNDefender 621

VPN-1/FireWall-1/n Issues 622

Supported Protocols and Interfaces 623

Inspecting 625

Administrative Issues 627

Performance 628

Index Index-i

Figures

FIGURE 1-1	Distributed VPN-1/FireWall-1 Configuration	3	FIGURE 2-8	Destination Directory window	30
FIGURE 1-2	Client/Server Configuration	4	FIGURE 2-9	Selecting Product Type window	30
FIGURE 1-3	FireWall and Inspection Modules	4	FIGURE 2-10	Selecting a VPN/FireWall Module Product	31
FIGURE 1-4	Configuration with One FireWalled Gateway and Router	9	FIGURE 2-11	Selecting an Inspection Module Product	31
FIGURE 1-5	Configuration with One FireWalled Gateway, a Separate Management Station and Router	10	FIGURE 2-12	Licenses window	32
FIGURE 1-6	Configuration With One FireWalled Gateway and Two Internal Networks	11	FIGURE 2-13	Add License window	32
FIGURE 1-7	Configuration with two FireWalled Gateways controlled by one Management Station	12	FIGURE 2-14	Administrators window	33
FIGURE 1-8	Configuration with Failover Gateways	13	FIGURE 2-15	Add Administrator window	34
FIGURE 1-9	VPN-1/FireWall-1 Client-Server configuration	14	FIGURE 2-16	IP Address window	35
FIGURE 2-1	Distributed VPN-1/FireWall-1 Configuration	23	FIGURE 2-17	GUI Clients window	36
FIGURE 2-2	Welcome window	25	FIGURE 2-18	Masters Configuration window	36
FIGURE 2-3	Existing Version Found window	26	FIGURE 2-19	Add Master window	37
FIGURE 2-4	Backward Compatibility window	27	FIGURE 2-20	Remote Modules window	38
FIGURE 2-5	Selecting Setup Type window	28	FIGURE 2-21	External IF window	39
FIGURE 2-6	Enterprise Product window	29	FIGURE 2-22	IP Forwarding window	40
FIGURE 2-7	Gateway/Server Module window	29	FIGURE 2-23	SMTP Security Server window	41
			FIGURE 2-24	High Availability window	42
			FIGURE 2-25	Key Hit Session window	43
			FIGURE 2-26	cpconfig reconfiguration options	51
			FIGURE 2-27	Check Point Configuration window	65
			FIGURE 2-28	Add Administrator window	66
			FIGURE 2-29	Edit Administrator window	67

FIGURE 2-30	Login window	68	FIGURE 4-16	Network Properties window — Address Translation Tab	116
FIGURE 2-31	Distributed VPN-1/FireWall-1 Configuration	69	FIGURE 4-17	Domain Properties window	117
FIGURE 2-32	Example of <code>control.map</code> file	75	FIGURE 4-18	Router Properties window — General tab	118
FIGURE 2-33	Centralized Logging Configuration	79	FIGURE 4-19	Router Properties window — Interfaces tab	120
FIGURE 2-34	Administrators and GUI Clients — VPN-1/FireWall-1 Installation	82	FIGURE 4-20	Interface Properties window — General and Security tabs	121
FIGURE 3-1	Policy Editor login window	88	FIGURE 4-21	Anti-Spoof Example Configuration with a Router	123
FIGURE 3-2	VPN-1/FireWall-1 Policy Editor window with Rule Base	88	FIGURE 4-22	Setup tab — 3Com and Cisco	126
FIGURE 3-3	Error message window	89	FIGURE 4-23	Router Properties — SNMP tab	127
FIGURE 3-4	VPN-1/FireWall-1 Toolbar	96	FIGURE 4-24	Router Properties — Setup for Cisco Router	128
FIGURE 3-5	VPN-1/FireWall-1 Status Bar	96	FIGURE 4-25	Router Properties— Setup for Bay Networks Router	130
FIGURE 4-1	Network Objects window	98	FIGURE 4-26	Router Properties window — Setup for 3Com Router	131
FIGURE 4-2	Object menu	99	FIGURE 4-27	Router Properties window - Setup for RRAS router	133
FIGURE 4-3	User Access window	100	FIGURE 4-28	Switch Properties window — General tab	138
FIGURE 4-4	Add Network Object menu	100	FIGURE 4-29	Switch Properties window — Setup tab	139
FIGURE 4-5	Workstation Properties window — General tab	102	FIGURE 4-30	Switch Properties window — VLANs tab	140
FIGURE 4-6	Workstation Properties window — Interfaces tab	104	FIGURE 4-31	VLAN Properties window	141
FIGURE 4-7	Interface Properties window — General and Security tabs	105	FIGURE 4-32	Integrated FireWall Properties window — General tab	142
FIGURE 4-8	Anti-Spoof Example Configuration	107	FIGURE 4-33	Cisco PIX Integrated FireWall Properties window — Setup A tab	143
FIGURE 4-9	Workstation Properties window — VPN tab	109	FIGURE 4-34	Cisco PIX Integrated FireWall Properties window — Setup B tab	145
FIGURE 4-10	Workstation Properties window — Authentication tab	110	FIGURE 4-35	PIX Encryption Keys window	146
FIGURE 4-11	Workstation Properties window — SNMP tab	111	FIGURE 4-36	Group Properties window	148
FIGURE 4-12	Workstation Properties window — Certificates tab	112	FIGURE 4-37	Adding a Group to a Group	149
FIGURE 4-13	Workstation Properties window — NAT (Address Translation) tab	113	FIGURE 4-38	Logical Server Properties window	149
FIGURE 4-14	Workstation Properties window — Account Unit tab	114	FIGURE 4-39	Address Range Properties window - General tab	150
FIGURE 4-15	Network Properties window — General tab	115			

FIGURE 4-40	Address Range Properties window — Address Translation Tab	151	FIGURE 5-21	Multiple Account Units - Example Configuration	178
FIGURE 5-1	Users window	154	FIGURE 5-22	LDAP Account Unit Properties window — General tab	179
FIGURE 5-2	New User Object Menu	154	FIGURE 5-23	External User Group (LDAP) window	179
FIGURE 5-3	User Definition Template window	155	FIGURE 5-24	External User Group in a Rule Base	180
FIGURE 5-4	User Properties window — General tab	157	FIGURE 5-25	Enforcing a Security Policy	181
FIGURE 5-5	User Properties window — Groups tab	158	FIGURE 6-1	Services window	192
FIGURE 5-6	User Properties window — Authentication tab — S/Key authentication	159	FIGURE 6-2	Add Service Object menu	193
FIGURE 5-7	User Properties window — Authentication tab — VPN-1/FireWall-1 Password authentication	161	FIGURE 6-3	TCP Service properties window	194
FIGURE 5-8	User Properties window — Authentication tab — RADIUS authentication	161	FIGURE 6-4	Services, Protocol Types and Resources	195
FIGURE 5-9	User Properties window — Authentication tab — TACACS authentication	162	FIGURE 6-5	UDP Service Properties window	196
FIGURE 5-10	User Properties window — Location tab	162	FIGURE 6-6	RPC Service Properties	197
FIGURE 5-11	User Properties window — Time tab	163	FIGURE 6-7	ICMP Service Properties window	199
FIGURE 5-12	User Properties window — Encryption tab	164	FIGURE 6-8	User Defined Service Properties window	200
FIGURE 5-13	Group Properties window	165	FIGURE 6-9	Port Range Properties window	202
FIGURE 5-14	Adding a Group to a Group	166	FIGURE 6-10	Group Properties window	202
FIGURE 5-15	Manage Users on Account Unit window	170	FIGURE 6-11	Adding a Group to a Group	203
FIGURE 5-16	External User Group (LDAP) window	171	FIGURE 6-12	Resources window	204
FIGURE 5-17	External User Group (LDAP) window with sub-branch defined	172	FIGURE 6-13	Resource Type menu	204
FIGURE 5-18	External User Group (LDAP) window with group in branch defined	173	FIGURE 6-14	URI Definition window — General tab	206
FIGURE 5-19	LDAP Tree Example	175	FIGURE 6-15	URI Definition window — Match tab (wild cards specification)	207
FIGURE 5-20	A typical Account Management configuration	176	FIGURE 6-16	URI components	211
			FIGURE 6-17	HTTP Browser connecting through FireWalled Gateway	212
			FIGURE 6-18	URI Definition window — Match tab (file specification)	213
			FIGURE 6-19	URI Definition window — Match tab (UFP specification)	214
			FIGURE 6-20	URI Definition window — Action tab	214
			FIGURE 6-21	SMTP Definition window — General tab	216

FIGURE 6-22	SMTP Definition window — Match tab	217	FIGURE 8-3	Open Policy window	263
FIGURE 6-23	SMTP Definition window — Action tabs	218	FIGURE 8-4	Rule menu	266
FIGURE 6-24	FTP Definition window — General tab	220	FIGURE 8-5	Policy Editor Object Menu	266
FIGURE 6-25	FTP Definition window — Match tab	221	FIGURE 8-6	Network Objects window	267
FIGURE 6-26	FTP Definition window — Action tab	222	FIGURE 8-7	User Access window	268
FIGURE 6-27	Group Properties window	223	FIGURE 8-8	Services window	270
FIGURE 6-28	Adding a Group to a Group	224	FIGURE 8-9	Services with Resource window	270
FIGURE 7-1	Properties Setup window — Security Policy tab	238	FIGURE 8-10	Time Objects window	276
FIGURE 7-2	Properties Setup window — Services tab	242	FIGURE 8-11	Comment window	276
FIGURE 7-3	Properties Setup window — Log and Alert tab	243	FIGURE 8-12	VPN-1/FireWall-1 Inspection Components - flow of information	279
FIGURE 7-4	Properties Setup — Access Lists tab	245	FIGURE 8-13	Authenticate Action Properties window for a User Authentication Rule	280
FIGURE 7-5	Properties Setup window — SYNDefender tab	247	FIGURE 8-14	Encryption Properties window	281
FIGURE 7-6	Properties Setup window — Security Servers tab	248	FIGURE 8-15	Policy Editor showing implied rules	282
FIGURE 7-7	Properties Setup window — LDAP tab	249	FIGURE 8-16	Mask menu	283
FIGURE 7-8	Properties Setup — Authentication tab	252	FIGURE 8-17	Rule Base with a hidden rule not displayed	284
FIGURE 7-9	Properties Setup — Encryption tab	253	FIGURE 8-18	Rule Base before defining masks	285
FIGURE 7-10	Properties Setup — Connect Control tab	254	FIGURE 8-19	Rule Base with FTP rules (rules 3 and 5) hidden	285
FIGURE 7-11	Properties Setup — High Availability tab	255	FIGURE 8-20	Named Masks window	286
FIGURE 7-12	Properties Setup window — IP Pool NAT tab	256	FIGURE 8-21	Store Mask As window	286
FIGURE 7-13	Properties Setup window — Desktop Security tab	257	FIGURE 8-22	Rule Base Queries window	288
FIGURE 7-14	Properties Setup window — Traffic Control tab	258	FIGURE 8-23	Rule Base Query window	289
FIGURE 8-1	Policy Editor window with Rule Base	262	FIGURE 8-24	Rule Base Query Clause window	289
FIGURE 8-2	“None of the Above” Rule	263	FIGURE 8-25	Rule Base Query window showing one query clause	290
			FIGURE 8-26	Rule Base Queries window showing one query	291
			FIGURE 8-27	Rule Base after being masked by the query	291
			FIGURE 8-28	Rule Base Query window showing two query clauses	292
			FIGURE 8-29	Rule Base after being masked by the modified query	293
			FIGURE 8-30	Rule Base Query Clause window showing FTP selected	294

FIGURE 8-31	Rule Base Queries window	295	FIGURE 10-11	RADIUS Server Properties window — General tab	330
FIGURE 8-32	Rule Base Query window	296	FIGURE 10-12	Group Properties window	331
FIGURE 8-33	Rule Base Query Clause window	297	FIGURE 10-13	Adding a Group to a Group	332
FIGURE 8-34	Rule Base with rule 1 and rule 3 disabled	298	FIGURE 10-14	TACACS Server Properties window — General tab	332
FIGURE 8-35	View Inspection Script Text	299	FIGURE 10-15	Defender Server Properties window — General tab	333
FIGURE 8-36	Install Policy window	300	FIGURE 10-16	Defender Server Properties window — General tab	334
FIGURE 8-37	Router Access Lists Operations window with import options	303	FIGURE 10-17	LDAP Account Unit Properties window — General tab	335
FIGURE 8-38	Router Access List Operations window	304	FIGURE 10-18	LDAP Branch Definition	337
FIGURE 8-39	View of a Cisco Access List	305	FIGURE 10-19	LDAP Account Unit Properties window — User Preferences tab	338
FIGURE 9-1	Time Objects window	311	FIGURE 10-20	LDAP Account Unit Properties window — Encryption tab	339
FIGURE 9-2	Add Time Object menu	312	FIGURE 11-1	A connection handled by the VPN-1/FireWall-1 Inspection (Kernel) Module	342
FIGURE 9-3	Time Object Properties window — General tab	313	FIGURE 11-2	A connection mediated by a VPN-1/FireWall-1 Security Server	342
FIGURE 9-4	Time Object Properties window — Days tab (Days in Month)	314	FIGURE 11-3	Protected FTP Server	344
FIGURE 9-5	Time Object window — Days tab (Days in Month)	315	FIGURE 11-4	Authentication Procedure	346
FIGURE 9-6	Group Properties window	316	FIGURE 11-5	VPN-1/FireWall-1 SMTP Security Server	349
FIGURE 9-7	Adding a Group to a Group	316	FIGURE 11-6	Proxy Configuration — Netscape 4.0 and Internet Explorer 3.0x	351
FIGURE 10-1	Server Objects window	319	FIGURE 11-7	HTTP Proxy and Security Proxy Settings — Netscape 4.0x and Internet Explorer 3.0x	352
FIGURE 10-2	New Server Object menu	319	FIGURE 11-8	Connection invoking a UFP Server	355
FIGURE 10-3	UFP Server Properties window — General tab	321	FIGURE 11-9	Properties Setup window - Security Servers tab	356
FIGURE 10-4	UFP Server Properties window — Dictionary tab	322	FIGURE 11-10	\$FWDIR/conf/fwauthd.conf — example	357
FIGURE 10-5	CVP Server Properties window — General tab	322	FIGURE 11-11	A connection mediated by the HTTP Security Server	361
FIGURE 10-6	Three CVP Servers invoked one after the other	323	FIGURE 11-12	Content Vectoring Server	362
FIGURE 10-7	Three CVP Servers with load sharing	324	FIGURE 11-13	URI Resource Definition	363
FIGURE 10-8	CVP Server Properties window	325			
FIGURE 10-9	CVP Mannager Configuration - No Load Sharing Example	326			
FIGURE 10-10	CVP Manager Configuration - Load Sharing Example	327			

FIGURE 11-14	URI Definition window — Match tab (UFP specification) 364	FIGURE 13-12	Find Date window 401
FIGURE 11-15	Rule Base using Resources 364	FIGURE 13-13	Find menu 401
FIGURE 11-16	SMTP Resource with CVP properties 366	FIGURE 13-14	Find in all Fields window 402
FIGURE 12-1	System Status Login window 370	FIGURE 13-15	Column Selection Menu 403
FIGURE 12-2	System Status Details View 371	FIGURE 13-16	Current Selection Criteria window 404
FIGURE 12-3	System Status Icons View - VPN-1/FireWall-1 and High Availability 376	FIGURE 13-17	Number Selection Criterion window 405
FIGURE 12-4	An object in Icons View 376	FIGURE 13-18	Interface Selection Window 406
FIGURE 12-5	Properties Window — General Tab 378	FIGURE 13-19	Source Object Selection Criterion window 407
FIGURE 12-6	Properties Window — VPN-1&FireWall-1 Tab 379	FIGURE 13-20	Xlated Dst Selection Criterion window 408
FIGURE 12-7	Properties Window — FloodGate-1 Tab 380	FIGURE 13-21	Xlated Source Port Selection Criterion window 409
FIGURE 12-8	Properties Window - Compression Tab 381	FIGURE 13-22	Type Selection Criterion Window 409
FIGURE 12-9	Properties Window - High Availability Tab 382	FIGURE 13-23	Action Selection Criterion window 411
FIGURE 12-10	Show/Hide Objects window 383	FIGURE 13-24	Product Selection window 412
FIGURE 12-11	Automatic Update window 383	FIGURE 13-25	Protocol Selection Criterion Window 413
FIGURE 12-12	Options window 384	FIGURE 13-26	Information Selection Criterion Window 414
FIGURE 12-13	Alerts window 385	FIGURE 13-27	Log File — Selection Criteria Not Applied 415
FIGURE 12-14	System Status Viewer Toolbar 388	FIGURE 13-28	Interface Selection window 416
FIGURE 13-1	Log Viewer Login window 390	FIGURE 13-29	Service Selection Criterion window 416
FIGURE 13-2	Log Viewer 391	FIGURE 13-30	Log Viewer Selection Manager Showing Two Criteria 417
FIGURE 13-3	Log Viewer showing Accounting Entries 392	FIGURE 13-31	Log File — Selection Criteria Applied 417
FIGURE 13-4	Log Viewer showing Active Connections 393	FIGURE 13-32	Options window — General tab 418
FIGURE 13-5	Block Intruder window 394	FIGURE 13-33	Log Viewer Toolbar 424
FIGURE 13-6	Block Request window 395	FIGURE 14-1	Example Network Configuration 427
FIGURE 13-7	Column Menu 398	FIGURE 14-2	NAT tab for localnet 430
FIGURE 13-8	Hide/Unhide menu 398	FIGURE 14-3	Hide Mode Address Translation 430
FIGURE 13-9	Width window 399	FIGURE 14-4	Hide Mode Automatically Generated Rules 431
FIGURE 13-10	Width Menu 399	FIGURE 14-5	Static Address Translation 432
FIGURE 13-11	Dragging the Vertical Column Header Border 400		

FIGURE 14-6	Address Translation using Static Source Mode	433	FIGURE 14-32	Address Translation Rule Base	459
FIGURE 14-7	Automatically Generated Address Translation rules for Static Translation	433	FIGURE 14-33	Gateway with Three Interfaces Example - Network	460
FIGURE 14-8	Address Translation using Static Destination Mode	434	FIGURE 14-34	Hiding localnet	460
FIGURE 14-9	Hiding a Network	435	FIGURE 14-35	Hiding PrivateNet	461
FIGURE 14-10	Hiding a Network Behind a Non-Existent IP Address	436	FIGURE 14-36	Translating HTTPServer	461
FIGURE 14-11	Hiding a Network Behind a Real IP Address	436	FIGURE 14-37	Automatically Generated Rules - Three Interfaces	462
FIGURE 14-12	Static Address Translation	438	FIGURE 14-38	Three Interfaces - Both Networks Statically Translated	463
FIGURE 14-13	Static Address Translation for mailsrvr	438	FIGURE 14-39	Rule Base - Both Networks Statically Translated	463
FIGURE 14-14	Static Address Translation rules	438	FIGURE 14-40	Multiple Translation Rules Added to Automatically Generated Rules	464
FIGURE 14-15	Automatic Address Translation for a Network	441	FIGURE 14-41	Example Configuration	467
FIGURE 14-16	Address Translation Rules in the Windows GUI	442	FIGURE 14-42	Address Range Properties — Inside Addresses and Global Addresses	468
FIGURE 14-17	Manually Added Address Translation Rules	443	FIGURE 14-43	Hide Mode rule	468
FIGURE 14-18	Multiple Translation rule	445	FIGURE 14-44	Workstation Properties — Inside Host and Corresponding Global Address	469
FIGURE 14-19	Add Network Object menu	446	FIGURE 14-45	Address Translation Rule Base with Static Address Translation rules	469
FIGURE 14-20	Address Range Properties window	446	FIGURE 14-46	Security Policy Rule Base	469
FIGURE 14-21	Add Service Object menu	447	FIGURE 14-47	Address Translation and Anti-Spoofing (Hide Mode)	471
FIGURE 14-22	Port Range Properties window	447	FIGURE 14-48	Address translation and Anti-Spoofing (Static Source Mode)	472
FIGURE 14-23	Address Translation Rules Editor	448	FIGURE 14-49	Address translation and Anti-Spoofing (Static Destination Mode)	473
FIGURE 14-24	Object Manager window	450	FIGURE 14-50	Address Translation and Anti-Spoofing (Example)	474
FIGURE 14-25	Services window	452	FIGURE 14-51	Hidden Internal Network	476
FIGURE 14-26	Select Target window	456	FIGURE 14-52	Invalid IP Addresses	479
FIGURE 14-27	Comment window	456	FIGURE 15-1	Authentication Rule	481
FIGURE 14-28	Gateway with Two Interfaces Example - Network	457	FIGURE 15-2	User Properties window — Authentication tab	483
FIGURE 14-29	mailserver - static translation	458	FIGURE 15-3	A connection mediated by the TELNET Security Server	485
FIGURE 14-30	PublicServers Address Range	458	FIGURE 15-4	Example configuration	487
FIGURE 14-31	localnet Network Properties and NAT tabs	459			

FIGURE 15-5	Example User Authentication Rule	487	FIGURE 15-28	Configuration window — SSL Configuration tab	520
FIGURE 15-6	User Properties window - Authentication tab and Location tab	488	FIGURE 15-29	SETUP.INI file	521
FIGURE 15-7	Group Properties window - LocalManagers group	488	FIGURE 15-30	SSL Configuration Tab — Session Authentication Agent	523
FIGURE 15-8	Workstation Properties window — Authentication tab	489	FIGURE 15-31	Session Authentication Action Authentication Properties window	523
FIGURE 15-9	Properties Setup window — Authentication tab	490	FIGURE 15-32	Session Authentication window — user prompt	525
FIGURE 15-10	User Authentication Action Properties window	492	FIGURE 15-33	Session Authentication window — password prompt	526
FIGURE 15-11	GUI FTP Authentication	494	FIGURE 15-34	Example Client Authentication Rule Base	527
FIGURE 15-12	Non-Transparent User Authentication.	496	FIGURE 15-35	Example configuration — Client Authentication	531
FIGURE 15-13	Properties Setup window — Security Servers and Authentication tabs	498	FIGURE 15-36	Example Client Authentication rule	532
FIGURE 15-14	HTTP Server Definition window	500	FIGURE 15-37	User Properties window - Authentication tab and Location tab	532
FIGURE 15-15	Defining the gateway as the HTTP proxy — Netscape 4.0	503	FIGURE 15-38	Group Properties window — Defining Permitted Users	533
FIGURE 15-16	HTTPS Service Definition	505	FIGURE 15-39	User Access window	533
FIGURE 15-17	A Typical User ID and Password Window	506	FIGURE 15-40	Workstation Properties window — Authentication tab	534
FIGURE 15-18	Example HTTP Server definition	511	FIGURE 15-41	Client Authentication Action Properties window — General tab	535
FIGURE 15-19	HTTP Servers behind a FireWalled gateway	513	FIGURE 15-42	Client Authentication Action Properties window — Limits tab	537
FIGURE 15-20	HTTP Server Definition — Server for Null Requests	514	FIGURE 15-43	Properties Setup window — Authentication tab	539
FIGURE 15-21	Session Authentication	516	FIGURE 15-44	Single Sign On Extension.	542
FIGURE 15-22	VPN-1/FireWall-1 Session Authentication Agent Prompt	516	FIGURE 15-45	Client Authentication Rule	545
FIGURE 15-23	Example configuration	517	FIGURE 15-46	Client Authentication - Standard Sign On for all Services and Destinations Allowed Under Rule	547
FIGURE 15-24	Example Session Authentication Rule	517	FIGURE 15-47	Client Authentication - Specific Sign On for two Services (Each One on a Different Host)	548
FIGURE 15-25	FireWall-1 Session Authentication window	518	FIGURE 15-48	Client Authentication - Signing Off	549
FIGURE 15-26	Configuration window — Passwords tab	519	FIGURE 15-49	HTTP session on port 900	549
FIGURE 15-27	Configuration window — Allowed FireWall-1 tab	520	FIGURE 15-50	VPN-1/FireWall-1 Session Authentication Agent prompt	551

FIGURE 15-51	Beginning an encrypted Client Authentication Session	553
FIGURE 15-52	\$FWDIR/conf/fwauthd.conf file	555
FIGURE 16-1	Two VPN/FireWall Modules in Synchronized Configuration	559
FIGURE 16-2	High Availability configuration	563
FIGURE 16-3	VPN-1/FireWall-1 Configuration - High Availability tab	568
FIGURE 16-4	Configure Shared Interfaces window	569
FIGURE 16-5	Load Balancing among several servers	582
FIGURE 16-6	Logical Server Properties window	585
FIGURE 16-7	Using Logical Servers in a Rule	586
FIGURE 17-1	FireWall and Inspection Modules	591
FIGURE 19-1	Accessing FTP through an HTTP proxy	611
FIGURE 19-2	Authenticating FTP through the HTTP Security Server	612
FIGURE 19-3	n FTP authenticating FireWalls	612
FIGURE 19-4	n HTTP Authenticating FireWalls	613
FIGURE 19-5	"connection to original-MTA failed"	614
FIGURE 19-6	TCP SYN handshake	617
FIGURE 19-7	SYN Attack	618
FIGURE 19-8	The SYN Attack unsuccessful, because Z' is reachable	619
FIGURE 19-9	SYNDefender Gateway	620
FIGURE 19-10	SYNDefender Passive Gateway	621
FIGURE 19-11	Incoming and Outgoing Communications	625
FIGURE 19-12	Protecting Internal Hosts	626

Tables

TABLE P-1	Typographic Conventions	xxvii	TABLE 4-2	Object Types	101
TABLE P-2	Shell Prompts	xxviii	TABLE 4-3	Default File Locations and Names	103
TABLE 1-1	Platform Summary	5	TABLE 4-4	Valid Addresses for each interface	107
TABLE 2-1	Components to Install on Each Computer	24	TABLE 4-5	Valid Addresses for each interface	123
TABLE 2-2	Minimum Requirements (GUI Client)	24	TABLE 5-1	User types	155
TABLE 2-3	Minimum Requirements (Management or VPN/FireWall Module)	25	TABLE 5-2	Authentication Schemes and windows	159
TABLE 2-4	Minimum Requirements (Unix Platforms)	44	TABLE 5-3	Object Class OIDs	182
TABLE 2-5	VPN-1/FireWall-1 package names	46	TABLE 5-4	Attributes	183
TABLE 2-6	fw putlic parameters	60	TABLE 6-1	Service Object Types	193
TABLE 2-7	Setting Administrator Permissions	63	TABLE 6-2	Specifying a Port Number	195
TABLE 2-8	VPN-1/FireWall-1 Components	70	TABLE 6-3	VPN-1/FireWall-1 Features Incompatible with Fast Mode enabled	196
TABLE 2-9	control.map access operations	74	TABLE 6-4	Default File Locations and Names	198
TABLE 2-10	Authentication methods	75	TABLE 6-5	Definitions in \$FWDIR/lib/base.def	201
TABLE 2-11	VPN-1/FireWall-1 distributed configuration - fw putkey	77	TABLE 6-6	Resource Types	204
TABLE 2-12	Backing Up a Security Policy	84	TABLE 6-7	Wild Card Usage	205
TABLE 3-1	Starting the Check Point Policy Editor	88	TABLE 6-8	URI components	211
TABLE 3-2	Displaying Policy Editor windows	91	TABLE 6-9	When Schemes Are Applied	212
TABLE 4-1	Network Object Actions	98	TABLE 6-10	URI Specification File Format	213

TABLE 6-11	TCP Services	224	TABLE 12-4	FloodGate-1 Data	373
TABLE 6-12	UDP Services	231	TABLE 12-5	Compression Data	374
TABLE 6-13	RPC Services	234	TABLE 12-6	High Availability Data	374
TABLE 6-14	ICMP Services	235	TABLE 12-7	Icons View — Check Point Product Status	377
TABLE 6-15	Other IP Protocol Services	236	TABLE 12-8	File Menu Commands	386
TABLE 8-1	Adding a Rule	265	TABLE 12-9	View Menu Commands	386
TABLE 8-2	Rule menu items	266	TABLE 12-10	Window Menu Commands	387
TABLE 8-3	Modifying Network Objects	267	TABLE 12-11	Toolbar Buttons and Corresponding Menu Commands	388
TABLE 8-4	Action Menu	272	TABLE 13-1	Starting the Log Viewer	390
TABLE 8-5	Difference between Reject and Drop	272	TABLE 13-2	Actions	396
TABLE 8-6	Track Menu	273	TABLE 13-3	Action Types	397
TABLE 8-7	Install On Menu	274	TABLE 13-4	Entry Types	410
TABLE 8-8	Rule Enforcement Directions	275	TABLE 13-5	Action icons	411
TABLE 8-9	Copying, Cutting and Pasting Rules	277	TABLE 13-6	File Menu Commands	421
TABLE 8-10	Deleting a Rule	277	TABLE 13-7	Edit Menu Commands	422
TABLE 8-11	Authenticate Action Properties window	280	TABLE 13-8	View Menu Commands	422
TABLE 8-12	Logging a Re-Established TCP Connections	310	TABLE 13-9	Select Menu Commands	423
TABLE 9-1	Time Object Actions	312	TABLE 13-10	Window Menu Commands	423
TABLE 10-1	Server Object Actions	319	TABLE 13-11	Help Menu Commands	424
TABLE 10-2	Server Types	320	TABLE 13-12	Toolbar Buttons and their corresponding menu commands	424
TABLE 10-3	Encryption Method Parameters	340	TABLE 14-1	Private Networks Address Space	439
TABLE 11-1	VPN-1/FireWall-1 Security Servers — features	343	TABLE 14-2	Address Translation — Service Restrictions	440
TABLE 11-2	FTP actions and commands	347	TABLE 14-3	Condition vs. Translation	443
TABLE 11-3	Fields in \$FWDIR/conf/smtp.conf	350	TABLE 14-4	Adding a Rule	449
TABLE 11-4	\$FWDIR/conf/fwauthd.conf fields	357	TABLE 14-5	Original Packet - Source	449
TABLE 11-5	Security Service binaries	358	TABLE 14-6	Original Packet - Destination	451
TABLE 12-1	Starting the System Status Viewer	370	TABLE 14-7	Original Packet - Services	451
TABLE 12-2	General Information	371	TABLE 14-8	Translated Packet - Source	452
TABLE 12-3	VPN-1/FireWall-1 field	372	TABLE 14-9	Translated Packet - Destination	454
			TABLE 14-10	Install On Menu	455

TABLE 14-11	Copying, Cutting and Pasting Rules 456
TABLE 14-12	Comparison of PIX and VPN-1/FireWall-1 in the Address Translation Rule Base 466
TABLE 14-13	Original Packet - Source 466
TABLE 15-1	Comparison of Authentication Types 483
TABLE 15-2	Meaning of “No Activity” 490
TABLE 15-3	Access Possibilities 493
TABLE 15-4	HTTP Security Server “Reason” messages 507
TABLE 15-5	Browser Messages 508
TABLE 15-6	HTTPS options 511
TABLE 15-7	Servers and URLs 513
TABLE 15-8	SSL options 522
TABLE 16-1	SyncMode values 573
TABLE 16-2	Explanation of Rule Base 586
TABLE 17-1	Routers and Blackboxes - supported VPN-1/FireWall-1 features 590
TABLE 17-2	Embedded Systems - supported FireWall-1 feature 592
TABLE 18-1	VPN-1/FireWall-1 MIB Variables 595
TABLE 18-2	Minimum Requirements 596
TABLE 18-3	FireWall Menu Commands 599
TABLE 19-1	Services available under both TCP and UDP 606
TABLE 19-2	Services available both as RPC and TCP or UDP 607
TABLE 19-3	Services Dependent on Other Services 607
TABLE 19-4	<code>sdconf.rec</code> directory 610
TABLE 19-5	Gateways - Direction of Enforcement 626
TABLE 19-6	Hosts - Direction of Enforcement 626

Preface

Scope

The VPN-1/FireWall-1 User Guide describes CheckPoint VPN-1/FireWall-1, and consists of the following books:

Getting Started with VPN-1/FireWall-1

This book introduces VPN-1/FireWall-1 and describes the VPN-1/FireWall-1 installation process.

VPN-1/FireWall-1 Administration Guide

This book is the technical reference to VPN-1/FireWall-1 features, including authentication and address translation. In addition, chapters on troubleshooting and Frequently Asked Questions (FAQ) are included.

Check Point Virtual Private Networks

This book describes how to implement the Virtual Private Network features in Check Point VPN-1/FireWall-1.

Check Point Reference Guide

This book describes INSPECT, the command line interface and other reference subjects, and includes a glossary.

Account Management Client

This book describes how to install and use the Check Point Account Management Client.

Who Should Use this User Guide

This User Guide is written for system administrators who are responsible for maintaining network security. It assumes you have a basic understanding and a working knowledge of:

- system administration
- the Unix or Windows operating system
- the Windows GUI
- Internet protocols (IP, TCP, UDP *etc.*)

Summary of Contents

Chapter 1, “Pre-Installation Configuration,” describes how to configure VPN-1/FireWall-1.

Chapter 2, “Installing and Configuring VPN-1/FireWall-1,” describes how to install VPN-1/FireWall-1.

Chapter 3, “Graphical User Interface,” describes how to use the Check Point Graphical User Interface (GUI).

Chapter 4, “Network Objects,” describes how to define network objects (gateways, hosts, routers, switches, and others).

Chapter 5, “Managing Users,” describes how to define and manage users, including users defined on an LDAP Server.

Chapter 6, “Services and Resources,” describes how to define network services.

Chapter 7, “Properties Setup,” describes how to define VPN-1/FireWall-1 properties.

Chapter 8, “Security Policy Rule Base,” describes how to define and enforce a Security Policy’s rules.

Chapter 9, “Time Objects,” describes how to define the time objects used in rules.

Chapter 10, “Server Objects,” describes how to define Server objects.

Chapter 11, “Security Servers and Content Security,” describes the VPN-1/FireWall-1 Security Servers and how they are used to implement the Content Security feature.

Chapter 12, “System Status Viewer,” describes the System Status Viewer.

Chapter 13, “Log Viewer,” describes the Log Viewer.

Chapter 14, “Network Address Translation,” describes VPN-1/FireWall-1’s Network Address Translation feature.

Chapter 15, “Authentication,” describes VPN-1/FireWall-1’s Authentication features.

Chapter 16, “Active Network Management,” describes VPN-1/FireWall-1’s Active Network Management features, including ConnectControl and Connection Accounting.

Chapter 17, “Routers and Embedded Systems,” describes the VPN-1/FireWall-1 features supported by third-party devices such as routers and switches.

Chapter 18, “SNMP and Network Management Tools,” describes how VPN-1/FireWall-1 interfaces to network management tools.

Chapter 19, “FAQ (Frequently Asked Questions),” is a compilation of Frequently Asked Questions about VPN-1/FireWall-1.

What Typographic Changes Mean

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

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	<div>machine_name% u Password:</div>
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type <code>rm filename</code> .
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User’s Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.
Save	Text that appears on an object in a window	Click on the Save button.



Note – This note draws the reader’s attention to important information.



Warning – This warning cautions the reader about an important point.



Tip – This is a helpful suggestion.

Shell Prompts in Command Examples

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

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	<i>machine_name%</i>
C shell superuser prompt	<i>machine_name#</i>
Bourne shell and Korn shell prompt	\$
Bourne shell and Korn shell superuser prompt	#
DOS	<i>current-directory></i>

Network Topology Examples

Network topology examples usually show a gateway's name as a city name (for example, Paris or London) and the names of hosts behind each gateway as names of popular sites in those cities (for example, Eiffel and BigBen).

Pre-Installation Configuration

In This Chapter

<i>Definitions</i>	<i>page 1</i>
<i>Overview</i>	<i>page 3</i>
<i>VPN-1/FireWall-1 Products</i>	<i>page 5</i>
<i>VPN-1 Products</i>	<i>page 7</i>
<i>Add-On Products</i>	<i>page 8</i>
<i>Example Configurations</i>	<i>page 9</i>
<i>VPN-1/FireWall-1 Client/Server Model</i>	<i>page 13</i>
<i>Client/Server Interaction</i>	<i>page 14</i>

Definitions

Following is a list of terms and their meanings as used in this chapter.

Enforcement Point

A machine that enforces at least some part of a VPN-1/FireWall-1 Security Policy. An enforcement point can be a workstation, router, switch or any machine that can be managed by a Management Module by installing a Security Policy or Access List.

FireWalled gateway or FireWalled host

A machine on which a VPN/FireWall Module or Inspection Module (see “VPN/FireWall Module” on page 4) is installed and running is known as a FireWalled gateway or FireWalled host.

Management Module

The Management Module is used to define a Security Policy. In the Client/Server deployment, a Management Station can be divided into a Management Server and a GUI Client, each running on a different machine.

Management Server

The server side of the Client/Server deployment. The Management Server is part of the Management Module (see “Management Module” on page 3).

Management Station or Management Point

A machine on which a Management Module (see “Management Module” on page 3) is installed is known as a Management Station.

node

A node is a computing device with an IP address connected to the protected network.

router

A router is a special purpose hardware device that functions as a packet filter. Filtering rules are defined in Access Lists, which are created by the VPN-1/FireWall-1 Management Module and installed on the router.



Note – A Bay Networks router can function in either of two modes: as a packet filter (in which case VPN-1/FireWall-1 installs an Access List on the router), or as a FireWalled router (in which case VPN-1/FireWall-1 installs a Security Policy on the router). Bay Networks routers cannot implement VPN-1/FireWall-1’s Encryption, Authentication or Address Translation features.

switch

A device which allows a connection to be established when necessary, and terminated when a session ends.



Note – A VPN-1/FireWall-1 Security Policy can be installed on a Xylan switch. However, a Xylan switch cannot implement VPN-1/FireWall-1’s Encryption, Authentication or Address Translation features.

Overview

VPN-1/FireWall-1 Architecture

VPN-1/FireWall-1 comprises two primary modules, the Management Module and the VPN/FireWall Module.

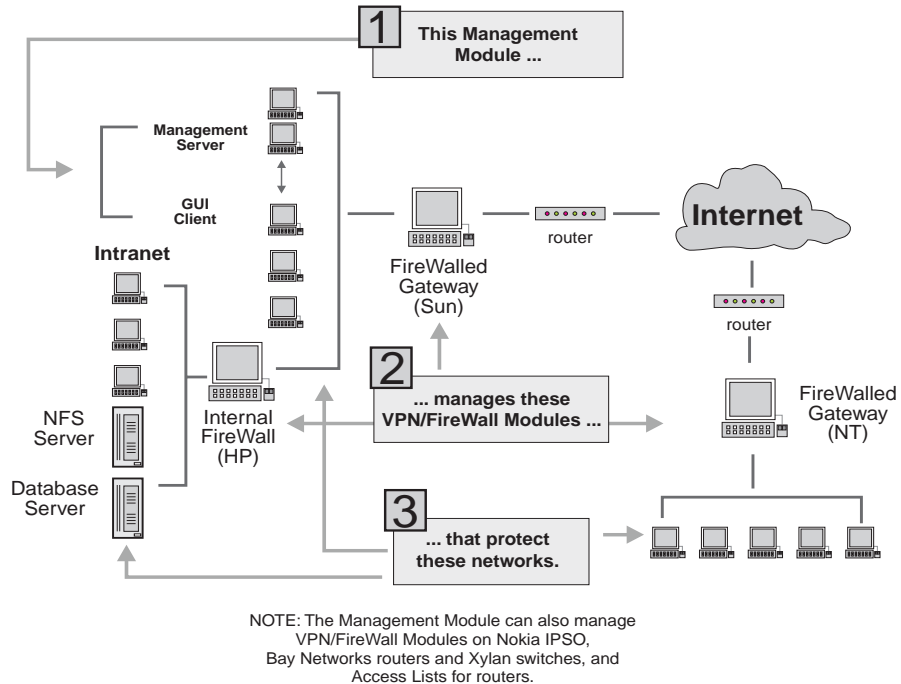


FIGURE 1-1 Distributed VPN-1/FireWall-1 Configuration

Management Module

The Management Module includes the Graphical User Interface (GUI) and the Management Server.

The GUI is the front end to the Management Server, which manages the VPN-1/FireWall-1 database: the Rule Base, network objects, services, users etc.

The Management Module can be deployed in a Client/Server configuration. The Client can run either a Windows 9x, Windows NT or X/Motif Graphical User Interface, and controls a Management Server running on any of the supported platforms.

The Client interacts with the user via the GUI, but all the data (the VPN-1/FireWall-1 database and configuration file) is maintained on the Management Server.

In the configuration depicted in FIGURE 1-2, the functionality of the Management Module is divided between two workstations (BigBen and Tower). The Management Server (including the VPN-1/FireWall-1 database) is on Tower. The GUI Client is on BigBen.

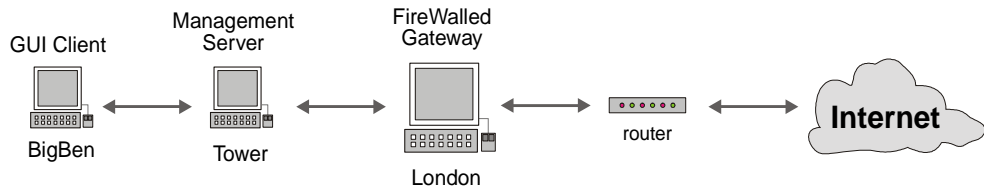


FIGURE 1-2 Client/Server Configuration

The user, working on BigBen, maintains the VPN-1/FireWall-1 Security Policy and database, which reside on Tower. The VPN/FireWall Module is installed on London, the FireWalled gateway, which enforces the Security Policy and protects the network.

VPN/FireWall Module

The VPN/FireWall Module includes the Inspection Module, the VPN-1/FireWall-1 Security Servers and the High Availability feature.

FIGURE 1-3 depicts the relationship between VPN/FireWall Module and Inspection Module features.

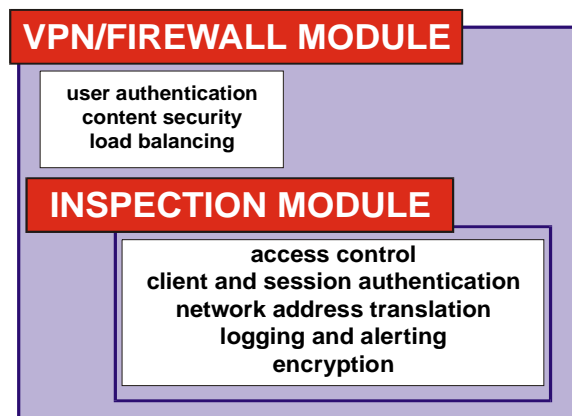


FIGURE 1-3 FireWall and Inspection Modules

The Inspection Module implements the Security Policy, logs events, and communicates with the Management Module using the VPN-1/FireWall-1 daemons. The Inspection Module can run on any of the supported platforms (see TABLE 1-1 on page 5). The VPN/FireWall Module adds the indicated features to those of the Inspection Module.

The GUI Client, the Management Server and the VPN/FireWall Module (or Inspection Module) can be installed on different computers, or on the same computer if its platform supports all three components. The system administrator uses the Management Module to define the Security Policy, but it is the FireWalled gateway (on which the VPN/FireWall Module is installed) that enforces the Security Policy.

TABLE 1-1 summarizes the availability of the VPN-1/FireWall-1 components on different platforms:

TABLE 1-1 Platform Summary

Component	Platforms
GUI Client	<ul style="list-style-type: none"> ■ Windows 9x, Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only ■ X/Motif (Solaris, HP-UX 10.20, IBM AIX)
Management Module, VPN/FireWall Module, SecureServer	<ul style="list-style-type: none"> ■ Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only ■ Solaris 2.6, Solaris Operating Environment 7 (formerly known as Solaris 2.7) in 32 bit installation mode only — SPARC and x86 ■ HP-UX 10.20, 11.0 ■ IBM AIX 4.2.1, 4.3.2 ■ Red Hat Linux 6.1 with kernel version 2.2.x
SecureClient, SecuRemote	Windows 9x, Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only

Bay Networks and Xylan Support

An Inspection Module can be installed on Bay Networks routers and Xylan switches. The standard Inspection Module features, with the exception of Address Translation and Client and Session Authentication, are supported. An Encryption Module cannot be added to an Inspection Module on Bay Networks and Xylan.

This feature enables a greatly improved level of security to be implemented at the router and switch levels.

VPN-1/FireWall-1 Products

Enterprise Products

Enterprise Security Console

This product includes:

- Management Module

The VPN-1/FireWall-1 Enterprise Security Console is a distributed management console for managing multiple security enforcement points. The VPN-1/FireWall-1 Enterprise Security Console can manage any number of VPN/FireWall Modules and Inspection Modules installed on other machines.

Enterprise Center

The VPN-1/FireWall-1 Enterprise Center includes:

- VPN-1/FireWall-1 Enterprise Security Console
- VPN/FireWall Module

The VPN/FireWall Module can be used to protect an unlimited number of nodes behind the gateway (the machine on which it is installed).

The Management Module and VPN/FireWall Module can be installed on the same machine or on different machines.

VPN-1/FireWall-1 Network Security Center

This product includes:

- VPN-1/FireWall-1 Enterprise Center
- Open Security Extension (see “Account Management for Enterprise Console” on page 9)

VPN-1/FireWall-1 Single Gateway Products

VPN-1/FireWall-1/n (VPN-1/FireWall-1/25, VPN-1/FireWall-1/50 etc.)

These products include:

- Management Module
- VPN/FireWall Module

VPN-1/FireWall-1 products enforce restrictions based on the number of protected hosts. If these restrictions are exceeded, VPN-1/FireWall-1 will issue an error message. These restrictions are:

- 1** number of internal hosts

Up to n nodes behind the gateway are allowed, where n is the number in the product name. For example, FireWall-1/50 is restricted to 50 nodes, VPN/FireWall-1/250 is restricted to 250 nodes, *etc.*

A node is defined as a computing device with an IP address. A multi-user computer with one IP address is counted as one node.

This restriction relates to the number of protected hosts. Every host behind VPN-1/FireWall-1 is protected by VPN-1/FireWall-1, even if no connections to the outside are initiated from that host.

Every node protected by VPN-1/FireWall-1 is counted against the limit, even if its IP address is hidden from VPN-1/FireWall-1 by a proxy or by other means.

2 number of external interfaces

For all VPN-1/FireWall-1/*n* products, only one external interface may be connected to the FireWalled machine.

There is *no* restriction on the number of internal interfaces on the FireWalled machine.

3 no external VPN/FireWall Modules

An additional restriction for these products is that they cannot manage external VPN/FireWall Modules, that is, the Management Module and the VPN/FireWall Module must both be on the same machine. However, the Management Module can be deployed in a Client/Server configuration.



Warning – If you exceed the restriction on the number of protected hosts, VPN-1/FireWall-1 will display warning messages on the system console notifying you that you have violated the terms of the VPN-1/FireWall-1 license. You should immediately upgrade to the appropriate product in order to be in compliance with the terms of the VPN-1/FireWall-1 license. In the meantime, your security is not compromised and VPN-1/FireWall-1 will continue to protect your network.

VPN-1 Products

VPN-1 Enterprise Products

VPN-1 Enterprise Security Console

This product includes:

- Management Module

The VPN-1 Enterprise Security Console is a distributed management console for managing multiple security enforcement points. The VPN-1 Enterprise Security Console can manage any number of VPN/FireWall Modules, Inspection Modules and Encryption Modules installed on other machines.

VPN-1 Enterprise Encryption Center

This product includes:

- VPN-1 Enterprise Security Console
- VPN/FireWall Module
- Encryption Module

The VPN/FireWall Module can be used to protect an unlimited number of nodes behind the gateway (the machine on which it is installed).

The Management Module and VPN/FireWall Module can be installed on the same machine or on different machines.

VPN-1 Enterprise Security Center

This product includes:

- VPN-1 Enterprise Encryption Center
- Connect Control Module (see “Connect Control” on page 9)

VPN-1 Global Security Center

This product includes:

- VPN-1 Enterprise Security Center
- Open Security Extension (see “Account Management for Enterprise Console” on page 9)

VPN-1 Single Gateway Products

VPN-1 Gateway/n (VPN-1 Gateway/25, VPN-1 Gateway etc.)

These products include:

- Management Module
- VPN/FireWall Module
- Encryption Module

The VPN-1 Single Gateway Products are subject to the same restrictions (number of protected hosts, number of external interfaces and the inability to control remote enforcement points) as are the VPN-1/FireWall-1 Single Gateway Products (see “VPN-1/FireWall-1 Single Gateway Products” on page 6).

Add-On Products

VPN/FireWall Module

This product is installed on a FireWalled gateway that is controlled by a remote Management Station, which must be separately acquired. It is available in limited and unlimited versions.

Encryption Module

This add-on product provides encryption capabilities, and is available in limited and unlimited versions. Export restrictions apply.

VPN-1 Module

This product combines an Encryption Module and a VPN/FireWall Module. It is available in limited and unlimited versions.

Customer Log Module (CLM)

This product is a VPN-1/FireWall-1 Management Server with a license that enables log management only. The Customer Log Module collects logs from remote VPN/FireWall Modules.

VPN-1 SecuRemote/*n*

This product licenses SecuRemote Client features.

Open Security Extension

This product enables a Management Module to generate and download Access Lists and configure router security for routers. It is available in limited and unlimited versions.

Connect Control

This product enables load balancing for an unlimited number of servers.

Account Management for Enterprise Console

This product enables VPN-1/FireWall-1 user management on LDAP Servers.

Example Configurations

One FireWalled Gateway

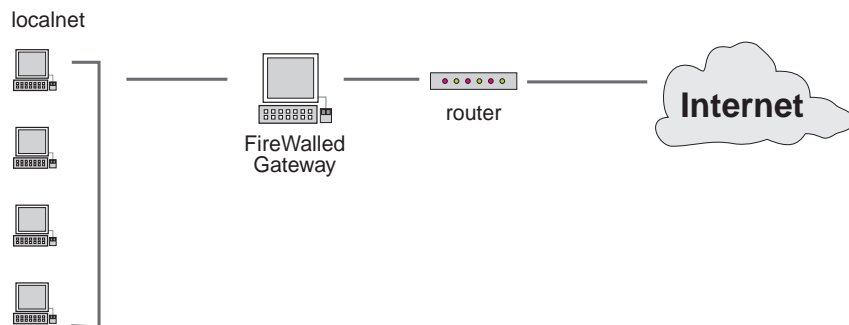


FIGURE 1-4 Configuration with One FireWalled Gateway and Router

This configuration requires one of the following products:

- Internet Gateway/*n* if the number of protected nodes behind the gateway is not greater than *n*, or
- Enterprise Center



Note – The Management Module can be deployed in a Client/Server configuration (see “Management Module” on page 3).

If encryption is required, the corresponding VPN-1 products should be used.

In addition, if the router is to be controlled by VPN-1/FireWall-1, then Open Security Extension/1 is also required.

One FireWalled Gateway and a Separate Management Station

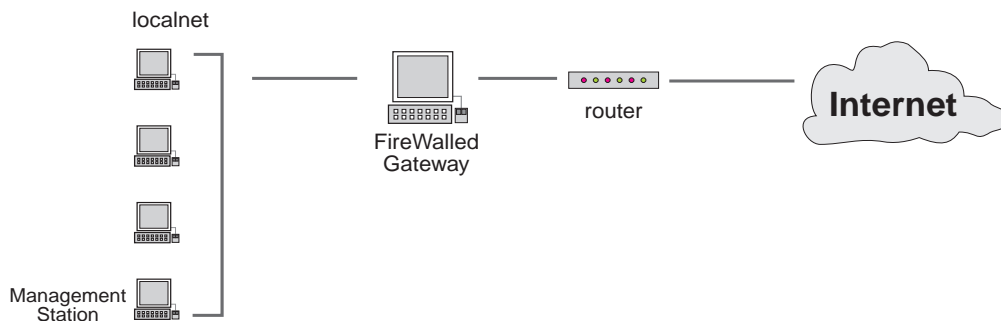


FIGURE 1-5 Configuration with One FireWalled Gateway, a Separate Management Station and Router

This configuration requires the following product:

- Enterprise Center for the gateway
Internet Gateway/*n* cannot be used in this configuration because the Management Station is not on the same machine as the VPN/FireWall Module.
- Even though only one product is required, different modules of the product must be installed on each of the two machines (the VPN/FireWall Module on the FireWalled gateway and the Management Module on the Management Station).



Note – The Management Module can be deployed in a Client/Server configuration (see “Management Module” on page 3).

If the Enterprise Center is installed, then the Management Station can be installed on a host in localnet, and any number of additional VPN/FireWall Modules or Inspection Modules on other gateways and hosts can be controlled from the Management Station. Each of the other FireWall or Inspection Modules is a separate product and must be acquired separately.

If encryption is required, the corresponding VPN-1 products should be used.

In addition, if the router is to be controlled by VPN-1/FireWall-1, then Open Security Extension/1 is also required.

One FireWalled Gateway and Two Internal Networks

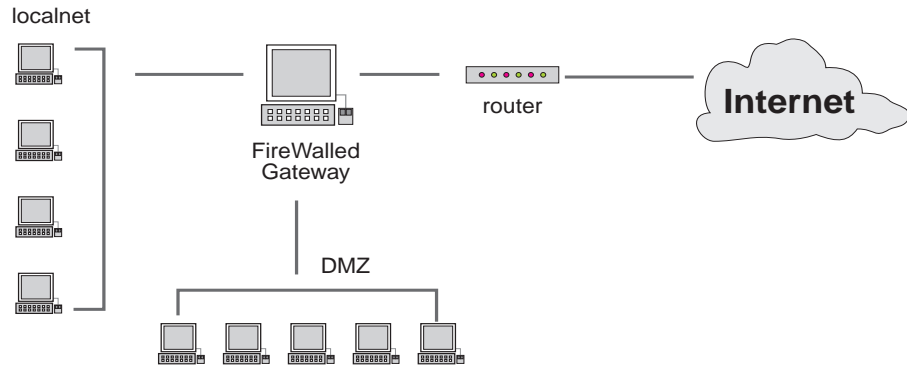


FIGURE 1-6 Configuration With One FireWalled Gateway and Two Internal Networks

This configuration requires one of the following products:

- Internet Gateway/ n if the total number of protected nodes behind the gateway (in both internal networks) is not greater than n , or
- Enterprise Center

If Enterprise Center is installed, then the Management Station can be installed on a host in one of the local networks, and any number of additional VPN/FireWall Modules or Inspection Modules on other gateways and hosts can be controlled from the Management Station. Each of the other VPN/FireWall Modules is a separate product and must be acquired separately.

In addition, if the router is to be controlled by VPN-1/FireWall-1, then Open Security Extension/1 is also required.

Two FireWalled Gateways Controlled by One Management Station

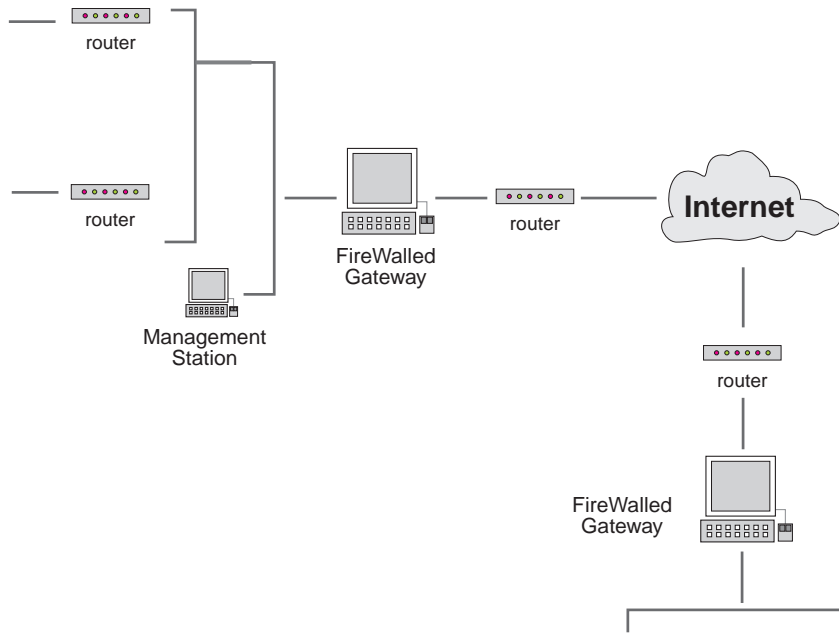


FIGURE 1-7 Configuration with two FireWalled Gateways controlled by one Management Station

This configuration requires the following products:

- VPN-1/FireWall-1 Enterprise Center for the Management Station and one gateway
- VPN/FireWall Module for the second gateway

The second gateway can be on the same premises as the first gateway, or connected to another network or located at a remote site. In any case, the second gateway is controlled by the Management Station, and the control connection between them is authenticated (and encrypted, if the Encryption feature is installed).



Note – The Management Module can be deployed in a Client/Server configuration (see “Management Module” on page 3).

In addition, if any of the routers are to be controlled by VPN-1/FireWall-1, then one of the Open Security Extension products is also required.

Alternatively, the Network Security Center can be installed in place of VPN-1/FireWall-1 Enterprise Center. The Management Station and the VPN/FireWall Module for the first gateway are part of the Network Security Center. The separate VPN/FireWall Module for the second gateway is still required.

Failover Gateways

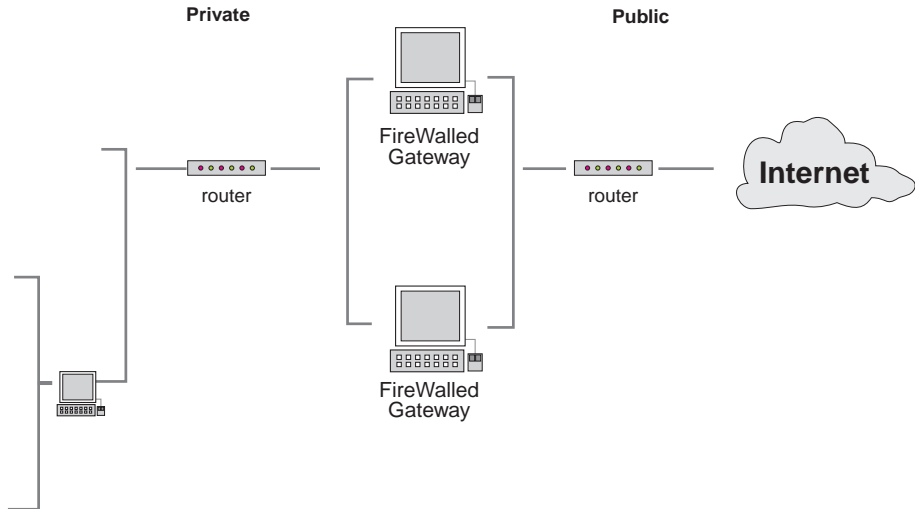


FIGURE 1-8 Configuration with Failover Gateways

This configuration requires the following product:

- VPN-1/FireWall-1 Enterprise Center

In addition, if any of the routers are to be controlled by VPN-1/FireWall-1, then one of the Open Security Extension products is also required. Alternatively, the Network Security Center can be installed in place of the VPN-1/FireWall-1 Enterprise Center.

VPN-1/FireWall-1 Client/Server Model

VPN-1/FireWall-1 Modules

VPN-1/FireWall-1 comprises two primary modules:

Management Module

The Management Module includes the Graphical User Interface (GUI) and the Management Server.

The GUI is the front end to the Management Module, which manages the VPN-1/FireWall-1 database: the Rule Base, network objects, services, users etc.

VPN/FireWall Module

The VPN/FireWall Module includes the Inspection Module and VPN-1/FireWall-1 daemons.

The VPN/FireWall Module implements the Security Policy, logs events, and communicates with the Management Module using the daemons.

Client/Server

The two components of the Management Module (the GUI and the Management Server) can be installed on the same machine or on two different machines. When they are installed on two different machines, VPN-1/FireWall-1 implements the Client/Server model, in which a GUI Client running on a Windows or X/Motif workstation controls a Management Server running on a Windows or Unix workstation.

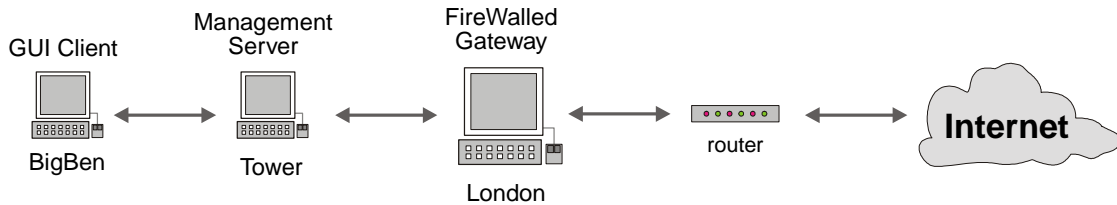


FIGURE 1-9 VPN-1/FireWall-1 Client-Server configuration

In the configuration depicted in FIGURE 1-9, the functionality of the Management Module is divided between two workstations (Tower and BigBen). The Management Server, including the VPN-1/FireWall-1 database is on Tower, the server. The GUI is on BigBen.

The user, working on BigBen, maintains the VPN-1/FireWall-1 Security Policy and database, which reside on Tower. The VPN/FireWall Module is installed on London, the FireWalled gateway, which enforces the Security Policy and protects the network.

The Management Server (see “fwm” on page 27 of *Check Point Reference Guide*) is also used for adding, updating and removing administrators, and must be running if you wish to use the GUI Client on one of the Client machines.

Client/Server Interaction

A GUI Client can manage the Server (that is, run the GUI Client to communicate with a Management Server) only if both the administrator running the GUI Client and the machine on which the GUI Client is running have been authorized to access the Management Server.

In practice, this means that the following conditions must both be met:

- 1** The machine on which the Client is running is defined as an allowed client.
You can add or delete GUI Clients using the VPN-1/FireWall-1 Configuration application (`cpconfig`). See Chapter 2, “Installing and Configuring VPN-1/FireWall-1,” for information about the VPN-1/FireWall-1 Configuration application.
- 2** The administrator (user) running the GUI has been defined to the Management Server.

You can add or delete administrators using the VPN-1/FireWall-1 Configuration application (`cpconfig`). See Chapter 2, “Installing and Configuring VPN-1/FireWall-1,” for information about the VPN-1/FireWall-1 Configuration application.

Installing and Configuring VPN-1/FireWall-1

In This Chapter

<i>Which Components to Install</i>	<i>page 23</i>
<i>Installation Procedure for a New Installation</i>	<i>page 20</i>
<i>Upgrading to a New Version of VPN-1/FireWall-1</i>	<i>page 21</i>
<i>Which Components to Install</i>	<i>page 23</i>
<i>Installing on Windows Platforms</i>	<i>page 24</i>
<i>Installing on Unix Platforms</i>	<i>page 44</i>
<i>Installing the X/Motif GUI Client</i>	<i>page 58</i>
<i>After Installing VPN-1/FireWall-1</i>	<i>page 58</i>
<i>Configuring VPN-1/FireWall-1</i>	<i>page 62</i>
<i>Authenticating VPN-1/FireWall-1 Administrators</i>	<i>page 68</i>
<i>Distributed Configurations</i>	<i>page 69</i>
<i>Configuring Centralized Logging</i>	<i>page 78</i>
<i>Frequently Asked Questions</i>	<i>page 83</i>

This chapter explains how to install VPN-1/FireWall-1 and obtain and install your license(s). The procedure given here can be used to install VPN-1/FireWall-1 for the first time, to reconfigure an existing installation, or to upgrade to a newer version of VPN-1/FireWall-1.

Before Installing VPN-1/FireWall-1

Before installing VPN-1/FireWall-1, you must first ensure that a number of pre-conditions exist (for example, that routing and DNS are correctly configured). Perform the procedure below *before* you begin the installation process.



Note – The software in this version is an upgrade to Check Point VPN-1/FireWall-1 Version 4.1. If you have an earlier version of VPN-1/FireWall-1 installed, it will be upgraded. If you do not have an earlier version installed, a full version of VPN-1/FireWall-1 will be installed.

Protecting the VPN-1/FireWall-1 Machine

- 1** If you are installing VPN-1/FireWall-1 on a Windows NT machine, disable the NetBEUI protocol on that machine.

If you do not disable NetBEUI, it will be possible to access the NT machine from within the LAN using the NetBEUI protocol. This access will not be intercepted by VPN-1/FireWall-1, since NetBEUI is not an IP protocol.
- 2** Review the services running on the VPN-1/FireWall-1 machine and remove any service that is not required.

Routing

- 3** Confirm that routing is correctly configured on the gateway, as follows:
 - a** Send an ICMP packet (PING) from a host inside your (trusted) network through the gateway to your router on the other (untrusted) side.
 - b** TELNET from a host inside your (trusted) network through the gateway to a host on the Internet, to confirm that you can reach that host.
 - c** TELNET from a host on the Internet to a host inside your (trusted) network.

If any of these tests fail, then find out why and solve the problem before continuing.

IP Forwarding

If IP Forwarding is enabled, the gateway will route packets to other IP addresses.

- 4** On NT, enable the **Enable IP Forwarding** option in the **Protocols>TCP/IP Protocol Properties>Routing** tab (accessible from the Network applet in the Control Panel).

On Solaris2 and HP-UX, disable IP Forwarding in the kernel.

When you install VPN-1/FireWall-1 on the Solaris2, HP-UX and Windows NT platforms, you can specify that VPN-1/FireWall-1 controls IP Forwarding, that is, that IP Forwarding will be enabled only when VPN-1/FireWall-1 is running. This ensures that whenever the gateway is forwarding packets, VPN-1/FireWall-1 is protecting the network.

For more information, see “IP Forwarding” on page 22 of *Check Point Reference Guide*.

DNS

- 5 Confirm that DNS is working properly.

The easiest way to do this is to start a Web browser on a host inside the internal network and try to view Web pages on some well-known sites. If you can't connect, solve the problem before continuing.

IP Addresses

- 6 Make a note of the names and IP addresses of all the gateway's interfaces.

You will need this information later when you define your Security Policy. Also, if you are installing a Single Gateway product, you must know the name of the external interface (the interface connected to the Internet).

NT — Use the `ipconfig /all` command to display information about all the interfaces. Note that NT uses the hyphen (“-”) rather than the colon (“:”) to separate the fields in the MAC address.

Solaris — Use the `ifconfig -a` command to display information about all the interfaces.

IBM AIX — The `ifconfig` command is available, but it's best to use `smit` or `smitty` instead.

HP-UX — The `ifconfig` command is available, but it's best to use `lanscan` instead.

- 7 Confirm that gateway's name, as given in the `hosts` (Unix) and `lmhosts` (Windows) files, corresponds to the IP address of the gateway's *external* interface.

This ensures that when you define the gateway as a network object and click on **Get Address** in the **Workstation Properties** window to retrieve its IP address, the **IP Address** field will specify the gateway's external interface. If you fail to do so, IKE encryption (among other features) will not work properly.

VPN-1/FireWall-1 Component Configuration

- 8 Familiarize yourself with the concepts of Management Module, Master and FireWalled host by reading Chapter 1, “Pre-Installation Configuration” of *VPN-1/FireWall-1 Administration Guide*.

To summarize, the Management Module (also known as the Management Server) is the computer on which the Security Policy is maintained. The Master is the computer to which logs and alerts are sent. A FireWalled host is a computer on which a VPN/FireWall Module has been installed and which enforces some part of the security policy.

- 9** Determine which VPN-1/FireWall-1 component is to be installed on each computer.

You must decide which computer(s) will host your Management Module(s), which will host your Master(s) and which will host your FireWalled host(s).

In addition, if you are installing a Client/Server configuration, then you must decide which computer will host your GUI Client and which will host your Management Module.



Note – If you are installing one of the Single Gateway Products, then the Management Module, Master and FireWalled Module must all be on the same machine, but you can still deploy the Management Module in the Client/Server configuration.

Connectivity

- 10** Confirm that there is connectivity between all the hosts (including GUI Clients) on which VPN-1/FireWall-1 components will be installed, in other words, that they can all talk to each other.

If you don't verify this before you install VPN-1/FireWall-1, then if you encounter connectivity problems later on, you will not know the source of the problem. You may end up spending a great deal of time in "debugging" VPN-1/FireWall-1 only to discover that the problem is elsewhere.

To verify that there is connectivity between all the machines, try pinging them from each other. If the pings are not successful, then determine what the problem is (using the standard network debugging tools) and fix it. Continue only after you have verified that the machines can all talk to each other.

- 11** Verify that you have the correct version of the software for your OS and platform for all the VPN-1/FireWall-1 components.
- 12** If a number of people will be administering the VPN-1/FireWall-1 system, create a Unix group before you install VPN-1/FireWall-1.
- 13** If VPN-1/FireWall-1 is running, stop it, including the GUI Client.

Installation Procedure for a New Installation

To install VPN-1/FireWall-1 for the first time, proceed as follows:

- 1** Install and start VPN-1/FireWall-1 on the Management Module computer.

At this point, the Management Module will log only itself. Since there are no rules, then by default everything will be allowed to pass.

You can change this behavior by disabling IP Forwarding. For more information about IP Forwarding, see “IP Forwarding” on page 22 of *Check Point Reference Guide*.

- 2** Install and start the VPN/FireWall Module on each of the managed (FireWalled) hosts.

Since there are no rules, then by default everything will be allowed to pass.
- 3** Return to the Management Module and start the VPN-1/FireWall-1 Graphic User Interface.
- 4** Build a Rule Base and install the Security Policy on the managed (FireWalled) hosts.

VPN-1/FireWall-1 will then begin to enforce your Security Policy.

Upgrading to a New Version of VPN-1/FireWall-1

Upgrading From a Version Before Version 4.0

You can upgrade to Version Check Point 2000 only from Version 3.0 and higher. If you are running a version prior to 3.0, then proceed as follows:

- 1** Upgrade from that version to Version 3.0.
- 2** Upgrade from Version 3.0 to Version Check Point 2000.

Backward Compatibility

VPN-1/FireWall-1 Version Check Point 2000 is installed in its own directory and does not overwrite previous versions of VPN-1/FireWall-1. After a successful installation, the `FWDIR` environment variable should be changed to point to Version Check Point 2000. If you uninstall Version Check Point 2000, the previous version is restored (that is, `FWDIR` is set to point to the previous version).

During the installation process, you will be asked whether to maintain backward compatibility with Version 4.0. If you choose to do so, you will be able to manage Version 4.0 and Version 3.0 VPN/FireWall Modules from a Version Check Point 2000 Management Station.

Note the following compatibility issues:

- A Version Check Point 2000 Management Module cannot manage a Version 2.1 (or earlier) VPN/FireWall Module.
- A Version Check Point 2000 Management Module can manage Version 4.0 and Version 3.0 VPN/FireWall Modules (only if Backward Compatibility is selected — see above), but some Version Check Point 2000 features (for example, multiple CAs) cannot be implemented on earlier VPN/FireWall Modules.

When upgrading to Version Check Point 2000 from Version 4.0, you must first upgrade the Management Module (including the GUI) and then upgrade the VPN/FireWall Modules. When you upgrade the Management Module, its version is set to

Check Point 2000 if it is also a VPN/FireWall Module. After you upgrade each VPN/FireWall Module to VPN-1/FireWall-1 Version Check Point 2000, you must then manually change its version to Check Point 2000 (in the **General** tab of its **Workstation Properties** window).

VPN-1/FireWall-1 Database

When you upgrade to a new version of VPN-1/FireWall-1, the installation procedure carries the following elements over to the new version:

- VPN-1/FireWall-1 database
- Properties
- Key database
- Encryption Parameters
- Rule Base

VPN-1/FireWall-1 attempts to merge your database with its own new database. For example, you will have the benefit of services defined in the new version and you will retain the services you defined in the previous version. In the case of a name conflict, the old objects (the ones you defined) will be retained.

The files containing these elements are not simply copied. The files are converted to the format of the new version of VPN-1/FireWall-1. This means that you *cannot* copy these files from a previous version to the new version.

Minimizing Downtime During Upgrades

If you would like to upgrade to the new version while minimizing downtime, proceed as follows:

- 1** Prepare another computer (the “new machine”) with the same IP address as the machine on which the previous version of VPN-1/FireWall-1 is installed (the “old machine”), but *do not connect the new machine to the network*.
- 2** Copy the entire disk from the old machine to the new machine.
The new machine is now an exact duplicate of the old machine.
- 3** Upgrade to the new version of VPN-1/FireWall-1 on the new machine.
- 4** Physically disconnect the old machine from the network and connect the new machine (which now has the new version of VPN-1/FireWall-1 installed) in its place.
Open connections through the old machine will be dropped.

This procedure is applicable to both VPN/FireWall Modules and Management Modules, because a Management Module cannot receive logs or alerts while it is being upgraded.

After Upgrading

After upgrading, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy on all FireWalls, even if there has been no change in the Security Policy.

Which Components to Install

FIGURE 2-1 depicts a distributed VPN-1/FireWall-1 configuration.

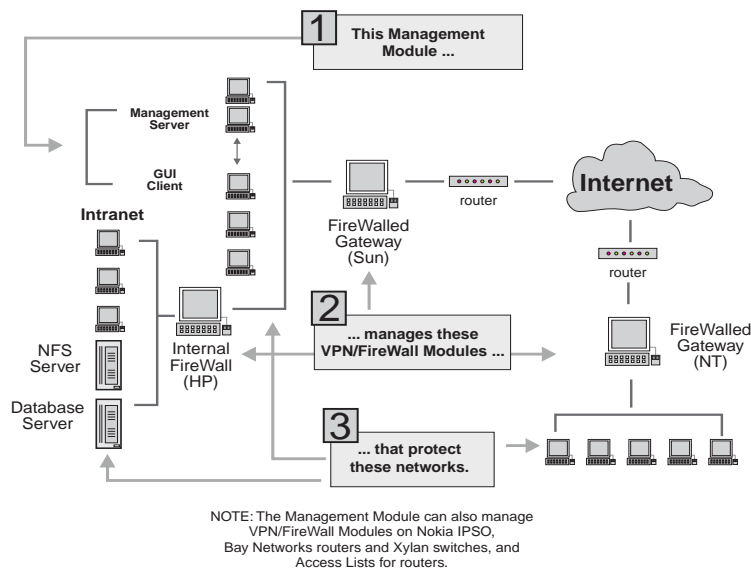


FIGURE 2-1 Distributed VPN-1/FireWall-1 Configuration

TABLE 2-1 lists the VPN-1/FireWall-1 components that must be installed on each computer.

TABLE 2-1 Components to Install on Each Computer

on this computer	install this component	see also
Management Server	Management Server	“Installing on Windows Platforms” on page 24, <i>or</i> “Installing on Unix Platforms” on page 44
GUI Client	Windows or X/Motif GUI Client	“Installing on Windows Platforms” on page 24, <i>or</i> “Installing the X/Motif GUI Client” on page 58
FireWalled Gateway (Solaris)	VPN/FireWall Module	“Solaris” on page 45
FireWalled Gateway (HP)	Inspection Module	“HP-UX” on page 46
FireWalled Gateway (NT)	VPN/FireWall Module	“IBM AIX” on page 48

For an explanation of the differences between an Inspection Module and a VPN/FireWall Module, see “VPN/FireWall Module” on page 4 of *VPN-1/FireWall-1 Administration Guide*.



Note – For information about installing Inspection Modules on embedded systems, consult the hardware vendor’s documentation. Also, see Chapter 17, “Routers and Embedded Systems” of *VPN-1/FireWall-1 Administration Guide*.

Installing on Windows Platforms

Minimum Installation Requirements

TABLE 2-2 lists the minimum hardware and operating system required for installing the VPN-1/FireWall-1 GUI Client.

TABLE 2-2 Minimum Requirements (GUI Client)

Platforms	Windows 9x, Windows NT 4.0 ¹ SP4, SP5 and SP6
Disk space	40 Mbytes
Memory	32 Mbytes
Network Interface	All interfaces supported by the operating systems.

1. An X/Motif GUI, functionally equivalent to the Windows GUI, is also available. For information on how to install the X/Motif GUI, see “Installing the X/Motif GUI Client” on page 58.

TABLE 2-3 lists the minimum hardware and operating system required for installing a VPN-1/FireWall-1 Management Module or VPN/FireWall Module.

TABLE 2-3 Minimum Requirements (Management or VPN/FireWall Module)

Operating System	Windows NT 4.0 SP4, SP5 and SP6
Processor	Intel Pentium II 300+ MHz or equivalent
Disk space	40 MBytes
Memory	64MB minimum, 128MB recommended
Network Interface	All interfaces supported by the operating systems.

Installing VPN-1/FireWall-1



Note – For information on installing the X/Motif GUI Client, see “Installing the X/Motif GUI Client” on page 58.

If you are installing VPN-1/FireWall-1 using the Single CD installation procedure (described in Chapter 10, “Check Point Software Installation” of *Getting Started Guide*), then proceed to step 5 on page 26.

Otherwise, insert the VPN-1/FireWall-1 CD-ROM in the drive and proceed as follows:

- 1** Open the **File** menu and choose **Run**.
- 2** Run the **SETUP** application in the **Windows** directory.

Installation

- 3** The **Welcome** window is displayed.



FIGURE 2-2 Welcome window

- 4 Click on **Next** to proceed to the next window.
- 5 If this is not the first time you have installed VPN-1/FireWall-1 on this computer, you will be asked whether to upgrade the existing configuration or replace it.
If this is the first time you are installing VPN-1/FireWall-1 on this computer, then proceed to step 8 on page 28.

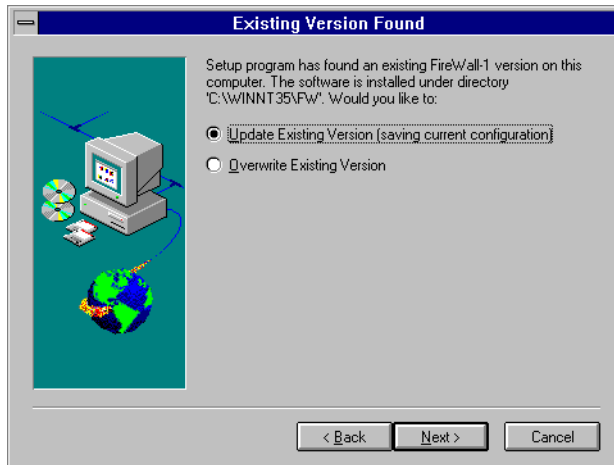


FIGURE 2-3 Existing Version Found window



Note – If a previous version of VPN-1/FireWall-1 is installed on this machine, then a new VPN-1/FireWall-1 version of the current configuration will now be installed. If you wish to install a new version of a different configuration, then you must first uninstall the previous version of VPN-1/FireWall-1.

During the installation, temporary files and directories will be created in the directory specified by the temp environment variable.

If VPN-1/FireWall-1 is running on the machine on which you are installing VPN-1/FireWall-1, it will be stopped. After the installation is complete, you will have to restart VPN-1/FireWall-1 and install your Security Policy.

- If you are updating an existing VPN-1/FireWall-1 configuration, your objects and Security Policy will be retained.
- If you overwrite an existing VPN-1/FireWall-1 configuration, your previous objects and Security Policy will be erased.

- 6 Click on **Next** to proceed to the next window.

- 7 Next you are asked whether to maintain backward compatibility with previous version of VPN-1/FireWall-1 (Management Stations only).

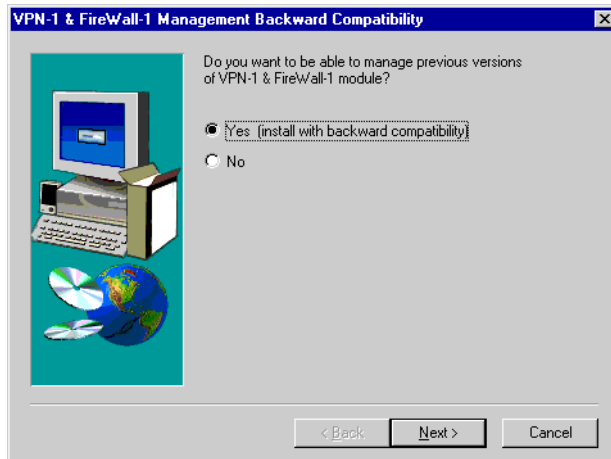


FIGURE 2-4 Backward Compatibility window

If a previous version of VPN-1/FireWall-1 is installed on this Management Station, then you may wish to preserve that version for backup (or backout) purposes. Even if no previous version is installed, then you still have the option of managing previous versions of remote VPN/FireWall Modules.



Note – If this is not the first time you have installed VPN-1/FireWall-1 on this computer, then at this point a new version of the current configuration of VPN-1/FireWall-1 will be installed, and the installation procedure will end.

- 8 In the **Selecting Setup Type** window, choose the VPN-1/FireWall-1 component you wish to install.

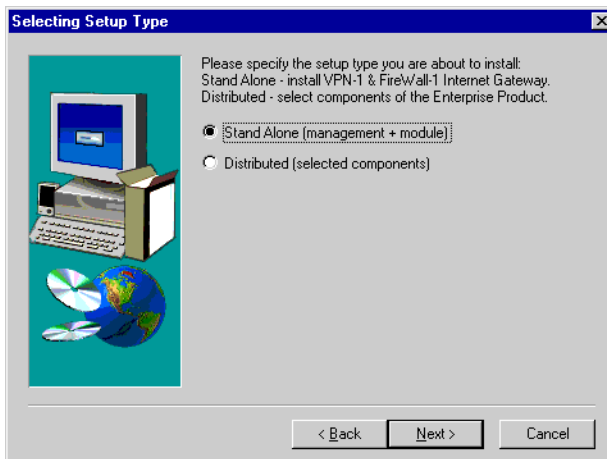


FIGURE 2-5 Selecting Setup Type window

- In a **Stand Alone** configuration, the Management Module and the VPN/FireWall Module are on the same computer.
- In a **Distributed** configuration, the Management Module and the VPN/FireWall Module are on different computers, and you will have to install each Module separately.



Note – The High Availability feature can be installed only in a distributed configuration.

In both cases, you can install the GUI Client on another computer.

- 9 Click on **Next** to proceed to the next window.
 - If you have selected **Stand Alone**, proceed to step 11 on page 29.
 - If you have selected **Distributed**, proceed to step 10 on page 29.

- 10** In the **VPN-1/FireWall-1 Enterprise Product** window, select the Module to install.

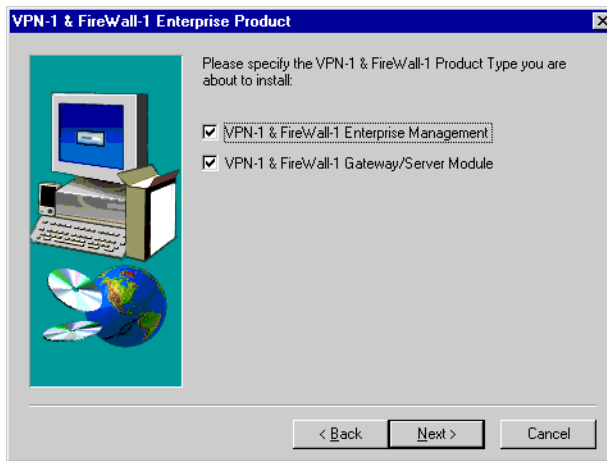


FIGURE 2-6 Enterprise Product window

If you select **VPN-1 & FireWall-1 Enterprise Management**, then proceed to step 12 on page 30.

If you select **VPN-1 & FireWall-1 Gateway/Server Module**, then proceed to the next step (step 11).

- 11** In the **VPN-1/FireWall-1 Gateway/Server Module** window, select the Module to install.

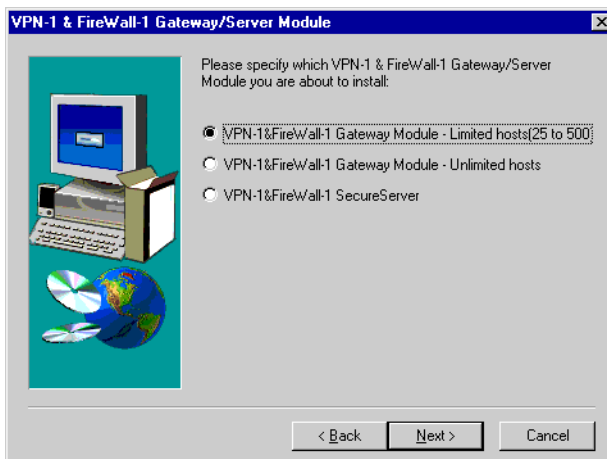


FIGURE 2-7 Gateway/Server Module window



Note – SecureServer is an internal VPN/FireWall Module that encrypts with SecureClients.

12 Specify the destination directory in the **Choose Destination Location** window.

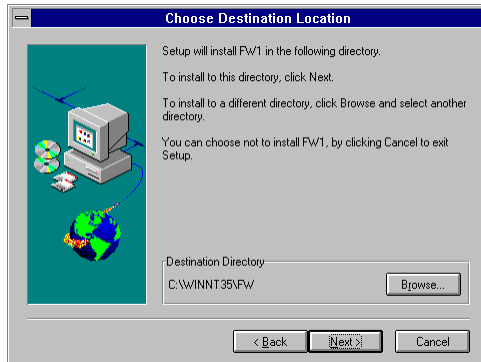


FIGURE 2-8 Destination Directory window

You can choose a different directory from the one suggested in the **Destination Directory** window by clicking on **Browse**.

If you install VPN-1/FireWall-1 in a directory different from the default directory specified in the **Choose Destination Location** window, then you must set the FWDIR environment variable to point to the directory in which you installed VPN-1/FireWall-1. Failure to do so will impair the functionality of the fwinfo debugging tool.

13 If you install a VPN-1/FireWall-1 Enterprise Product, you will be asked to specify the VPN-1/FireWall-1 Module to install (FIGURE 2-9).

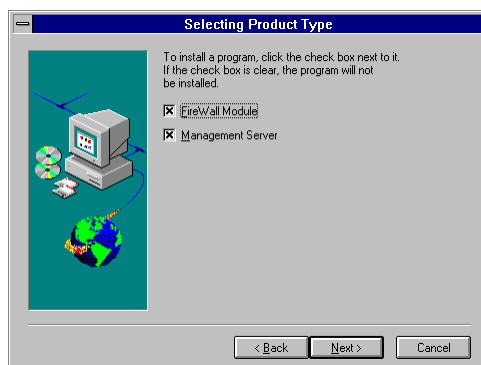


FIGURE 2-9 Selecting Product Type window

- To install the VPN/FireWall Module, choose **VPN/FireWall Module**.
- To install the Management Server, choose **Management Server**.

14 If you install a VPN-1/FireWall-1 VPN/FireWall Module Product, then you will be asked to specify the specific product (FIGURE 2-10).

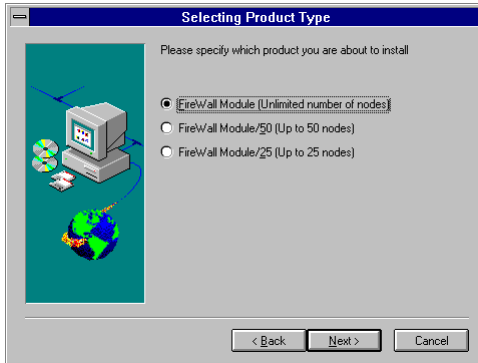


FIGURE 2-10 Selecting a VPN/FireWall Module Product

15 If you install a VPN-1/FireWall-1 Inspection Module Product, then you will be asked to specify the specific product (FIGURE 2-11).

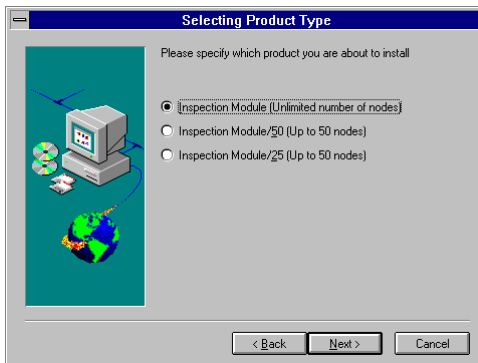


FIGURE 2-11 Selecting an Inspection Module Product

Configuration

The VPN-1/FireWall-1 software is then installed, and the VPN-1/FireWall-1 Configuration Wizard displays the configuration option windows one after the other.



Note – The options displayed depend on the VPN-1/FireWall-1 components you have installed on this host. You will not necessarily see all the windows described here during your configuration process.

Configure each option and then proceed to the next window by clicking on **Next**. If you wish to modify an option, you can return to a previous window by clicking on **Back**.

You can modify the configuration at any time by running the VPN-1/FireWall-1 Configuration application. When you do so, the different configuration options will be displayed as different tabs in the **Configuration** window.

Licenses

16 Add the required licenses for this host.

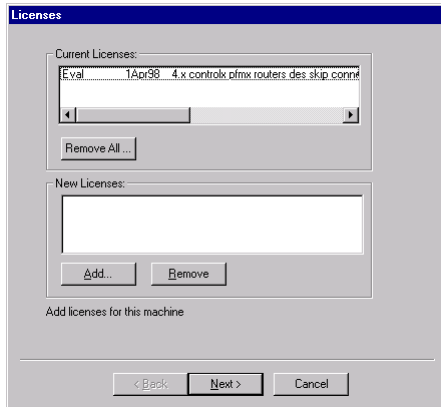


FIGURE 2-12 Licenses window

17 Click on **Add** to add a license.

The **Add License** window (FIGURE 2-13) is displayed.

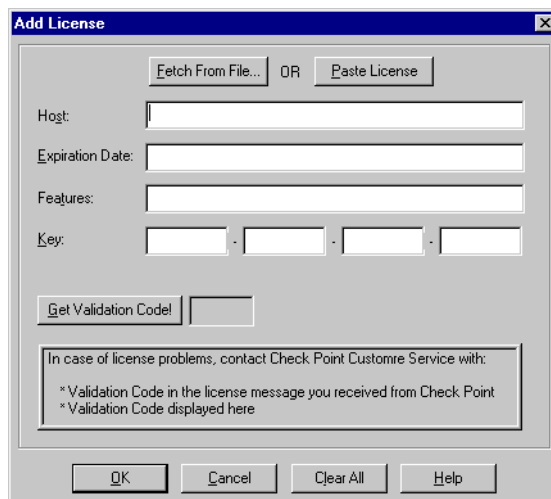


FIGURE 2-13 Add License window

18 Enter the license data and click on **OK**.

- TABLE 2-6 on page 60 lists the elements of the license string.
- You do not need a license to run the Windows GUI Client.

- If you have not yet obtained your license(s), see “Obtaining Licenses” on page 58.

19 Click on **Next** to proceed to the next window.

Administrators

20 Next, you are asked to specify Administrators.

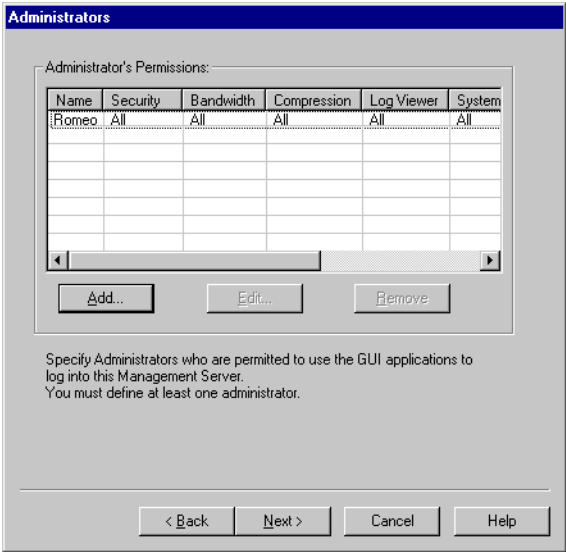


FIGURE 2-14 Administrators window

Specify the administrators who are permitted on the GUI Client side, that is, the administrators who will be allowed to use the GUI Client with the Management Server you have just installed.

You must define at least one administrator, otherwise no one will be able to use the Management Server you have just installed.

- 21** Click on **Add** to specify an administrator. The **Add Administrator** window is displayed.

FIGURE 2-15 Add Administrator window

- 22** Enter the **Administrator Name**.

- 23** Enter the **Password**.

The password should be no more than 8 characters long and should contain both alphabetic and numeric characters.

You must enter the password twice in order to confirm it.

- 24** Specify the Administrator's **Permission**.

See "Access Control" on page 62 of *VPN-1/FireWall-1 Administration Guide* for information about administrator permissions.

To modify an administrator's details, click on **Edit** in the **Administrators** window (FIGURE 2-14 on page 33).

- 25** Click on **Next** to proceed to the next window.

- 26** Confirm that the machine's IP Address (as specified in the `hosts` file) is correct.

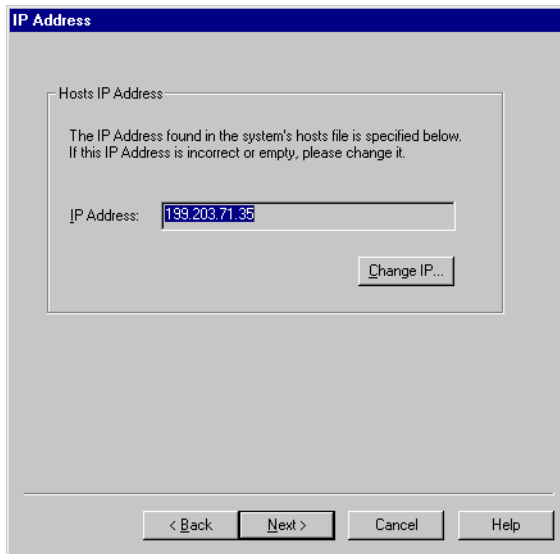


FIGURE 2-16 IP Address window

If **IP Address** is incorrect, click on **Change IP** to change it. The change will be made in the `hosts` file as well.

GUI Clients

- 27** Specify the GUI Clients, that is, the remote computers from which administrators will be allowed to use the GUI Client with the Management Server you have just installed.

If you do not define at least one GUI Client, you will be able to manage the Management Server you have just installed only from a GUI Client running on the same machine.

Enter the GUI Client's name and click on **Add** to add it to the list of allowed GUI Clients.

To remove a GUI Client from the allowed list, select it and click on **Remove**.

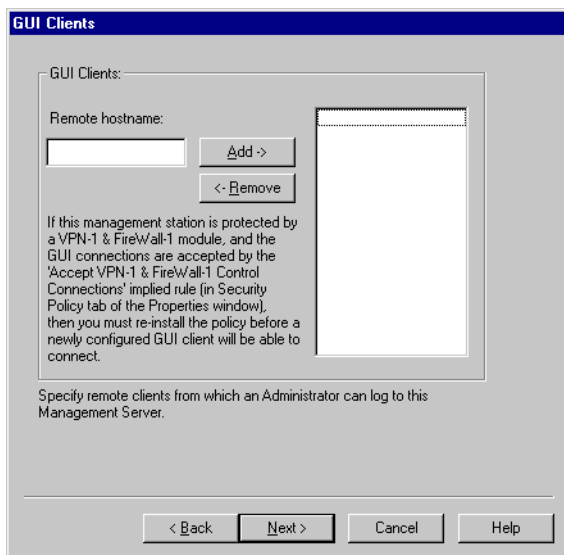


FIGURE 2-17 GUI Clients window

28 Click on **Next** to proceed to the next window.

Masters

If you have installed only a VPN/FireWall Module on this computer, you must specify the Master, that is, the computer to which logs and alerts will be sent, and from which the VPN/FireWall Module will obtain its Security Policy.

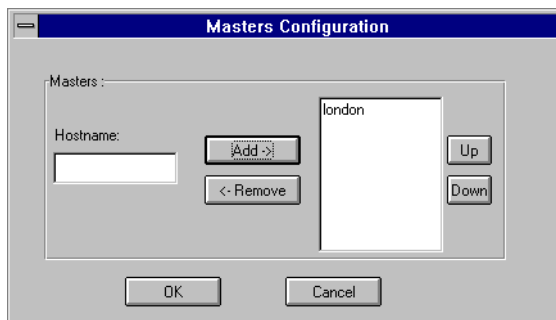


FIGURE 2-18 Masters Configuration window

- 29** Enter a host name and select **Add** to add the host to the list of Masters.

You may enter any number of Masters. The VPN/FireWall Module will use the first Master in the list with which it can establish contact, so the order of the names in the list is important. For additional information, see “Redirecting Logging to Another Master” on page 420 of *VPN-1/FireWall-1 Administration Guide*.

To move a Master up in the list, select it and then select **Up**. To move a Master down, select it and then select **Down**.

Password

When you add a Master, you must specify an authentication password that the Masters (Management Modules) and VPN/FireWall Modules use when communicating with each other. This is the same password you will use when you issue the `fw putkey` command on the Master. See “fw putkey” on page 12 of *Check Point Reference Guide* for more information about `fw putkey`.



FIGURE 2-19 Add Master window

For additional information, see “Distributed Configurations” on page 69 of *VPN-1/FireWall-1 Administration Guide*.

- 30** Enter the password (limited to 8 characters in length) twice and then click on **OK**.
- 31** Click on **Next** to proceed to the next window.

Remote Enforcement Points

If you have installed a Management Module on this computer, you must specify the remote VPN/FireWall Modules for which this Management Module is defined as Master.

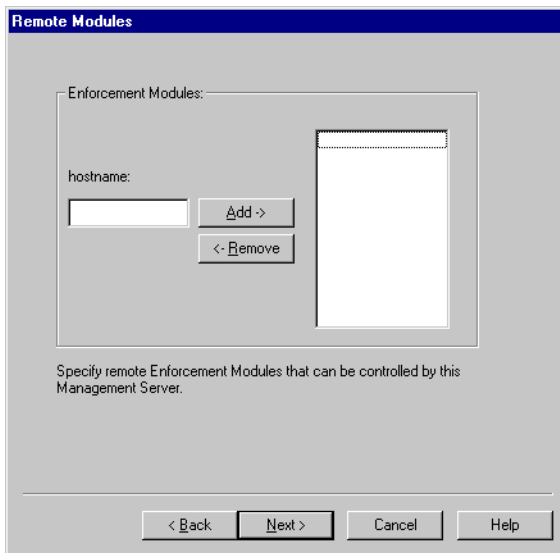


FIGURE 2-20 Remote Modules window

- 32** Enter a host name and click on **Add** to add the host to the list of remote VPN/FireWall Modules.

Click on **OK** when you have finished entering the list of host names.

- 33** When you add a remote VPN/FireWall Module, you must specify an authentication password that the Masters (Management Modules) and the remote VPN/FireWall Modules use when communicating with each other. This is the same password you will use when you issue the `fw putkey` command on the remote FireWalled host. See “fw putkey” on page 12 of *Check Point Reference Guide* for more information about `fw putkey`.

For additional information, see “Distributed Configurations” on page 69 of *VPN-1/FireWall-1 Administration Guide*.

- 34** Click on **Next** to proceed to the next window.

External Interface (for the Single Gateway, VPN/FireWall Module/n and Inspection Module/n products only)

35 Specify the name of the external interface.

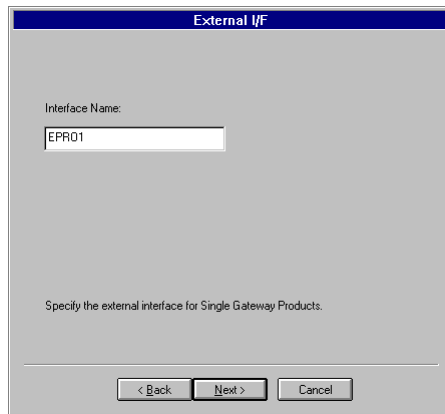


FIGURE 2-21 External IF window

Specify the name, for example “EPRO1,” *not* the IP address.

To see a list of the interfaces attached to the computer, type `ipconfig` at the command prompt. The interface name is the one appearing in the first line describing the interface. For example, suppose the first line reads:

```
Ethernet Adapter E159x1
```

The interface name in this case is E159x1.

IP Forwarding

- 36** Specify whether you want VPN-1/FireWall-1 to control IP Forwarding on the gateway.

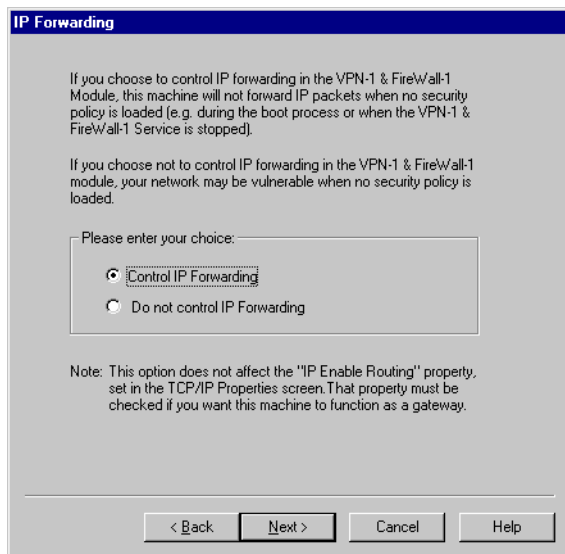


FIGURE 2-22 IP Forwarding window

If you do not allow VPN-1/FireWall-1 to control IP Forwarding, you are taking the risk that your system will be unprotected when no Security Policy is loaded, for example, when the system is being re-booted. For more information about IP Forwarding, see “IP Forwarding” on page 22 of *Check Point Reference Guide*.

- 37** Click on **Next** to proceed to the next window.

SMTP Security Server

38 Specify the parameters of the SMTP Security Server.

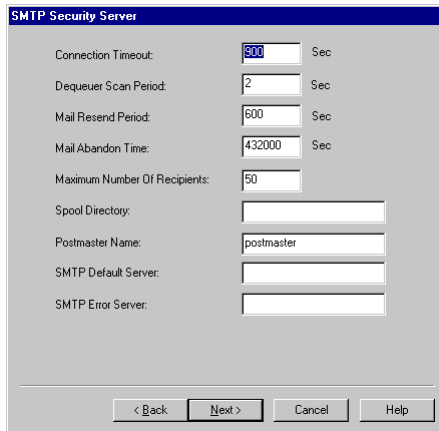
The image shows a Windows-style dialog box titled "SMTP Security Server". It contains several configuration fields with labels and input boxes. The fields are: "Connection Timeout:" with a value of "800" and a unit of "Sec"; "Dequeuer Scan Period:" with a value of "2" and a unit of "Sec"; "Mail Resend Period:" with a value of "600" and a unit of "Sec"; "Mail Abandon Time:" with a value of "432000" and a unit of "Sec"; "Maximum Number Of Recipients:" with a value of "50"; "Spool Directory:" with an empty text box; "Postmaster Name:" with a value of "postmaster"; "SMTP Default Server:" with an empty text box; and "SMTP Error Server:" with an empty text box. At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help". The "Next >" button is highlighted with a mouse cursor.

FIGURE 2-23 SMTP Security Server window

These parameters are described in “SMTP Security Server” on page 348 of *VPN-1/FireWall-1 Administration Guide*.

39 Click on **Next** to proceed to the next window.

High Availability

- 40** If you have installed only a VPN/FireWall Module on this computer, specify in the **High Availability** window (FIGURE 2-24) whether this gateway is a member of a High Availability configuration.

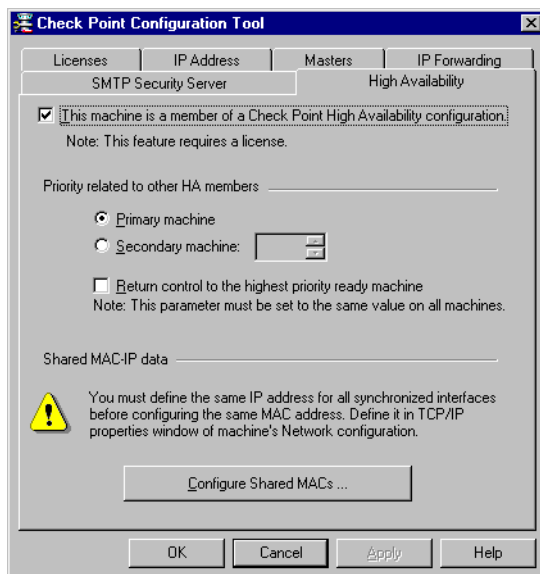


FIGURE 2-24 High Availability window

If you check **This machine is a member of a Check Point High Availability configuration**, then you must configure the machine's IP and MAC addresses accordingly. See "High Availability" on page 3 for information on how to configure a High Availability environment.

Random Key Generation

- 41** In order to generate seeds for random encryption keys, follow the instructions in the **Key Hit Session** window.

Enter the characters with a delay of a few seconds between them. Do not type the same character twice in succession, and try to vary the delay between the characters.

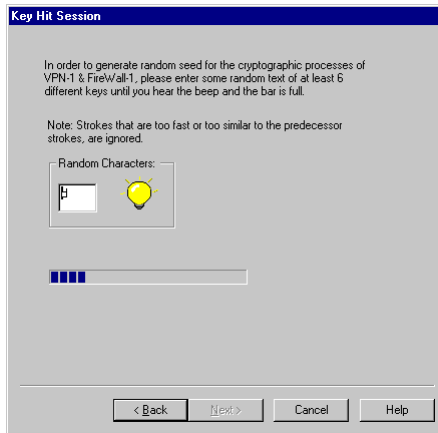


FIGURE 2-25 Key Hit Session window

42 Click on **Finish** to conclude the configuration process.

43 You have now reached the end of the installation procedure.

If you do not configure these options now, you can configure them at a later time by running the VPN-1/FireWall-1 Configuration application. When you do so, the different configuration options will be displayed as individual tabs in the **Configuration** window.

Uninstalling VPN-1/FireWall-1 (NT)

To uninstall VPN-1/FireWall-1, double-click on the **Uninstaller** icon in the VPN-1/FireWall-1 program group.

Stopping VPN-1/FireWall-1 (NT)

There are three ways to stop the VPN-1/FireWall-1 from inspecting communications:

- **Uninstall the Security Policy**

This method leaves the Inspection Module in-place, but the Security Policy is empty. VPN-1/FireWall-1 still functions but the net result is that all packets are accepted and no logging occurs.

- **Stop Inspection**

To stop inspecting under this method, proceed as follows:

- 1** Select **Services** in the **Control Panel** program group.
- 2** Select **VPN-1/FireWall-1 daemon**.
- 3** Click on **Stop**.

When VPN-1/FireWall-1 is stopped in this way, packets still pass through VPN-1/FireWall-1, but it does nothing.

■ **Disabling VPN-1/FireWall-1**

This method disables VPN-1/FireWall-1. To stop inspecting under this method, proceed as follows:

- 1** Select **Devices** in the **Control Panel** program group.
- 2** Select **VPN-1/FireWall-1**.
- 3** Click on **Startup**.
- 4** Choose **Disabled**.
- 5** Reboot the computer.

After you reboot, VPN-1/FireWall-1 will no longer be in the stack.

Reconfiguring VPN-1/FireWall-1 (NT)

To reconfigure VPN-1/FireWall-1, run the VPN-1/FireWall-1 Configuration application (see “cpconfig” on page 4 of *Check Point Reference Guide*).

Installing on Unix Platforms

Minimum Installation Requirements

TABLE 2-4 lists the minimum hardware and operating system required for installing a VPN-1/FireWall-1 Management Module or VPN/FireWall Module.

TABLE 2-4 Minimum Requirements (Unix Platforms)

Operating System	<ul style="list-style-type: none"> ■ Solaris 2.6, Solaris Operating Environment 7 (formerly known as Solaris 2.7) — SPARC and x86 ■ HP-UX 10.20, HP-UX 11.0 ■ IBM AIX 4.3.1 and 4.3.2
Disk space	40 Mbytes (software installation only)
Memory	64MB minimum, 128MB recommended
Network Interface	All interfaces supported by the operating systems.



Note – VPN-1/FireWall-1 is supported on the 32-bit versions of these operating systems only.

Installing VPN-1/FireWall-1

You can install VPN-1/FireWall-1 either directly from the CD-ROM, or you can recursively copy the installation files from the CD-ROM to a directory on your disk and install from there.

<i>Solaris</i>	<i>page 45</i>
<i>HP-UX</i>	<i>page 46</i>
<i>IBM AIX</i>	<i>page 48</i>

Solaris



Note – See TABLE 2-4 for a list of the OS versions supported by VPN-1/FireWall-1.

You will use the command line utility `pkgadd (1m)` to install VPN-1/FireWall-1.

To install VPN-1/FireWall-1, proceed as follows:

- 1** Become superuser.
- 2** Before beginning the installation process, make sure that the environment variable `FW_BOOT_DIR` is not defined by entering the following command:

```
hostname# unset FW_BOOT_DIR
```

- 3** Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).
- 4** Start the installation process.

```
hostname# pkgadd -d .
```

For information about the `pkgadd` command, refer to the Unix documentation.

- 5** `pkgadd` presents a lists of packages, and asks you to choose one to install.

Specify the package you wish to install by entering either its name or its number (see TABLE 2-5).

TABLE 2-5 VPN-1/FireWall-1 package names

name	component
CPfw1-41	VPN-1/FireWall-1
CPgui-41	VPN-1/FireWall-1 GUI
CPla-41	Load Agent

6 At the command prompt, enter the following commands.

```
hostname# setenv FWDIR /opt/CPfw1-41
hostname# set path=($FWDIR/bin $path)
```

7 Proceed to “Configuring VPN-1/FireWall-1” on page 51.

HP-UX



Note – See TABLE 2-4 for a list of the OS versions supported by VPN-1/FireWall-1.

Special Notes for HP-UX 10



Note – VPN-1/FireWall-1 on HP-UX 10 requires that the “transitional links” option be enabled. You can obtain the necessary OS patches from HP’s support site.

The first time you boot, VPN-1/FireWall-1 will fail, because there is no Security Policy at this point. After you have defined a Security Policy, subsequent re-boots will proceed normally.

HP-UX 10.20

This version of HP-UX already includes the PFS package. Please check the man page for the `pfs_mount` command for details on setting up an `/etc/pfs_fstab` file.

VPN-1/FireWall-1 requires that the `aC++` library, `/usr/lib/libCsup.1`, is at level 07 or higher.

The VPN-1/FireWall-1 installation procedure checks that the library is at the required level. If not, the installation will stop and report the problem.

You can obtain the correct library version from your reseller or from the HP-UX support site.

HP-UX 11

The X/Motif GUI is not supported in HP-UX 11.

Installation



Note – If you encounter a problem with the depth of the CD-ROM directories, use the files in `hpux/TarFiles`.

In HP-UX, VPN-1/FireWall-1 is installed using the `swinstall` application.

- 1** Insert the VPN-1/FireWall-1 CD-ROM in the drive.
- 2** Copy the installation files to the `/tmp` directory.
- 3** If the `/tmp` directory has not been registered as an installation directory, enter the following command to register it.

```
hostname# swreg -l depot -x select_local=true /tmp
```

For information about the `swreg` command, refer to the HP-UX documentation.

- 4** Type the following command to install VPN-1/FireWall-1:

```
hostname# swinstall &
```

- 5** The **SD Install - Software Selection** window is displayed, and then the **Specify Source** window is displayed on top of it.
- 6** Click on **Source Depot Path**.
- 7** In the **Depot Path** window, select the CD-ROM.
- 8** Click on **OK** to close the **Depot Path** window.
- 9** Click on **OK** to close the **Specify Source** window.
- 10** In the **SD Install - Software Selection** window, select **VPN-1/FireWall-1**.
If you double-click on **VPN-1/FireWall-1**, you will be able to select individual VPN-1/FireWall-1 components to install (see TABLE 2-5 on page 46).
- 11** From the **Actions** menu, select **Install (analysis)**.
- 12** When the analysis phase completes, click on **OK**.

- 13** When the installation phase completes, click on **Done**.



Note – VPN-1/FireWall-1 for HP-UX is always installed in the /CPfw1-41 directory, so you cannot choose an arbitrary \$FWDIR.

- 14** From the **File** menu, select **Exit**.

- 15** Read “Special Notes for HP-UX 10” on page 46 before proceeding to the next step.

- 16** At the command prompt, enter the following commands.

```
hostname# setenv FWDIR /CPfw1-41
hostname# set path=($FWDIR/bin $path)
```

- 17** Proceed to “Configuring VPN-1/FireWall-1” on page 51.

IBM AIX



Note – See TABLE 2-4 for a list of the OS versions supported by VPN-1/FireWall-1.

Special Notes for IBM AIX

Please note the following issues:

- 1** By default, AIX does not enable IP Forwarding.



Warning – If you enable IP Forwarding while VPN-1/FireWall-1 is not running, you will be exposing your network. Make sure that it is not turned on in one of the .rc scripts during boot. Turn it on (with the `no -o ipforwarding=1` command) in the `fwstart` script after VPN-1/FireWall-1 starts enforcing a Security Policy, and turn it off (with the `no -o ipforwarding=0` command) in the `fwstop` script just before VPN-1/FireWall-1 stops.

Because of this AIX feature, it is not possible to control IP Forwarding from within VPN-1/FireWall-1, so you will not be asked to configure this feature during the installation process.

See “IP Forwarding” on page 22 of *Check Point Reference Guide* for more information.

- 2** VPN-1/FireWall-1 Version 4.0 for AIX does not support the Default Security Policy feature, so you will not be asked to configure this feature during the installation process. This is not considered to be a security risk, because of the AIX boot sequence does not expose the computer.

See “Default Security Policy” on page 305 of *VPN-1/FireWall-1 Administration Guide* for more information.

- 3 In order for the X/Motif GUI to function properly, the `LANG` environment variable must be defined.
- 4 SecurID authentication is not available.
- 5 When installing a VPN-1/FireWall-1 component, verify that there are no other VPN-1/FireWall-1 components running.
- 6 The FireWall X/Motif GUI uses the Release 5 X/Motif libraries. AIX 4.3 installs Release 6 X/Motif libraries by default, so the user must manually install the Release 5 libraries in order to use the VPN-1/FireWall-1 X/Motif GUI.

Installation

In IBM AIX, VPN-1/FireWall-1 is installed using the `smit` application.

If you have a version of VPN-1/FireWall-1 already installed and you want to overwrite it, you will not be able to do this using `smit`'s overwrite option. Instead, uninstall VPN-1/FireWall-1 and then install it.

It is recommended that you run `fwstop` before performing an upgrade or uninstalling VPN-1/FireWall-1.

- 1 Become superuser.
- 2 Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).
- 3 Enter the following command to install VPN-1/FireWall-1:

```
hostname# smit &
```

- 4 Click on **Software Installation and Maintenance**.
- 5 Click on **Install and Update Software**.
- 6 Click on **Install Software Products at Latest Level**.
- 7 Click on **New Software Products at Latest Level**.
- 8 In the **New Software Products at Latest Level** window, enter the input device or the name of the directory where the VPN-1/FireWall-1 installation files are located.

If you are installing from a CD-ROM, click on **List** and select the CD device in the dialog box.



Note – VPN-1/FireWall-1 for AIX is always installed in the `/usr/lpp/CPfw1-41` directory, so you cannot choose an arbitrary `$FWDIR`.

- 9** A dialog box is displayed in which you are asked to review the installation parameters and confirm them.
- 10** In **SOFTWARE to install**, click on **List**.
- 11** Select **VPN-1/FireWall-1**.
- 12** Click on **OK** to start the installation process.
- 13** When the installation completes, exit `smit`.
- 14** At the command prompt, enter the following commands.

```
hostname# setenv FWDIR /usr/lpp/CPfw1-41
hostname# set path=($FWDIR/bin $path)
```

- 15** Proceed to “Configuring VPN-1/FireWall-1” on page 51.

Configuring VPN-1/FireWall-1

The configuration process (the `cpconfig` application) starts automatically when you install VPN-1/FireWall-1.

Upgrade

If `cpconfig` detects a previous VPN-1/FireWall-1 installation, `cpconfig` displays the following screen (FIGURE 2-26) and you can configure whichever options you wish to, in any sequence.

```

Welcome to VPN-1/FireWall-1 Configuration Program.
=====
This program will let you re-configure your VPN-1/FireWall-1
configuration.

Configuration Options:
-----
(1)  Licenses
(2)  Administrators
(3)  GUI clients
(4)  Remote Modules
(5)  Security Servers
(6)  SMTP Server
(7)  SNMP Extension
(8)  Groups
(9)  IP Forwarding
(10) Default Filter
(11) Random Pool
(12) CA Keys
(13) Secured Interfaces
(14) High Availability MAC Addresses
(15) High Availability

(16) Exit

Enter your choice (1-16) :
Thank You...

```

FIGURE 2-26 `cpconfig` reconfiguration options

When you have finished, select the **Exit** option. For information about the configuration options, see “`cpconfig`” on page 4 of *Check Point Reference Guide*.

The rest of this section describes the configuration process for a new installation of VPN-1/FireWall-1.

New Installation



Note – The questions you will be asked in the configuration process sometimes depend on your answers to earlier questions, so you may not be asked to answer all the questions listed here.

- 1** If `cpconfig` does not detect a previous VPN-1/FireWall-1 installation, `cpconfig` asks you to confirm your consent to the license agreement.
- 2** `cpconfig` then configures VPN-1/FireWall-1 by asking you a series of questions. First, the following screen is displayed:

```

Choosing Installation
-----
(1) VPN-1 & FireWall-1 Stand Alone Installation
(2) VPN-1 & FireWall-1 Distributed Installation

Option (1) will install VPN-1 & FireWall-1
Internet GateWay (Management Server and Enforcement Module)
on a single machine.
Option (2) will allow you to install specific
components of the VPN-1 & FireWall-1 Enterprise Products
on different machines.

Enter your selection (1-2/a):

```

- To install all the VPN-1/FireWall-1 components on this machine, choose (1) (VPN-1 & FireWall-1 Stand Alone Installation) and proceed to step 4 on page 53.

In this case, the Management Server and Enforcement (VPN/FireWall) Module will both be installed on this machine, and the Management Module will be unable to manage Enforcement Modules on other machines. You can install the GUI Client on any machine.

- To install the VPN-1/FireWall-1 components on different machines, choose (2) VPN-1 & FireWall-1 Distributed Installation and proceed to the next step.

- 3** If you choose (2) VPN-1 & FireWall-1 Distributed Installation, the following screen is displayed:

```

Which of the following VPN-1 & FireWall-1 options do you wish to
install/configure ?
-----
(1) VPN-1 & FireWall-1 Enterprise Management
(2) VPN-1 & FireWall-1 Gateway/Server Module
(3) VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module

```

- If you choose VPN-1 & FireWall-1 Enterprise Management, then proceed to step 6 on page 53.
- If you choose VPN-1 & FireWall-1 Gateway/Server Module or VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module, then proceed to the next step (step 4).

4 Choose one of the following:

Which Module would you like to install ?

- ```

(1) VPN-1 & FireWall-1 Gateway Module - Limited hosts (25, 50, 100.,
 250 or 500)
(2) VPN-1 & FireWall-1 Gateway Module - Unlimited hosts
(3) VPN-1 & FireWall-1 SecureServer
```



**Note** – VPN-1/FireWall-1 SecureServer is an internal VPN/FireWall Module that encrypts with VPN-1 SecureClients.

- 5** If you choose the first option (VPN-1 & FireWall-1 Gateway Module - Limited hosts), you will be asked to specify the external interface (the one connected to the Internet), for example, leO.
- 6** Next, you are asked whether you wish to start VPN-1/FireWall-1 automatically at boot time.

```
Start VPN-1/FireWall-1 automatically from /etc/rc y/n [y]?
```

Type **y** if you want VPN-1/FireWall-1 to start automatically each time the system boots.

- 7** Next, you are asked to enter group names.

```
Please specify group name [<RET> for no group permissions]:
```

If you have created a VPN-1/FireWall-1 group, enter its name now. If you have not yet set up a VPN-1/FireWall-1 group, press <Return>. The script prompts for confirmation of your group name.

- 8** Next, you are asked if you have a VPN-1/FireWall-1 license:

If you have not yet obtained your license(s), see “Obtaining Licenses” on page 58.

If you have already obtained your license, enter `y`, and enter your license when prompted. If you have not yet obtained your license, then enter `n`. You may complete the installation process and add your license later.

- 9** Next, you are asked to enter a list of administrators, that is, people who are allowed to use the GUI clients (computers) to administer the VPN-1/FireWall-1 Security Policy on the Management Server.

You may now define administrators that are allowed to use the GUI clients (i.e., the Windows GUI).  
At any later time you can modify administrators and passwords by running `fwm -a`  
You must define at least one administrator in order to use the GUI clients.

If you choose not to define any administrators now, you will not be able to use the VPN-1/FireWall-1 Client/Server configuration until you do so, using the `fwm` program (see “fwm” on page 27 of *Check Point Reference Guide* for more information).

- 10** Next, you are asked to enter a list of trusted GUI clients.

You should now enter a list of trusted hosts that may be used as GUI clients (i.e., on which you may run the Windows GUI).  
At any later time you can add hosts to this list by modifying `$FWDIR/conf/gui-clients`.

At least one GUI client must be defined if you wish to use the VPN-1/FireWall-1 Client/Server configuration. If you do not define one now, you can do so later by modifying the file `$FWDIR/conf/gui-clients`. This file consists of IP addresses or resolvable names, one per line.

- 11** If you have installed a Management Module on this computer, you must specify the remote VPN/FireWall Modules for which this Management Module is defined as Master.

Enter the IP addresses or resolvable names of all hosts this Management Module controls.

Enter a single IP address or resolvable name on each line then terminate the list with `Ctrl-D` or your EOF character.

A host name is the name returned by the `hostname` command.

- 12** The screen will show your entries and ask you for confirmation.

```
Is this correct y/n [y] ?
```

If the list of hosts on the screen is correct, press <Return>. If it is incorrect, type n, and make the necessary corrections.

- 13** Next, you are asked to configure the SMTP Security Server.

- 14** Next, you are asked to configure the SNMP daemon.

- 15** If you have installed only a Management Server (Module) on this computer, you must specify the name(s) of the machine(s) that will be this machine's Master(s).

Enter the IP addresses or resolvable names of all hosts allowed to perform control operations on this host.

Enter a single IP address or resolvable name on each line then terminate the list with Ctrl-D or your EOF character.

A host name is the name returned by the `hostname` command.

- 16** The screen will show your entries and ask you for confirmation.

```
Is this correct y/n [y] ?
```

If the list of hosts on the screen is correct, press <Return>. If it is incorrect, type n, and make the necessary corrections.

- 17** If you have installed only a VPN/FireWall Module on this computer, specify whether this gateway is a member of a High Availability configuration.

```
Would you like to install the High Availability product (y/n) [n] ? y
```

If you answer yes, you must configure the machine's IP and MAC addresses accordingly. See "High Availability" on page 3 for information on how to configure a High Availability environment.

- 18** Next, you are asked to type in random characters that will be used to generate a Certificate Authority key.

Enter the characters with a delay of a few seconds between them. Do not type the same character twice, and try to vary the delay between the characters.

- 19** If you are installing a Management Module or a VPN/FireWall Module, you are asked to specify an authentication password to be used by the Management and VPN/FireWall Modules to validate communication between them.

Enter the same authentication password for all hosts and gateways managed by the same Management Module. For additional information, see “Distributed Configurations” on page 69 of *VPN-1/FireWall-1 Administration Guide*.

- 20** (All Platforms Except IBM AIX) Next, you are asked whether to disable IP Forwarding in the kernel, and allow VPN-1/FireWall-1 to control IP Forwarding.

For more information about IP Forwarding, see “IP Forwarding” on page 22 of *Check Point Reference Guide*.

- 21** (All Platforms Except IBM AIX) Next, you are asked whether to install a default Security Policy at boot time, to protect your network until VPN-1/FireWall-1 starts.

The default Security Policy provides basic protection until the VPN-1/FireWall-1 Security Policy is loaded. For information about the default Security Policy, see “IP Forwarding” on page 22 of *Check Point Reference Guide*.

- 22** If necessary, remove the files that were extracted to your /tmp directory, for example:

```
hostname# cd /tmp
hostname# rm fwtar.gz*
hostname# rm fwinstall
hostname# rm gunzip
```

- 23** You have now reached the end of the installation procedure.

If you have your license(s), but have not yet installed them, see “Installing Licenses” on page 59. If you have not yet obtained your license(s), see “Obtaining Licenses” on page 58.

## Special Notes

### Special Note for Management Servers

If you have installed the VPN-1/FireWall-1 Management Server, you must first define administrators (people who are allowed to manage the VPN-1/FireWall-1 Management Server using a Windows GUI Client) and GUI Clients (computers from which administrators will be allowed to manage the VPN-1/FireWall-1 Management Server).

Administrators

To define administrators, run the program `fwm` on the VPN-1/FireWall-1 Management Server, as follows:

To add an administrator, enter the following command at the system prompt:

```
hostname# fwm -a
```



You will be prompted to type the user's name, password and permissions. You will be asked to confirm the password by typing it a second time.

To delete an administrator, enter the following command at the system prompt:

```
hostname# fwm -r
```

You will be prompted to type the user's name.

For additional information, see “fwm” on page 27 of *Check Point Reference Guide*.

### GUI Clients

To define GUI Clients, you must edit the file `$FWDIR/conf/gui-clients`. The file consists of IP addresses or resolvable names, one per line.

## Upgrading

When upgrading, the currently defined services are merged with the services defined in the new version of VPN-1/FireWall-1. In case of conflict, the previous definition takes precedence over the one in the new version.

## Installation Problems

- 1** If you receive a message that a file is missing, you are in the wrong directory.
- 2** You can safely ignore any tty warnings during the installation procedure.

## Reconfiguring VPN-1/FireWall-1

You can modify your VPN-1/FireWall-1 configuration by running `cpconfig`. See “cpconfig” on page 4 of *Check Point Reference Guide* for more information.

## Uninstalling VPN-1/FireWall-1 (Unix)



**Note** – If you have a previous Version 4.0 installation, then uninstalling Version 4.1 will reactivate Version 4.0.

### HP-UX and IBM AIX

To uninstall VPN-1/FireWall-1 on HP-UX and IBM AIX, use the same administration application you used to install it.

### Solaris2

To uninstall VPN-1/FireWall-1 on Solaris2, use `pkgrm`.

When you uninstall VPN-1/FireWall-1, a message is displayed instructing you to reboot the computer using the `shutdown` command. Make sure you use the `shutdown` command in `/usr/sbin`, which recognizes the `-y` parameter.

## Installing the X/Motif GUI Client

The VPN-1/FireWall-1 X/Motif GUI Client enables you to run the VPN-1/FireWall-1 GUI Client under X/Motif, which provides a Windows “look and feel” on a Unix machine.



**Note** – For instructions on installing the Windows GUI Client, see “Installing on Windows Platforms” on page 24.

The X/Motif GUI Client can be installed as part of the VPN-1/FireWall-1 installation process. See “Installing on Unix Platforms” on page 44 for more information.

The FireWall X/Motif GUI Client uses the Release 5 X/Motif libraries.

## After Installing VPN-1/FireWall-1

### Reinstalling the Security Policy

After upgrading to a new version, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy on all FireWalls, even if there has been no change in the Security Policy.

### Obtaining Licenses

All VPN-1/FireWall-1 products require a license to enable their operation. Licenses are installed on the Management Station and FireWall and Inspection Modules. Licenses are not required on GUI Clients. For an embedded system, the license is installed on its Management Station.

#### Evaluation Licenses

If you have a Certificate Key for your copy of VPN-1/FireWall-1, then you can obtain an evaluation license by following the procedure for obtaining a permanent license.

If you do not have a Certificate Key for your copy of VPN-1/FireWall-1, then you can obtain an evaluation license from your VPN-1/FireWall-1 reseller.

#### Permanent Licenses

To obtain a permanent license, proceed as follows:

- 1 Obtain a Certificate Key from your VPN-1/FireWall-1 reseller.

- 2 Contact <http://license.checkpoint.com/> to obtain a permanent license.

When you install a permanent license, it is best to remove any expired evaluation licenses. See “fw dbload” on page 13 of *Check Point Reference Guide* for information on how to remove old licenses.

## X/Motif Licenses

You need a special license to use the X/Motif GUI, which you can obtain from your VPN-1/FireWall-1 reseller. The X/Motif license must be installed on the Management Server.

## Installing Licenses

You must have a license to use VPN-1/FireWall-1 products. If you did not enter your license(s) during installation, use the following procedures for installing your license(s) now, according to the platform(s) on which you installed each product.

For embedded systems, the license must be installed on the Management Server.

## Windows Platforms

You can install your license when you install the VPN-1/FireWall-1 software, or at a later time by running the VPN-1/FireWall-1 Configuration application. This is the same application that you ran when you installed the Management Server (see “Installing on Windows Platforms” on page 24).

## Unix Platforms

- 1 At a root prompt type the following command:

```
hostname# fw putlic hostid date licensekey features certificatekey
```

- *date*, *features*, and *certificatekey* are case insensitive.

- The variable information (the license string) represents the alphanumeric code you will receive from the License Distribution Center.

TABLE 2-6 fw putlic parameters

| Element        | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------|---------|--------------------------------------------------------|-------|----------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------------------------------------------------|----|--------------------------------------------------------------------------------------|
| hostid         | If the license is an evaluation license, enter "eval". Otherwise, enter a string as follows:                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
|                | <table><tr><th>platform</th><th>type</th></tr><tr><td>Solaris</td><td>the response to the hostid command (beginning with 0x)</td></tr><tr><td>HP-UX</td><td>the response to the uname -i command (beginning with 0d)</td></tr><tr><td>AIX</td><td>the response to the uname -l command (beginning with 0d), <i>or</i> the response to the uname -m command (beginning and ending with 00)</td></tr><tr><td>NT</td><td>IP address of the external interface (in dot notation); last part cannot be 0 or 255</td></tr></table> | platform                                                                                                                                | type | Solaris | the response to the hostid command (beginning with 0x) | HP-UX | the response to the uname -i command (beginning with 0d) | AIX | the response to the uname -l command (beginning with 0d), <i>or</i> the response to the uname -m command (beginning and ending with 00) | NT | IP address of the external interface (in dot notation); last part cannot be 0 or 255 |
|                | platform                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | type                                                                                                                                    |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
|                | Solaris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | the response to the hostid command (beginning with 0x)                                                                                  |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
|                | HP-UX                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | the response to the uname -i command (beginning with 0d)                                                                                |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
|                | AIX                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | the response to the uname -l command (beginning with 0d), <i>or</i> the response to the uname -m command (beginning and ending with 00) |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
| NT             | IP address of the external interface (in dot notation); last part cannot be 0 or 255                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
| date           | The date format is DDmonYYYY for evaluation licenses and "never" for permanent licenses.                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
| licensekey     | This is the License Key string you received from the License Distribution Center, for example:<br>aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
| features       | This is a string listing the features included in the license, for example:<br>CPSUITE-EVAL-3DES-v41                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |
| certificatekey | This is the Certificate Key string, for example:<br>CK0123456789ab                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                         |      |         |                                                        |       |                                                          |     |                                                                                                                                         |    |                                                                                      |

- 2 When you enter your license, you will get a response similar to the following example:

|                      |                |            |                       |
|----------------------|----------------|------------|-----------------------|
|                      | Host           | Expiration | Features              |
| Eval                 | 199.213.71.172 | 21Jul1999  | CPSUITE-EVAL-3DES-v41 |
| License file updated |                |            |                       |

In this example:

- The license is an evaluation license.
- The license expires on July 21, 1999.
- The features are "CPSUITE-EVAL-3DES-v41".
- The Certificate Key is "CK0123456789ab".

**3** Confirm that you are using the correct licenses by the following procedure:

- a** Run `fwstop`.
- b** Run `fwstart`.
- c** Print the license using the `fw printlic` command.

The last part of the response (the part beginning with “CK”) is the Certificate Key.

For information on these commands, see Chapter 1, “Command Line Interface” of *Check Point Reference Guide*.

## Enabling Logging for FloodGate-1 and Third Party Products

FloodGate-1 uses the OPSEC Event Logging API (ELA) Proxy Server to write log entries to the common VPN-1/FireWall-1 log database. Third party products, such as RealSecure, also use the ELA Proxy Server. Check your product’s documentation to verify whether the ELA Proxy is used. Start the ELA Proxy if your product requires it.

### Windows NT

To start the service, enter the following command:

```
net start elservice
```

Alternatively, select `elservice` from the **Services** applet in the Windows **Control Panel** and click on **Start**.

To stop the service, enter the following command:

```
net stop elservice
```

Alternatively, select `elservice` from the **Services** applet in the Windows **Control Panel** and click on **Stop**.

### Solaris 2.x

To run `ela_proxy`, enter the following command:

```
$FWDIR/bin/ela_proxy
```

The procedure for stopping the `ela_proxy` process is the same as for other Unix processes.

# Configuring VPN-1/FireWall-1

## Access Control

Administrators are assigned access privilege levels (see TABLE 2-7 on page 63) beginning with the least-privileged level. Each privilege level has the privileges of all the lower privilege levels.

Whenever an administrator logs in, all his or her actions are recorded on the Management Server in a file called `$FWDIR/cpconfig.aud`.

## Changing Privileges and Adding Administrators

You can change an administrator's privileges by using the `cpconfig` application. See "cpconfig" on page 4 of *Check Point Reference Guide* for information about the `cpconfig` application.



**Tip** – Use TABLE 2-7 on page 63 to plan your assignments of administrator privileges before you run `cpconfig`.

## Unix

The `cpconfig` application allows you to add administrators and to change their access privileges through an interactive dialogue. When you add administrators, you will be asked to provide their name and password, and to confirm their password. Then you will be asked a series of questions for assigning them access privileges. TABLE 2-7 on page 63 provides a hierarchical view of the access privileges you will be asked to assign.

The availability of permissions depends on the licenses you installed. The Enterprise Permissions section of TABLE 2-7 describes how permissions are granted for the major applications (which are Security, Bandwidth, and Compression) and for their subsidiary applications Log Viewer and System Status. The Permissions for Other Products section of TABLE 2-7 does the same for the Reporting Module.

Options described as disabled in TABLE 2-7 will not appear in your interactive dialogue. The dialogue will proceed approximately from top to bottom and left to right through TABLE 2-7. You will be presented a list of choices. You will respond by entering a single letter abbreviation representing your selection. (Abbreviations will take the form of 'Y' for 'yes', 'N' for 'no', 'R' for 'read', 'W' for 'write', etc.). As you make decisions during the dialogue, some options in the table will be disabled and you will not be asked to accept them in your remaining selections.

In the dialogue you will be asked to provide either None, Read Write, or Custom permission to the major products. These permissions are mutually exclusive. If you select None or Read Write, you provide the permissions listed at the top right of TABLE 2-7. You will then only be able to assign permissions to the Reporting Tool or the Log Consolidator (if they are licensed).

If you select Custom, you enter a more detailed dialogue which covers the topics in the Enterprise Permissions section of TABLE 2-7. The actual dialogue will be limited to the products for which you installed a license.

**TABLE 2-7**    Setting Administrator Permissions

| High Level Selections         | Mid-Level Selections | Low Level Selections | Last level of Selection | Permissions Granted                                |
|-------------------------------|----------------------|----------------------|-------------------------|----------------------------------------------------|
| <b>Enterprise Permissions</b> |                      |                      |                         |                                                    |
| <b>Read Write All</b>         | All options disabled | All options disabled |                         | All, for products for which a license is installed |
| <b>None</b>                   | All options disabled | All options disabled |                         | None                                               |

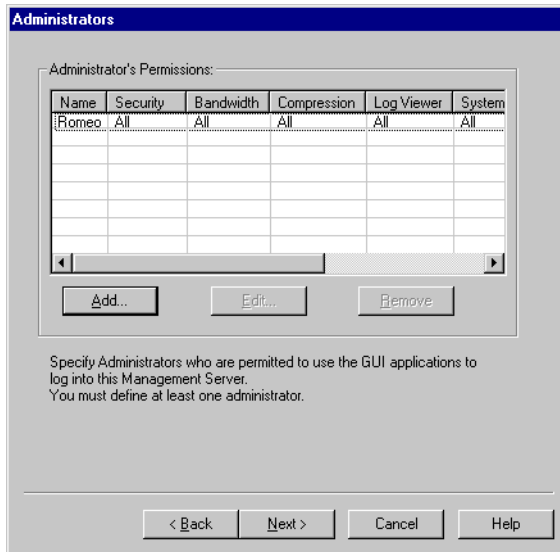
**TABLE 2-7** Setting Administrator Permissions (continued)

| High Level Selections          | Mid-Level Selections             | Low Level Selections                                               | Last level of Selection                         | Permissions Granted                                                                        |
|--------------------------------|----------------------------------|--------------------------------------------------------------------|-------------------------------------------------|--------------------------------------------------------------------------------------------|
| Customized                     |                                  |                                                                    |                                                 |                                                                                            |
|                                | Allow objects edit               | Disabled                                                           |                                                 | (The granting of this permission always depends on the granting of the other permissions.) |
|                                | Allow user edit                  |                                                                    | If selected, the administrator can edit users.  |                                                                                            |
|                                | Allow rules edit                 | Enables setting permissions when product licenses are installed    |                                                 | If selected, rules edit permissions depend on the lower level selection.                   |
|                                |                                  | Security                                                           | Enabled if license is installed. Select one of: |                                                                                            |
|                                |                                  |                                                                    | None                                            | None                                                                                       |
|                                |                                  |                                                                    | Read Only                                       | Read Only                                                                                  |
|                                |                                  |                                                                    | Rules Edit                                      | Rules Edit                                                                                 |
|                                |                                  | Bandwidth                                                          | Enabled if license is installed. Select one of: |                                                                                            |
|                                |                                  |                                                                    | None                                            | None                                                                                       |
|                                |                                  |                                                                    | Read Only                                       | Read Only                                                                                  |
|                                |                                  |                                                                    | Rules Edit                                      | Rules Edit                                                                                 |
|                                |                                  | Compression                                                        | Enabled if license is installed. Select one of: |                                                                                            |
|                                |                                  |                                                                    | None                                            | None                                                                                       |
|                                |                                  |                                                                    | Read Only                                       | Read Only                                                                                  |
|                                |                                  |                                                                    | Rules Edit                                      | Rules Edit                                                                                 |
|                                | Log Viewer                       | Enabled when one of the above products is licensed. Select one of: |                                                 |                                                                                            |
|                                |                                  |                                                                    | Read Only                                       | Read Only                                                                                  |
|                                |                                  |                                                                    | Read Write                                      | Read Write                                                                                 |
|                                | System Status                    |                                                                    |                                                 | Read, if selected                                                                          |
| Permissions for Other Products |                                  |                                                                    |                                                 |                                                                                            |
| Reporting Tool                 |                                  |                                                                    | Enabled if license is installed. Select one of: |                                                                                            |
|                                |                                  |                                                                    | Read Only                                       | Read Only                                                                                  |
|                                |                                  |                                                                    | Read Write                                      | Read Write                                                                                 |
| Log Consolidator               | Enabled if license is installed. |                                                                    |                                                 | Read, if selected                                                                          |



## Windows NT

You can modify an administrator's privileges by using the Check Point Configuration application. Start the Check Point Configuration application and click on **Administrators** to display the **Administrators** tab (FIGURE 2-27).



**FIGURE 2-27** Check Point Configuration window

In the **Administrator's Permissions** table, the columns correspond to the installed product licenses. Permissions can be set or changed only for products for which you have a license. The minimum display has only the **Name** column, which always appears on the left. Additional columns may be:

- Security (VPN-1/FireWall-1)
- Bandwidth (FloodGate-1)
- Compression
- Log Viewer
- System Status
- Log Consolidator
- Reporting Module

The window supports horizontal scrolling. Each row corresponds to an administrator whose name you entered. Vertical scrolling is also supported.

To add administrators, click on the **Add** button. The **Add Administrator** window (FIGURE 2-28) will be displayed.

- 1** Enter an administrator's name and password.
- 2** Confirm the password.

3 Define the administrator's permissions.

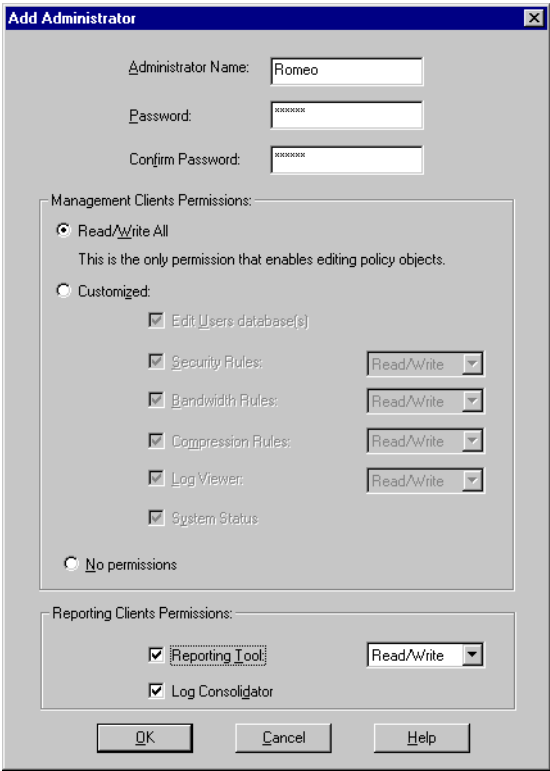


FIGURE 2-28 Add Administrator window

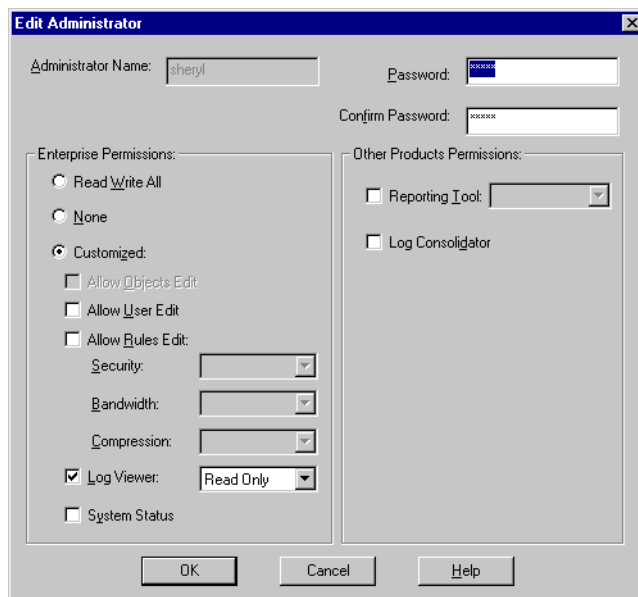
The available permissions depend on the installed licenses. TABLE 2-7 on page 63 presents the settings and the permissions that can be granted. The **Add Administrator** window (FIGURE 2-28) enables you to assign permissions in a hierarchical fashion from the highest to the lowest level.

The first column lists the highest level choices which are **Read Write All**, **None**, and **Customized** in the **Enterprise Permissions** section of TABLE 2-7 on page 63, the **Reporting Tool**, and the **Log Consolidator**. **Read Write All**, **None**, and **Customized** are mutually exclusive.

The last column presents the permissions that are granted according to the selections you made. The three major products are listed in the third column. If **Customized** is selected, assignment of access rights for each product requires that the product be selected. The fourth column shows the contents of the drop down selection windows for product selection. The **Reporting Tool** options are also listed in the fourth column.

As you make your selections, the remaining options in the window (FIGURE 2-28) become available or unavailable as required. When you are finished, click on **OK** to confirm and save the result.

If you click on **Edit** in the **Check Point Configuration** window (FIGURE 2-27 on page 65), the **Edit Administrator** window (FIGURE 2-29) is displayed. The procedure to change the administrator's permissions is the same as that of the **Add Administrator** window.



**FIGURE 2-29** Edit Administrator window

You can remove an administrator by selecting the name in the **Administrators** tab (FIGURE 2-27) and clicking on **Remove**.

## Concurrent Sessions

In order to prevent more than one administrator from modifying a Security Policy at the same time, VPN-1/FireWall-1 implements a locking mechanism.

Any number of administrators can view a Security Policy at the same time, but only one of them can have write permission at any given moment. Upon opening a Security Policy, an administrator is granted write permission only if both of the following conditions are true:

- The administrator has been assigned a Read/Write or User Edit privileges (see “Access Control” on page 62).
- No other administrator currently has write permission for the Security Policy at this time.

For example, suppose Bob and Alice are both administrators. Bob has Read/Write privileges and Alice has User Edit privileges. Suppose no one has the Security Policy Editor open. If Alice opens the Security Policy Editor, she will be granted User Edit permission. If Bob opens the same Security Policy before Alice closes it on her

workstation, then Bob will not be granted Read/Write permission. Instead, he will be asked whether he wishes to quit or to open the Security Policy with Read Only permission.

## Read Only Sessions

An administrator with Read/Write or User Edit privileges can open a Read Only session by checking the **Read Only** checkbox in the **Check Point Policy Editor Login** window (FIGURE 2-30).



**FIGURE 2-30** Login window

During the Read Only session, another administrator with Read/Write privileges can log in and be granted write permission.

## Authenticating VPN-1/FireWall-1 Administrators

You may wish to authenticate VPN-1/FireWall-1 administrators, even if they are defined as administrators and connecting from authorized GUI Clients.



**Note** – VPN-1/FireWall-1 administrators are always authenticated. This section describes how to implement additional authentication mechanisms.

To authenticate VPN-1/FireWall-1 administrators, proceed as follows:

- 1** Configure your Management Station so that it is protected by a VPN/FireWall Module.  
The VPN/FireWall Module can be on the same machine as the Management Module or on a different machine.
- 2** In the **Security Policy** tab of the **Properties Setup** window, disable the **Accept VPN-1 & FireWall-1 Control Connections** property (see FIGURE 7-1 on page 238).

- 3** Add a rule to the Rule Base specifying Client Authentication or Client Encryption as the **Action**, for example, the rule shown below:

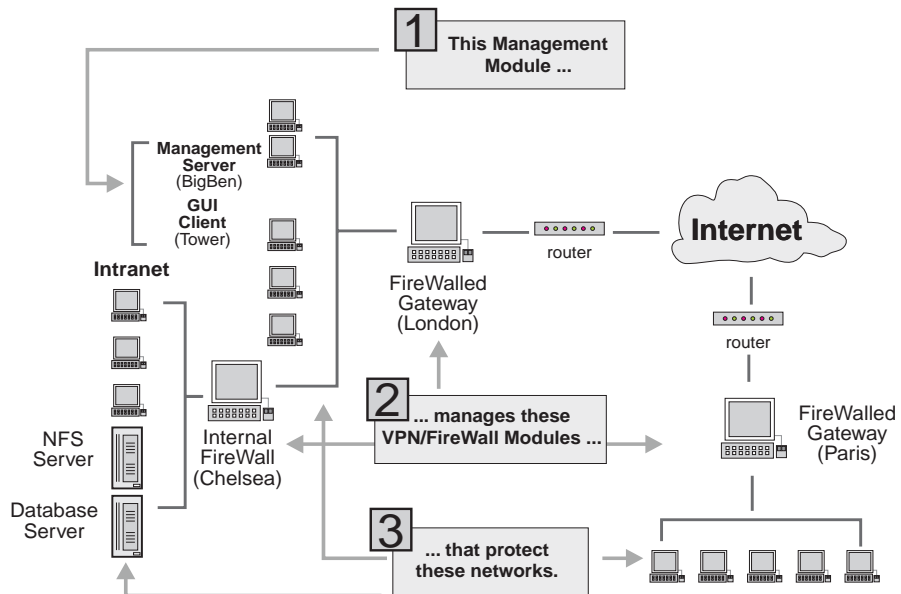
| Source       | Destination | Services | Action            | Track    | Install On                                                          |
|--------------|-------------|----------|-------------------|----------|---------------------------------------------------------------------|
| FW1Admin@Any | MgmtStation | FW1_fgmt | Client Encryption | Long Log | <i>the VPN/FireWall Module that protects the Management Station</i> |

The FW1\_mgmt service is a TCP service on port 258.

- 4** Add rules to the Rule Base that allow the other control connections you need, (since you disabled them in step 2 on page 68).

## Distributed Configurations

Consider the distributed VPN-1/FireWall-1 configuration depicted in FIGURE 2-31.



**FIGURE 2-31** Distributed VPN-1/FireWall-1 Configuration

In this example, the Management Module is deployed in the Client/Server configuration, where BigBen is the Management Server and Tower is the GUI Client. You would install VPN-1/FireWall-1 as shown in TABLE 2-8.

**TABLE 2-8** VPN-1/FireWall-1 Components

| machine | VPN-1/FireWall-1 component            |
|---------|---------------------------------------|
| BigBen  | Management Module - Management Server |
| Tower   | Management Module - GUI Client        |
| Chelsea | VPN/FireWall Module                   |
| London  | VPN/FireWall Module                   |
| Paris   | VPN/FireWall Module                   |

In this configuration, BigBen is the only Master and manages both FireWalled gateways.

**“Master” and “Management Module”**

The Master serves two functions:

- 1** It is the repository of the Security Policy and allows the Security Policy to be fetched by all the FireWalls for which it is defined as Master.
- 2** VPN/FireWall Modules send their log messages to the Master.

On each FireWall, the file `$FWDIR/conf/masters` contains a list of names or IP addresses of the machines it regards as its Masters. The VPN/FireWall Module attempts to connect to the first Master in the list; if it fails, it tries the second, and so on.

Usually, the Master and the Management Module are the same machine, which is listed in `$FWDIR/conf/masters`. If the Management Module is the first Master in the list, then by definition, it has a copy of the Security Policy. If it is not the first Master, then when the VPN/FireWall Module needs to download its Security Policy, it will go down the list of Masters until it finds a Management Module from which it can download a Security Policy.

If for some reason you require that a VPN/FireWall Module’s Management Module not be one of its Masters, then you will have to ensure that one of the Masters has an up-to-date copy of the Security Policy maintained by the Management Module.

Management of Security Policies and of VPN-1/FireWall-1 logs can be distributed to two separate Masters — one Management Module is the repository of the Security Policies while the other Management Module is the repository of log information (the logging station). You can create the file `$FWDIR/conf/loggers` to direct logs to a centralized logging station separate from the Security Policy repository. For more information, see “Configuring Centralized Logging” on page 78. You can direct logging to another Master, or to more than one Master. See “Redirecting Logging to Another Master” on page 420 for information on how to do this.

## Communications within the Management Module

On BigBen, Tower must be defined as one of the GUI clients authorized to use the Management Server on BigBen.

For information on how to do this, see “Access Control” on page 62.

## Communications between the Management Module(s) and the VPN/FireWall Modules

In this context BigBen is the Master (the repository of both the Security Policy and the Log File), while London, Chelsea and Paris are the Clients (the recipients and enforcers of the Security Policy).

When you install the VPN-1/FireWall-1 Management Module, you are asked to specify the IP addresses of the remote VPN/FireWall Modules for which the Management Module is defined as Master. Conversely, when you install the VPN/FireWall Module software, you are asked to specify the IP address(es) of the Master(s). On the basis of this information, VPN-1/FireWall-1 establishes the Master-Client relationship.

The control link is the communication channel between a Master and its Clients.

On the Master(s) and on each of the Clients, the file `$FWDIR/lib/control.map` defines access privileges and authentication measures for the control link (see “`$FWDIR/lib/control.map`” on page 73). This file is created when VPN-1/FireWall-1 is installed.

Communications between a Master and its Clients are authenticated according to the specifications in `$FWDIR/lib/control.map`. If the Encryption feature is installed, then communication is encrypted as well. If the Encryption feature is not installed, then communication is not encrypted.

## Modifying an Existing Configuration

If you wish to modify an existing configuration, reinstall VPN-1/FireWall-1 on all the affected machines and choose the configure option. See Chapter 2, “Installing and Configuring VPN-1/FireWall-1,” for a description of the installation process. The optional `$FWDIR/conf/loggers` file, used to define separate Central Log Modules, must be edited manually.

Alternatively, you can reconfigure VPN-1/FireWall-1 by manually modifying the `$FWDIR/conf/masters` and the optional `$FWDIR/conf/loggers` files.

To manually modify the VPN-1/FireWall-1 configuration, proceed as follows on each of the affected hosts:



**Note** – The syntax given here is the Unix syntax. See Chapter 1, “Command Line Interface” of *Check Point Reference Guide* for information on how to use these commands on different platforms.

- 1** Stop VPN-1/FireWall-1 by typing `fwstop`.

**2** Modify `$FWDIR/conf/masters` and `$FWDIR/conf/loggers`, as required.

**3** Use the `fw putkey` command to synchronize passwords.

For information on how to use the `fw putkey` command, see “fw putkey” on page 12 of *Check Point Reference Guide*.

**4** Start VPN-1/FireWall-1 by typing `fwstart`.

## Masters File

The file `$FWDIR/conf/masters` contains a list of IP addresses (or resolvable names), one per line, for each of the Management Servers designated as Masters that install Security Policies on VPN/FireWall Modules. When the FireWall remote Module starts working, it reads this file to determine where to retrieve the Security Policy, and, if the `$FWDIR/conf/loggers` does not exist, to direct logging.

If the file `$FWDIR/conf/masters` and the `$FWDIR/conf/loggers` do not exist, then the remote Module directs logging to the machine on which it is running. If the file `$FWDIR/conf/masters` does exist, then the remote Module directs logging to the first IP address in the file to which it can connect (this can also be the IP address of the local machine). If the connection to the Master goes down, the remote Module scans `$FWDIR/conf/masters` once again, looking for an IP address to which it can connect both to retrieve the latest Security Policy and to direct logging.

If the file `$FWDIR/conf/loggers` exists, logging is directed to the machines listed as masters in that file, and the machines listed in the `masters` file do not provide the logging function.

For additional information, see “Loggers File” on page 79.

A Master maintains the most recent Security Policy for each of the remote Modules it controls. If a remote Module goes down, the Module can retrieve an up to date Security Policy from a Master. The remote Module always has the last installed Security Policy. If it cannot connect to a Master, then it retrieves the last installed Policy from the machine on which it is running.

The following `$FWDIR/conf/masters` file lists two masters:

```
192.34.56.78
199.123.4.6
```

If the VPN/FireWall Module is trying to fetch a Security Policy, it will attempt to connect to each IP address according to the order in the list. The VPN/FireWall Module will try to obtain a Security Policy from the first address listed — 192.34.56.78. If it does not succeed it will try the next address — 199.123.4.6.



## \$FWDIR/lib/control.map

The file \$FWDIR/lib/control.map defines access privileges and authentication measures for the control link, for example:

```
MASTERS: stat/none */skey
CLIENT : load,db_download,fetch,log/fwal */none
*: stat/none load,unload,db_download/deny */skey
```



**Note** – The only case in which the user should manually modify the control.map file is when upgrading from a non-encryption-enabled VPN-1/FireWall-1 Version 4.0 configuration to VPN-1/FireWall-1 Version 4.1 configuration. See “Upgrading From Non-Encrypted Version 4.0 to Version 4.1” on page 76 for more information.

The entry to the left of the colon (:) can be any of the following:

- an IP address
- a resolvable name
- an asterisk (\*)
- a fully qualified name
- the keywords “MASTERS” or “CLIENT”
- the keyword “NON-ENCRYPTED”

On Management Stations, the allowed entries are:

- “CLIENT”, which defines how the Management Station communicates with the VPN/FireWall Modules it manages
- “\*”, which defines how the Management Station expects other hosts to communicate with it
- “NON-ENCRYPTED”, followed by a comma-separated list of the VPN/FireWall Modules with which this Management Station *always* conducts non-encrypted communications

On VPN/FireWall Modules, the allowed entries are:

- “MASTERS”, which defines how the VPN/FireWall Module expects the Management Station to communicate with it
- “CLIENT”, which defines how the VPN/FireWall Module communicates with the Management Station

Following the colon are strings in the following format:

```
<access> / <authentication method>
```

For example:

stat/none       \*/skey

means no authentication is required for status inquiries, but everything else requires S/Key authentication.

MASTERS means everything listed in \$FWDIR/conf/masters.

If the Management Station and VPN/FireWall Module define different levels of authentication, then the authentication used is the most secure of the two. For example, if the Management Station expects the VPN/FireWall Module to use fwa1 while the VPN/FireWall Module expects the Management Station to use S/Key, then fwa1 will be used. If the VPN/FireWall Module cannot use fwa1 (usually because the Encryption feature is not installed), then the communication will be denied.

On the Management Station(s), \$FWDIR/conf/masters and \$FWDIR/conf/loggers are empty (or do not exist), and a standard \$FWDIR/lib/control.map is created by VPN-1/FireWall-1 during installation.

Following is a list of access operations:

**TABLE 2-9** control.map access operations

| operation    | meaning                                                              |
|--------------|----------------------------------------------------------------------|
| stat         | status enquiry                                                       |
| tab_stat     | Get table information                                                |
| get_tab_name | Get table id.                                                        |
| get_logdom   | Get log format or log domain.                                        |
| db_download  | Download User Database.                                              |
| fetch        | Fetch Security Policy from Master.                                   |
| load         | Load Security Policy.                                                |
| unload       | Unload Security Policy.                                              |
| refresh      | Notify daemon that a new Security Policy was installed.              |
| getkey       | Get public encryption key or CA key.                                 |
| gettopo      | Download SecuRemote topolgy.                                         |
| gettopssl    | Download SecuRemote topolgy using SSL authentication and encryption. |
| certreq      | Generate certificate on the VPN/FireWall Module.                     |
| fwnl_opsec   | authenticated connection to OPSEC                                    |
| ssl_opsec    | authenticated and encrypted SSL connection to OPSEC                  |

**TABLE 2-9** control.map access operations

|           |                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------|
| log       | send log entries                                                                                       |
| ioctl     | command that controls the VPN-1/FireWall-1 Module kernel driver. It is for internal use and dangerous. |
| logswitch | command that switches log files                                                                        |

If you have modified `control.map`, you should restart VPN-1/FireWall-1 (that is, run `fwstop` and then `fwstart`) in order for your modifications to take effect.

**TABLE 2-10** Authentication methods

| method | meaning                                                 |
|--------|---------------------------------------------------------|
| none   | The communication is not authenticated.                 |
| skey   | The S/Key authentication method is used.                |
| fwal   | The VPN-1/FireWall-1 fwal authentication method is used |
| deny   | Permission is always denied.                            |



**Note** – `fwal` is a highly secure internal VPN-1/FireWall-1 authentication scheme, used primarily for encryption. If the VPN-1/FireWall-1 Encryption feature is not installed, `fwal` cannot be used for authentication.

## Example

FIGURE 2-32 shows an example of the `$FWDIR/lib/control.map` file.

```
#
This file maps access privileges and authentication measures for
FW's # control link.
#
MASTERS:stat,getkey,refresh/none */fwal
CLIENT :load,db_download,fetch,log/fwal */none
* :stat,getkey,refresh/none load,db_download/deny */fwal
```

**FIGURE 2-32** Example of `control.map` file

In this example, the line:

```
MASTERS: stat,getkey,refresh/none */fwal
```

indicates that for all the hosts listed in the file `$FWDIR/conf/masters:`

- `stat`, `getkey`, and `refresh` functions are not authenticated.
- All other functions are authenticated using `fwal`.

The line:

```
CLIENT : load,db_download,fetch,log /fwal */none
```

indicates that:

- This host identifies itself to its Master using the `fwal` authentication scheme for `load`, `db_download`, `fetch` and `log`.
- Other functions do not require any authentication.

Finally, the line:

```
* : stat,getkey,refresh/none load,db_download/deny */fwal
```

indicates that for all other hosts:

- `stat`, `getkey` and `refresh` require no authentication.
- `load` and `db_download` are not allowed.
- All other functions require `fwal` authentication.

## Upgrading From Non-Encrypted Version 4.0 to Version 4.1

The only case in which the user should manually modify the `control.map` file is when upgrading from a non-encryption-enabled VPN-1/FireWall-1 Version 4.0 configuration to VPN-1/FireWall-1 Version 4.1 configuration.

After the upgrade, a “NON-ENCRYPTED” line is added to `control.map`, listing the Management Station (on the VPN/FireWall Modules) and all the VPN/FireWall Modules (on the Management Station). Otherwise, `control.map` is unchanged and continues to specify non-encrypted control connections (S/Key).

Even though no encryption license is installed, it is still possible to encrypt control connections, as follows:

- 1** Delete the “NON-ENCRYPTED” line from `control.map`.
- 2** Change the “`skey`” parameter in `control.map` to “`fwal`”.
- 3** Synchronize authentication passwords between the Management Station and the VPN/FireWall Modules using the `fw putkey` command (see “Synchronizing Authentication Passwords” below).

## Synchronizing Authentication Passwords

The VPN/FireWall Modules on the hosts and gateways managed by a Management Station validate communication between them using an authentication password. When you install VPN-1/FireWall-1 on a machine, you are asked to specify an authentication

password for this purpose. You must specify the same authentication password for each of the hosts and gateways managed by the same Management Station, as well as for the Management Station.

If you are re-configuring VPN-1/FireWall-1 manually, then you must install the authentication passwords yourself on each machine, using `fw putkey`. For the configuration depicted in FIGURE 2-31 on page 69 in which BigBen is the Management Station, this means that you must provide the authentication passwords for three control links by performing `fw putkey` as follows:

**TABLE 2-11** VPN-1/FireWall-1 distributed configuration - `fw putkey`

| from   | to      | and conversely, from | to     |
|--------|---------|----------------------|--------|
| BigBen | Chelsea | Chelsea              | BigBen |
| BigBen | London  | London               | BigBen |
| BigBen | Paris   | Paris                | BigBen |

To do this (using the same password for all hosts), proceed as follows:

- 1 Login to BigBen (the Management Station) and enter the following command:

```
fw putkey -p <password> Chelsea London Paris
```

If you do not enter the password in the command line (using the `-p <password>` syntax), you will be prompted for the password twice, as follows:

```
fw putkey Chelsea London Paris
Enter secret key: <password>
Again secret key: <password>
```

- 2 Login to Chelsea and enter the following command:

```
fw putkey -p <password> BigBen
```

- 3 Login to London and enter the following command:

```
fw putkey -p <password> BigBen
```

- 4 Login to Paris and enter the following command:

```
fw putkey -p <password> BigBen
```

Alternatively, you can use a different password for every host pair, as follows:

- 1 Login to BigBen and enter the following commands:

```
fw putkey -p <password1> Chelsea
fw putkey -p <password2> London
fw putkey -p <password3> Paris
```

- 2 Login to Chelsea and enter the following command:

```
fw putkey -p <password1> BigBen
```

- 3 Login to London and enter the following command:

```
fw putkey -p <password2> BigBen
```

- 4 Login to Paris and enter the following command:

```
fw putkey -p <password3> BigBen
```

Only after you have done this will the four machines be able to communicate on the control links.



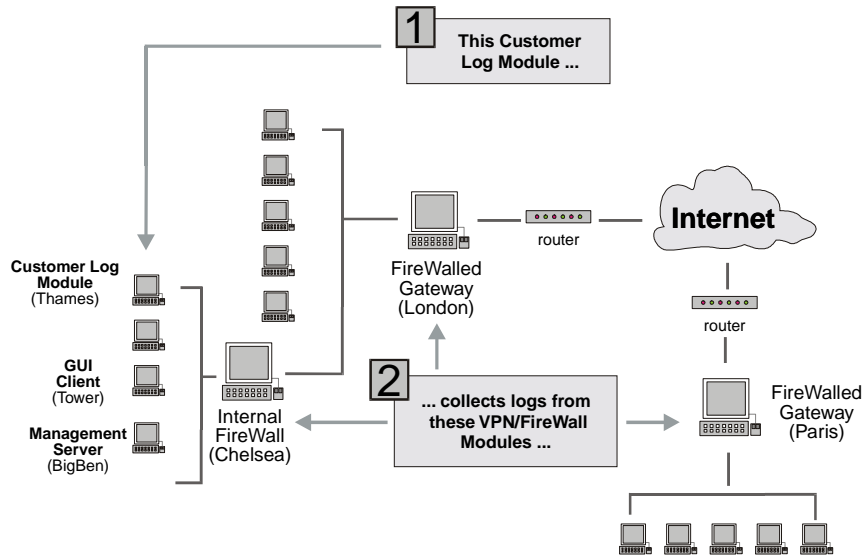
**Note** – If you specify names (rather than IP addresses), all machines must have the same name resolution for the other side. In this example, all machines must resolve BigBen in the same way (to the same interface). You can use the `-n` parameter for the `fw putkey` command on the Management Station to ensure this. Alternatively, instead of a machine's name, you can specify its IP address (or a comma-separated list of the IP addresses of its different interfaces).

## Configuring Centralized Logging

### Customer Log Module

The Customer Log Module is a Management Server with logging and alerting functionality only. The Customer Log Module collects logs and alerts from all VPN/FireWall Modules in the enterprise, but it does not maintain or manage a Security Policy.

The Customer Log Module enables centralized log management in configurations with multiple VPN/FireWall Modules. FIGURE 2-33 depicts a configuration in which centralized logging is enabled.



**FIGURE 2-33** Centralized Logging Configuration

The Customer Log Module on Thames collects log data from three VPN/FireWall Modules, each of which protects a separate network. The VPN-1/FireWall-1 Log Viewer on the GUI Client can connect to the Customer Log Module to display logged events and alerts on network activity for all VPN/FireWall Modules.

## Deployment

The Customer Log Module is a Management Server with a limited license allowing log and alerts management only. The Customer Log Module is deployed at only one of the FireWalled sites in the enterprise — either on the FireWalled host or on a standalone machine. All FireWalled machines must be configured to send logs to the Customer Log Module.

### ▼ To direct logging to the Customer Log Module

The Customer Log Module is a logging station only — it does not maintain a Security Policy for any Remote Module. Create a `loggers` file on the remote VPN/FireWall Module to enable Remote Modules to send log data and alerts to the Customer Log Module(s) but do not try to fetch a Security Policy from it.

## Loggers File

Since the `loggers` file is not created by default during installation, you have to create the `$FWDIR/conf/loggers` file through a text editor.

The file `$FWDIR/conf/loggers` contains a list of IP addresses (or resolvable names), one per line, for each of the Management Station(s) designated as Customer Log Modules that receive logs from the VPN/FireWall Modules. This file has the same syntax as `$FWDIR/conf/masters`.

VPN-1/FireWall-1 directs logs and alerts to the machines designated as Masters in the `loggers` file. If the file `$FWDIR/conf/loggers` is empty, VPN-1/FireWall-1 directs logging to the default destination, which is the machine on which the VPN/FireWall Module is running. If the file `$FWDIR/conf/loggers` does not exist, VPN-1/FireWall-1 directs logs and alerts to the Masters in the `$FWDIR/conf/masters` file.

If the file `$FWDIR/conf/loggers` does exist, then the VPN/FireWall Module directs logging to the first IP address in the file to which it can connect (this can also be the IP address of the local machine). If the network object has more than one interface, then the IP address given in `$FWDIR/conf/loggers` should be the one facing the VPN/FireWall Module (that is, connected to the machine on which the VPN/FireWall Module is running).

If any of the IP addresses in `$FWDIR/conf/loggers` is preceded by a `+` symbol, then logging will be directed to all the IP addresses preceded by a `+` symbol. In this way, it is possible to direct logging to more than one IP address at the same time. If VPN-1/FireWall-1 cannot connect to any of the IP addresses is preceded by a `+` symbol, then logging will be directed to the first IP address not preceded by a `+` symbol to which the VPN/FireWall Module can connect.

If the connection to the Customer Log Module goes down, the VPN/FireWall Module scans `$FWDIR/conf/loggers` once again, looking for an IP address to which it can connect. If it finds one, it redirects logging to that address. Otherwise, it directs logging to the machine on which it is running.

To direct VPN-1/FireWall-1 logging to the Customer Log Module, proceed as follows:

- 1** Create the `$FWDIR/conf/loggers` manually since the `cpconfig` GUI cannot generate it.
- 2** In the `$FWDIR/conf/loggers` file on each VPN/FireWall Module, define the Customer Log Module.

IP addresses preceded by the `@` symbol will receive alert messages only.

### Examples

In the following `$FWDIR/conf/loggers`, Thames is the Customer Log Module.

```
+Thames
+localhost
@199.123.4.6
```



localhost appears with a + to indicate the direction of logging to both Thames and the localhost of the VPN/FireWall Module. The 199.123.4.6 host is prefixed with a “@” to indicate it receives alerts only.

For the following `$FWDIR/conf/loggers` file:

```
192.23.45.67
+192.45.67.89
192.34.56.78
+194.98.76.54
```

- a** The VPN/FireWall Module will attempt to log to both 192.45.67.89 and 194.98.76.54.
- b** If the VPN/FireWall Module fails to connect to both these IP addresses, it will try to connect to 192.23.45.67.
- c** If the VPN/FireWall Module fails to connect to 192.23.45.67, it will try to connect to 192.34.56.78.
- d** If the VPN/FireWall Module also fails to connect to 192.34.56.78 (in other words, if it cannot connect to any of the IP addresses in `$FWDIR/conf/loggers`) it will direct logging to itself.

### 3 Define Authentication Password

You must define the authentication password that will be used to enable control connections between the Customer Log Module and the VPN/FireWall Module.

- a** On the VPN/FireWall Module, issue the `fw putkey` command as follows:

```
fw putkey [-p password] <IP address of the Customer Log Module>
```

`-p password` is a password that will be used to authenticate communication between the Customer Log Module and the VPN/FireWall Module. The password can be entered on the command line (using the `-p` argument). If you do not enter a password on the command line, you will be prompted for one.

- b** On the Customer Log Module, issue the `fw putkey` command as follows:

```
fw putkey [-p password] <IP address of the Remote Module>
```

You must use the same password you used when you issued the `fw putkey` command on the VPN/FireWall Module.

## Log Viewing and Management

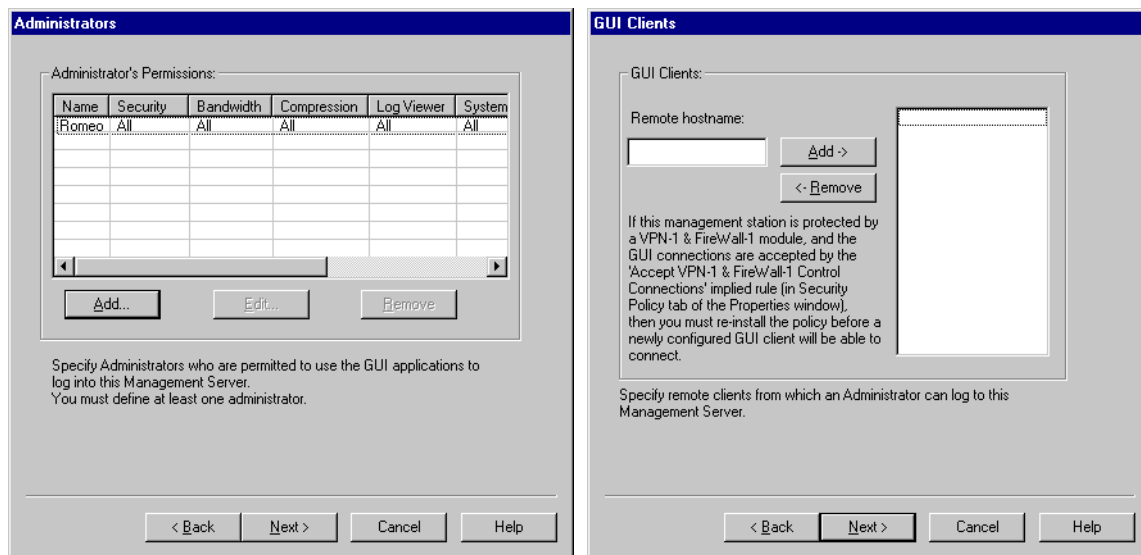
You can view logs maintained by the Customer Log Module using the Log Viewer on a Check Point GUI Client.

For information on installing the Check Point GUI Client, see Chapter 2, “Installing and Configuring VPN-1/FireWall-1” in this book.

For information on using the VPN-1/FireWall-1 Log Viewer, see Chapter 13, “Log Viewer” in this book.

You can also use standard VPN-1/FireWall-1 log commands for log management. For more information, see Chapter 1, “Command Line Interface” of *Check Point Reference Guide*.

To access Logs using the Log Viewer, you must define the GUI Clients and VPN-1/FireWall-1 Administrators that can connect to the Customer Log Module. GUI Clients and Administrators are defined during the installation of the VPN-1/FireWall-1 Management Server that functions as the Customer Log Module.



**FIGURE 2-34** Administrators and GUI Clients — VPN-1/FireWall-1 Installation

For more information, see Chapter 2, “Installing and Configuring VPN-1/FireWall-1” in this book.

After installation, you can add VPN-1/FireWall-1 Administrators and GUI Clients in the following ways:

## Administrators

- If your logging station is running under Windows NT, you can add or delete administrators using the Check Point Configuration application on a VPN-1/FireWall-1 GUI client.
- If your logging station is running under Unix, then you can add or delete administrators using the `cpconfig` command. See “cpconfig” in Chapter 1, “Command Line Interface” of *Check Point Reference Guide*.

## GUI Clients

- If your logging station is running under Windows NT, you can add or delete GUI Clients using the Check Point Configuration application on a VPN-1/FireWall-1 GUI client.
- If your logging station is running under Unix, then you can add or delete GUI Clients by using the `cpconfig` command. See “cpconfig” in Chapter 1, “Command Line Interface” of *Check Point Reference Guide*.

## Frequently Asked Questions

How do I move VPN-1/FireWall-1 to another machine?

First of all, you must ensure that you have a valid license for the new machine. Once the license issue is resolved, the simplest procedure is as follows:

- 1** Install VPN-1/FireWall-1 on the new machine.  
If your Management Module manages VPN/FireWall Modules on other machines, you must repeat the `fw putkey` procedure for all the machines (see “Distributed Configurations” on page 69).
- 2** Make a copy of the Security Policy files from the old machine.  
For information on which files to backup, see “How do I back up my Security Policy?” on page 84.
- 3** Restore the Security Policy backup files (see step 2 above) to the new machine.
- 4** Start the GUI on the new machine to confirm that the Security Policy was successfully transferred.
- 5** If the new machine is the FireWalled gateway, then define the new machine as a gateway.  
In the new machine’s **Workstation Properties** window, check the **Gateway** flag.
- 6** Delete the old machine from the Network Object Manager.  
Alternatively, you can leave the old machine, but uncheck the **VPN-1 & FireWall-1 Installed** flag in its **Workstation Properties** window.
- 7** Install the Security Policy.

The above procedure describes the simplest case: where the Management Module and VPN/FireWall Modules are on one machine, and the Security Policy is installed on gateways. If your configuration is more complicated, you will have to modify the procedure accordingly.

How do I back up my Security Policy?

To back up your Security Policy, make copies of the following files:

**TABLE 2-12** Backing Up a Security Policy

| to back up      | make a copy of these files                         |
|-----------------|----------------------------------------------------|
| network objects | \$FWDIR/conf/objects.C                             |
| Rule Base       | ■ \$FWDIR/conf/*.W<br>■ \$FWDIR/conf/rulebases.fws |
| user database   | \$FWDIR/database/fwauth.NDB*                       |

What Objects are Carried Over from the Previous Version?

When you upgrade to a new version of VPN-1/FireWall-1, the installation procedure carries the following elements over to the new version:

- VPN-1/FireWall-1 database (users and network objects)
- Properties
- Key database
- Encryption Parameters
- Rule Base

VPN-1/FireWall-1 attempts to merge your database with its own new database. For example, you will have the benefit of services defined in the new version and you will retain the services you defined in the previous version. In the case of a name conflict, the old objects (the ones you defined) will be retained.

What files are modified during re-configuration?

The following files are created modified during reconfiguration:

- control.map
- fwauthd.conf
- masters
- cp.license
- fwauth.keys
- external.if (for VPN-1/FireWall-1/25, VPN-1/FireWall-1/50, etc.)

You must create and modify the loggers file manually.

Must I re-install the Security Policy after upgrading?

After upgrading, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy.

If I change the IP address of a network object, when does the change take effect?

You must re-install the Security Policy for the change to take effect.

When you re-install a Security Policy, VPN-1/FireWall-1 internal state tables are cleared, so there is the possibility that some connections may be lost, as follows:

- FTP data connections  
If you have an open FTP connection and the Security Policy is re-installed before the FTP server attempts to open the back connection, then the back connection will be rejected.
- UDP connections
- TCP connections, in very rare circumstances
- An open encrypted session will be dropped if the newly installed Security Policy allows the session to be unencrypted.

If you are concerned about losing these connections, then you should take care to re-install your Security Policy during off-peak hours.



# Graphical User Interface

---

## In This Chapter

|                                         |                |
|-----------------------------------------|----------------|
| <i>Managing VPN-1/FireWall-1</i>        | <i>page 87</i> |
| <i>The Check Point Policy Editor</i>    | <i>page 88</i> |
| <i>Displaying Policy Editor Windows</i> | <i>page 91</i> |
| <i>Menus</i>                            | <i>page 92</i> |
| <i>VPN-1/FireWall-1 Toolbar</i>         | <i>page 96</i> |
| <i>VPN-1/FireWall-1 Status Bar</i>      | <i>page 96</i> |

## Managing VPN-1/FireWall-1

The easiest way to FireWall your network is to use the Check Point Policy Editor. You can use the command line interface, if you wish, instead of the Policy Editor. For additional information about the FireWall-1 command line interface, see Chapter 1, “Command Line Interface” of *FireWall-1 Reference Guide*.



**Note** – The FireWall-1 command line interface runs only on the Management Server.

For information about the FireWall-1 Client/Server model, see “VPN-1/FireWall-1 Client/Server Model” on page 13.

# The Check Point Policy Editor

## Starting the Policy Editor

To start the Check Point Policy Editor, proceed as follows:

**TABLE 3-1** Starting the Check Point Policy Editor

| Windows System | Action                                  |
|----------------|-----------------------------------------|
| Windows        | Double-click on the Policy Editor icon. |
| X/Motif        | Run \$FWDIR/bin/fwpolicy.               |

The **Policy Editor Login** window (FIGURE 3-1) is then displayed.

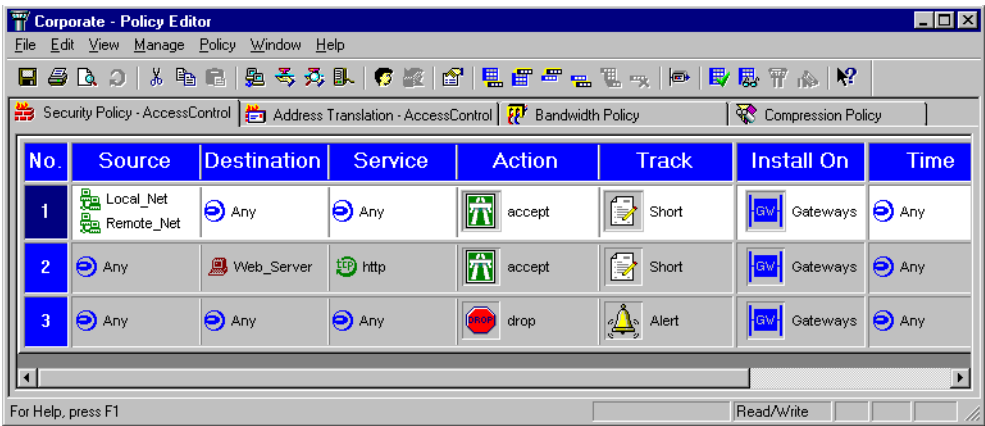


**FIGURE 3-1** Policy Editor login window

Enter your user name, password and the name of the Management Server to which to connect. Then click on **OK**.

If you do not wish to modify a policy, check **Read Only** before clicking on **OK**.

After a brief delay, during which the FireWall-1 database is loaded, the VPN-1/FireWall-1 **Policy Editor** window (FIGURE 3-2) is displayed.



**FIGURE 3-2** VPN-1/FireWall-1 Policy Editor window with Rule Base



The **Policy Editor** window's title shows the name of the Security Policy currently displayed.

Depending on your license (the VPN-1/FireWall-1 features your Management Station is licensed to implement), you may see as many as four tabs in the **Policy Editor** window:

- **Security Policy**

The Security Policy Rule Base is described in Chapter 8, "Security Policy Rule Base."

- **Address Translation**

The Address Translation Rule Base is described in Chapter 14, "Network Address Translation."

- **Bandwidth Policy**

The Bandwidth Policy is described in the book *Check Point FloodGate-1 Architecture and Administration*.

- **Compression Policy**

This feature will be implemented in a future release.

## Problems in Connecting to the Management Server

If the FireWall-1 GUI cannot connect to the Management Server, an error message window like the one shown in FIGURE 3-3 is displayed.



**FIGURE 3-3** Error message window

When this happens, the problem is usually one of the following:

- 1 The specified Management Server is inaccessible for one of the following reasons:

- There may be no such server.
- The specified Management Server may be inaccessible or down at the moment.
- The request may have timed out.

In this case, an error message "No Response from Server" will be displayed.

By default the GUI waits 15 seconds for the Management Server to respond to requests. In certain cases the server may be very loaded and certain operations (queries for example) may take longer than 15 seconds. If this happens, you can change the default 15 second timeout as follows:

- Windows NT

Set a registry DWORD value named `ServerTimeout` under the key `HKEY_LOCAL_MACHINE\Software\CheckPoint\Policy Editor\4.1` to the desired timeout in seconds.

■ X/Motif

Set an environment parameter named `SERVER_TIMEOUT` to the desired timeout in seconds.

- The specified Management Server's name is not being correctly resolved, perhaps because you misspelled it.
- The Caps Lock key is down.

**2** You did not enter your password correctly.

Re-enter your password and try again.

**3** The machine you are working on is not one of the GUI Clients permitted by the server.

If your Management Server is running under Windows NT, you can add or delete GUI Clients using the VPN-1/FireWall-1 Configuration application. See Chapter 2, "Installing and Configuring VPN-1/FireWall-1," for information about the VPN-1/FireWall-1 Configuration application.

If your Management Server is running under Unix, then you can add or delete GUI Clients by using any text editor to modify the file `$FWDIR/conf/gui-clients` directly. The file consists of IP addresses or resolvable names, one per line.

**4** You are not one of the allowed administrators.

If your Management Server is running under Windows NT, you can add or delete administrators using the VPN-1/FireWall-1 Configuration application. See Chapter 2, "Installing and Configuring VPN-1/FireWall-1," for information about the VPN-1/FireWall-1 Configuration application.

If your Management Server is running under Unix, then you can add or delete administrators using the `-a` and `-r` options of the `fwm` program. See "fwm" on page 27 of *Check Point Reference Guide* for more information.

**5** The versions of the GUI Client and Management Server are incompatible.

This can happen when mixing encryption and non-encryption versions.







**6** A rule or property disallows the connection between the GUI Client and Management Server.

See "Accept VPN-1 & FireWall-1 Control Connections" on page 239 for more information.

## Displaying Policy Editor Windows





TABLE 3-2 shows how to display each of the more important Policy Editor windows.

**TABLE 3-2** Displaying Policy Editor windows





| to display this window         | in the Policy Editor window                                                                                                                                  | in the toolbar                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Network Objects Manager</b> | Choose <b>Network Objects</b> from the <b>Manage</b> menu or right-click on a rule's <b>Source</b> or <b>Destination</b> (see Chapter 4, "Network Objects"). |  |
| <b>Users Manager</b>           | Choose <b>Users</b> from the <b>Manage</b> menu or right-click on a rule's <b>Source</b> (see Chapter 5, "Managing Users").                                  |  |
| <b>Services Manager</b>        | Choose <b>Services</b> from the <b>Manage</b> menu or right-click on a rule's <b>Services</b> (see Chapter 6, "Services and Resources").                     |  |
| <b>Resources Manager</b>       | Choose <b>Resources</b> from the <b>Manage</b> menu (see Chapter 6, "Services and Resources").                                                               |  |
| <b>Servers Manager</b>         | Choose <b>Servers</b> from the <b>Manage</b> menu (see Chapter 10, "Server Objects").                                                                        |  |
| <b>Properties Setup</b>        | Choose <b>Properties</b> from the <b>Policy</b> menu (see Chapter 7, "Properties Setup").                                                                    |  |
| <b>System Status</b>           | Double-click on the System Status icon on the desktop, or choose <b>System Status</b> from the <b>Window</b> menu.                                           | none                                                                                |
| <b>Log Viewer</b>              | Double-click on the Log Viewer icon on the desktop or choose <b>Log Viewer</b> from the <b>Window</b> menu.                                                  | none                                                                                |

## Menus

### File Menu

| Menu Entry                | Toolbar Button                                                                    | Description                                                                          | See                                    |
|---------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------|
| <b>New</b>                | none                                                                              | Create a new Security Policy.                                                        | “Creating a New Policy” on page 264    |
| <b>Open</b>               | none                                                                              | Open an existing Security Policy.                                                    | “Opening a Policy” on page 263         |
| <b>Installed Policies</b> |                                                                                   | View a policy installed on a VPN/FireWall Module managed by this Management Station. | Chapter 8, “Security Policy Rule Base” |
| <b>Refresh</b>            |  | Refresh the Security Policy from the Management Server.                              |                                        |
| <b>Save</b>               |  | Save the current Security Policy and all system objects.                             | “Saving a Policy” on page 264          |
| <b>Save As</b>            | none                                                                              | Save the current Security Policy and all system objects.                             | “Saving a Policy” on page 264          |
| <b>Delete</b>             |                                                                                   |                                                                                      |                                        |
| <b>Print</b>              |  | Print the current Security Policy.                                                   | Chapter 8, “Security Policy Rule Base” |
| <b>Print Preview</b>      |  | Print Preview of the current Security Policy.                                        |                                        |
| <b>Print Setup</b>        | none                                                                              | Open the standard <b>Print Setup</b> window.                                         |                                        |
| <b>Exit</b>               | none                                                                              | Exit the application.                                                                |                                        |

## Edit Menu







| Menu Entry          | Toolbar Button                                                                    | Description                                                    | See                                              |
|---------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------|
| <b>Add Rule</b>     | none                                                                              | Add a rule to the Rule Base.                                   | “Adding a Rule” on page 265                      |
| <b>Delete Rule</b>  |  | Delete the selected rule.                                      | “Deleting a Rule” on page 277                    |
| <b>Cut</b>          |  | Delete the selected rule (or rules) and copy to the Clipboard. | “Copying, Cutting and Pasting Rules” on page 277 |
| <b>Copy</b>         |  | Copy the selected rule (or rules) to the Clipboard.            | “Copying, Cutting and Pasting Rules” on page 277 |
| <b>Paste</b>        |  | Paste the rule that is in the Clipboard.                       | “Copying, Cutting and Pasting Rules” on page 277 |
| <b>Hide Rule</b>    |                                                                                   |                                                                |                                                  |
| <b>Disable Rule</b> |                                                                                   | Disable the selected rule.                                     | “Disabling Rules” on page 298                    |

## View Menu







| Menu Entry                 | Toolbar Button | Description                                                                                          | See                                      |
|----------------------------|----------------|------------------------------------------------------------------------------------------------------|------------------------------------------|
| <b>Toolbar</b>             | none           | Toggle the display of the VPN-1/FireWall-1                                                           | “VPN-1/FireWall-1 Toolbar” on page 96    |
| <b>Status Bar</b>          | none           | Toggle the display of the VPN-1/FireWall-1 Status Bar.                                               | “VPN-1/FireWall-1 Status Bar” on page 96 |
| <b>Mask (hiding rules)</b> | none           | Hide or unhide rules according to masks.                                                             | “Masking Rules” on page 283              |
| <b>Queries</b>             | none           |                                                                                                      | “Querying the Rule Base” on page 288     |
| <b>Implied Rules</b>       | none           | Toggle the display of the implied rules (the rules derived from the <b>Properties Setup</b> window). | “Implied Rules” on page 282              |

The **Policy Editor** toolbar (see page 96) is displayed below the menu. The **Policy Editor** Status Bar (see page 96) is displayed at the bottom of the **Policy Editor** window.

## Manage Menu

| Menu Entry                   | Toolbar Button                                                                    | Description                                                                   | See                                                                                                                      |
|------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Network Objects</b>       |  | Manage Network Objects.                                                       | Chapter 4, “Network Objects”                                                                                             |
| <b>Services</b>              |  | Manage Services.                                                              | Chapter 6, “Services and Resources”                                                                                      |
| <b>Resources</b>             |  | Manage Resources.                                                             | Chapter 6, “Services and Resources”                                                                                      |
| <b>Servers</b>               |  | Manage Servers.                                                               | Chapter 10, “Server Objects”                                                                                             |
| <b>Users</b>                 |  | Manage Users.                                                                 | Chapter 5, “Managing Users”                                                                                              |
| <b>Users on Account Unit</b> |  | Manage Users on an LDAP Account Unit using the Account Management GUI Client. | “External Users and Groups” on page 169” and <i>FireWall-1 Account Management Client</i>                                 |
| <b>Time</b>                  | none                                                                              | Manage Time Objects.                                                          | Chapter 9, “Time Objects”                                                                                                |
| <b>Keys</b>                  | none                                                                              | Manage Encryption Keys.                                                       | “Defining an SPI” on page 121 in Chapter 8, “Encryption Properties” of <i>Virtual Private Networking with FireWall-1</i> |

## Policy Menu

| Menu Entry              | Toolbar Button                                                                    | Description                                                  | See                                                       |
|-------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------|
| <b>Verify</b>           |  | Verify the Security Policy.                                  | “Verifying the Rule Base and Security Policy” on page 298 |
| <b>View</b>             |  | View the Inspection Script.                                  | “Viewing the Inspection Script” on page 299               |
| <b>Install</b>          |  | Install the Security Policy on the targets.                  | “Installing the Security Policy” on page 300              |
| <b>Uninstall</b>        |  | Remove the Security Policy from the targets.                 | “Uninstalling the Security Policy” on page 301            |
| <b>Access Lists</b>     |  | Display the <b>Router Access Lists Operations</b> window.    | “Installing Access Lists” on page 302                     |
| <b>Properties</b>       |  | Display the <b>Properties Setup</b> window.                  | Chapter 7, “Properties Setup”                             |
| <b>Install Database</b> | none                                                                              | Install the Database to selected FireWalled network objects. | “Database Installation” on page 167                       |

## Window Menu

| Menu Entry               | Toolbar Button | Description                    | See                                                            |
|--------------------------|----------------|--------------------------------|----------------------------------------------------------------|
| <b>Log Viewer</b>        | none           | Open the Log Viewer.           | Chapter 13, “Log Viewer”                                       |
| <b>System Status</b>     | none           | Open the System Status Viewer. | Chapter 12, “System Status Viewer”                             |
| <b>Real Time Monitor</b> | none           | Open the Real-Time Monitor.    | <i>Check Point FloodGate-1 Architecture and Administration</i> |

## Help Menu

| Menu Entry                 | Toolbar Button | Description                                    |
|----------------------------|----------------|------------------------------------------------|
| <b>Help Topics</b>         | none           | Display Help.                                  |
| <b>About Policy Editor</b> | none           | Display the <b>About Policy Editor</b> window. |


























## VPN-1/FireWall-1 Toolbar



**FIGURE 3-4** VPN-1/FireWall-1 Toolbar

The toolbar buttons are shortcuts for menu commands.

### Toolbar Buttons and Menu Commands

| Toolbar Button                                                                      | Menu Command           | Toolbar Button                                                                      | Menu Command                 | Toolbar Button                                                                      | Menu Command        |
|-------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------|---------------------|
|    | File>Save              |    | Manage>Resources             |    | Policy>Properties   |
|    | File>Print             |    | Manage>Servers               |    | Policy>Access Lists |
|    | File>Print Preview     |    | Manage>Users                 |    | Policy>Verify       |
|    | Refresh                |    | Manage>Users on Account Unit |    | Policy>View         |
|    | Edit>Cut               |    | Edit>Add Rule>Bottom         |    | Policy>Install      |
|   | Edit>Copy              |   | Edit>Add Rule>Top            |   | Policy>Uninstall    |
|  | Edit>Paste             |  | Edit>Add Rule>Before         |  | Help                |
|  | Manage>Network Objects |  | Edit>Add Rule>After          |                                                                                     |                     |
|  | Manage>Services        |  | Edit>Delete Rule             |                                                                                     |                     |

## VPN-1/FireWall-1 Status Bar



**FIGURE 3-5** VPN-1/FireWall-1 Status Bar

The VPN-1/FireWall-1 Status Bar, displayed at the bottom of the VPN-1/FireWall-1 window, shows information on the state of VPN-1/FireWall-1, as well as explanations of menu items and toolbar buttons.



# Network Objects

---

## In This Chapter

|                                       |                 |
|---------------------------------------|-----------------|
| <i>Defining Network Objects</i>       | <i>page 97</i>  |
| <i>Workstation Properties</i>         | <i>page 102</i> |
| <i>Network Properties</i>             | <i>page 115</i> |
| <i>Domain Properties</i>              | <i>page 117</i> |
| <i>Router Properties</i>              | <i>page 118</i> |
| <i>Switch Object Properties</i>       | <i>page 137</i> |
| <i>Integrated FireWall Properties</i> | <i>page 141</i> |
| <i>Network Object Groups</i>          | <i>page 147</i> |
| <i>Logical Server Properties</i>      | <i>page 149</i> |
| <i>Address Range Properties</i>       | <i>page 150</i> |

## Defining Network Objects

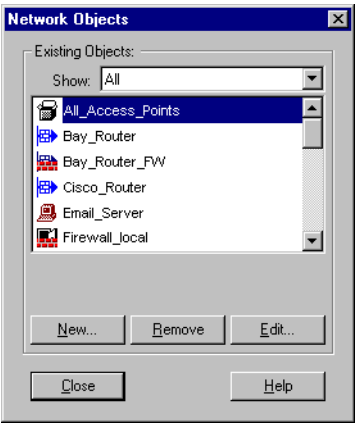
Network objects include workstations, gateways, routers, networks, switches, Logical Servers, gateway clusters, and domains. Before you can include a network object in a rule, you must define it and its properties.

Network objects can be organized in hierarchical groups to form higher-level objects and easier to read rules.

You do not have to define every object in your networks to VPN-1/FireWall-1 — only those objects that are used in the Rule Base. For example, if a rule refers to a network, you must define the network, but it's not necessary to define every host in the network.

## Modifying an Object from the Policy Editor

To add a network object to a rule from the Rule Base, right-click on the rule’s **Source** or **Destination** in the Policy Editor and choose **Add** from the menu. The **Network Objects** window is displayed (FIGURE 4-1).



**FIGURE 4-1** Network Objects window

The objects displayed depend on what you have selected from the **Show** dropdown list.

To add an existing network object to a rule, select the object from the listbox and click on **OK**. The selected object is added to the rule and the **Network Objects** window is closed.

To create a new object and add that object to the rule, click on **New**.

**TABLE 4-1** Network Object Actions

| for a description of how to ... | ... see                             |
|---------------------------------|-------------------------------------|
| create a network object         | “Creating a New Object” on page 100 |
| modify a network object         | “Modifying an Object” on page 101   |
| delete a network object         | “Deleting an Object” on page 101    |

The new network object is added to the rule in which you began this procedure. For example, if you right-clicked in a rule’s **Destination**, then the new object is added to the rule’s **Destination**.

To modify a network object from the Policy Editor, proceed as follows:

- 1 Right-click on a rule's **Source** or **Destination** in the Policy Editor.

The **Object** menu is displayed (FIGURE 4-2).



**FIGURE 4-2** Object menu

The items that appear in the Object menu (FIGURE 4-2) depend on whether you right-clicked in the **Source** or **Destination** column.

- 2 Choose one of the menu items.

**Add** — Open the **Network Objects** window (FIGURE 4-1 on page 98).

**Add User Access** — Open the **User Access** window (FIGURE 4-3 on page 100).

**Edit** — Open the appropriate **Edit Object** window for this object.

**Delete** — Delete the object(s) from the rule.

**Negate** — Negate the object(s) in the rule.

For example, if a rule's **Source** is a host network object named monk, then the rule applies when the communication's **Source** is monk. However, if you negate monk, then the rule applies when the communication's **Source** is not monk.

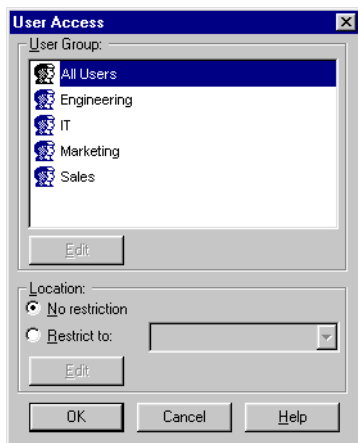
You cannot negate individual objects. For example, if two hosts are given as a rule's **Source**, then you can negate both of them or none of them, but not just one of them.

**Cut** — Delete the object(s) from the rule and put the object on the clipboard.

**Copy** — Copy the object(s) to the clipboard.

**Paste** — Paste the object(s) on the Clipboard into the rule at this point.


The network object is added to the rule in which you began this procedure. For example, if you right-clicked in a rule's **Destination**, then the new object is added to the rule's **Destination**.



**FIGURE 4-3** User Access window

## Modifying an Object from the Network Object Manager

To define a network object from the Network Object Manager, open the **Network Objects** window (FIGURE 4-1 on page 98) by:

- choosing **Network Objects** from the **Manage** menu, *or*
- selecting  from the toolbar.

### ▼ Creating a New Object

To create a new object, click on **New**. A menu (FIGURE 4-4) is displayed that lists the types of objects you can create.



**FIGURE 4-4** Add Network Object menu

Choose a type from the menu. A window is displayed prompting you to enter the properties of the selected object type.



**Note** – If you opened the **Network Objects** window from the Rule Base, then the **Add Network Object** menu displays the valid choices for the column from which it was opened. These vary from column to column. For example, **Logical Servers** is a valid choice under **Destination** but not under **Source**. On the other hand, if you opened the **Network Objects** window from the menu or from the toolbar, then all the possible choices are displayed in the **Add Network Object** menu.

TABLE 4-2 summarizes the available options.

**TABLE 4-2** Object Types

| to create an object of type ... | ... see                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| workstation                     | “Workstation Properties” on page 102                                                                                                       |
| network                         | “Network Properties” on page 115                                                                                                           |
| domain                          | “Domain Properties” on page 117                                                                                                            |
| router                          | “Router Properties” on page 118                                                                                                            |
| switch                          | “Switch Object Properties” on page 137                                                                                                     |
| integrated firewall             | “Integrated FireWall Properties” on page 141                                                                                               |
| group                           | “Network Object Groups” on page 147                                                                                                        |
| logical server                  | “Logical Server Properties” on page 149                                                                                                    |
| address range                   | “Address Range Properties” on page 150                                                                                                     |
| gateway cluster                 | “Connect Control” on page 254 and Chapter 12, “High Availability for Encrypted Connections” of <i>Check Point Virtual Private Networks</i> |

## ▼ Deleting an Object

To delete an object, select the object and click on **Remove**.

## ▼ Modifying an Object

To modify an object, select the object and click on **Edit**, or double-click on the object.

You can also modify an object from the Policy Editor (see “Modifying an Object from the Policy Editor” on page 98).

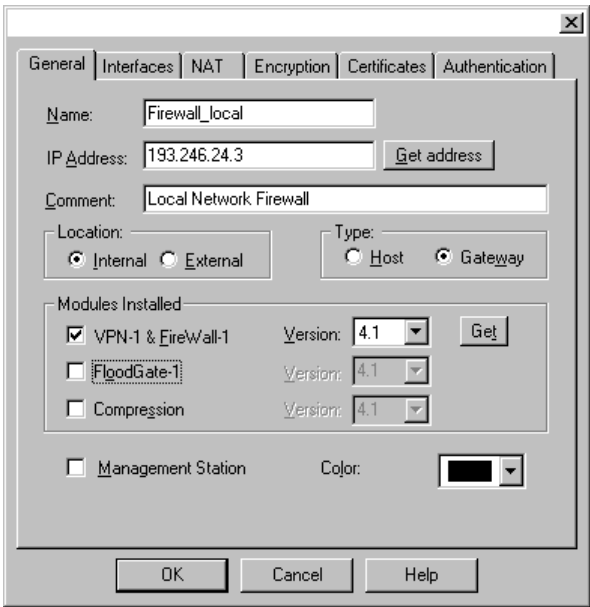
If the IP addresses of network objects have been modified or new ones added since the GUI was invoked, restart the GUI to refresh the GUI’s internal cache of addresses. Network objects that have already been defined are not affected. If their properties have been edited, however, updated data will be retrieved.

# Workstation Properties

## In This Section

|                                                                              |                 |
|------------------------------------------------------------------------------|-----------------|
| <i>Workstation Properties Window — General Tab</i>                           | <i>page 102</i> |
| <i>Workstation Properties Window — Interfaces Tab</i>                        | <i>page 104</i> |
| <i>Interface Properties window — General and Security tabs</i>               | <i>page 105</i> |
| <i>Workstation Properties Window — VPN Tab</i>                               | <i>page 109</i> |
| <i>Workstation Properties Window — Authentication Tab</i>                    | <i>page 110</i> |
| <i>Workstation Properties Window — Certificates tab</i>                      | <i>page 112</i> |
| <i>Workstation Properties Window — SNMP Tab</i>                              | <i>page 111</i> |
| <i>Workstation Properties Window — NAT (Network Address Translation) Tab</i> | <i>page 113</i> |
| <i>Workstation Properties Window — Account Unit Tab</i>                      | <i>page 114</i> |

## Workstation Properties Window — General Tab



**FIGURE 4-5** Workstation Properties window — General tab

**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):



- To define a new workstation, click on **New**.
- To edit the properties of an existing workstation, select the workstation and click on **Edit**.

**Name** — the workstation's name

The name given here should be identical to the name as it appears in the OS environment, as given in TABLE 4-3.

**TABLE 4-3** Default File Locations and Names

| Unix          | NT                                          |
|---------------|---------------------------------------------|
| /etc/hosts    | c:\\winnt\\system32\\drivers\\etc\\lmhosts  |
| /etc/networks | c:\\winnt\\system32\\drivers\\etc\\networks |

If NIS is being used, VPN-1/FireWall-1 automatically retrieves the information from the NIS. If the network object is one that can respond to a Unix `hostname` command, use the name returned by that command. The IP address is the one shown by the command `grep hostname /etc/hosts`.



**Warning** – Do not rename a gateway for which encryption properties are defined.

**IP Address** — the workstation's IP address

You can get the IP address of previously defined network objects from the database of network objects by clicking on **Get Address**.

**Note** –



- For a gateway, the **IP Address** field in the **Workstation Properties** window (see FIGURE 4-5) must specify the gateway's external interface. If you fail to do so, SKIP and IKE encryption will not function properly.
- It is recommended that you list workstation objects in your `hosts` (Unix) and `lmhosts` (Windows) files in addition to defining them in the VPN-1/FireWall-1 database.

**Get Address** — Click on this button to resolve the object's name to an IP address, by consulting the files in TABLE 4-3 on page 103.

**Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

**Color** — Select a color from the drop-down list.

**Location: Internal/External** — relevant for only for workstations on which a VPN/FireWall Module is installed

Only **Internal** objects appear in the System Status View (see Chapter 12, "System Status Viewer").

A FireWalled object is internal to its own Management Station and external to other Management Stations. You cannot install a Security Policy on an object from a Management Station where the object is defined as external.


**Type: Host/Gateway** — whether this object is a host or gateway

**Modules Installed** — Specifies the Check Point Modules installed on this workstation, and their version numbers.

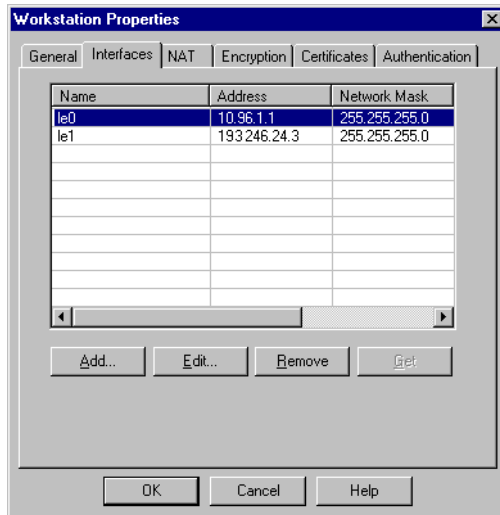
The Policy Editor installs policy on a workstation compatible with the Module version on the workstation.

If **VPN-1/FireWall Installed** is checked, then:

- The **Authentication** tab (FIGURE 4-10 on page 110) becomes available.
- The **Account Unit** tab (FIGURE 4-14 on page 114) becomes available if **Use LDAP Account Management** is checked on the **LDAP** tab of the **Properties Setup** window.

In order to make the newly available tabs visible, you may have to click on  to scroll them.

## Workstation Properties Window — Interfaces Tab



**FIGURE 4-6** Workstation Properties window — Interfaces tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the workstation in the **Network Objects** window (FIGURE 4-1 on page 98) and click on **Edit** and then on the **Interfaces** tab.

**Get** — Retrieve the network interfaces information for this workstation and display it in this window.



The **Get** button is the recommended way to define interfaces.



**Warning** – If you do not define all of the object's interfaces, you may be unable to properly define anti-spoofing and the Security Policy may be incorrectly enforced.

To add an interface, click on **Add**. The **Interface Properties** window (FIGURE 4-7) is displayed.

To edit an interface, select the interface and click on **Edit** or double-click on the interface. The **Interface Properties** window (FIGURE 4-7) is displayed.

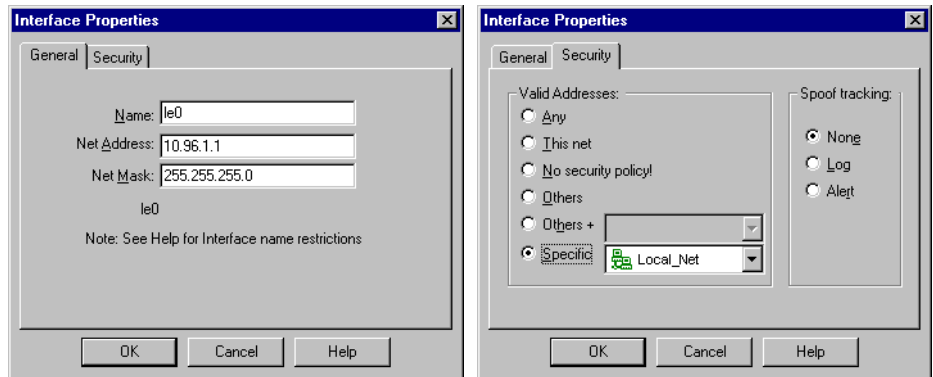
To delete an interface, select the interface and click on **Remove**.

## Interface Properties Window

The **Interface Properties** window (FIGURE 4-7) enables you to provide information about additional connections to a network object. It is essential to understand the difference between a network object and its interfaces.

A single network object can have many network interfaces; that is, one network object may be connected to numerous networks. Each interface has its own IP address and net mask.

You can use the **Get** button (in the **Interfaces** tab of the **Workstation Properties** window) to fetch interface data automatically.



**FIGURE 4-7** Interface Properties window — General and Security tabs



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the network object in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit**, click on the **Interfaces** tab and then:

- To define a new interface, click on **Add**.
- To edit the properties of an existing interface, select the interface and click on **Edit**.

**Name** — name of the network interface as specified in the interface configuration scheme of the host, gateway, or router; for example, *lo0* for loopback; *le0* for Ethernet interface; *sl0* for serial interface 0, etc.

**Net Address** — a 32-bit address that uniquely identifies this interface.



**Note** – A host does not have the same IP address on all the networks to which it is connected.

See “IP Address” on page 103.

**Net Mask** — If the network is a standard Class A, B, or C network, the Net Mask does not need to be specified.

### Valid Addresses

Spoofing is a technique where an intruder attempts to gain unauthorized access by altering a packet’s IP address to make it appear as though the packet originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be disguised as a local packet. If undetected, this packet might then have unrestricted access to internal networks.

You can defend your network against these attacks by defining the addresses that are considered valid on each interface.

The meaning of **Valid Addresses** for an interface is:

- A packet whose source IP address belongs to **Valid Addresses** is allowed to enter the network object through the interface.
- A packet whose source IP address does not belong to **Valid Addresses** is not allowed to enter the network object through the interface.

In the **Valid Addresses** box, specify the network on the other side of this interface. Choose one of the following:

**Any** — (default) no spoof tracking and no auto-scoping (routers only)

For more information on auto-scoping, see “Defining Router Anti-Spoofing Properties” on page 122.

**No security policy!** — No Security Policy at all is installed on this interface.

This option is used when the Security Policy is to be enforced on another interface of this object, while leaving this interface open.



**Warning** – This option should be used with extreme caution.

**Others** — All packets are allowed, except those whose source IP addresses belong to the networks listed under **Valid Addresses** for this object’s other interfaces.

**Others +** — All packets are allowed, except those whose source IP addresses belong to the networks listed under **Valid Addresses** for this object's other interfaces. However, packets from the addresses listed under **Others +** are allowed. (The **+** adds valid addresses.)

This option is used when an object is connected to more than one interface.

**This Net** — Only packets whose source IP addresses are part of the network connected to this interface are allowed.

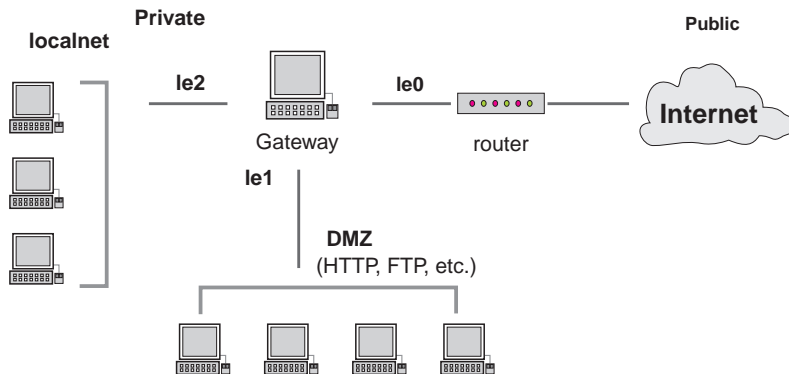
This option is typically used for internal interfaces of the last network (that is, a network with no networks behind it).

**Specific** — Only packets from this object are allowed.

When anti-spoofing is specified, an implicit anti-spoof rule is generated, which comes first in the Rule Base (even before properties specified as **First** in the **Security Policy** tab of the **Properties Setup** window).

#### Anti-Spoofing Example

Consider the network depicted in FIGURE 4-8.



**FIGURE 4-8** Anti-Spoof Example Configuration

Anti-spoofing should be defined on the gateway's three interfaces as follows:

**TABLE 4-4** Valid Addresses for each interface

| interface | Valid addresses |
|-----------|-----------------|
| le2       | This Net        |
| le1       | This Net        |
| le0       | Others          |

On interface le2, only packets with source IP addresses belonging to the internal network should be allowed to enter. A packet with another source IP address coming in on le2 is spoofed.

The same is true of le1.

On leO, only packets with source IP addresses belonging to neither DMZ nor localnet should be allowed to enter. A packet entering on leO whose source IP address belongs to either DMZ or localnet is spoofed. Packets from these networks should enter from one of the other interfaces and leave from leO.

#### Broadcast Addresses and Anti-Spoofing

If you choose **Others+**, you can specify a group of additional addresses that are considered legal. This feature enables you to prevent broadcast packets from being erroneously identified as spoofed packets, as follows:

- 1** Define a host named broadcast-255 with an IP address of 255.255.255.255.
- 2** Define a host named broadcast-O with an IP address of 0.0.0.0.
- 3** Define a group named BROADCAST consisting of broadcast-255 and broadcast-O.
- 4** Specify **Others+** and BROADCAST under **Valid Addresses** for the external interface.

#### Spoof Tracking

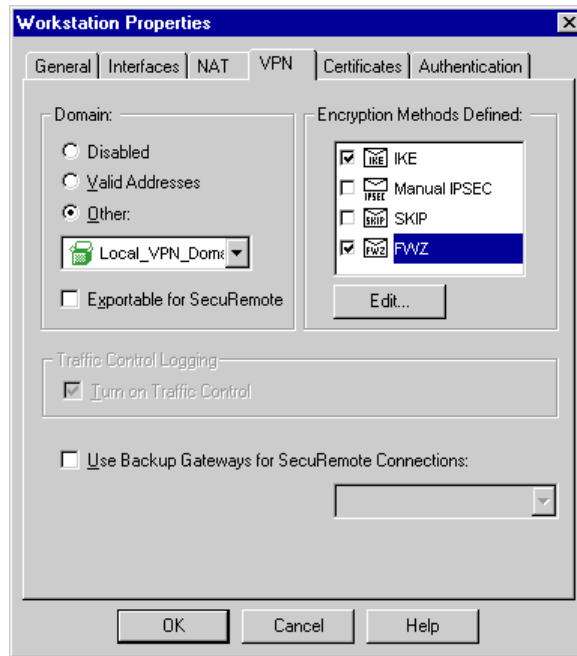
Spoofed packets are always dropped, but you can specify an additional action to be taken by selecting one of the options in the **Spoof Tracking** group box, as follows:

**None** — No additional action is taken.

**Log** —The spoofing attempt is logged.

**Alert** — The action specified in the **Anti Spoof Alert Command** field in the **Logging and Alerting** tab of the **Properties Setup** window is taken (see Chapter 7, “Properties Setup”).

## Workstation Properties Window — VPN Tab



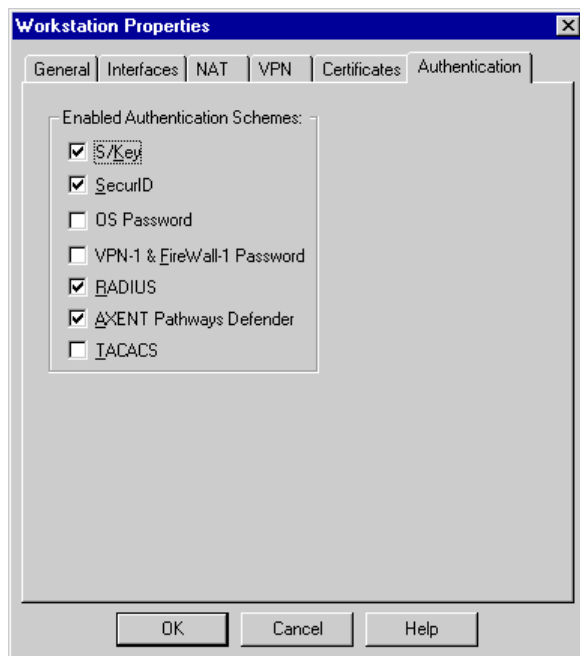
**FIGURE 4-9** Workstation Properties window — VPN tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the network object in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **VPN** tab.

This window specifies a network object's VPN parameters. For additional information regarding VPN-1/FireWall-1's VPN feature, see *Check Point Virtual Private Networks*.

## Workstation Properties Window — Authentication Tab



**FIGURE 4-10** Workstation Properties window — Authentication tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the workstation in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Authentication** tab.

The **Authentication** tab is available only when **VPN-1 & FireWall-1 Installed** is checked on the **General** tab.

Check the authentication schemes that are enforced on this gateway. A user for whom another authentication scheme is defined will not be allowed access through this gateway.

For additional information regarding VPN-1/FireWall-1's Authentication features, see Chapter 15, "Authentication."

## Workstation Properties Window — SNMP Tab

This window enables you to retrieve or set SNMP information for the network object.

The screenshot shows the 'Workstation Properties Window' with the 'SNMP' tab selected. The window contains the following elements:

- Tabs: General, Interfaces, **SNMP**, NAT, VPN, Certificates, Authentication.
- Fields:
  - sysName: [text box] with a 'Get' button.
  - sysLocation: [text box] with a 'Set' button.
  - sysContact: [text box]
  - sysDescription: [large text area]
- Buttons: 'Get' (next to sysName), 'Set' (next to sysLocation).
- Community Fields: 'Read community: [text box]' and 'Write community: [text box]'.

**FIGURE 4-11** Workstation Properties window — SNMP tab



**Getting Here** — To display this window, choose **Manage>Network Objects** in the menu, select the workstation in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **SNMP** tab.

**sysName** — the object's name

**sysLocation** — the object's location

**sysContact** —the name of a contact person

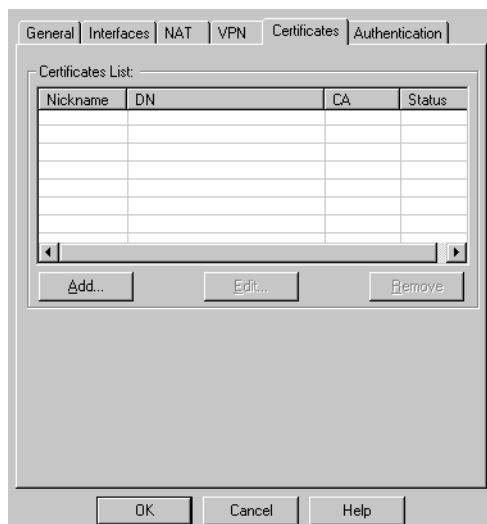
**Get** — You can use this button to retrieve information about this network object and display it in this window.

**Set** — Set the object's properties to those shown in this window.

**Read Community** — the community with read permission for this object

**Write Community** — the community with write permission for this object

## Workstation Properties Window — Certificates tab



**FIGURE 4-12** Workstation Properties window — Certificates tab

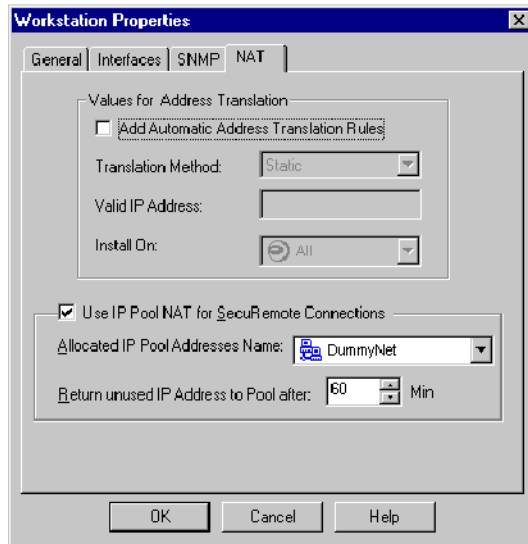
To add a certificate for the workstation, click on Add.



**Note** – Before adding certificates, you must first create a CA (Certificate Authority) Server object (see Chapter 3, “Certificate Authorities” of *Check Point Virtual Private Networks*).



## Workstation Properties Window — NAT (Network Address Translation) Tab



**FIGURE 4-13** Workstation Properties window — NAT (Address Translation) tab



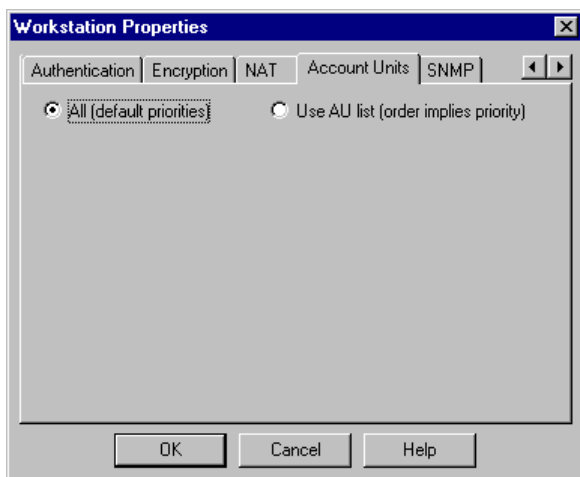
**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the workstation in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **NAT** tab.

This window specifies the parameters for automatically generated Address Translation rules for the network object.

For information about automatically generated Address Translation rules, see “Generating Address Translation Rules Automatically” on page 440.

For information about IP Pools, see “Multiple Entry Point (MEP) Example Configuration” on page 244 of *Check Point Virtual Private Networks*.

## Workstation Properties Window — Account Unit Tab



**FIGURE 4-14** Workstation Properties window — Account Unit tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the workstation in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Account Unit** tab.

The **Account Unit** tab is available only when both of the following conditions are true:

- **VPN-1 & FireWall-1 Installed** is checked in the **General** tab of the **Workstation Properties** window.
- **Use LDAP Account Management** is checked in the **LDAP** tab of the **Properties Setup** window.

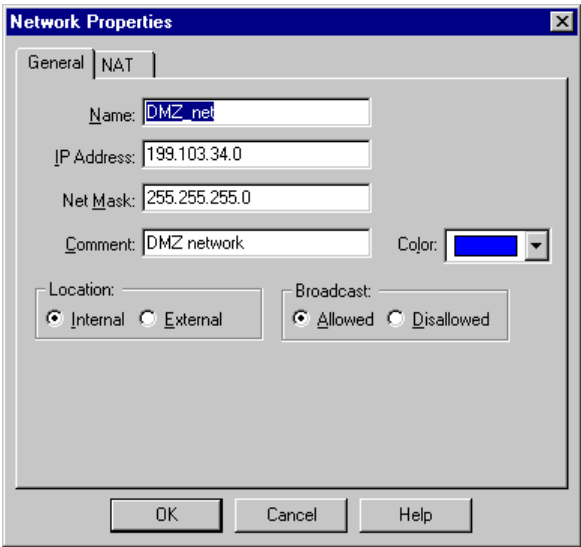
# Network Properties

## In This Section

|                                                                  |                 |
|------------------------------------------------------------------|-----------------|
| <i>Network Properties Window — General Tab</i>                   | <i>page 115</i> |
| <i>Network Properties Window — NAT (Address Translation) Tab</i> | <i>page 116</i> |

## Network Properties Window — General Tab

FIGURE 4-15 shows an example of a **Properties** windows for a network object of type *network*.



**FIGURE 4-15** Network Properties window — General tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new network, click on **New**.
- To edit the properties of an existing network, select the network and click on **Edit**.

**Name** — the network’s name

**IP Address** — a 32-bit address that uniquely identifies this interface

For networks, the host portion of the IP address is ignored, so it is best to enter the network address as x.y.z.0 (for a class C network).

See “IP Address” on page 103.

**Net Mask** — see “Net Mask” on page 106.

**Location: Internal/External** — relevant for FireWalled objects only

Only **Internal** objects appear in the System Status View (see Chapter 12, “System Status Viewer”).

A FireWalled object is internal to its own Management Station and external to other Management Stations. You cannot install a Security Policy on an object from a Management Station where the object is defined as external.

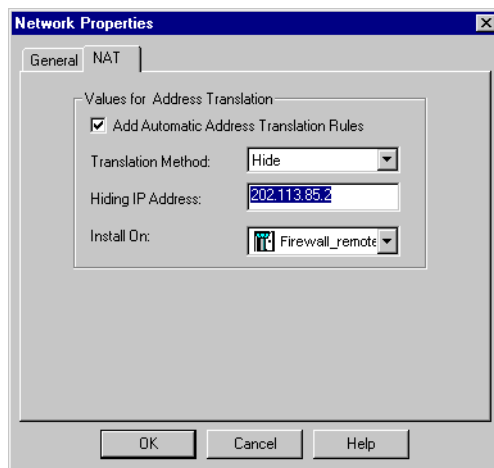
**Broadcasts: Allow/Disallow** — Allows you to specify whether to consider the network's broadcast IP address as being in the network.

If this is set to **Allow**, then in rules which allow access (that is, rules whose Action is neither **Reject** nor **Drop**) and in which this network object is either the **Source** or the **Destination**, the last address in the network is considered to be part of the network.

**Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

**Color** — Select a color from the drop-down list.

## Network Properties Window — NAT (Address Translation) Tab



**FIGURE 4-16** Network Properties window — Address Translation Tab



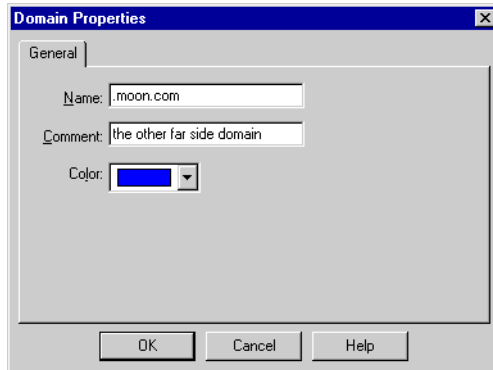
**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the network in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **NAT** tab.

This window specifies the parameters for automatically generated Address Translation rules for the network object.

For information about automatically generated Address Translation rules, see “Generating Address Translation Rules Automatically” on page 440.

## Domain Properties

### Domain Properties Window



**FIGURE 4-17** Domain Properties window



**Getting Here** – To display this window, choose **Manage**►**Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new domain, click on **New**.
- To edit the properties of an existing domain, select the domain and click on **Edit**.

**Name** —the domain’s name

Domain names begin with a period (“.”). For example, “.moon.com” is a domain name.

**Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

**Color** — Select a color from the drop-down list.

### Using Domain Objects in a Rule

When a domain object is used in a rule’s **Source** or **Destination**, the VPN-1/FireWall-1 Inspection Module must determine whether the packet’s IP address belongs to the domain by reverse resolving the address. VPN-1/FireWall-1 then confirms the reverse resolution by resolving the domain name.

The first time a rule containing a domain object is applied to a specific IP address, there is a slight delay while the Inspection Module reverse resolves the IP address. The resolved address is then stored in a local cache, so the delay occurs only once per IP address.

In order to minimize these delays, it is recommended that rules containing domain objects should be positioned as far down as possible in the Rule Base.



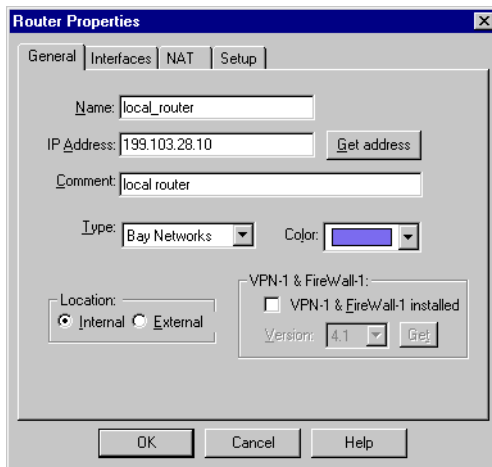
**Note** – VPN-1/FireWall-1 reverse resolves the IP address using DNS. Because VPN-1/FireWall-1's decision on whether to allow a communication depends on the information received from the DNS, it is imperative that you ensure you are using a trusted DNS.

## Router Properties

### In This Section

|                                                  |                 |
|--------------------------------------------------|-----------------|
| <i>Router Properties Window — General Tab</i>    | <i>page 118</i> |
| <i>Router Properties Window — Interfaces Tab</i> | <i>page 120</i> |
| <i>Router Properties Window — SNMP Tab</i>       | <i>page 127</i> |
| <i>Cisco Setup</i>                               | <i>page 128</i> |
| <i>Bay Networks Setup</i>                        | <i>page 130</i> |
| <i>3Com Setup</i>                                | <i>page 131</i> |
| <i>Microsoft RRAS Setup</i>                      | <i>page 133</i> |

### Router Properties Window — General Tab



**FIGURE 4-18** Router Properties window — General tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new router, click on **New**.
- To edit the properties of an existing router, select the router and click on **Edit**.

**Name** — the router's name

The name given here should be identical to the name as it appears in the system database on the server.

**Get Address** — click on this button to resolve the name to an address



**Note** – It is recommended that you list router objects in your `hosts` (Unix) and `lmhosts` (Windows) files in addition to defining them in the VPN-1/FireWall-1 database.

**Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

**Color** — Select a color from the drop-down list.

**Location: Internal/External** — relevant for FireWalled objects only

Only **Internal** objects appear in the System Status View (see Chapter 12, “System Status Viewer”).

A FireWalled object is internal to its own Management Station and external to other Management Stations. You cannot install a Security Policy on an object from a Management Station where the object is defined as external.

**Type** — choose one of the following from the drop-down menu:

- Cisco Systems
- Bay Networks
- 3Com
- Steelhead
- (Choose Steelhead for Microsoft RRAS.)
- Other



**Note** – A Bay Networks router can function in either of two modes: as a packet filter (in which case VPN-1/FireWall-1 installs an Access List on the router), or as a FireWalled router (in which case VPN-1/FireWall-1 installs a Security Policy on the router). Bay Networks routers do not support VPN-1/FireWall-1’s Encryption, Authentication or Address Translation features.

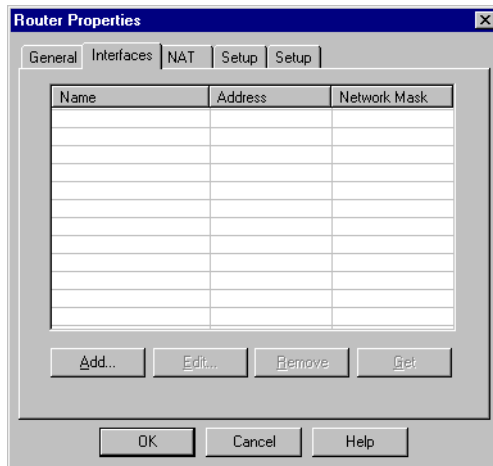
**VPN-1 & FireWall-1 Installed** —whether a VPN/FireWall Module was loaded on this router

This field is enabled only for Bay Networks routers.

If VPN-1/FireWall-1 is installed on a Bay Network router, then a Security Policy can be enforced on the router (with the exception of the Authentication, Encryption and Address Translation features).

If VPN-1/FireWall-1 is not installed on a Bay Network router, then a Security Policy cannot be installed on the router, only Access Lists.

## Router Properties Window — Interfaces Tab



**FIGURE 4-19** Router Properties window — Interfaces tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the router in the **Network Objects** window (FIGURE 4-1 on page 98) and click on **Edit** and then on the **Interfaces** tab.

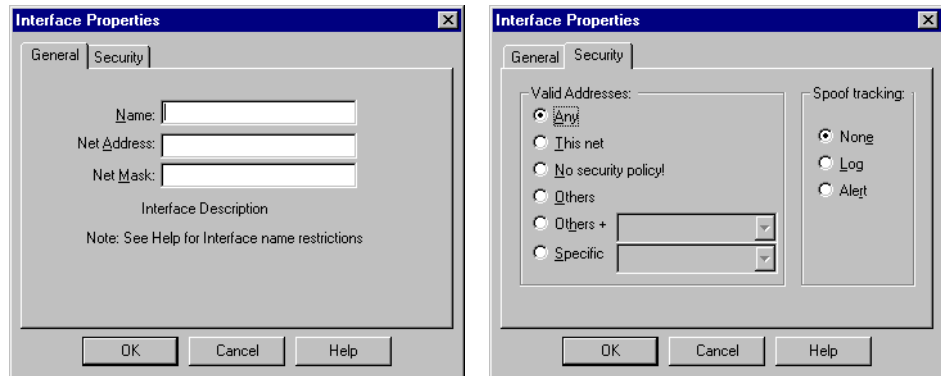
Routers report their network interfaces and setup at boot time. Each router has a different command for listing its configuration.

To add an interface, click on **Add**. The **Interface Properties** window (FIGURE 4-20) is displayed.

To edit an interface, select the interface and click on **Edit**, or double-click on the interface. The **Interface Properties** window (FIGURE 4-20 on page 121) is displayed.



To delete an interface, select the interface and click on **Remove**.



**FIGURE 4-20** Interface Properties window — General and Security tabs



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit**, click on the **Interfaces** tab and then:

- To define a new interface, click on **Add**.
- To edit the properties of an existing interface, select the interface and click on **Edit**.

The manner in which names are specified for router interfaces is different from the manner in which they are specified for interfaces of other network objects.

**Name** — name of the network interface as specified in the router's interface configuration scheme

This name does not include a trailing number.

For information regarding the other fields in the **Interface Properties** window for routers, see “Interface Properties Window” on page 105.

**Net Address** — a 32-bit address that uniquely identifies this interface.



**Note** – A host does not have the same IP address on all the networks to which it is connected.

See “IP Address” on page 103.

**Net Mask** — see “Net Mask” on page 106.

## Defining Router Anti-Spoofing Properties

The **Interface Properties** window allows you to define router anti-spoofing parameters when installing Access Lists on routers. For more information on spoofing, see “Valid Addresses” on page 106.

The following routers support anti-spoofing:

- Bay Networks
- Cisco (Version 10.x and higher)
- 3Com

Interface Properties Window — Valid Addresses

You can defend your network from incoming spoof attacks by defining the addresses that are considered valid source IP addresses on each router interface. Valid IP addresses are defined in the **Interface Properties** window. The meaning of **Valid Addresses** for an interface is:

- A packet whose source IP address belongs to **Valid Addresses** is allowed to enter the network object through the interface.
- A packet whose source IP address does not belong to **Valid Addresses** is not allowed to enter the network object through the interface.

In the **Valid Addresses** box, specify the network on the other side of this interface. Choose one of the following:

**Any** — (default) no spoof tracking.

**This Net** — Only packets whose source IP addresses are part of the network connected to this interface are allowed.

This option is typically used for internal interfaces connected to a “final” network (that is, a network with no networks behind it).

**No Security Policy!** — No Security Policy at all is installed on this interface.



**Warning** – If you check **No Security Policy** on an internal interface, then the anti-spoofing parameters defined on a router’s external interface (see **Others** below) will not block incoming packets which are disguised as packets coming from the network connected to this internal interface.

**Others** — All packets are allowed, except those whose source IP addresses belong to the networks listed under **Valid Addresses** for this object’s other interfaces.

This option is typically used for external router interfaces.

**Specific** — Only packets from this object are allowed.

This option can be used for interfaces connected to more than one network (for example, a network group).



**Note** – To implement anti-spoofing for 3Com and Cisco (version 10.x and higher), you must define additional properties in the **Setup** tab of each router after you define the Valid Addresses in the Interfaces Properties window. For more information, see “Anti-spoofing Parameters and Router Setup (Cisco and 3Com)” on page 125.

### Spoof Tracking

Spoofed packets are always dropped, but you can specify an additional action to be taken by selecting one of the options in the **Spoof Tracking** group box, as follows:

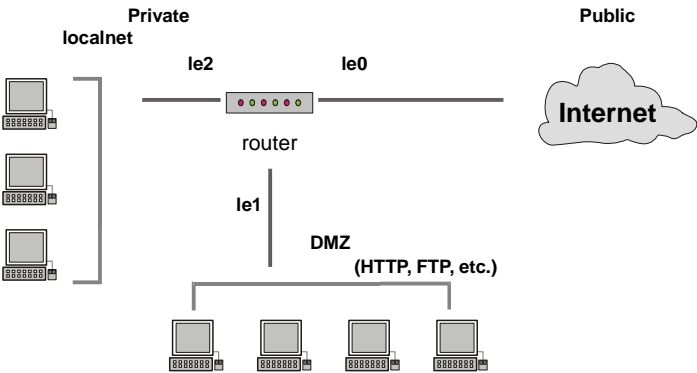
- None** — No additional action is taken.
- Log** — A spoofing attempt is logged through the `syslog` facility of the router.



**Note** – Logging for spoofing attempts is available for external interfaces only.

## Anti-Spoofing Example

In order to implement anti-spoofing on a router’s external interface, you must define the appropriate **Valid Addresses** (either **This Net** or **Specific**) for all internal interfaces. Consider the network depicted in FIGURE 4-8.



**FIGURE 4-21** Anti-Spoof Example Configuration with a Router

Anti-spoofing should be defined on the router’s three interfaces as follows:

**TABLE 4-5** Valid Addresses for each interface

| interface      | Valid addresses |
|----------------|-----------------|
| le2 (internal) | This Net        |
| le1 (internal) | This Net        |
| le0 (external) | Others          |

The above interface configuration assures that inbound packets are checked for spoofing attempts. On le0, only packets with source IP addresses belonging to neither DMZ nor localnet should be allowed to enter. A packet entering on le0 whose source IP address belongs to either DMZ or localnet is spoofed.

Anti-spoofing for inbound packets is implemented differently in the router filter rules generated for external and internal interfaces. External interfaces should have **Others** defined as **Valid Addresses**. Internal interfaces should have either **This Net** or a specific object (**Specific**) defined as **Valid Addresses**.

#### External Interfaces

Anti spoofing is implemented by automatically generating rules that reject packets with internal IP addresses arriving on the external interface. These rules are defined before any other rules on the external interface. The internal IP addresses are the objects defined as **Valid Addresses** for the router's internal interfaces.

#### Internal Interfaces — "Scoping"

Anti-spoofing is implemented on internal interfaces through a mechanism called "scoping." In the Rule Base, the **Source** object in a rule is intersected with the objects specified under **Valid Addresses** in the **Router Properties** window. The rule is generated and enforced on the relevant interface only if the intersection is not empty.

Consider the following rule:

| Source | Destination | Service | Action | Track | Install On |
|--------|-------------|---------|--------|-------|------------|
| any    | any         | telnet  | Accept | Long  | Routers    |

For the configuration depicted in FIGURE 4-21 on page 123, the following filter rules will be generated on each of the router's interfaces.



**Note** – These rules are enforced on incoming packets only.

#### On le1:

| Source | Destination | Service | Action |
|--------|-------------|---------|--------|
| DMZ    | any         | telnet  | Accept |

#### On le2:

| Source   | Destination | Service | Action |
|----------|-------------|---------|--------|
| localnet | any         | telnet  | Accept |

On le0:

| Source   | Destination | Service | Action |
|----------|-------------|---------|--------|
| localnet | any         | any     | Reject |
| dmz      | any         | any     | Reject |
| any      | any         | telnet  | Accept |

The filter rules generated on each internal interface accept telnet connections only from the network behind that interface.



**Note** – In order to reject any other packets, you must define a rule at the end of the Rule Base which rejects all other connections. This rule is automatically generated for 3Com and Cisco (version 10 and higher) routers. For Bay routers, you must define this rule explicitly.

The filter rules generated for the external interface (le0) reject any packets with a source IP address from localnet or the DMZ. All other telnet connections are allowed.

**Anti-spoofing Parameters and Router Setup (Cisco and 3Com)**

For Cisco (Version 10.x and higher) and 3Com routers, you must specify the direction of the filter rules generated from anti-spoofing parameters. The direction of enforcement is specified in the **Setup** tab of each router (FIGURE 4-22).

For 3Com routers, the direction of enforcement is defined by the **Interface Direction: Spoof Rules** property.

For Cisco routers, the direction of enforcement is defined by the **Spoof Rules Interface Direction** property.

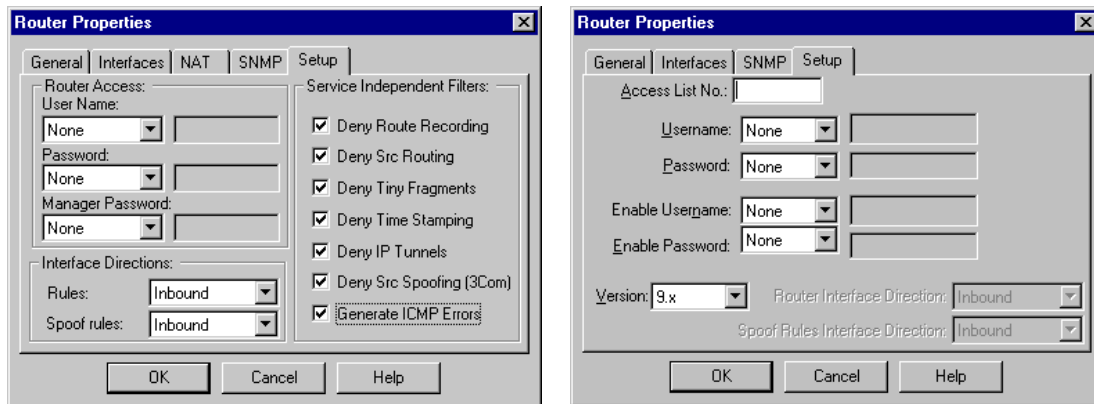


FIGURE 4-22 Setup tab — 3Com and Cisco



**Getting Here** – To display either window, choose **Manage>Network Objects** in the menu, select the router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit**, and then click on the router's **Setup** tab.

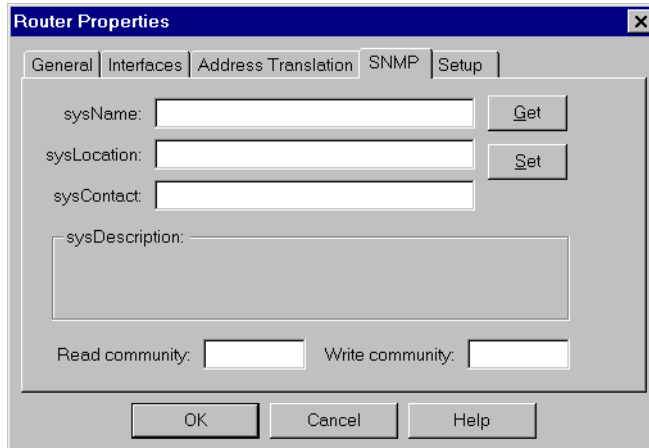
For each router, **Inbound** is the default setting for this property. If you specify **Inbound**, the anti-spoofing parameters defined in the **Interface Properties** window are implemented, and your internal networks are protected from incoming spoofing attempts. **Inbound** is the recommended setting to enforce anti-spoofing for incoming packets.



**Warning** – If you specify **Outbound**, then the anti-spoofing parameters specified in the **Interface Properties** window are disabled, and internal networks are *not* protected from spoofing attacks.

## Router Properties Window — SNMP Tab

This window enables you to retrieve or set SNMP information for the router.



**FIGURE 4-23** Router Properties — SNMP tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **SNMP** tab.

**Name** — the router's name

**Location** — the router's location

**Contact** —the name of a contact person

**Get** — If the router has an SNMP agent, you can use this button to retrieve about the router and display it in this window.

**Set** — Set the router's properties to those shown in this window.

**Read Community** — the community with read permission for this router

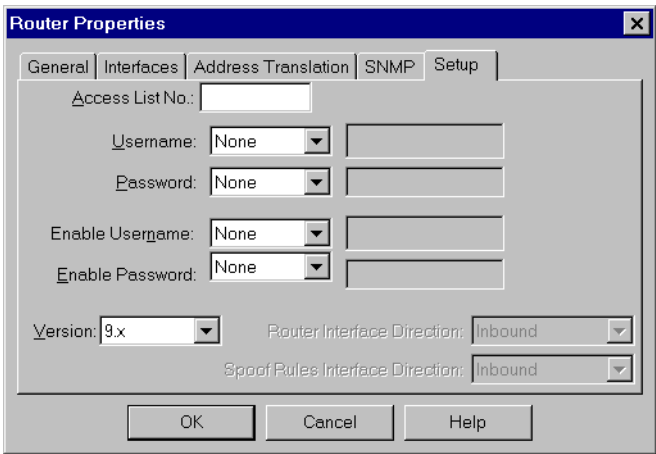
**Write Community** — the community with write permission for this router

# Router Setup

## In This Section

|                             |                 |
|-----------------------------|-----------------|
| <i>Cisco Setup</i>          | <i>page 128</i> |
| <i>Bay Networks Setup</i>   | <i>page 130</i> |
| <i>3Com Setup</i>           | <i>page 131</i> |
| <i>Microsoft RRAS Setup</i> | <i>page 133</i> |

## Cisco Setup



**FIGURE 4-24** Router Properties — Setup for Cisco Router



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the Cisco router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Setup** tab.

**Access List No** — See the Cisco documentation.



**Note** – VPN-1/FireWall-1 restricts the **Access List No.** to the range 101-190 even though the valid Cisco range is 100-199. This does not affect functionality of a Cisco router.

**UserName** — the name required to log on to the router. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter’s value
- **Prompt** — indicates that the user will be prompted for this parameter



**Password** — the password required to log on to the router. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

**Enable UserName** — user name required for installing Access Lists. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

**Enable Password** — password required for installing access lists. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

**Version** — select the router version from the drop-down menu.

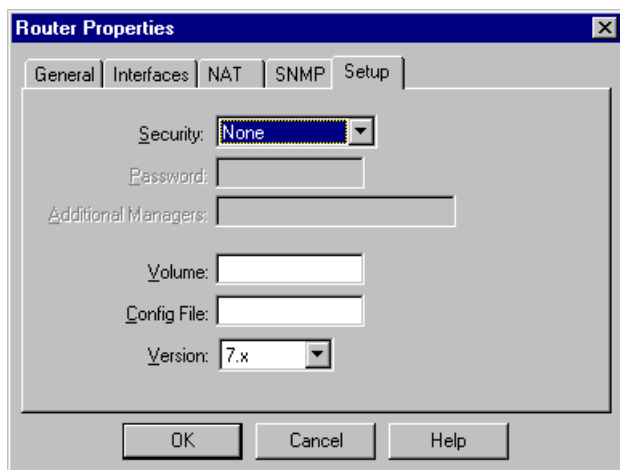
**Router Interface Direction** — Installed rules are enforced on packets traveling in this direction on all interfaces.

**Spoof Rules Interface Direction** — Spoof tracking rules are enforced on packets traveling in this direction on all interfaces.



**Note** – (version 10.x and higher) If you have defined anti-spoofing parameters in the router's **Interface Properties** window, you must choose **Inbound** in order to protect internal networks from incoming spoofed packets. For more information, see "Defining Router Anti-Spoofing Properties" on page 122.

## Bay Networks Setup



**FIGURE 4-25** Router Properties— Setup for Bay Networks Router



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the Bay Networks router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Setup** tab.

**Security** — Select one of the options.

**Password** — See the Bay Networks documentation.

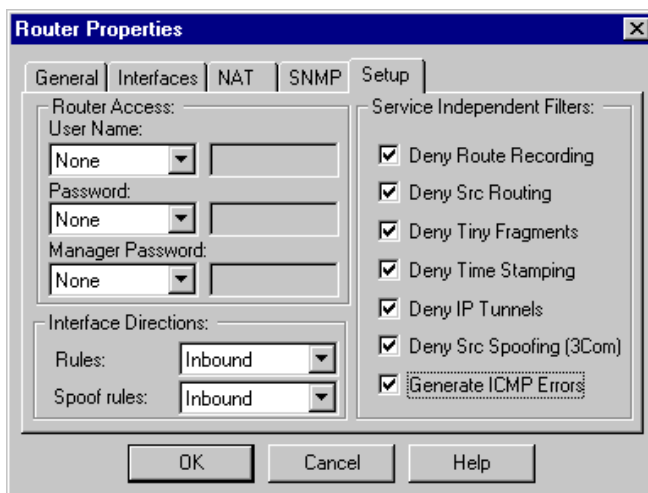
**Additional Managers** — as defined in the Bay Networks Site Manager software

**Volume** — the file system on the router

**Config File** — the configuration on the router

**Version** — the version of the Bay Networks Site Manager software installed on the router

## 3Com Setup



**FIGURE 4-26** Router Properties window — Setup for 3Com Router



**Getting Here** — To display this window, choose **Manage>Network Objects** in the menu, select the 3Com router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Setup** tab.

The fields in this window are explained below. More detailed information about these fields is available in the 3Com documentation.

### Router Access

**UserName** — Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

**Password** — the password required to configure the router. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

**Manager Password** — the password required to install Access Lists. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

## Service Independent Filters

**Deny Route Recording** — Specifies whether or not the received packet should be dropped if the record-route option is present in the IP header.

**Deny Src Routing** — Specifies whether or not the received packet should be dropped if the source-route option is present in the IP header.

**Deny Tiny Fragments** — Specifies whether tiny TCP fragment checks (RFC 1858) are performed.

**Deny Time Stamping** — Specifies whether or not the received packet should be dropped if the time-stamp option is present in the IP header.

**Deny IP Tunnels** — Specifies whether or not IP tunnel packets are allowed.

IP tunnel packets are IP-over-IP encapsulation.

**Deny SrcSpoofing (3Com)** — Specifies whether packets are subject to source-spoofing checks.

The source address of incoming packets is checked against the routing table. If the routing information shows that the source address is unreachable, or reachable on different interfaces, then it is a SrcSpoofing attack.

This is a CPU-intensive option and generally results in performance degradation. You should disable this option except on interfaces where external, untrusted traffic is received.

**Generate ICMP Error Messages** — For denied packets, this option specifies whether or not the router should generate ICMP destination administratively unreachable messages (ICMP type 13).

## Interface (Filter) Directions

**Rules** — choose a direction from the menu.



**Note** – Eitherbound means both inbound and outbound.

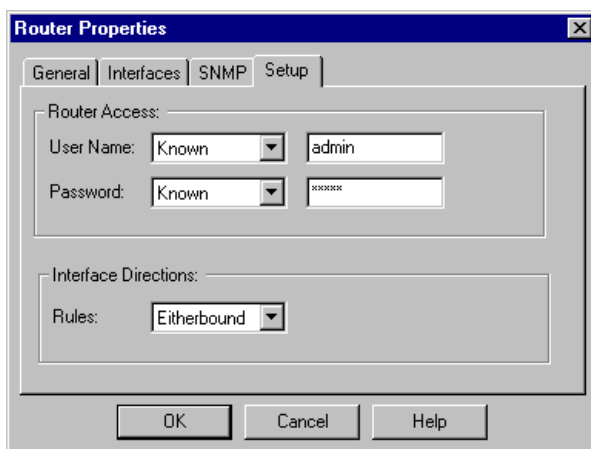
**Spoof Rules** — The enforcement direction for filter rules generated from anti-spoofing parameters defined in the router's **Interface Properties** window. **Inbound** is the default setting.



**Note** – If you have defined anti-spoofing parameters in the router's **Interface Properties** window, you must choose **Inbound** in order to protect internal networks from incoming spoofed packets. For more information, see "Defining Router Anti-Spoofing Properties" on page 122.

## Microsoft RRAS Setup

Microsoft RRAS (Routing and Remote Access Service) is a Windows NT based routing application. RRAS was formerly known as Steelhead.



**FIGURE 4-27** Router Properties window - Setup for RRAS router



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the RRAS router in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Setup** tab.

## Router Access

**UserName** — the user name for permissions to configure the router. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter's value
- **Prompt** — indicates that the user will be prompted for this parameter

**Password** — the password required to configure the router. Choose one of the following:

- **None** — indicates that this parameter is not needed
- **Known** — enter the parameter’s value
- **Prompt** — indicates that the user will be prompted for this parameter

**Interface Directions**

**Rules** — Choose a direction from the menu.



**Note** – Eitherbound means both inbound and outbound.

**Router Management**

This section describes router management guidelines when working with the Open Security Extension feature.

**In This Section**

|                                           |                 |
|-------------------------------------------|-----------------|
| <i>All Routers</i>                        | <i>page 134</i> |
| <i>Bay Routers</i>                        | <i>page 134</i> |
| <i>Cisco Routers</i>                      | <i>page 135</i> |
| <i>3Com Routers</i>                       | <i>page 136</i> |
| <i>Microsoft RRAS (Steelhead) Routers</i> | <i>page 136</i> |

**All Routers**

You must specify a separate rule for response packets for UDP services.

**Bay Routers**

- 1 You must define a rule which accepts SNMP connections from the Management Server host to the router.  
  
Without this rule, SNMP sessions to the router will be rejected after you download the Security Policy for the first time. You will be unable to download the Security Policy in future sessions, and you will have to configure Access Lists directly on the router console.
- 2 When installing the Security Policy on Bay routers, you must define a rule at the end of the Rule Base which rejects all communication attempts that are not described by the other rules.  
  
In this rule, **Source** is “Any”, **Destination** is “Any”, and **Action** is “Reject”. Without this rule, all communications will be accepted.

- 3** You cannot specify **Wellfleet** for the **Security** option in the **Setup** tab of the **Router Properties** window.  
You must choose **Other** or **None** for this option.
- 4** **SNMP Get** for virtual interfaces fails.
- 5** **SNMP Set** does not work on Bay routers.
- 6** Access Lists cannot be installed from the Management Server on Serial interfaces.

## Cisco Routers

- 1** You must define a rule which accepts Telnet connections from the Management Server host to the router.  
Without this rule, Telnet sessions to the router will be rejected after you download the Security Policy for the first time. You will be unable to download the Security Policy in future sessions, and you will have to configure Access Lists directly on the router console.
- 2** When you negate an object in a rule, Cisco routers automatically generate two filter rules in the Access List.  
The first rule applies to the negated object, the second rule either accepts or denies all other communications, depending on the rule's **Action**. Consider the following examples:

Action is Reject

| Source | Destination | Services | Action | Track | Install On |
|--------|-------------|----------|--------|-------|------------|
| Any    | Any         | 8telnet  | Reject | Long  | CiscoRtr   |

In the above example, the first filter rule generated will accept all TELNET connections. The second filter rule will deny all other connections. Since the Rule Base is examined sequentially, any rules defined after the above negate rule will not be applied. A negate rule in which **Action** is reject should therefore be placed at the end of the Rule Base.

Action is Accept

| Source | Destination | Services | Action | Track | Install On |
|--------|-------------|----------|--------|-------|------------|
| Any    | Any         | 8telnet  | Accept | Long  | CiscoRtr   |

In the above example, the first filter rule generated denies all TELNET connections. The second rule accepts all other connections.



**Warning** – A negate rule in which **Action** is **Accept** exposes your network and should not be used.

## 3Com Routers

### Managing 3Com Filters

3Com routers support three filtering specifications: Service Dependent filters, Service Independent filters and Generic filters. VPN-1/FireWall-1 generates Generic and Service Independent filters from the Rule Base. Service Dependent filters are not generated from the Rule Base.

3Com routers enforce any predefined Service Dependent filters before enforcing filters generated by VPN-1/FireWall-1. For example, preconfigured Service Dependent filters on your 3Com router may currently allow incoming FTP connections, but the Rule Base does not. The 3Com router will allow incoming FTP packets into the network, regardless of what is specified in the Rule Base.

To correctly enforce your Security Policy, you must check that the Service Dependent filter rules do not contradict the VPN-1/FireWall-1 Rule Base. In the above example, you can reconfigure Service Dependent filters to deny incoming FTP connections. For more information on configuring Service Dependent filters, refer to the 3Com documentation.

### Rule Base

You must define a rule which accepts Telnet connections from the Management Server host to the router. Without this rule, Telnet sessions to the router will be rejected after you download the Security Policy for the first time. You will be unable to download the Security Policy in future sessions, and you will have to configure Access Lists directly on the router console.

## Microsoft RRAS (Steelhead) Routers

- 1** Microsoft RRAS does not support anti-spoofing.
- 2** You must define a rule which accepts nbssession connections from the Management Server host to the router.



Without this rule, nbssession sessions to the router will be rejected after you download the Security Policy for the first time. You will be unable to download the Security Policy in future sessions, and you will have to configure Access Lists directly on the router console.

- 3 Microsoft RRAS does not support established TCP connections.  
VPN-1/FireWall-1 Version 4.1 enables you to support established TCP with Microsoft RRAS by automatically generating filter rules for reverse TCP connections. To enable established TCP, check **Accept Established TCP Connections** in the **Access Lists** tab of the **Properties Setup** window. Alternatively, you can define rules for response packets.
- 4 Microsoft RRAS does not support Accept and Reject rules together in the same Security Policy.

All rules installed on a RRAS router must specify the same **Action**.



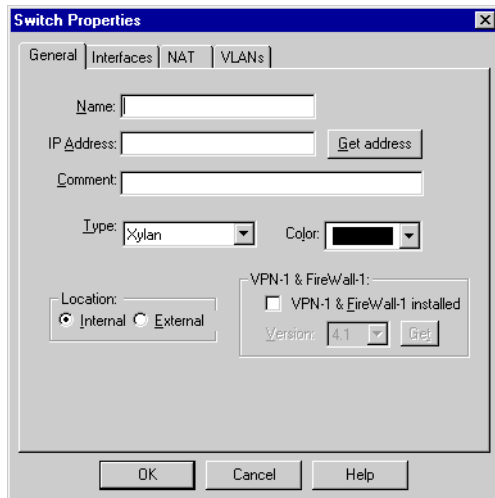
**Warning** – If you define Reject rules, RRAS automatically generates a final rule in its Access List. This rule accepts connections not rejected by the previous rules and exposes your network.

## Switch Object Properties

### In This Section

|                                                           |                 |
|-----------------------------------------------------------|-----------------|
| <i>Switch Properties Window — General Tab</i>             | <i>page 138</i> |
| <i>Switch Properties Window — Interfaces Tab</i>          | <i>page 139</i> |
| <i>Switch Properties Window — Address Translation Tab</i> | <i>page 139</i> |
| <i>Switch Properties Window — SNMP Tab</i>                | <i>page 139</i> |
| <i>Switch Properties Window — Setup Tab</i>               | <i>page 139</i> |
| <i>Switch Properties Window — VLANs Tab</i>               | <i>page 140</i> |

## Switch Properties Window — General Tab



**FIGURE 4-28** Switch Properties window — General tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new switch, click on **New**.
- To edit the properties of an existing switch, select the switch and click on **Edit**.

**Name** — the object's name

**IP Address** — a 32-bit address that uniquely identifies this switch

See “IP Address” on page 103.

**Get Address** — Click on this button to resolve the switch's name to an IP address.

**Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

**Color** — Select a color from the drop-down list.

**Type** — Select a value from the menu.

**Location: Internal/External** — relevant for FireWalled objects only

Only **Internal** objects appear in the System Status View (see Chapter 12, “System Status Viewer”).

A FireWalled object is internal to its own Management Station and external to other Management Stations. You cannot install a Security Policy on an object from a Management Station where the object is defined as external.

**VPN-1 & FireWall-1 Installed** —whether the VPN/FireWall Module was loaded on this network object

A switch is FireWalled if the VPN/FireWall Module is loaded on it. VPN/FireWall Modules are installed when the VPN-1/FireWall-1 software is installed. The VPN/FireWall Module enforces the Security Policy.

## Switch Properties Window — Interfaces Tab

This window is identical to the **Interfaces** tab of the **Workstation Properties** window (FIGURE 4-6 on page 104). See “Workstation Properties Window — Interfaces Tab” on page 104 for more information.

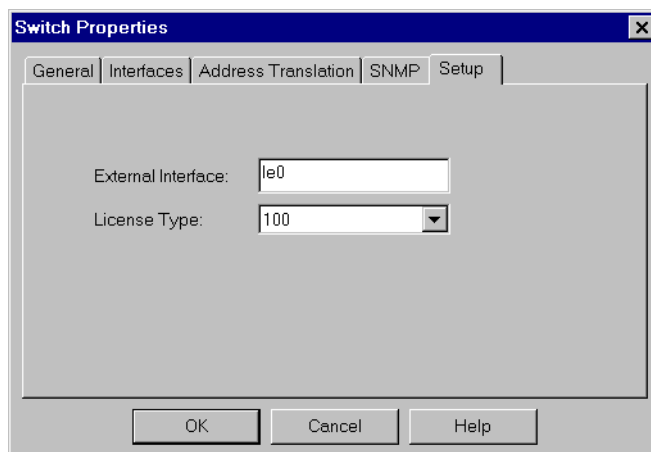
## Switch Properties Window — Address Translation Tab

This window is identical to the **Address Translation** tab of the **Workstation Properties** window (FIGURE 4-13 on page 113). See “Workstation Properties Window — NAT (Network Address Translation) Tab” on page 113 for more information.

## Switch Properties Window — SNMP Tab

This window is identical to the **SNMP** tab of the **Workstation Properties** window (FIGURE 4-11 on page 111). See “Workstation Properties Window — SNMP Tab” on page 111 for more information.

## Switch Properties Window — Setup Tab



**FIGURE 4-29** Switch Properties window — Setup tab



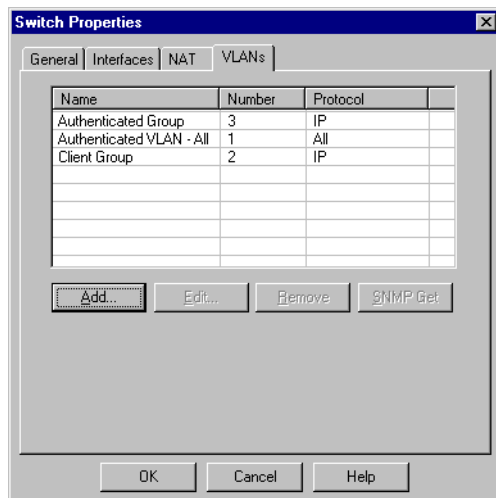
**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the switch in the **Network Objects** window (FIGURE 4-1 on page 98) and click on **Setup**.

**External Interface** — the name of the external interface, for example, le0.

**License Type** — Choose a license type from the menu.

## Switch Properties Window — VLANs Tab

The VLANs tab allows you to configure and display the properties of the VLANs associated with a Xylan switch. This tab is enabled only if your license permits management of authenticated VLANs.



**FIGURE 4-30** Switch Properties window — VLANs tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the switch in the **Network Objects** window (FIGURE 4-1 on page 98) and click on **VLANs**.

**Get** — Retrieve VLAN information from the switch console.

The **Get** button is the recommended way to configure VLAN properties.

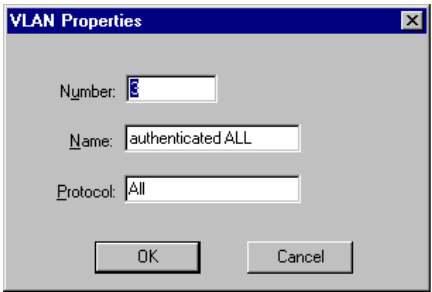
To add an VLAN, click on **Add**. In the **VLAN Properties** window (FIGURE 4-30 on page 140), define the VLAN's properties.

To edit a VLAN, select the VLAN and click on **Edit** or double-click on the interface. In the **VLAN Properties** window (FIGURE 4-30 on page 140), define the VLAN's properties.

To delete a VLAN, select the VLAN from the list and click on **Remove**.

## VLAN Properties Window

The **VLAN Properties** window specifies the parameters of a switch's VLAN.



**FIGURE 4-31** VLAN Properties window



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the switch in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit**, click on the **VLANs** tab and then:

- To define a new VLAN, click on **Add**.
- To edit the properties of an existing VLAN, select the VLAN and click on **Edit**.

**Number** — the VLAN's number, as defined on the switch console

**Name** — the VLAN's name, as defined on the switch console

**Protocol** — the protocol associated with the VLAN

Enter one of the following:

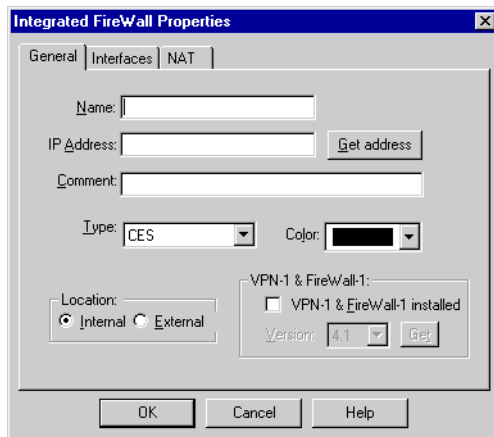
- IP
- DECNET
- Protocol specified by SNAP
- Protocol specified by ether-type
- IPX
- APPLETALK
- ALL PROTOCOLS
- Protocol specified by DSAP/SSAP

## Integrated FireWall Properties

### In This Section

|                                                                |                 |
|----------------------------------------------------------------|-----------------|
| <i>Integrated FireWalls window — General tab</i>               | <i>page 142</i> |
| <i>Integrated FireWalls Properties Window — Interfaces Tab</i> | <i>page 143</i> |
| <i>Integrated FireWalls Properties Window — SNMP Tab</i>       | <i>page 143</i> |
| <i>Integrated FireWalls Properties Window — NAT Tab</i>        | <i>page 143</i> |
| <i>Cisco PIX Firewall — Setup A Tab</i>                        | <i>page 143</i> |
| <i>Cisco PIX Firewall — Setup B Tab</i>                        | <i>page 145</i> |

## Integrated FireWalls window — General tab



**FIGURE 4-32** Integrated FireWall Properties window — General tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new Integrated FireWall, click on **New**.
- To edit the properties of an existing Integrated FireWall, select the Integrated FireWall and click on **Edit**.

**Name** — the name of the Integrated FireWall

**IP Address** — a 32-bit address that uniquely defines this interface

**Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.

**Color** — Select a color from the drop-down list.

**Type** — choose one of the following from the drop-down list:

- CISCO — Cisco PIX Firewall
- Other

**VPN-1 & FireWall-1 Installed** — whether a VPN/FireWall Module or Inspection Module is loaded on this object.



**Note** – If you are defining a CISCO PIX firewall, this field is not enabled. A Security Policy cannot be installed on the PIX Integrated FireWall, only Access Lists.

**Location: Internal/External** — relevant for FireWalled objects only

Only **Internal** objects appear in the System Status View (see Chapter 12, “System Status Viewer”).

A FireWalled object is internal to its own Management Station and external to other Management Stations. You cannot install a Security Policy on an object from a Management Station where the object is defined as external.

## Integrated FireWalls Properties Window — Interfaces Tab

This window is identical to the **Interfaces** tab of the **Workstation Properties** window (FIGURE 4-6 on page 104). See “Workstation Properties Window — Interfaces Tab” on page 104 for more information.

## Integrated FireWalls Properties Window — SNMP Tab

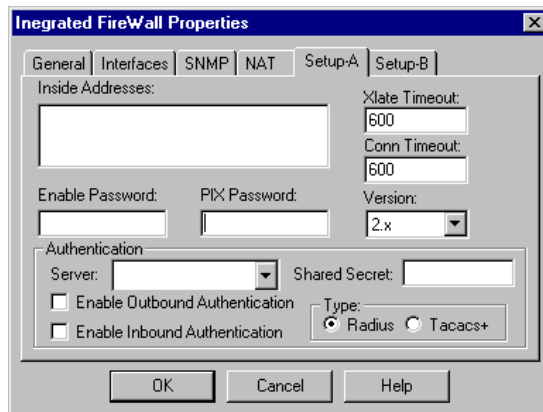
This window is identical to the **SNMP** tab of the **Workstation Properties** window (FIGURE 4-11 on page 111). See “Workstation Properties Window — SNMP Tab” on page 111 for more information.

## Integrated FireWalls Properties Window — NAT Tab

This window is identical to the **NAT** tab of the **Workstation Properties** window (FIGURE 4-11 on page 111). See “Workstation Properties Window — NAT (Network Address Translation) Tab” on page 113 for more information.

## Cisco PIX Firewall — Setup A Tab

The **Setup A** tab defines PIX access privileges, Authentication, and Network Address Translation properties. More information about these fields is available in the Cisco PIX documentation.



**FIGURE 4-33** Cisco PIX Integrated FireWall Properties window — Setup A tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the Cisco PIX Integrated FireWall in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **SetupA** tab.

**Inside Addresses** — the internal networks for which the PIX Integrated FireWall performs address translation.

**Enable Password** — Specify a password in order to modify PIX settings.

**PIX Password** — Specify a password to enable communication between the Management Server and the PIX Integrated FireWall.

The default password is `cisco`.

**Xlate Timeout** — Specify the time after which a PIX address translation slot times out and a global address is returned to the available pool.

**Conn Timeout** — Specify the period after which a PIX connection slot times out.

**Version** — Select the PIX version from the drop-down list.

## Authentication

**Server** — Select the appropriate authentication server from the drop-down list.

You must have first defined the authentication server as a workstation. For information, see “Workstation Properties” on page 102.

**Enable Outbound Authentication** — Request authentication for outbound connections.

**Enable Inbound Authentication** — Request authentication for inbound connections.

**Shared Secret** — Specify a public key to encrypt communication between PIX and the authentication server.

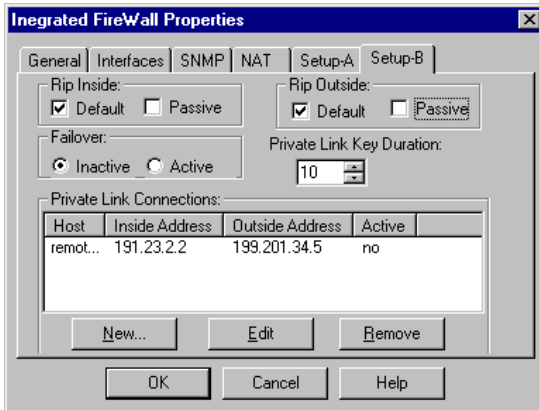
**Type** — Choose one of the following authentication schemes:

- RADIUS
- TACACS+



## Cisco PIX FireWall — Setup B Tab

The **Setup B** tab specifies Private Link encryption parameters, routing and general connection properties. For more information on these parameters, refer to the PIX documentation.



**FIGURE 4-34** Cisco PIX Integrated FireWall Properties window — Setup B tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the Cisco PIX Integrated FireWall in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **SetupB** tab.

### Routing and Connection Properties

**RIP Inside** — defines RIP settings on the PIX inside interface.

- **Default** — Broadcast a default route to the inside network.
- **Passive** — Enable passive RIP.

**RIP Outside** — defines RIP settings for the PIX outside interface.

- **Default** — broadcast a default route to the inside network.
- **Passive** — enable passive RIP.

**Failover** — defines the PIX failover feature, in which a secondary PIX firewall takes over connections if the primary PIX fails. Specify one of the following:

- **Inactive**
- **Active**

### Encryption

**Private Link Key Duration** — Specify the interval in minutes at which PIX Private Link keys are changed.

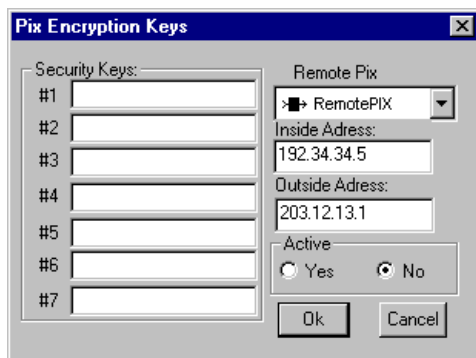
**Private Link Connections** — Specify remote PIX units with which you want to establish PIX Private Link communications. Connections between the local PIX blackbox and the remote PIX blackbox will be encrypted.

To add a remote PIX, click on **Add**. The **PIX Encryption Keys** window (FIGURE 4-35) is displayed.

To delete a remote PIX, select the Integrated FireWall and click on **Remove**.

To edit the encryption properties of the remote Integrated FireWall, select the Integrated FireWall and click on **Edit**, or double-click on the firewall name. The **PIX Encryption Keys** window (FIGURE 4-35) is displayed.

## PIX Encryption Keys window



**FIGURE 4-35** PIX Encryption Keys window

**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the Cisco PIX Integrated FireWall in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit**, click on the **SetupB** tab, and :

- To define encryption keys for a new Private Link Connection, click on **New**.
- To edit the properties of an existing Private Link Connection, select the Remote PIX under **Private Link Connections** and click on **Edit**.

**Security Keys** — Enter up to seven PIX Private Link keys. Each key may consist of up to 14 hexadecimal digits.

**Note** – You must specify the same keys in the same order for both the local and remote blackbox.

**Remote PIX** — Select a remote PIX unit from the drop-down menu. The IP addresses of the PIX unit's interfaces are displayed in the **Inside Address** and **Outside Address** fields.

The remote PIX unit must already be defined as an Integrated FireWall. For more information on PIX Private Link connections and encryption keys, see the “link” command in the PIX documentation.

## Managing PIX

### General Notes

- PIX follows the same security principle as VPN-1/FireWall-1 — connections that are not explicitly permitted in the Rule Base are dropped.
- The Management Server must be installed on a machine located on the PIX inside interface in order to install the Security Policy.

### Rule Base

- 1** You must define a rule which accepts TELNET connections from the Management Server host to the PIX blackbox.

Without this rule, TELNET sessions to the PIX Integrated Firewall will be rejected after you download the Security Policy for the first time. You will be unable to download the Security Policy in future sessions, and you will have to configure Access Lists directly on the PIX console.

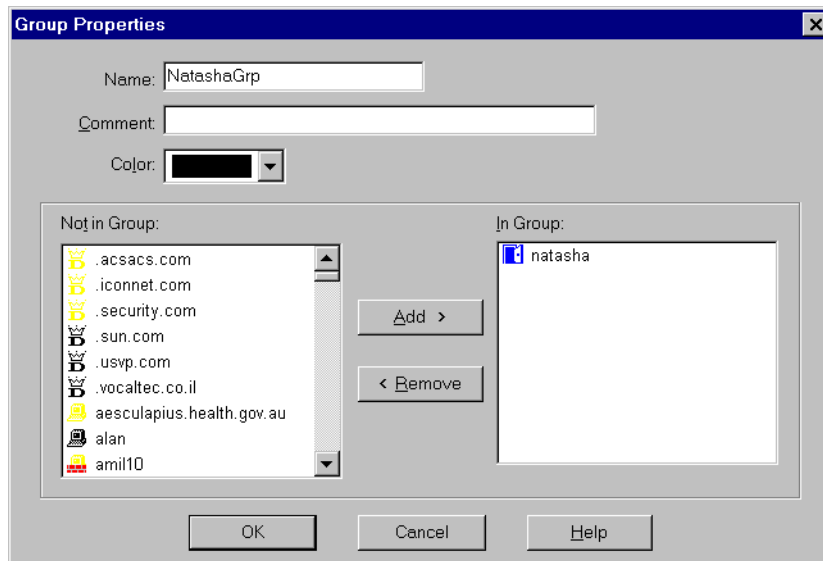
- 2** Properties defined in the **Properties Setup** window are not applied to PIX blackboxes.
- 3** When installing a Security Policy on PIX integrated firewalls, you must define a final rule which rejects all communication attempts that are not described by the previous rules.
- 4** PIX does not support ICMP services.
- 5** **SNMP Get** does not retrieve interface properties for a PIX integrated firewall. You must manually configure integrated firewall interface properties.
- 6** You cannot specify per-rule logging.  
If one rule specifies logging, all TCP and UDP connections will be logged.
- 7** PIX does not support rules which reject specific inbound connections. For example, you cannot reject connections which include a specific global or external object under **Source**. For rules in which Rule Base **Source** is “Any” and **Action** is “Reject”, **Source** applies only to internal hosts (i.e., outbound connections).

## Network Object Groups

You can simplify the Rule Base by defining a group of network objects and using the group in rules.

## Creating a Group

To create a group, create an object of type Group using the Network Object Manager (see “Creating a New Object” on page 100). Next, add objects to the group using the **Group Properties** window (FIGURE 4-36 on page 148).



**FIGURE 4-36** Group Properties window



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new group, click on **New** and select **Group** from the menu (FIGURE 4-2 on page 99).
- To edit the properties of an existing group, select a group and click on **Edit**.

## Adding an Object to a Group

In the left listbox (labeled **Not in Group**), select the objects you wish to include in the group. Use the **Add** button to add individual objects and to add groups to the group.

You add a group to another group in one of two ways:

- 1** You can individually add all the objects in one group to another group, without nesting. Click on **Yes** in reply to the question in the window (FIGURE 4-37).

- 2 You can nest groups inside groups to create a group hierarchy of any desired complexity. Click on **No** in reply to the question in the window.

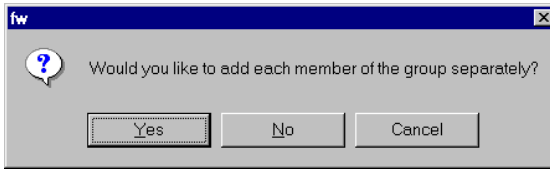


FIGURE 4-37 Adding a Group to a Group

## Deleting an Object from a Group

Select the objects to be deleted from the right listbox (labeled **In Group**), and then click on **Remove**.

## Logical Server Properties

A Logical Server is a group of machines that provide the same services, and which are treated as a group among whose members a workload is distributed.

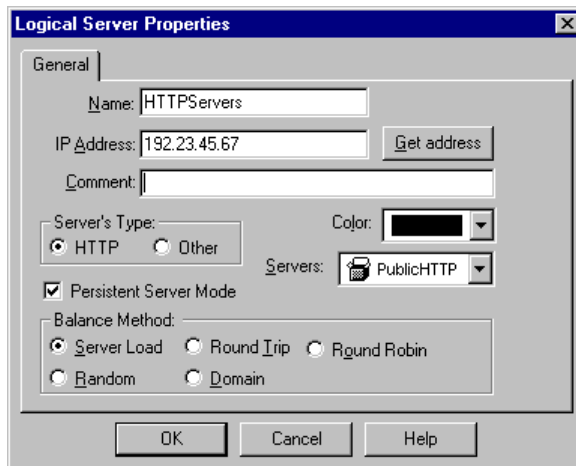


FIGURE 4-38 Logical Server Properties window

**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):



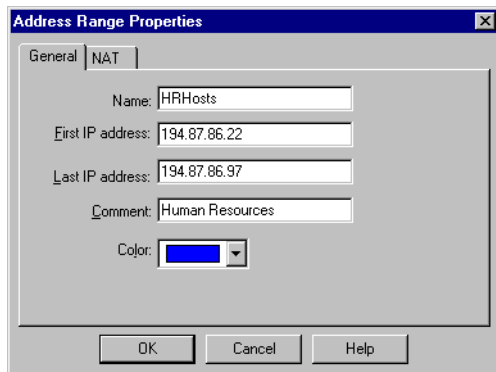
- To define a new Logical Server, click on **New**.
- To edit the properties of an existing Logical Server, select the Logical Server and click on **Edit**.

For information about Logical Servers, see “Server Load Balancing” on page 581.

## Address Range Properties

### Address Range Properties Window — General Tab

An Address Range object is a range of IP Addresses, used in Network Address Translation.



**FIGURE 4-39** Address Range Properties window - General tab

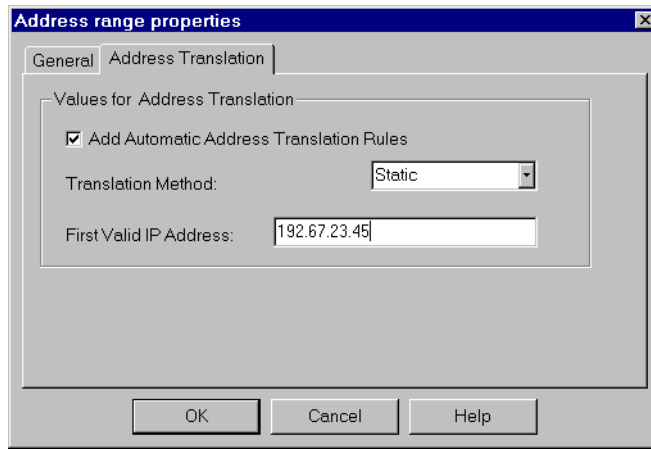


**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, and in the **Network Objects** window (FIGURE 4-1 on page 98):

- To define a new Address Range, click on **New**.
- To edit the properties of an existing Address Ranges, select the Address Range and click on **Edit**.

For information about VPN-1/FireWall-1's Address Translation feature, see Chapter 14, "Network Address Translation."

## Address Range Properties Window — Address Translation Tab



**FIGURE 4-40** Address Range Properties window — Address Translation Tab



**Getting Here** – To display this window, choose **Manage>Network Objects** in the menu, select the Address Range in the **Network Objects** window (FIGURE 4-1 on page 98), click on **Edit** and then click on the **Address Translation** tab.

This window specifies the parameters for automatically generated Address Translation rules for the Address Range.

For information about automatically generated Address Translation rules, see “Generating Address Translation Rules Automatically” on page 440.





# Managing Users

---

## In This Chapter

|                                                 |                 |
|-------------------------------------------------|-----------------|
| <i>Overview</i>                                 | <i>page 153</i> |
| <i>VPN-1/FireWall-1 Proprietary Users</i>       | <i>page 153</i> |
| <i>User Database</i>                            | <i>page 166</i> |
| <i>Generic User</i>                             | <i>page 167</i> |
| <i>External Users and Groups</i>                | <i>page 169</i> |
| <i>VPN-1/FireWall-1 LDAP Account Management</i> | <i>page 174</i> |

## Overview

When you define users and user groups to VPN-1/FireWall-1, you are then able to use those user groups as the **Source** in rules which specify Authentication (User, Client, or Session) as the **Action**. The user's properties (for example, those defined in the **Location** and **Time** tabs of the **User Properties** window) are then applied. In this way, you can specify, for example, that users in one group can connect only during the day, while users in another group can connect only at night.

There are two ways to define users in VPN-1/FireWall-1:


- using the VPN-1/FireWall-1 proprietary user database — see “VPN-1/FireWall-1 Proprietary Users” on page 153
- using an LDAP directory — see “External Users and Groups” on page 169

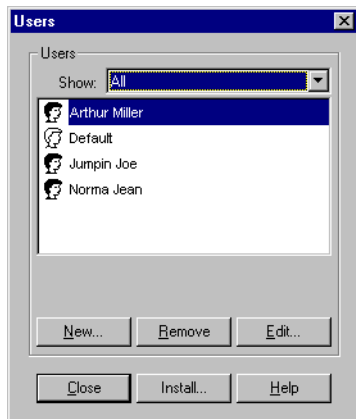
## VPN-1/FireWall-1 Proprietary Users

### Defining Users and Groups

You can define users and groups of users in the **Users** window (FIGURE 5-1 on page 154). In addition, you can define templates upon which future user definitions will be based.

To display the **Users** window,

- choose **Users** from the **Manage** menu, *or*
- click on  in the toolbar.



**FIGURE 5-1** Users window

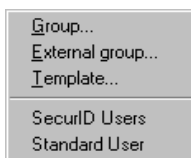
Click on **Install** to install the User Database to the VPN/FireWall modules on which the Security Policy is installed (see “VPN-1/FireWall-1 LDAP Account Management” on page 174).

To view specific types of users, select the desired type from the **Show** drop-down list.

## Creating a New Object (User, Group or Template)

To create a new object (User, Group or Template), click on **New**. The **New User Object** menu is displayed (FIGURE 5-2), listing the types of objects you can create.

Choose a type from the menu. A window is displayed prompting you to enter the properties of the selected object type.



**FIGURE 5-2** New User Object Menu

You can create a Group, an External Group (a group defined in an LDAP Server), a User Template, or a new user based on one of the User Templates already defined.

The User Templates already defined are listed in the bottom part of the menu. In the example shown above (FIGURE 5-2 on page 154), there are two User Templates: **SecurID Users** and **Standard User**.

TABLE 5-1 User types

| to create an object of type | see                                     |
|-----------------------------|-----------------------------------------|
| Group                       | “Creating a Group” on page 155          |
| External Group              | “External Users and Groups” on page 169 |
| Template                    | “Creating a Template” on page 155       |
| User                        | “Creating a New User” on page 156       |

Modifying a User

To modify an existing user, select the user in the **Users** window and click on **Edit**.

Deleting a User

To delete an existing user, select the user in the **Users** window and click on **Remove**.

Creating a Group

To create a new group, choose **Group** from the **New User Object** menu (FIGURE 5-2 on page 154). The **Group Properties** window (FIGURE 5-13 on page 165) is then displayed.

To add users or groups to a group, follow the instructions in “User Groups” on page 165.

Creating a Template

To create a new template, choose **Template** from the **New User Object** menu (FIGURE 5-2 on page 154). The **User Definition Template** window (FIGURE 5-3) is then displayed.

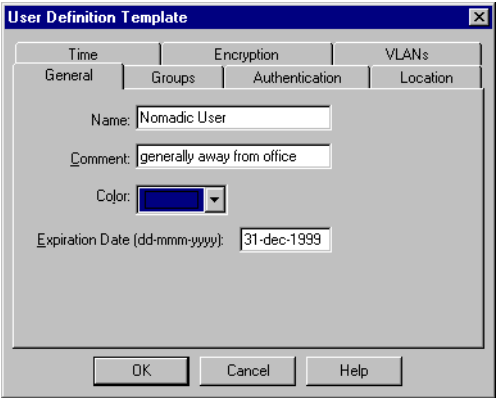


FIGURE 5-3 User Definition Template window

The **User Definition Template** window is identical to the **User Properties** window and has the same tabs. Enter the data (properties) for the template in the same way you enter data for a user (see “User Properties” on page 156).

Once you have created a template, any user you create based on the template will inherit all of the template’s properties, including membership in groups.

If you modify a template’s properties, the change will affect all users created from the template in the future. Users already created from the template will not be affected.



**Note** – In contrast to VPN-1/FireWall-1 templates, LDAP templates are live links. Changes to an LDAP template change the properties of all users linked to the template. For more information, see “VPN-1/FireWall-1 LDAP Account Management” on page 174.

## Creating a New User

To create a new user, choose the template on which the new user’s properties will be based from the **New User Object** menu (FIGURE 5-2 on page 154). The **User Properties** window (FIGURE 5-4 on page 157) is then displayed.

Enter the data for the user (see “User Properties” on page 156). For any user, you can freely change the properties that user inherited from the template, but they will be changed for the user only. The template remains unchanged.

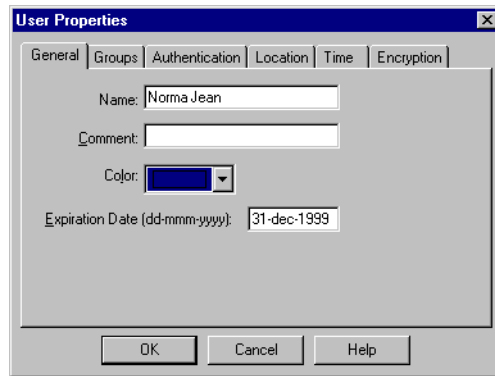
## User Properties

To display the **User Properties** windows (FIGURE 5-4 on page 157 through FIGURE 5-12 on page 164), double-click on a user name in the **Users** window (FIGURE 5-1 on page 154) and then select the appropriate tab.

### In This Section

|                                                    |                 |
|----------------------------------------------------|-----------------|
| <i>User Properties Window — General tab</i>        | <i>page 157</i> |
| <i>User Properties Window — Groups tab</i>         | <i>page 158</i> |
| <i>User Properties Window — Authentication tab</i> | <i>page 158</i> |
| <i>User Properties Window — Location tab</i>       | <i>page 162</i> |
| <i>User Properties Window — Time tab</i>           | <i>page 163</i> |
| <i>User Properties Window — Encryption tab</i>     | <i>page 164</i> |

## User Properties Window — General tab



**FIGURE 5-4** User Properties window — General tab



**Getting Here** – To display this window, choose **Manage>Users** in the menu, and in the **Users** window (FIGURE 5-1 on page 154):

- click on **New** to define a new user, or
- select a user and click on **Edit** (to edit the properties of an existing user).

**Name** — the user's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Users** window when this user is selected.

**Color** — the color of the user's icon

Select the desired color from the drop-down list.

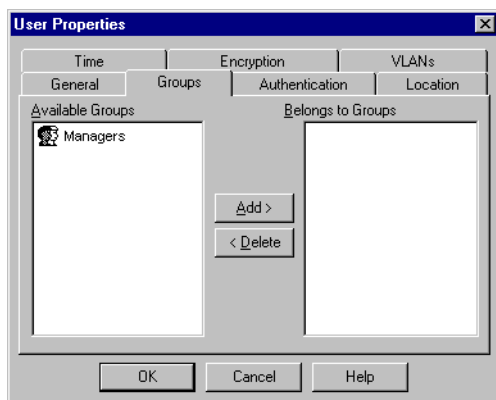
**Expiration** — date after which the user will be denied access

Date format is dd-mmm-yy[yy], where:

- mmm is one of the following: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
- yy[yy] — If two digits are specified, the year is assumed to be less than 2000. For example, “99” means “1999”.

To specify a year after 1999, enter all four digits of the year, for example, “2031”.

## User Properties Window — Groups tab



**FIGURE 5-5** User Properties window — Groups tab



**Getting Here** – To display this window, choose **Manage>Users** in the menu, select the user in the **Users** window (FIGURE 5-1 on page 154), click on **Edit** and then click on the **Groups** tab.

### Adding the User to a Group

To add the user to a group, select the groups in the left list box (labeled **Available Groups**) to which you wish to add this user, and then click on **Add**.

### Deleting the User from a Group

To delete the user from a group, select the groups in the right listbox (labeled **Belongs to Groups**) from which you wish to delete this user, and then click on **Delete**.

## User Properties Window — Authentication tab



**Getting Here** – To display this window, choose **Manage>Users** in the menu, select the user in the **Users** window (FIGURE 5-1 on page 154), click on **Edit** and then click on the **Authentication** tab.

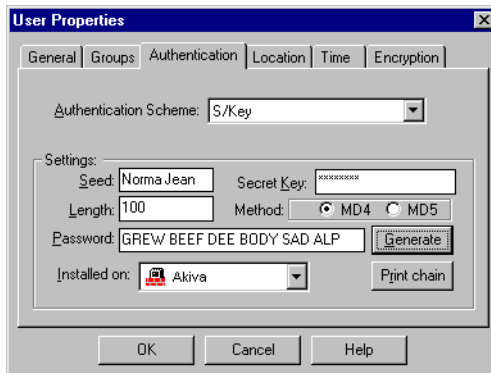
**Authentication Scheme** —the scheme used to authenticate this user

Select a scheme from the list. The **Settings** group shows the fields relevant to the selected scheme. For information about Authentication schemes, see “Authentication Schemes” on page 484.

**TABLE 5-2** Authentication Schemes and windows

| authentication scheme   |                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Undefined               | No authentication scheme is defined for this user in the VPN-1/FireWall-1 user database, though one may be defined on an LDAP Server. |
| S/Key                   | See “S/Key Authentication” on page 159.                                                                                               |
| SecurID                 | There are no scheme-specific parameters for the SecurID authentication scheme.                                                        |
| VPN-1/FireWall-1        | See “VPN-1/FireWall-1 Password Authentication” on page 161.                                                                           |
| OS Password             | There are no scheme-specific parameters for the OS Password authentication scheme.                                                    |
| RADIUS                  | See “RADIUS Authentication” on page 161.                                                                                              |
| AXENT Pathways Defender | There are no scheme-specific parameters for the AXENT Pathways Defender authentication scheme.                                        |
| TACACS                  | See “TACACS Authentication” on page 162.                                                                                              |

## S/Key Authentication



**FIGURE 5-6** User Properties window — Authentication tab — S/Key authentication

**Seed** — an arbitrary number

**Secret Key** — chosen by the user

**Secret Key** should be at least 10 characters long.

**Length** — number of iterations

**Installed On** — the gateway that will perform the authentication

**Method** — the hashing method

**Print Chain** — Print the password chain.

This option is available only immediately after generating a new chain.

There are several options for using the S/Key Authentication settings, as follows:

- To generate and save a sequence of one-time passwords, proceed as follows:

**1** Enter **Seed**, **Secret Key** and **Length**.

**Secret Key** should be at least 10 characters long.

**2** Click on **Generate**.

- If the user has already generated a sequence of one-time passwords, proceed as follows:

**1** Enter **Seed**, **Length** (the number of the last password used), and the last-used **Password**.

**2** Click on **OK**.



**Warning** – Do *not* click on **Generate**.

The S/Key password is saved. If **Seed** and **Length** are not entered, the user is prompted for them.

- To generate new S/Key passwords for a user who has forgotten his or her passwords, proceed as follows:

**1** In the user's **User Properties** window, enter a new **Secret Key** (or leave it blank and let one be chosen randomly).

**2** Enter a **Length**.

**3** Click on **Generate**.

The keys are then generated and saved to a file.

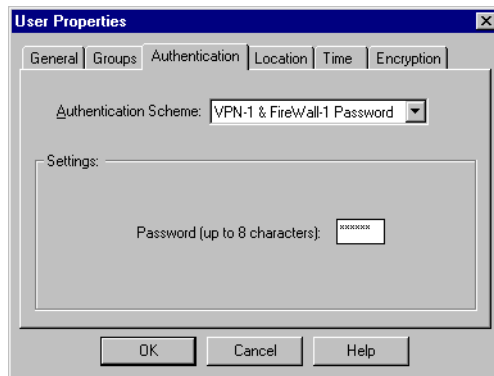
**4** Download the User Database by choosing **Policy**►**Download Database** from the menu or by clicking on **Install** in the **Users** window (FIGURE 5-1 on page 154).

For more information, see “Database Installation” on page 167 .

The former “forgotten” keys are no longer valid, and the new keys will be used for all future authentication.



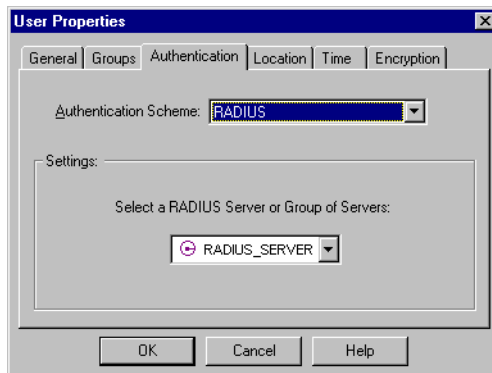
## VPN-1/FireWall-1 Password Authentication



**FIGURE 5-7** User Properties window — Authentication tab — VPN-1/FireWall-1 Password authentication

**Password** —Enter a password up to eight characters in length.

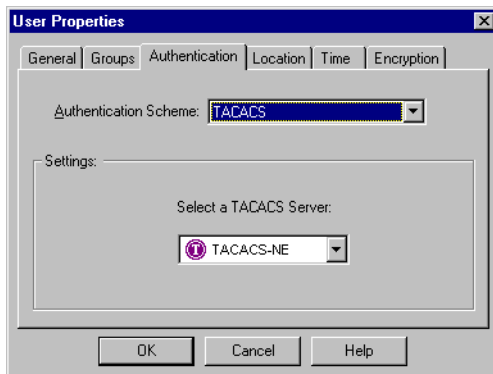
## RADIUS Authentication



**FIGURE 5-8** User Properties window — Authentication tab — RADIUS authentication

Select a RADIUS Server or group of RADIUS Servers from the menu. For information on how to define RADIUS Servers, see “RADIUS Servers” on page 329.

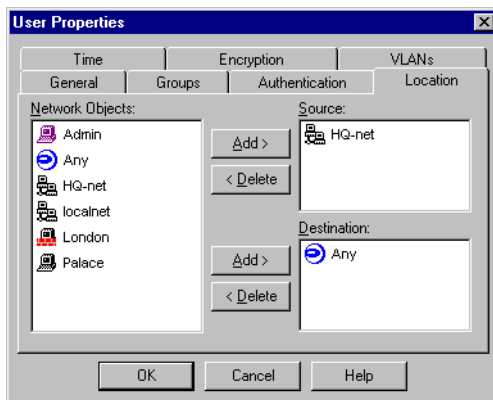
## TACACS Authentication



**FIGURE 5-9** User Properties window — Authentication tab — TACACS authentication

Select a TACACS Server from the menu. For information on how to define TACACS Servers, see “TACACS Servers” on page 332.

## User Properties Window — Location tab



**FIGURE 5-10** User Properties window — Location tab



**Getting Here** – To display this window, choose **Manage>Users** in the menu, select the user in the **Users** window (FIGURE 5-1 on page 154), click on **Edit** and then click on the **Location** tab.

**Source** — The user will be allowed access only from the listed network objects.

- To add a network object, select the object from the left list box (labeled **Network Objects**), and then click on the **Add** button to the left of the **Source** list box.
- To delete a network object, select the object in the **Source** list box and click on the **Delete** button to the left of the **Source** list box.

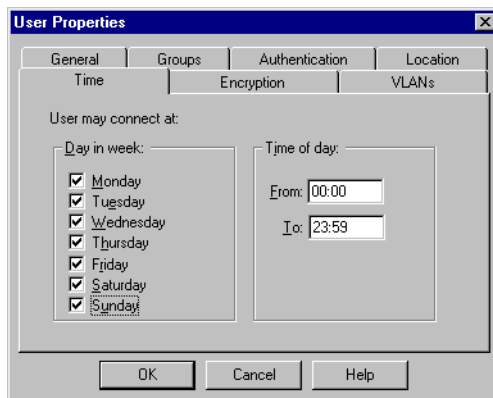
For information on how to override this field for a specific rule, see Chapter 15, “Authentication.”

**Destination** — The user will be allowed access only to the listed network objects.

- To add a network object, select the object from the left list box (labeled **Network Objects**), and then click on the **Add** button to the left of the **Destination** list box.
- To delete a network object, select the object in the **Destination** list box and click on the **Delete** button to the left of the **Destination** list box.

For information on how to override this field for a specific rule, see Chapter 15, “Authentication.”

## User Properties Window — Time tab



**FIGURE 5-11** User Properties window — Time tab

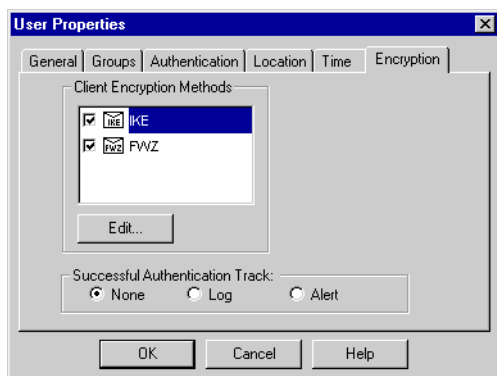


**Getting Here** — To display this window, choose **Manage>Users** in the menu, select the user in the **Users** window (FIGURE 5-1 on page 154), click on **Edit** and then click on the **Time** tab.

**Day in Week** — days on which the user will be allowed access

**Time of Day: From and To** — hours between which the user will be allowed access

## User Properties Window — Encryption tab



**FIGURE 5-12** User Properties window — Encryption tab



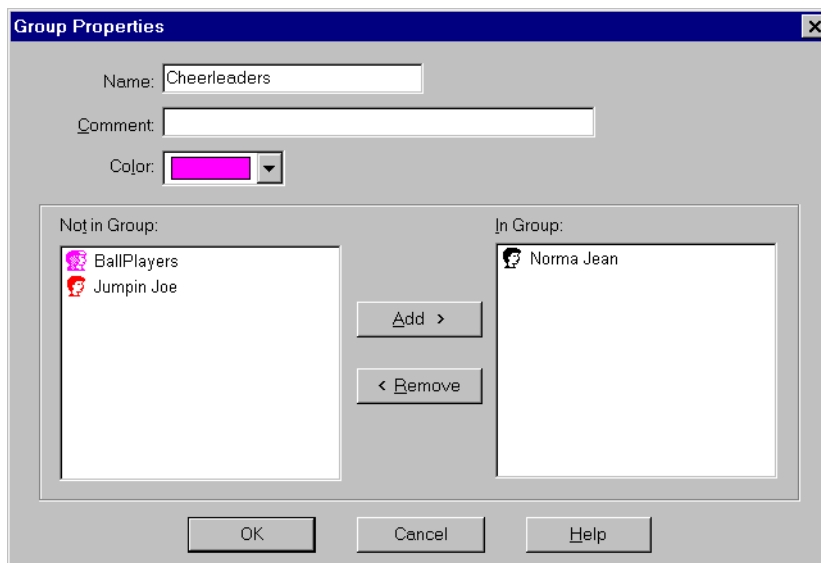
**Getting Here** – To display this window, choose **Manage>Users** in the menu, select the user in the **Users** window (FIGURE 5-1 on page 154), click on **Edit** and then click on the **Encryption** tab.

The **Encryption** tab enables you to specify parameters relating to the user's SecuRemote encryption.

For information about encryption, see *Check Point Virtual Private Networks*.

## User Groups

To display and update a group's members, double-click on the group's name in the **Users** window (FIGURE 5-1 on page 154). The **Group Properties** window (FIGURE 5-13) is then displayed.



**FIGURE 5-13** Group Properties window



**Getting Here** – To display this window, choose **Manage>Users** in the menu, and in the **Users** window (FIGURE 5-1 on page 154):

- To define a new group, click on **New** and select **Group** from the menu (FIGURE 5-2 on page 154).
- To edit the properties of an existing group, select a group and click on **Edit**.

**Name** — the group's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Users** window when this group is selected.

**Color** — the color of the group's icon

Select the desired color from the drop-down list.

In the left list box (labeled **Not in Group**), select the users or groups you wish to include in the group and click on **Add**.

You can add a group to another group in one of two ways:

- 1** You can individually add all the users in one group to another group, without nesting. Click on **Yes** in reply to the question in the window (FIGURE 5-14).

- 2 You can nest groups inside groups to create a group hierarchy of any desired complexity. Click on **No** in reply to the question in the window.



**FIGURE 5-14** Adding a Group to a Group

## Deleting a User or Group from a Group

To delete a user or group from a group, double-click on the group's name in the **Users** window (FIGURE 5-1 on page 154). The **Group Properties** window (FIGURE 5-13 on page 165) is then displayed.

Select the users or groups to be deleted from the right list box (labeled **In Group**), and then click on **Remove**.

## User Database

The VPN-1/FireWall-1 User Database contains information about each user defined in VPN-1/FireWall-1, including authentication schemes and encryption keys. The User Database resides on the Management Station and on the FireWalled machines (enforcement points).

The VPN-1/FireWall-1 User Database does *not* contain information about users defined externally to VPN-1/FireWall-1, for example, users in external groups (see “External Users and Groups” on page 169), but it does contain information about the external group (for example, on which Account Unit the external group is defined). For this reason, changes to external groups take effect only after the Security Policy is installed or the User Database is downloaded.

When the properties of a user defined in the VPN-1/FireWall-1 User Database change, the change does not take effect immediately. The VPN/FireWall modules on which the Security Policy is installed must be notified of the change, in one of three ways:

- 1 Install the User Database by choosing **Install Database** from the **Policy** menu.
- 2 Install the User Database by clicking on **Install** in the **Users** window (FIGURE 5-1 on page 154).
- 3 Install the Security Policy by choosing **Install** from the **Policy** menu.  
This installs the Security Policy in addition to updating the User Database.

## Database Installation

When you install the User Database from the GUI (by choosing **Install Database** from the **Policy** menu or clicking on **Install** in the **Users** window), VPN-1/FireWall-1 runs the `fw dbload` command with the `dbload` argument (see “fw dbload” on page 13 of *Check Point Reference Guide* for more information).

You can modify this behavior so that VPN-1/FireWall-1 runs a program or shell script (batch file) of your choice instead of `fw dbload`. For example, to run `bigapple`, add the following statement to the `setup.C` file:

```
dbload_program ("bigapple")
```

`bigapple` will be run with the same argument list that `fw` would have received (where the first argument is `dbload`). It is then your responsibility to ensure that `bigapple` correctly processes its arguments and installs the Database. Of course, `bigapple` can also perform any other functions you wish.



**Note** – The implicit installation of the User Database that occurs when a Security Policy is installed is not affected by the `dbload_program` parameter.

## Generic User

### Overview

If you have already defined a large number of users in an external database, you can define these users in VPN-1/FireWall-1 either by entering them manually or by importing them using the `fw dbimport` command (see “fw expdate” on page 46 of *Check Point Reference Guide*). In either case, all the users will be defined and maintained in both databases.

You can avoid the burden of maintaining multiple user databases by defining a user named “generic\*” whom VPN-1/FireWall-1 treats in a special way. VPN-1/FireWall-1 applies the restrictions specified in the **User Properties** window (for example, **Allowed Sources**), but for authentication purposes, uses the name typed in by the user instead of “generic\*.” In this way, the external authentication server “sees” the user’s real name and authenticates him or her accordingly.

### Example

#### Definition

For example, suppose you have already defined a large number of users to the Security Dynamics database and they are all authenticating themselves with their SecurID cards. Now, you want to integrate this authentication with VPN-1/FireWall-1, but you do not want to define all your SecurID users in the VPN-1/FireWall-1 User Database.

You can use the generic user feature as follows:

- 1** Define a user group named **SecurIDUsers** (for example).
- 2** Define a user named **generic\*** as a member of **SecurIDUsers**.
- 3** Specify **SecurID** as the **Authentication Scheme** for **generic\***.
- 4** Add a rule to the Rule Base similar to this:

| Source           | Destination | Services | Action   | Track    | Install On |
|------------------|-------------|----------|----------|----------|------------|
| SecurIDUsers@Any | tower       | telnet   | UserAuth | Long Log | Gateways   |

- 5** Install the Security Policy.



**Note** – The above rule will not be applied to users who are defined in the VPN-1/FireWall-1 User Database, only to users who are *not* defined in the VPN-1/FireWall-1 User Database.

## Using the Generic User Feature

Suppose that Alice is a SecurID user, but she is not defined in the VPN-1/FireWall-1 User Database. When she TELNETs to tower (and the above rule is applied), the following sequence of events takes place:

- 1** VPN-1/FireWall-1 prompts Alice for her user name.
- 2** Alice enters her name.
- 3** VPN-1/FireWall-1 determines that Alice is an unknown user, that is, that she is *not* defined in the VPN-1/FireWall-1 User Database (or in any LDAP directory accessed by VPN-1/FireWall-1).
- 4** VPN-1/FireWall-1 determines that there is a user named **generic\*** defined in the User Database, whose **Authentication Method** is **SecurID**.

If there is no user named **generic\***, VPN-1/FireWall-1 issues the “illegal user name” error message and disallows the connection.

- 5** VPN-1/FireWall-1 prompts Alice to enter her SecurID password.
- 6** Alice enters her SecurID password.
- 7** VPN-1/FireWall-1 contacts the SecurID server and asks to authenticate user Alice, supplying the password Alice entered.
- 8** The SecurID server notifies VPN-1/FireWall-1 whether Alice was successfully authenticated.
- 9** VPN-1/FireWall-1 either allows or disallows the connection, depending on whether Alice was successfully authenticated.



## Notes

- 1 By using this feature with an external server, you disable VPN-1/FireWall-1's ability to detect invalid user names.  
  
The responsibility of authenticating the user is passed to the external server. You will only get an alert or log if the authentication fails on the external server. Without this option, it is possible to get an alert or log when an invalid user name is entered.
- 2 By default, all the users defined in the external server are allowed access.  
  
There is no way to treat the users differently (but see item 3 below). The System Administrator should carefully consider the implications of allowing this blanket access.
- 3 If you wish to deny access to a specific user, define that user in the VPN-1/FireWall-1 User Database and set the user's **Authentication Scheme** to **Undefined**.
- 4 To disable this feature, delete **generic\*** from the VPN-1/FireWall-1 User Database, or set **generic\***'s **Authentication Scheme** to **Undefined**.
- 5 This feature does not work with the S/Key and VPN-1/FireWall-1 Password Authentication Schemes.  
  
The user **generic\*** will always fail S/Key and VPN-1/FireWall-1 Password authentication, because these schemes are implemented directly by VPN-1/FireWall-1 and not by external servers, so their users must be defined in the VPN-1/FireWall-1 User Database.  
  
Nevertheless, there is still an advantage to be gained by defining a user **generic\*** with the VPN-1/FireWall-1 Password Authentication Scheme. An attacker who guesses at a user name will not see the error message "unknown user." Instead, the attacker will see a message indicating that the authentication failed, and will not know whether it is the name or the password that is invalid.
- 6 **generic\*** cannot be used as the name of a real user.

## External Users and Groups

An external group is a user group whose members are defined in an external LDAP directory server. The LDAP directory can be managed independently of VPN-1/FireWall-1.

An external group can be used in a Security Policy in the same way that a VPN-1/FireWall-1 group can be used. The only difference between them is where the users are defined.


VPN-1/FireWall-1 includes an Account Management Client for managing users in an external LDAP directory, but its use is optional. For information about the VPN-1/FireWall-1 Account Management Client, see the book *Check Point Account Management Client*.

For information about VPN-1/FireWall-1 Account Management, see “VPN-1/FireWall-1 LDAP Account Management” on page 174.

## Managing External Users

You can manage external users with the VPN-1/FireWall-1 Account Management Client or with a third-party LDAP Client.

To start the VPN-1/FireWall-1 Account Management Client from within the VPN-1/FireWall-1 GUI:

- choose **Manage External Users** from the **User** menu, *or*
- click on  in the toolbar.

The **Manage Users on Account Unit** window (FIGURE 5-15) is displayed.



**FIGURE 5-15** Manage Users on Account Unit window

Select an Account Unit and click on **Manage**.

The Account Units listed are those that were defined as LDAP servers. For information about how to define LDAP Servers, see Chapter 10, “Server Objects.”

## Managing External Groups




**Note** – Changes to external groups take effect after the Security Policy is installed or the User Database is downloaded.

### Creating an External Group

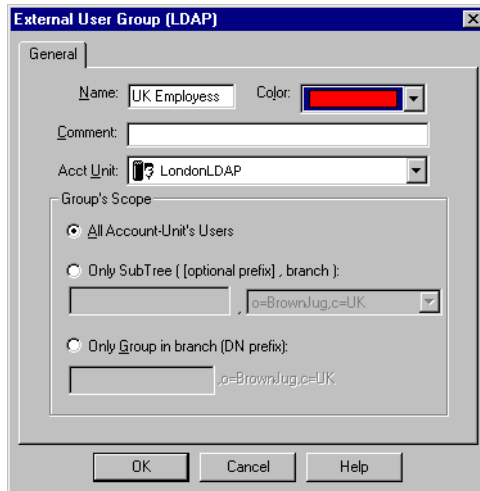
To use externally defined users in a Security Policy, you should define external groups that include those users.

To create an external group, proceed as follows:

- 1 To display the **Users** window (FIGURE 5-1 on page 154):
  - choose **Users** from the **Manage** menu, *or*
  - click on  in the toolbar.
- 2 Click on **New**.  
The **New User Object** menu is displayed (FIGURE 5-2 on page 154), listing the types of objects you can create.
- 3 Select **External group** from the menu to display the **External User Group (LDAP)** window.

The **External User Group (LDAP)** window (FIGURE 5-16) is displayed.

### External User Group (LDAP) window



**FIGURE 5-16** External User Group (LDAP) window

**Name** — the group's name

This is the name that will be used in the Rule Base.

**Color** — the color of the group's icon

Select the desired color from the drop-down list.

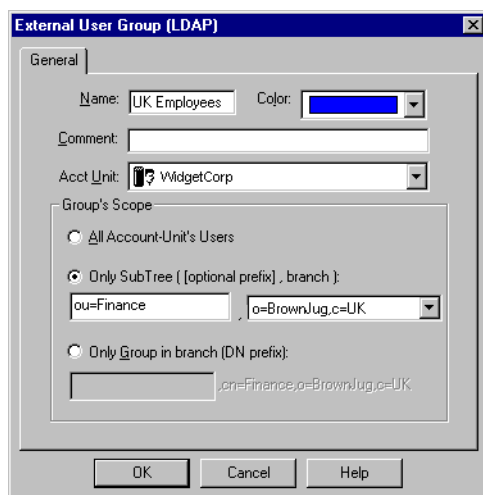
**Account Unit** — the Account Unit (LDAP server) on which the external group is defined

Select an Account Unit from the drop-down list. The Account Units listed are those that were defined as LDAP Account Units in the **LDAP Account Unit Properties** window (FIGURE 10-17 on page 335).

There are three possible ways of defining an external group:

- 1 All Account Unit's Users** — The external group includes all the users defined on the Account Unit.
- 2 Only Branch** — The external group includes all the users defined in the specified branch on the Account Unit.

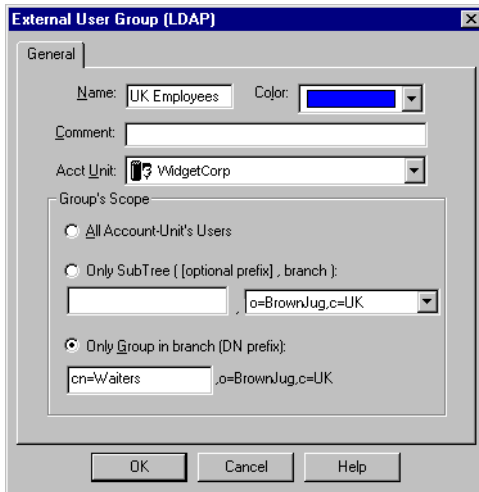
Select a branch from the drop-down list. You can specify a sub-branch within the selected branch by typing the remaining part of its DN (that is, its RDN or prefix) in the left box (see FIGURE 5-17).



**FIGURE 5-17** External User Group (LDAP) window with sub-branch defined

- 3 Only Group in Branch** — The external group includes all the users defined in the specified group on the Account Unit (see FIGURE 5-18).


You can specify the DN of either a group or a user.



**FIGURE 5-18** External User Group (LDAP) window with group in branch defined

## Modifying an External Group

To modify an existing external group, proceed as follows:

- 1 Display the **Users** window (FIGURE 5-1 on page 154) by:
  - choosing **Users** from the **Manage** menu, or
  - clicking on  in the toolbar.
- 2 Select the external group you wish to modify and click on **Edit**.  
The **External User Group (LDAP)** window (FIGURE 5-16 on page 171) is displayed.
- 3 Modify the details of the external group and click on **OK**.



**Note** – To add or delete users from an external group, or to modify users in an external group, you must use an LDAP Client, for example the Check Point Account Management Client described in the book *Check Point Account Management Client*. Note that an LDAP group cannot contain other LDAP groups — only users.

## Deleting an External Group

To delete an existing external group, proceed as follows:

- 1 Display the **Users** window as above.
- 2 Select the external group you wish to delete and click on **Remove**.

# VPN-1/FireWall-1 LDAP Account Management

## Overview

The VPN-1/FireWall-1 Account Management system enables the Security Manager to integrate VPN-1/FireWall-1 with LDAP Servers, allowing user data to be shared between VPN-1/FireWall-1 and other applications.

The LDAP Servers and VPN-1/FireWall-1 can reside on different hosts and be maintained by different people. Separating the functionality of the two systems provides the following benefits:

- The system administrator can use existing LDAP-compliant databases without the need to import user data into VPN-1/FireWall-1.
- A single VPN-1/FireWall-1 system can be used by several departments or customers, each of which can manage its own users independently using a separate management client.
- Users can maintain and change their own passwords.
- There is no limit to the number of users that can be defined.

An additional feature is the live template. In the VPN-1/FireWall-1 user management model, changes made to a user template do not affect users previously defined using that template. In contrast, in the VPN-1/FireWall-1 Account Management system, changes made to a live template immediately apply to all users linked to the template.

Users wishing to continue using the proprietary VPN-1/FireWall-1 user database may do so. Groups defined in both systems can be freely mixed in the Rule Base.

## The LDAP Model

LDAP (Lightweight Directory Access Protocol) is a lightweight version of the X.500 directory access protocol. LDAP is based on a Client/Server model in which an LDAP Client makes a TCP connection to an LDAP server, over which it sends requests and receives responses.

The LDAP information model is based on the entry, which contains information about some object (for example, a person). Entries are composed of attributes, which have a type and one or more values. The schema lists the attributes, their data types (for example, ASCII text, a JPEG photograph, etc.) and how those values behave during directory operations (for example, whether case is significant in comparisons).

Entries are organized in a tree structure, usually based on political, geographical, and organizational boundaries. Each entry is uniquely named relative to its sibling entries by its RDN (relative distinguished name) consisting of one or more distinguished attribute values from the entry. For example, the entry for the person Babs Jensen might be named with the "Barbara Jensen" value from the commonName attribute.

A globally unique name for an entry, called a DN (distinguished name), is constructed by concatenating the sequence of RDNs from the root of the tree down to the entry. For example, if Babs worked for the University of Michigan, the DN of her University of Michigan entry might contain:

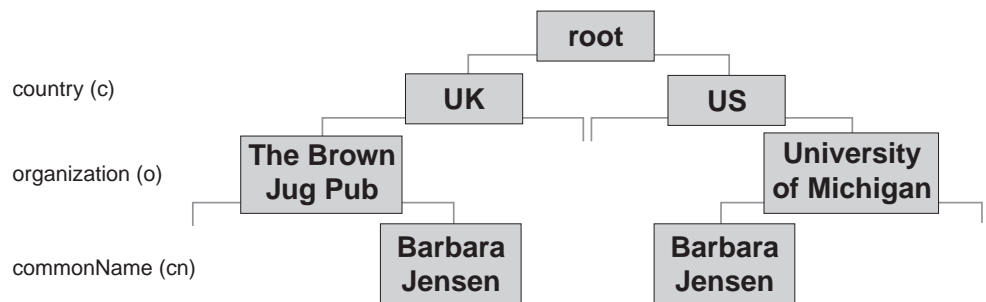
```
"cn=Barbara Jensen, o=University of Michigan, c=US"
```

A DN is expressed in the “bottom up” sequence, that is, starting at the lowest level and moving up to the root of the tree.

A different Barbara Jensen who works at The Brown Jug Pub in London, England might have a DN of:

```
"cn=Barbara Jensen, o=The Brown Jug Pub, c=UK"
```

This is illustrated in FIGURE 5-19.



**FIGURE 5-19** LDAP Tree Example

LDAP provides operations to authenticate, search for and retrieve information, modify information, and add and delete entries from the tree.

## LDAP Servers

The LDAP information model is most appropriate for directory services, that is, information which is read much more frequently than it is modified. An LDAP Server makes the data in an LDAP-compliant directory available to LDAP Clients.

An LDAP directory can be indexed, which improves performance at the cost of the directory taking up more disk space.

## LDAP Schema

An LDAP schema is a description of the structure of the data in an LDAP directory.

## Account Management Configuration

### Account Management Components

The Account Management system consists of four components:

- 1** VPN-1/FireWall-1 Management Module (Version 4.0 and higher)
- 2** VPN/FireWall Module (Version 4.0 and higher)
- 3** Check Point Account Management Client (AM Client)

The AM Client can be run from within the VPN-1/FireWall-1 GUI or as an independent stand-alone application. As a stand-alone application, it does not require that the VPN-1/FireWall-1 GUI be installed on the same machine as the AM Client.

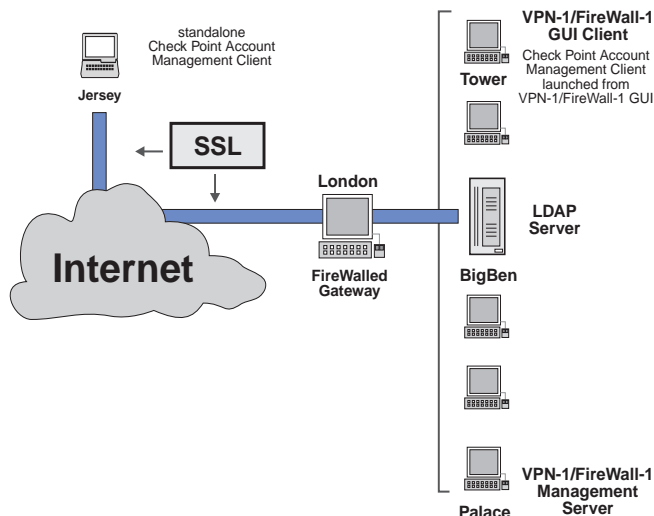
The AM Client is described in *Check Point Account Management Client*.

- 4** LDAP Server (any LDAP Version 2.0 or higher compliant third-party server)

The LDAP server must be accessible to both the AM Client and to the VPN/FireWall Module, that is, both when a Security Policy is defined and when it is enforced.

### A Typical Configuration

A typical configuration is depicted in FIGURE 5-20.



**FIGURE 5-20** A typical Account Management configuration

Palace, the VPN-1/FireWall-1 Management Server, is the repository of the VPN-1/FireWall-1 database, which includes users defined with the proprietary VPN-1/FireWall-1 User Manager.



Palace's VPN-1/FireWall-1 GUI Clients, for example Tower, can define two kinds of users:

- VPN-1/FireWall-1 users — users defined in the VPN-1/FireWall-1 User Manager, using the VPN-1/FireWall-1 GUI and stored in the VPN-1/FireWall-1 proprietary database
  - LDAP users — users defined on BigBen, the LDAP server, using the AM Client
- These users can be shared between VPN-1/FireWall-1 and other network applications.

Jersey, on which VPN-1/FireWall-1 is not installed, can update only LDAP users, using the AM Client. In the configuration depicted in FIGURE 5-20, this communication channel is secured with SSL (Secure Socket Layer).

A system administrator can define a Security Policy on Palace, using the GUI Client on Tower, and define rules that specify VPN-1/FireWall-1 groups and LDAP groups. When the Security Policy is installed on the FireWalled gateway (London), the User Database (proprietary information about VPN-1/FireWall-1 users) is downloaded to London.

When a VPN-1/FireWall-1 user (a user defined in the VPN-1/FireWall-1 proprietary database) logs on to London, London has immediate access to the required authentication information in the VPN-1/FireWall-1 User Database. In contrast, when an LDAP user (a user defined in an LDAP Server) logs on and must be authenticated, London must communicate with the LDAP Server to obtain the required information.

In addition to maintaining LDAP users with the VPN-1/FireWall-1 Account Management Client and LDAP Server, it is possible to maintain LDAP users using any LDAP Version 2.0 and higher compatible server.

## Account Units

An LDAP Server can contain multiple branches (“o=University of Michigan,c=US”, for example, is a branch). An LDAP Server and a subset of its branches constitute a VPN-1/FireWall-1 Account Unit. It is possible to maintain the LDAP user database using more than one Account Unit. The advantages of using more than one Account Unit are:

- *compartmentalization* — A large number of users can be distributed across several LDAP servers which may be partitioned into several Account Units, each of which is managed by a different administrator (see FIGURE 5-21 on page 178). In this way, both efficiency and security can be enhanced.
- *high availability* — Information can be duplicated on several servers. Some LDAP servers provide automatic tools for synchronizing servers.
- *remote sites* — It may be efficient to provide each geographically remote VPN/FireWall Module with a close at hand LDAP server.

FIGURE 5-21 depicts a configuration with four Account Units (two of them on the same LDAP server), each of which is managed from a different client.

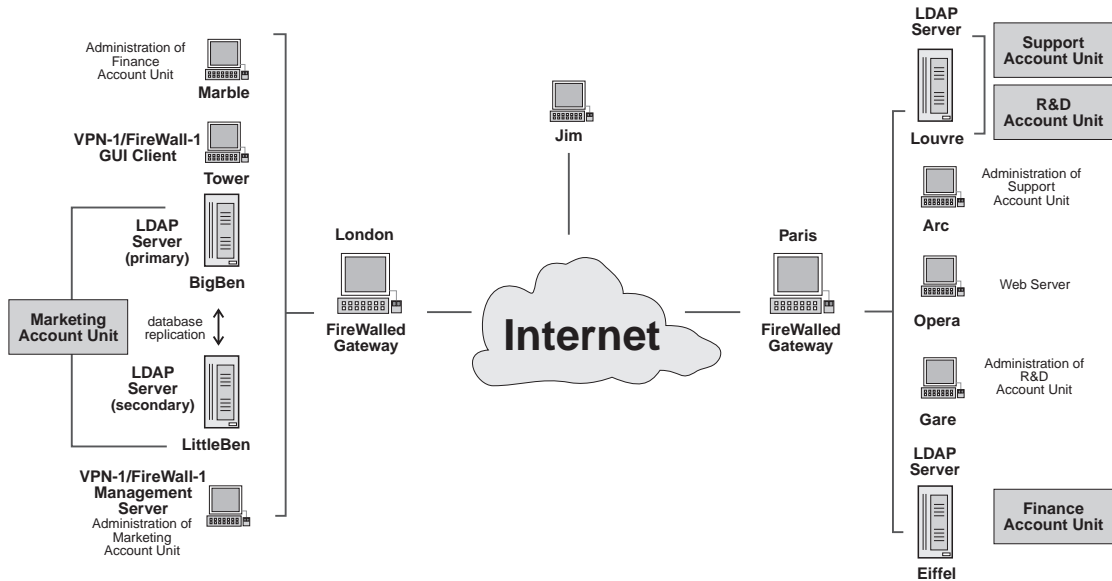


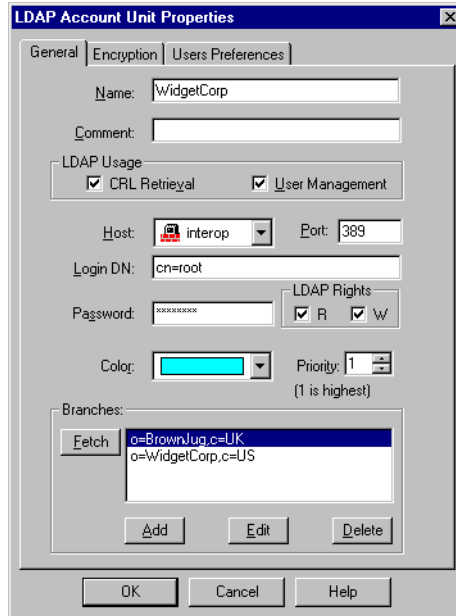
FIGURE 5-21 Multiple Account Units - Example Configuration

## Defining a Security Policy

To define a Security Policy that references users defined in an LDAP Account Unit, proceed as follows (in VPN-1/FireWall-1):

- 1 Define the LDAP properties in the **LDAP** tab of the **Properties Setup** window (see “Exporting Users from the VPN-1/FireWall-1 User Database” on page 188).
- 2 Define the LDAP Server as a network object.  
See Chapter 4, “Network Objects” for information on how to define network objects.

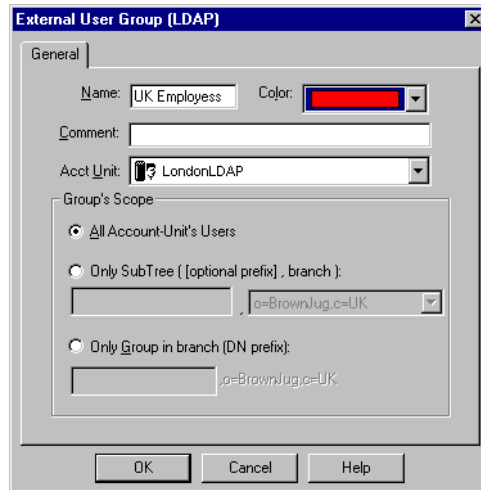
- 3** Define an LDAP Account Unit in the **LDAP Account Unit Properties** window (FIGURE 5-22).



**FIGURE 5-22** LDAP Account Unit Properties window — General tab

For information on defining Account Units, see Chapter 10, “Server Objects

- 4** Define an external user group in the **External User Group (LDAP)** window (FIGURE 5-23).



**FIGURE 5-23** External User Group (LDAP) window

For information on defining external user groups, see “External Users and Groups” on page 169.

- 5 Use the external group in a rule.

As illustrated in FIGURE 5-24, external groups are used in a Rule Base in exactly the same way as ordinary VPN-1/FireWall-1 groups are used.

| Security Policy |                    | Address Translation |         |        |       |            |
|-----------------|--------------------|---------------------|---------|--------|-------|------------|
| No.             | Source             | Destination         | Service | Action | Track | Install On |
| 1               | UK Employees@UKNet | Any                 | http    | accept | Short | Gateways   |
| 2               | Any                | Any                 | Any     | reject | Long  | Gateways   |

FIGURE 5-24 External User Group in a Rule Base

For information on using groups in a rule, see Chapter 8, “Security Policy Rule Base.”

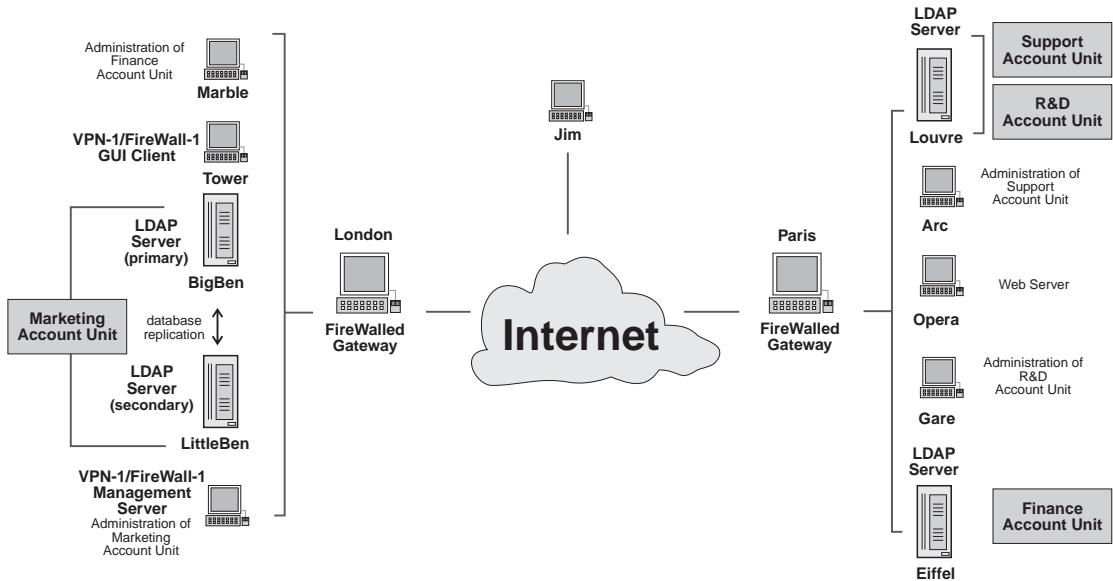
### Enforcing a Security Policy

This section describes what happens when a user attempts to establish a connection through a VPN/FireWall Module when the Security Policy specifies groups defined on Account Units. The network configuration is depicted in FIGURE 5-25 on page 181.

Suppose user Jim attempts to connect to Opera, one of the computers protected by the FireWalled gateway Paris.

- 1 Paris scans its Rule Base and determines that the relevant rule is an authentication rule.
- 2 Paris asks Jim to identify himself (user name).  
Jim can enter his login name or his full LDAP Distinguished Name, for example, “cn=Jim Smith,o=WidgetCorp,c=US”.

Paris searches its VPN-1/FireWall-1 User Database for user Jim.



**FIGURE 5-25** Enforcing a Security Policy

- 3** If Jim is found in the VPN-1/FireWall-1 User Database, then Paris authenticates Jim according to the attributes (authentication scheme, password *etc.*) defined in Jim's **User Properties** window (in the VPN-1/FireWall-1 GUI).



**Note** – The VPN-1/FireWall-1 User Database always has priority over Account Units. It is recommended that you define network and system administrators as VPN-1/FireWall-1 users, so that they will always be able to log in to the FireWall, even if the LDAP connection is down.

The other parameters (**Allowed Source**, **Allowed Destination**, **Time** *etc.*) must also be applicable. If Jim authenticates himself correctly, the connection is allowed; otherwise it is refused. In either case, the scenario ends at this point.

- 4** If Jim is *not* found in the VPN-1/FireWall-1 User Database, then Paris queries all its Account Units, asking if any of them knows about Jim.
- 5** The query process terminates when any one of the following conditions is true:
  - All Account Units have replied.
  - The timeout period (see “Exporting Users from the VPN-1/FireWall-1 User Database” on page 188) has elapsed.
  - The user was found in the highest priority Account Unit (see “LDAP Account Unit Properties Window — General Tab” on page 335).
  - The user was found in an Account Unit *and* all Account Units with higher priorities have already replied that they do not know about the user.
- 6** If the user was not found in any Account Unit, then the authentication fails.

- 7** If the user was found, then Paris chooses the first user named Jim received from the Account Unit with the highest priority and ignores the other Account Units (if any). Suppose this is BigBen.



**Note** – If there is more than one user with the same name in an Account Unit, the first one is chosen and any others are ignored. If the **Display user’s DN at login** property is enabled in the **LDAP** tab of the **Properties Setup** window (FIGURE 7-7 on page 249), you can verify that the correct entry is being used.

- 8** Paris queries BigBen to determine the groups to which Jim belongs.
- 9** Paris queries BigBen to determine Jim’s template and applies the template values to Jim (if Jim is defined to inherit his values from a template).
- 10** Paris confirms the authentication scheme.

Jim’s authentication scheme (as defined in the **Authentication** tab of his **User Properties** window in the Account Management Client GUI) must be:

- one of those allowed in the **Authentication** tab of BigBen’s **LDAP Account Unit** window, *and*
- one of those selected in the **Authentication** tab of Paris’ **Workstation Properties** window

If either of these conditions is not met, the connection is refused and the scenario ends.

- 11** Paris authenticates Jim according to his authentication scheme.

If Jim authenticates himself correctly, the connection is allowed; otherwise it is refused.

## LDAP Schema

The VPN-1/FireWall-1 LDAP schema is in `$FWDIR\lib\ldap\schema.ldif`.

## Proprietary Attributes

### OID

Each of the proprietary object classes and attributes (all of which begin with “fw1”) has a proprietary Object Identifier (OID), listed below.

**TABLE 5-3** Object Class OIDs

| object class | OID               |
|--------------|-------------------|
| fw1template  | 1.3.114.7.3.2.0.1 |
| fw1person    | 1.3.114.7.3.2.0.2 |

The OIDs for the proprietary attributes begin with the same prefix (“1.3.114.7.4.2.0.X”). Only the value of “X” is different for each attribute. The value for “X” is given in the table below.

## Attributes

**TABLE 5-4** Attributes

| attribute   | "X" in OID | fw1person | fw1template | default    | remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|------------|-----------|-------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cn          |            |           |             |            | <p>The entry's name.</p> <p>In the Account Management Client, this is referred to as "Common Name". For users this can be different from the uid attribute — the name used to login to the VPN/FireWall Module. This attribute is also used to build the LDAP entry's distinguished name, that is, it is the RDN of the DN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| uid         |            |           |             |            | <p>The user's login name, that is, the name used to login to the VPN/FireWall Module. This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication schemes.</p> <p>The login name is used by VPN-1/FireWall-1 to search the LDAP server(s). For this reason, each user entry should have its own unique uid value. It is also possible to login to the VPN/FireWall Module using the full DN. The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing. The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different LDAP Servers.</p> |
| description |            |           |             | "no value" | Descriptive text about the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| mail        |            |           |             | "no value" | User's email address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| member      |            |           |             |            | <p>An entry can have zero or more values for this attribute.</p> <p><b>In a template:</b> The DN of user entries using this template. DNs that are not users (object classes that are not one of: "person", "organizationalPerson", "inetOrgPerson" or "fw1person") are ignored.</p> <p><b>In a group:</b> The DN of user, group or live template entries that are members of this group.</p>                                                                                                                                                                                                                                                                                                                                                                                         |

TABLE 5-4 Attributes

| attribute    | "X" in OID | fw1person | fw1template | default | remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|------------|-----------|-------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| userPassword |            |           |             |         | <p>Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is:</p> <p>"{crypt}xyyyyyyyyyyy"</p> <p>where "xx" is the "salt" and "yyyyyyyyyyy" is the hashed password.</p> <p>It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the LDAP Server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password.</p> <p>The VPN/FireWall Module never reads this attribute, though it does write it. Instead, the LDAP bind operation is used to verify a password.</p> |



TABLE 5-4    Attributes

| attribute             | "X" in OID                                                            | fw1person | fw1template | default     | remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |            |             |                                                                       |                 |                                                              |                       |                         |
|-----------------------|-----------------------------------------------------------------------|-----------|-------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------|-------------|-----------------------------------------------------------------------|-----------------|--------------------------------------------------------------|-----------------------|-------------------------|
| fw1auth-method        | 1                                                                     | ✓         | ✓           | "undefined" | <p>One of the following:</p> <table><tr><td>■ "S/Key"</td><td>■ "RADIUS"</td></tr><tr><td>■ "SecurID"</td><td>■ "TACACS"</td></tr><tr><td>■ "OS Password"</td><td>■ "Defender"</td></tr><tr><td>■ "Internal Password"</td><td>■ "undefined"</td></tr></table> <p>This default value for this attribute is overridden by <b>Default Scheme</b> in the <b>Authentication</b> tab of the <b>Account Unit</b> window in the VPN-1/FireWall-1 GUI (see "LDAP Account Unit Properties Window — User Preferences Tab" on page 337 of <i>VPN-1/FireWall-1 Administration Guide</i>). For example: an LDAP server can contain LDAP entries that are all of the object-class "person" even though the proprietary object-class "fw1person" was not added to the server's schema. If <b>Default Scheme</b> in the VPN-1/FireWall-1 GUI is "Internal Password", all the users will be authenticated using the password stored in the "userPassword" attribute.</p> | ■ "S/Key" | ■ "RADIUS" | ■ "SecurID" | ■ "TACACS"                                                            | ■ "OS Password" | ■ "Defender"                                                 | ■ "Internal Password" | ■ "undefined"           |
| ■ "S/Key"             | ■ "RADIUS"                                                            |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| ■ "SecurID"           | ■ "TACACS"                                                            |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| ■ "OS Password"       | ■ "Defender"                                                          |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| ■ "Internal Password" | ■ "undefined"                                                         |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| fw1auth-server        | 2                                                                     | ✓         | ✓           |             | <p>The name of the server that will perform the authentication This field must be given if fw1auth-method is "S/Key" or "RADIUS" or "TACACS". For all other values of fw1auth-method, it is ignored. Its meaning is given below:</p> <table><tr><th>method</th><th>meaning</th></tr><tr><td>S/Key</td><td>name of the workstation on which the VPN/FireWall Module is installed</td></tr><tr><td>RADIUS</td><td>name of a RADIUS server, a group of RADIUS servers, or "Any"</td></tr><tr><td>TACACS</td><td>name of a TACACS server</td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                                 | method    | meaning    | S/Key       | name of the workstation on which the VPN/FireWall Module is installed | RADIUS          | name of a RADIUS server, a group of RADIUS servers, or "Any" | TACACS                | name of a TACACS server |
| method                | meaning                                                               |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| S/Key                 | name of the workstation on which the VPN/FireWall Module is installed |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| RADIUS                | name of a RADIUS server, a group of RADIUS servers, or "Any"          |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |
| TACACS                | name of a TACACS server                                               |           |             |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |            |             |                                                                       |                 |                                                              |                       |                         |

**TABLE 5-4** Attributes

| attribute          | "X" in OID | fw1person | fw1template | default                                                          | remarks                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|------------|-----------|-------------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fw1pwdLastMod      | 3          | ✓         | ✓           | If no value is given, then the password has never been modified. | The date on which the password was last modified. The format is <i>yyyymmdd</i> (for example, 20 August 1998 is 19980820). A password can be modified using the Account Management Client (see "New User Window - Authentication Tab" on page 45 of <i>Account Management Client</i> ), or through the VPN/FireWall Module as a part of the authentication process. |
| fw1Skey-number     | 4          | ✓         | ✓           |                                                                  | Length of initial S-Key chain. This attribute is required if the authentication method is S/Key.                                                                                                                                                                                                                                                                    |
| fw1Skey-seed       | 5          | ✓         | ✓           |                                                                  | The seed from which the S-Key chain was generated (with the addition of a secret). This attribute is required if the authentication method is S/Key.                                                                                                                                                                                                                |
| fw1Skey-passwd     | 6          | ✓         | ✓           |                                                                  | The last value of the initial S-Key chain. This attribute is required if the authentication method is S/Key.                                                                                                                                                                                                                                                        |
| fw1Skey-mdm        | 7          | ✓         | ✓           | MD4                                                              | The hash function used by S/Key. Valid values are "MD4" and "MD5". This attribute is required if the authentication method is S/Key.                                                                                                                                                                                                                                |
| fw1expiration-date | 8          | ✓         | ✓           | "no value"                                                       | The last date on which the user can login to a VPN/FireWall Module, or "no value" if there is no expiration date. The format is <i>yyyymmdd</i> (for example, 20 August 1998 is 19980820). The default is "no value".                                                                                                                                               |
| fw1hour-range-from | 9          | ✓         | ✓           | "00:00"                                                          | The time from which the user can login to a VPN/FireWall Module. The format is <i>hh:mm</i> (for example, 8:15 AM is 08:15).                                                                                                                                                                                                                                        |
| fw1hour-range-to   | 10         | ✓         | ✓           | "23:59"                                                          | The time until which the user can login to a VPN/FireWall Module. The format is <i>hh:mm</i> (for example, 8:15 AM is 08:15).                                                                                                                                                                                                                                       |
| fw1day             | 11         | ✓         | ✓           | all days of the week                                             | The days on which the user can login to a VPN/FireWall Module. Can have the values "SUN", "MON", ...etc.                                                                                                                                                                                                                                                            |

**TABLE 5-4** Attributes

| attribute             | "X" in OID | fw1person | fw1template | default    | remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|------------|-----------|-------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fw1allowed-src        | 12         | ✓         | ✓           | "no value" | The names of one or more network objects from which the user can run a client, or "Any" to remove this limitation, or "no value" if there is no such client. The names should match the name of network objects defined in VPN-1/FireWall-1 management station.                                                                                                                                                                                                                                                                   |
| fw1allowed-dst        | 13         | ✓         | ✓           | "no value" | The names of one or more network objects which the user can access, or "Any" to remove this limitation, or "no value" if there is no such network object. The names should match the name of network objects defined on the VPN-1/FireWall-1 Management Station.                                                                                                                                                                                                                                                                  |
| fw1allowed-vlan       | 14         | ✓         | ✓           | "no value" | currently not used                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| fw1SR-keym            | 15         | ✓         | ✓           | "Any"      | The algorithm used to encrypt the session key in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".                                                                                                                                                                                                                                                                                                                                                                                                                              |
| fw1SR-datam           | 16         | ✓         | ✓           | "Any"      | The algorithm used to encrypt the data in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| fw1SR-mdm             | 17         | ✓         | ✓           | "none"     | The algorithm used to sign the data in SecuRemote. Can be "none" or "MD5".                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| fw1enc-fwz-expiration | 18         | ✓         | ✓           |            | The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the VPN/FireWall Module.                                                                                                                                                                                                                                                                                                                                                                                                           |
| fw1sr-auth-track      | 19         | ✓         | ✓           | "none"     | The exception to generate on successful authentication via SecuRemote. Can be "none", "cryptlog" or "cryptalert".                                                                                                                                                                                                                                                                                                                                                                                                                 |
| fw1groupTemplate      | 20         | ✓         | ✓           | "FALSE"    | This flag is used to resolve a problem related to group membership.<br>The group membership of a user is stored in the group entries to which it belongs and not in the user entry itself. Therefore there is no clear indication in the user entry if information from the template about group relationship should be used.<br>If this flag is "TRUE", then the user is taken to be a member of all the groups to which the template is a member. This is in addition to all the groups in which the user is directly a member. |

**TABLE 5-4** Attributes

| attribute                     | "X" in OID | fw1person | fw1template | default          | remarks                                                                                                                                                                                                                                        |
|-------------------------------|------------|-----------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fw1ISAKMP-EncMethod           | 21         | ✓         | ✓           | "DES",<br>"3DES" | The key encryption methods for SecuRemote users using IKE <sup>1</sup> . This can be one or more of: "DES", "3DES". A user using IKE may have both methods defined.                                                                            |
| fw1ISAKMP-AuthMethods         | 22         | ✓         | ✓           | "signatures"     | The allowed authentication methods for SecuRemote users using IKE <sup>1</sup> . This can be one or more of: "preshared", "signatures".                                                                                                        |
| fw1ISAKMP-HashMethods         | 23         | ✓         | ✓           | "MD5",<br>"SHA1" | The data integrity method for SecuRemote users using IKE <sup>1</sup> . This can be one or more of: "MD5", "SHA1". A user using IKE must have both methods defined.                                                                            |
| fw1ISAKMP-Transform           | 24         | ✓         | ✓           | "ESP"            | The IPSec Transform method for SecuRemote users using IKE <sup>1</sup> . This can be one of: "AH", "ESP".                                                                                                                                      |
| fw1ISAKMP-DataIntegrityMethod | 25         | ✓         | ✓           | "SHA1"           | The data integrity method for SecuRemote users using IKE <sup>1</sup> . This can be one of: "MD5", "SHA1".                                                                                                                                     |
| fw1ISAKMP-SharedSecret        | 26         | ✓         | ✓           |                  | The pre-shared secret for SecuRemote users using IKE <sup>1</sup> .<br>The value can be calculated using the fw <code>ikecrypt</code> command line (see "VPN-1 Accelerator Card" on page 57 of <i>Check Point Account Management Client</i> ). |
| fw1ISAKMP-DataEncMethod       | 27         | ✓         | ✓           | "DES"            | The data encryption method for SecuRemote users using IKE <sup>1</sup> .                                                                                                                                                                       |
| fw1enc-Methods                | 28         | ✓         | ✓           | "FWZ"            | The encryption method allowed for SecuRemote users. This can be one or more of: "FWZ", "ISAKMP" (meaning IKE).                                                                                                                                 |

1. IKE was formerly known as ISAKMP or ISAKMP/OAKLEY.

## Exporting Users from the VPN-1/FireWall-1 User Database

You can export users from the VPN-1/FireWall-1 internal user database to an LDAP directory by using the `fw dbexport` command with the `-l` parameter. This command exports users or groups to an LDAP format file readable by most LDAP Servers.

For information about the `fw dbexport` command, see "fw dbexport" on page 41 of *Check Point Reference Guide*.

## Configuring an LDAP Server for VPN-1/FireWall-1

### LDAP Version

VPN-1/FireWall-1 is LDAP Version 2.0 compliant. The only Version 3.0 feature that VPN-1/FireWall-1 uses is the implementation of the **Fetch** button in the **General** tab of the **Account Unit Properties** window and in the Check Point Account Management Client (see “Branches” on page 336).

### Indexing

To maximize an LDAP Server’s performance, it’s recommended to index the LDAP Server according to the following attributes:

- DN
- UID
- member
- objectclass

These indexes reduce lookup time, but there is a trade-off between faster lookup times and the extra disk space needed to store the additional indexes.

### Schema Checking

When schema checking is enabled, LDAP requires that every object class and its associated attributes be defined in the directory schema.

When you first begin to use VPN-1/FireWall-1 Account Management, you should disable schema checking. Later, after you have entered the VPN-1/FireWall-1 object classes and attributes to the LDAP Server’s schema, you can enable schema checking.

### Security Issues

#### Access Control

You should set the following parameters on the LDAP Server to the specified values:

- default access — none
- username and password for FireWall — read/write access to branches containing VPN-1/FireWall-1 users

#### VPN-1/FireWall-1 - LDAP Server Communication

There are three alternatives for securing communication between a VPN/FireWall Module or an Account Management Client and an LDAP Server:

- 1** If the LDAP Server is SSL-enabled, the VPN/FireWall Module and the Account Management Client can use SSL to communicate with the LDAP Server.
- 2** Use a VPN (Virtual Private Network) for the communication.

- 3** Put the LDAP Server inside a network protected by VPN-1/FireWall-1.

## Damage Control

You can limit security exposure by not allowing the LDAP Server to authenticate users, and specifying only third-party authentication schemes (TACACS, RADIUS, AXENT) implemented on other machines.



**Note** – The VPN-1/FireWall-1 User Database always has priority over Account Units. It is recommended that you define network and system administrators as VPN-1/FireWall-1 users, so that they will always be able to log in to the FireWall, even if the LDAP connection is down.

## Troubleshooting

### VPN-1/FireWall-1 rejects the user's password

This might happen if the user is defined differently in the VPN-1/FireWall-1 user database, or in an Account Unit with a higher priority.

Check the **Display user's DN at login** field in the **LDAP** tab of the **Properties Setup** window (FIGURE 7-7 on page 249) and try again. The user's DN will be displayed, and you will know from where VPN-1/FireWall-1 is getting the user's password.

### User not found

Make sure that **Use LDAP Account Management** in the **LDAP** tab of the **Properties Setup** window (FIGURE 7-7 on page 249) is checked.

Using the Account Management Client, verify that the user is indeed defined on the Account Unit.

### Changes made in the Account Management Client do not affect VPN-1/FireWall-1

Changes take effect only after one of the following happens:

- the cache times out (see FIGURE 7-7 on page 249)
- the Security Policy is installed
- the User Database is downloaded (see “Database Installation” on page 167).

### Log Records do not Reach Log Data Base

FloodGate-1 and some third party products need the ELA Proxy Server to output log records to the log database. Refer to “Enabling Logging for FloodGate-1 and Third Party Products” on page 61.

# Services and Resources

---

## In This Chapter

|                                                                  |                 |
|------------------------------------------------------------------|-----------------|
| <i>Defining Services</i>                                         | <i>page 192</i> |
| <i>TCP Service Properties</i>                                    | <i>page 194</i> |
| <i>UDP Service Properties</i>                                    | <i>page 196</i> |
| <i>RPC Service Properties</i>                                    | <i>page 197</i> |
| <i>ICMP Service Properties</i>                                   | <i>page 199</i> |
| <i>User Defined (or “Other” or “Generic”) Service Properties</i> | <i>page 200</i> |
| <i>Port Range</i>                                                | <i>page 202</i> |
| <i>Service Groups</i>                                            | <i>page 202</i> |
| <i>Resources</i>                                                 | <i>page 203</i> |
| <i>URI Resources</i>                                             | <i>page 205</i> |
| <i>SMTP Resources</i>                                            | <i>page 215</i> |
| <i>FTP Resources</i>                                             | <i>page 220</i> |
| <i>Resource Groups</i>                                           | <i>page 222</i> |
| <i>List of Supported Services</i>                                | <i>page 224</i> |


## Defining Services

FireWall-1 allows you to control access to a host, not only based on the source and destination of each communication, but also according to the service requested. Services include those based on TCP, UDP, RPC, and other protocols. Before you can use a service in a Rule Base, you must define its properties.

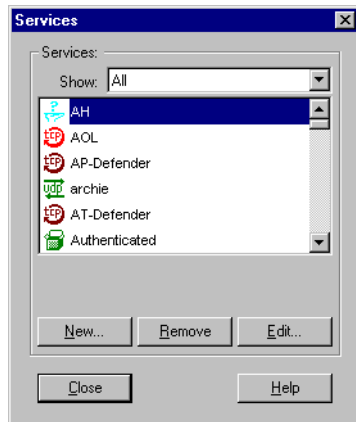


**Note** – For a list of services supported out-of-the-box by VPN-1/FireWall-1, see “List of Supported Services” on page 224.

To display the **Services** window (FIGURE 6-1),

- choose **Services** from the **Manage** menu, *or*
- click on  in the toolbar.

The listbox displays all currently defined services of the type in the **Show** box.



**FIGURE 6-1** Services window

To view the properties defined for any existing service, double-click on its icon or name in the listbox, or select the service and click on **Edit**.



## ▼ Creating a New Service

To create a new service, click on **New**. A menu appears (FIGURE 6-2), listing the types of services you can create:



**FIGURE 6-2** Add Service Object menu

Choose a service type from the menu. A window appears prompting you to enter the properties of the selected service type.

**TABLE 6-1** Service Object Types

| to create an object of type .... | see                                                                     |
|----------------------------------|-------------------------------------------------------------------------|
| TCP                              | "TCP Service Properties" on page 194                                    |
| UDP                              | "UDP Service Properties" on page 196                                    |
| RPC                              | "RPC Service Properties" on page 197                                    |
| ICMP                             | "ICMP Service Properties" on page 199                                   |
| Other                            | "User Defined (or "Other" or "Generic") Service Properties" on page 200 |
| Group                            | "TCP Service Properties" on page 194                                    |
| Port Range                       | "Port Range" on page 202                                                |

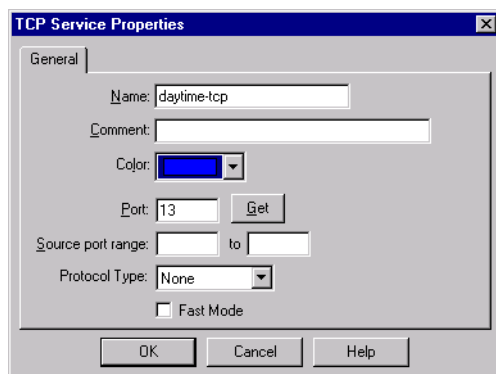
## ▼ Deleting a Service

Select the service and click on **Remove**.

## ▼ Modifying a Service

To modify an existing service, double-click on its icon or name in the listbox, or select the service and click on **Edit**.

## TCP Service Properties



**FIGURE 6-3** TCP Service properties window



**Getting Here** – To display this window, choose **Manage>Services** in the menu, and in the **Services** window (FIGURE 6-1 on page 192):

- click on **New** to define a new service and select **TCP** from the menu (FIGURE 6-2 on page 193), or
- select a service and click on **Edit** (to edit the properties of an existing service).

**Name** — the service's name

The name assigned here should be identical to the service name (as it appears in the `services` file, so that VPN-1/FireWall-1 will be able to retrieve some properties automatically. If NIS is being used, VPN-1/FireWall-1 will automatically retrieve the information from the NIS.

**Comment** — descriptive text

This text is displayed on the bottom of the **Services** window when this service is selected.

**Color** — the color of the service's icon

Select the desired color from the drop-down list.

**Port** — number of the port used to provide this service

If the port number is omitted, VPN-1/FireWall-1 will attempt to resolve the port number (based on the service's name) when the Security Policy is installed. If resolution fails, an error message is issued and the Security Policy installation will fail.

**TABLE 6-2** Specifying a Port Number

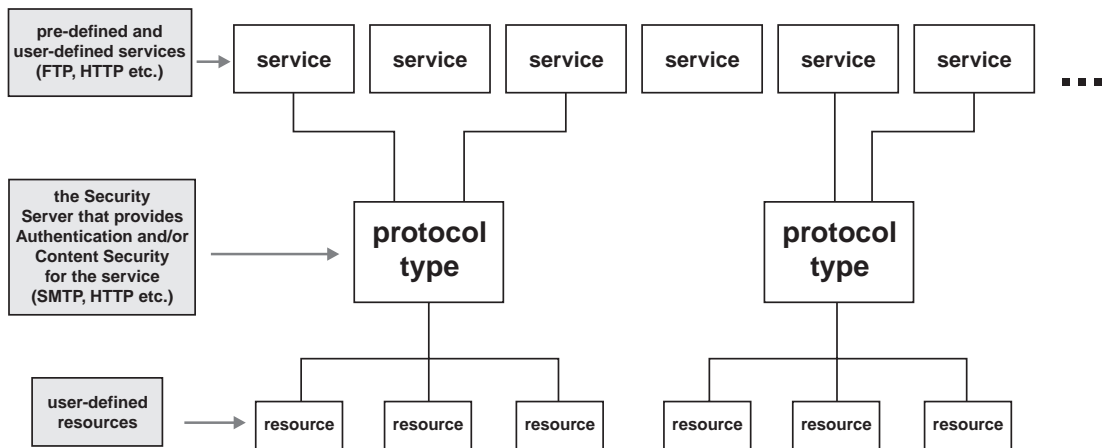
| to specify ...                               | ... type                                            | example |
|----------------------------------------------|-----------------------------------------------------|---------|
| a port number                                | the port number                                     | 805     |
| a range of port numbers                      | the lower and upper limits, separated by a hyphen   | 800-899 |
| all port numbers greater than a given number | > followed by the largest port number not included  | > 799   |
| all port numbers smaller than a given number | < followed by the smallest port number not included | < 800   |

**Source Port Range** — You may specify a range of port numbers available on the client side of the service.

If specified, only those source port numbers will be Accepted, Dropped, or Rejected when inspecting packets of this service. Otherwise, source port number is not inspected.

**Protocol Type** — specifies which protocol type is associated with the service, and by implication, the Security Server that enforces Content Security and Authentication for the service.

FIGURE 6-4 depicts the relationship between services, protocol types and resources.



**FIGURE 6-4** Services, Protocol Types and Resources

For additional information, see Chapter 11, “Security Servers and Content Security” and Chapter 15, “Authentication”.

**Fast Mode** — Use Fast Mode for this service, which speeds inspection.

The Fast Mode option takes advantage of the fact that all non-SYN/NO-ACK packets must be part of an established TCP connection. A host receiving non-SYN/NO-ACK packets that are not part of an authorized session will consider these packets to be out of context and will require the sender to properly establish the connection by sending a SYN/NO-ACK packet.

When Fast Mode is enabled for a TCP service, VPN-1/FireWall-1 does not enter these connections in the connections table and passes all non-SYN/NO-ACK packets, increasing the connections-per-second rate. Security is not compromised because these packets are all associated with connections already allowed by VPN-1/FireWall-1.

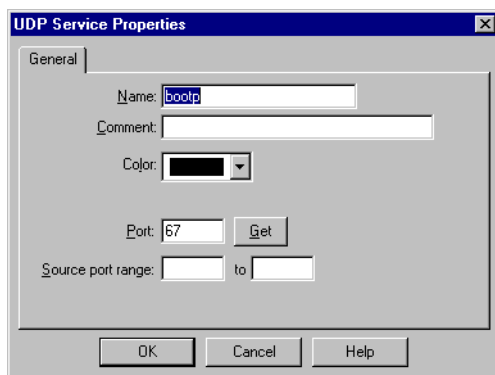
Services that open back connections (for example, FTP, VDOLive, H.323) cannot be used with **Fast Mode** enabled.

TABLE 6-3 lists the VPN-1/FireWall-1 features that cannot be used if Fast Mode is enabled.

**TABLE 6-3** VPN-1/FireWall-1 Features Incompatible with Fast Mode enabled

| feature    | reason for incompatibility                     |
|------------|------------------------------------------------|
| encryption | key information is stored in connections table |
| accounting | requires connections table                     |

## UDP Service Properties



**FIGURE 6-5** UDP Service Properties window

**Getting Here** – To display this window, choose **Manage>Services** in the menu, and in the **Services** window (FIGURE 6-1 on page 192):



- click on **New** to define a new service and select **UDP** from the menu (FIGURE 6-2 on page 193), or
- select a service and click on **Edit** (to edit the properties of an existing service).

**Name** — the service's name

The name assigned here should be identical to the service name (as it appears in the `services` file, so that VPN-1/FireWall-1 will be able to retrieve some properties automatically. If NIS is being used, VPN-1/FireWall-1 will automatically retrieve the information from the NIS.

**Comment** — descriptive text

This text is displayed on the bottom of the **Services** window when this service is selected.

**Color** — the color of the service's icon

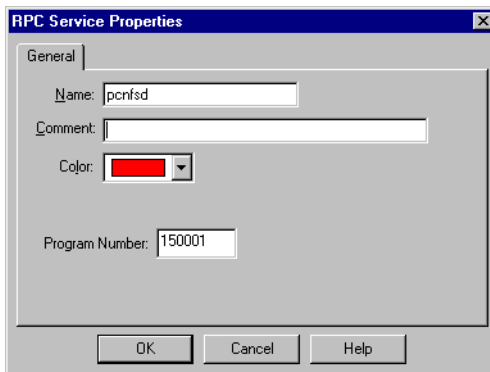
Select the desired color from the drop-down list.

**Source Port Range** — A datagram whose source port field is in this range is considered to belong to this service.

## RPC Service Properties

RPC-based services do not use pre-defined port numbers. They use (usually) UDP. Simple tracking of port numbers fails for RPC because port allocation is dynamic and often changes over time.

FireWall-1 dynamically and transparently tracks RPC port numbers using the port mappers in the system. The application information is extracted from the packet in order to identify the program used. A cache is maintained, mapping RPC program numbers to their associated port numbers in a fashion similar to that described above for UDP.



**FIGURE 6-6** RPC Service Properties

**Getting Here** – To display this window, choose **Manage>Services** in the menu, and in the **Services** window (FIGURE 6-1 on page 192):

- click on **New** to define a new service and select **RPC** from the menu (FIGURE 6-2 on page 193), or
- select a service and click on **Edit** (to edit the properties of an existing service).



FireWall-1 implements two RPC tracking strategies: passive and active:

- The passive strategy tracks portmapper requests and “sniffs” (monitors) RPC traffic, verifying port numbers against a list of valid ports.
- The active strategy is used when an application relies on prior knowledge of port numbers and initiates communication without portmapper requests. FireWall-1 monitors these applications by issuing its own requests to portmapper.

**Name** — the service’s name

The name assigned here should be identical to the server service name (as it appears in the OS files (see TABLE 6-4), so that VPN-1/FireWall-1 will be able to retrieve some properties automatically. If NIS is being used, VPN-1/FireWall-1 will automatically retrieve the information from the NIS.

**TABLE 6-4** Default File Locations and Names

| Unix          | NT                                     |
|---------------|----------------------------------------|
| /etc/services | c:\winnt\system32\drivers\etc\services |

**Comment** — descriptive text

This text is displayed on the bottom of the **Services** window when this service is selected.

**Color** — the color of the service’s icon

Select the desired color from the drop-down list.

**Program Number** — number of the RPC program to be accessed

For standard services, you can retrieve the program number from the RPC database.

If the program number is omitted, VPN-1/FireWall-1 will attempt to resolve the program number (based on the service’s name) when the rule base is installed. If resolution fails, an error message is issued and installation will fail.

## ICMP Service Properties

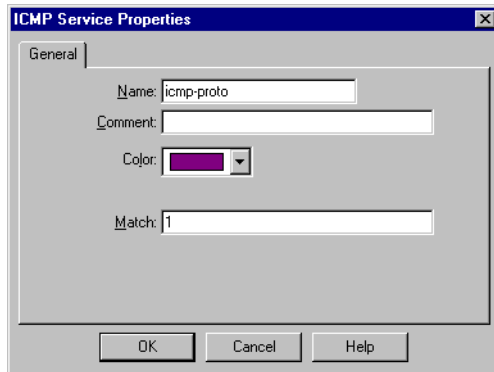


FIGURE 6-7 ICMP Service Properties window



**Getting Here** – To display this window, choose **Manage>Services** in the menu, and in the **Services** window (FIGURE 6-1 on page 192):

- click on **New** to define a new service and select **ICMP** from the menu (FIGURE 6-2 on page 193), or
- select a service and click on **Edit** (to edit the properties of an existing service).

**Name** — the service’s name

The name assigned here should be identical to the server service name (as it appears in the `services` file, so that VPN-1/FireWall-1 will be able to retrieve some properties automatically. If NIS is being used, VPN-1/FireWall-1 will automatically retrieve the information from the NIS.

**Comment** — descriptive text

This text is displayed on the bottom of the **Services** window when this service is selected.

**Color** — the color of the service’s icon

Select the desired color from the drop-down list.

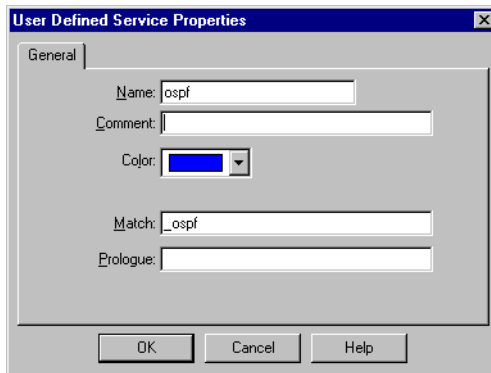
**Match** — Enter the code string (in the FireWall-1 INSPECT language) which determines whether the packet belongs to this service. The file `tcpip.def` lists some predefined components that can be used in expressions.



**Note** – ICMP Service objects require the user to be familiar with the INSPECT language. See Chapter 3, “The INSPECT Language” of *VPN-1/FireWall-1 Reference Guide* for a description of the VPN-1/FireWall-1 INSPECT language.

For an example of how to use the **Match** field, see “User-Defined Service Properties Example” on page 201.

## User Defined (or "Other" or "Generic") Service Properties



**FIGURE 6-8** User Defined Service Properties window



**Getting Here** – To display this window, choose **Manage>Services** in the menu, and in the **Services** window (FIGURE 6-1 on page 192):

- click on **New** to define a new service and select **Other** from the menu (FIGURE 6-2 on page 193), or
- select a service and click on **Edit** (to edit the properties of an existing service).

The User Defined Service Properties window allows you to create a service other than TCP, UDP or RPC.

**Name** — the service's name

The name assigned here should be identical to the server service name (as it appears in the `services` file, so that VPN-1/FireWall-1 will be able to retrieve some properties automatically. If NIS is being used, VPN-1/FireWall-1 will automatically retrieve the information from the NIS.

**Comment** — descriptive text

This text is displayed on the bottom of the **Services** window when this service is selected.

**Color** — the color of the service's icon

Select the desired color from the drop-down list.

**Match** — Enter the code string (in the FireWall-1 INSPECT language) which determines whether the packet belongs to this service (for example, `dport = telnet`).

The file `tcpip.def` lists some predefined components that can be used in expressions.

**Pre Match** — Enter a code string which determines whether the packet belongs to this service (for example, `vdolive_prematch;`).



This code string is added to the rules at the head of the Rule Base, before the Properties macros, and after the **Prologue**.

The file `$FWDIR/lib/base.def` list some predefined lists some predefined components that can be used in expressions.

**Prologue** — (optional) Add a fixed code string to the rules at the head of the Rule Base, before the Properties macros.



**Note** – User-Defined Service objects require the user to be familiar with the INSPECT language. See Chapter 3, “The INSPECT Language” of *VPN-1/FireWall-1 Reference Guide* for a description of the INSPECT language.

For an example of how to use the **Match** and **Prologue** fields, see “User-Defined Service Properties Example” below.

## User-Defined Service Properties Example

To define a user-defined service, you must enter INSPECT code in the **Match** field, so you must have at least a basic familiarity with INSPECT.

Suppose the **Match** field has the following value:

```
udp, uh_dport > 33000, ip_ttl < 30
```

To understand the meaning of the **Match** field, consider the relevant definitions in `$FWDIR/lib/base.def`:

**TABLE 6-5** Definitions in `$FWDIR/lib/base.def`

| Name     | Definition    | Meaning                  |
|----------|---------------|--------------------------|
| udp      | { ip_p = 17 } | the service is UDP       |
| uh_dport | [ 22 : 2, b]  | the UDP destination port |
| p_ttl    | [8 : 1]       | IP Time To Live          |

Since the comma operand in INSPECT means “and” the meaning of **Match** is:

- the service is UDP
- AND the destination port greater than 33000
- AND packet’s time to live is less than 30

Suppose you wish to pass IP protocol number 53, similar to ospf, egp, and bgp.

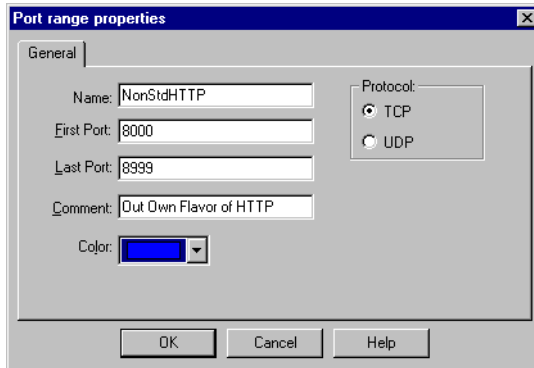
Then define a user-defined service whose **Match** field is:

```
ip_p = 53
```

The macro `ip_p` is defined in `tcpip.def` and its meaning is “the IP protocol.”

## Port Range

A Port Range object is a range of port numbers, used in Address Translation.

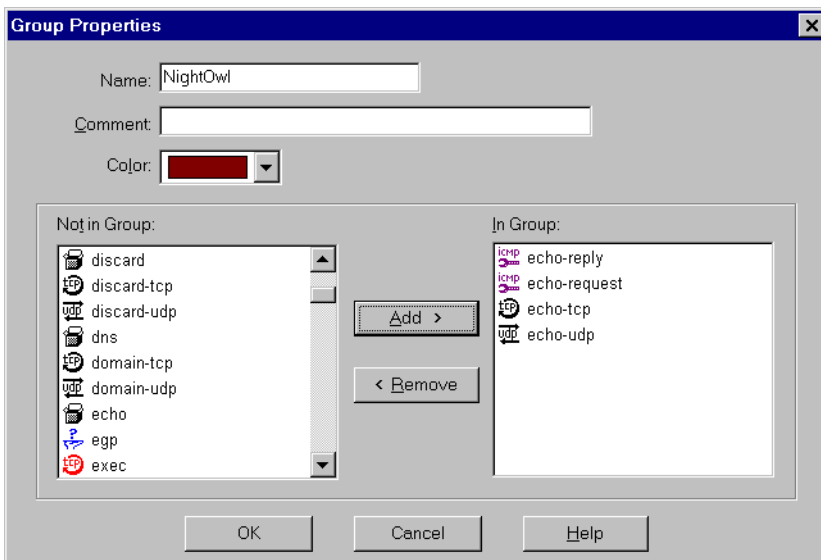


**FIGURE 6-9** Port Range Properties window

For information about VPN-1/FireWall-1’s Address Translation feature, see Chapter 14, “Network Address Translation.”

## Service Groups

If you choose **Group**, the **Group Properties** window (FIGURE 6-10) is displayed.



**FIGURE 6-10** Group Properties window

**Name** — the group’s name

**Comment** — descriptive text

This text is displayed on the bottom of the **Services** window when this group is selected.

**Color** — the color of the user's icon

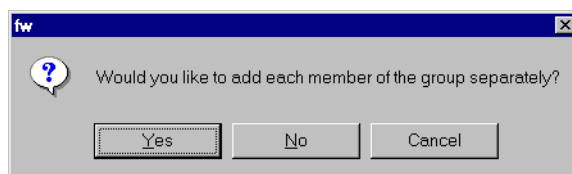
Select the desired color from the drop-down list.

## Adding a service to a group

In the left listbox (labeled **Not in Group**), select the users or groups you wish to include in the group and click on **Add**.

You can add a group to another group in one of two ways:

- 1** You can individually add all the users in one group to another group, without nesting. Click on **Yes** in reply to the question in the window (FIGURE 6-11).
- 2** You can nest groups inside groups to create a group hierarchy of any desired complexity. Click on **No** in reply to the question in the window.



**FIGURE 6-11** Adding a Group to a Group

## Deleting a service from a group

Select the services to be deleted from the right listbox (labeled **In Group**), and then click on **Remove**.

# Resources

## Overview

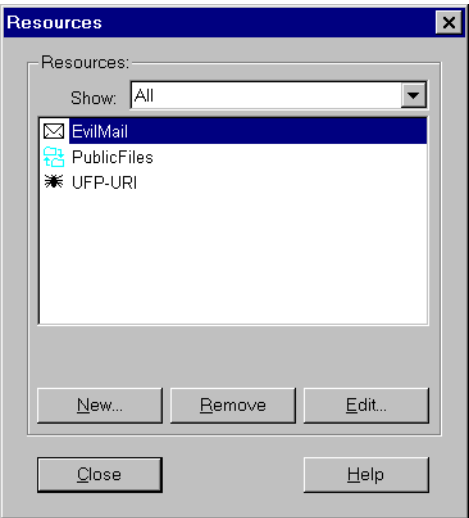
Content Security is enabled by a VPN-1/FireWall-1 object of type Resource. A VPN-1/FireWall-1 Resource specification defines a set of entities which can be accessed by a specific protocol. You can define a VPN-1/FireWall-1 Resource based on HTTP, FTP and SMTP.

VPN-1/FireWall-1 provides content security for HTTP, FTP and SMTP connections, using the VPN-1/FireWall-1 Security Servers. For each connection established through the VPN-1/FireWall-1 Security Servers, the Security Administrator is able to control specific access according to fields that belong to the specific service: URLs, file names, FTP PUT/GET commands, type of requests and more.

For detailed information about VPN-1/FireWall-1's Content Security feature, see Chapter 11, "Security Servers and Content Security."


## Resource Windows

You can define resources and groups of resources in the **Resources** window.



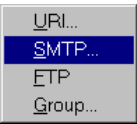
**FIGURE 6-12** Resources window

To display the **Resources** window,

- select **Resources** from the **Manage** menu, *or*
- click on  in the toolbar.

## Creating a New Resource

To create a new resource, click on **New**. A menu is displayed (FIGURE 6-13), from which you must select the type of resource you wish to create.



**FIGURE 6-13** Resource Type menu

**TABLE 6-6** Resource Types

| to create a resource of type ... | ... see ...                   |
|----------------------------------|-------------------------------|
| URI                              | “URI Resources” on page 205   |
| SMTP                             | “SMTP Resources” on page 215  |
| FTP                              | “FTP Resources” on page 220   |
| Group                            | “Resource Groups” on page 222 |

## Modifying a Resource

To modify an existing resource, select it in the **Resources** window and click on **Edit**.

## Deleting a Resource

To delete an existing resource, select it in the **Resources** window and click on **Remove**.

## Wild Cards

You can use the following wild card characters when entering data in many of the fields in the **Resource Definition** windows.

**TABLE 6-7** Wild Card Usage

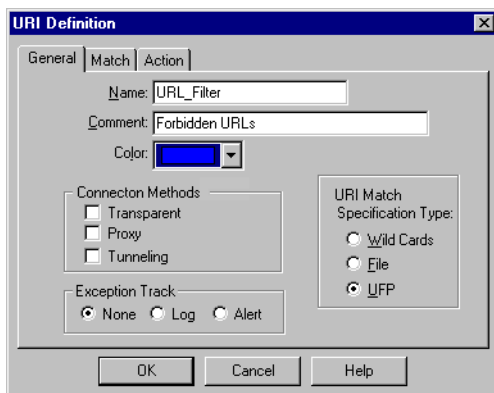
| character     | matches                                                                                                                                                                 | example                                                                                                                                                                                                      |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *             | any string of any length                                                                                                                                                | *@elvis.com matches lisa@elvis.com and priscilla@elvis.com.<br>lisa*@elvis.com matches lisamarie@elvis.com and lisa@elvis.com.<br>For file names, /elvis/*/*.c matches /elvis/marie/*.c and /elvis/lisa/*.c. |
| +             | any single character                                                                                                                                                    | mar+@elvis.com matches mary@elvis.com but not marie@elvis.com.<br>For file names, /elvis/mar+/*.c matches /elvis/mary/*.c and /elvis/mark/*.c, but not /elvis/marie/*.c.                                     |
| & (SMTP only) | The & character is used only in the translated part of a pair, and means use whatever text matched the wild card characters (*,+) in the untranslated part of the pair. | If the untranslated part is *@elvis.com and the translated part is &@buddy.com, then jerrylee@elvis.com becomes jerrylee@buddy.com.                                                                          |
| {,}           | any of the listed characters                                                                                                                                            | {a,b,c} matches a or b or c.<br>lisamarie@{elvis,michael}.com matches lisamarie@elvis.com and lisamarie@michael.com.                                                                                         |

## URI Resources

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific case.

## URI Definition window — General tab

The **General** tab of the **URI Definition** window specifies the basic parameters of a URI resource.



**FIGURE 6-14** URI Definition window — General tab

**Name** — the resource's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Resources** window when this resource is selected.

**Color** — the color of the resource's icon

Select the desired color from the drop-down list.

**Connection Methods** — check any combination of the following:

- **Transparent** — match all connections that are not in proxy mode.

This option is relevant only if a proxy to the Web browser is not defined.

- **Proxy** — match connections in proxy mode

This option is relevant only if a proxy to the Web browser is defined.

- **Tunneling** — match connections using the HTTP "CONNECT" method.

This option is relevant only if the HTTP Security Server is defined as the proxy to the Web browser.

The CONNECT method only specifies the hostname and port number to connect to. When **Tunneling** is specified, FireWall-1 does not examine the content of the request, not even the URL — only the hostname and port number are checked. Therefore, if **Tunneling** is specified, all Content Security options in the URI specification are disabled.

**Exception Track** — This option determines if an action specified in the **Action** tab (FIGURE 6-20 on page 214) that is taken as a result of a resource definition is to be logged.

For example, if the user attempts to use an unsupported scheme or method, or if a file is invalid and **CVP** in the **Action** tab is not set to **None**, then the tracking specified here is performed.

Select one of the following:

- **None** — no logging or alerting
- **Log** — log the event
- **Alert** — issue an alert

**URI Match Specification Type** — Select one of the following:

- **Wild Cards** —The URIs are described on the **Match** tab of the **Resource** window.

Under this method, many URIs are described by a single wild card. For example, the wild card **www.elvis\*** describes a large number of URIs. The URIs will be allowed or disallowed, depending on the **Action** in the rule that uses the resource.

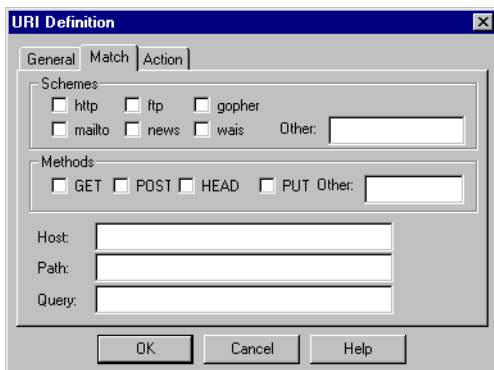
- **File** — The URIs are listed by name in the file specified the **Match** tab of the **Resource** window.

Under this method, each URI is individually listed in the given file. The URIs will be allowed or disallowed, depending on the **Action** in the rule that uses the resource. See TABLE 6-5 on page 201 for more information.

- **UFP** — A list of URIs in selected categories is provided by the server specified in the **Match** tab of the **Resource** window.

## URI Definition window — Match tab (wild cards specification)

The **Match** tab of the **URI Definition** window (wild cards specification) specifies the parameters defining a Wild Card URI resource (see “URI Definition window — General tab” on page 206).



**FIGURE 6-15** URI Definition window — Match tab (wild cards specification)

**Schemes** — the URI schemes to which this VPN-1/FireWall-1 resource applies

Select one or more of the following:

- **http** — Hypertext Transfer Protocol
- **ftp** — File Transfer Protocol
- **gopher** — Gopher
- **mailto** — SMTP
- **news** — NNTP
- **wais** — Wide Area Information Service
- **Other** — Specify another scheme here. You may use wild card characters in the specification (see “Wild Cards” on page 205).

This field is relevant only when the HTTP Security Server is defined as a proxy to the browser.

**Methods** — the HTTP method, as defined in the Hypertext Transfer Protocol. A brief explanation of each of these methods is given here.

Select one or more of the following:

**GET** — The GET method means retrieve whatever information (in the form of an entity) is identified by the URI. If the URI refers to a data-producing process, it is the produced data which is returned as the entity in the response and not the source text of the process, unless that text happens to be the output of the process.

**POST** — The POST method is used to request that the destination server accept the entity enclosed in the request as a new subordinate of the resource identified by the URI in the Request-Line. POST is usually used to provide a block of data, such as the result of submitting a form, to a data-handling process. The actual function performed by the POST method is determined by the server and is usually dependent on the URI.

**HEAD** — The HEAD method is identical to GET except that the server does not return any Entity-Body in the response. This method is often used for testing hypertext links for validity, accessibility, and recent modification.

**PUT** — The PUT method requests that the enclosed entity be stored under the supplied URI.

**Other** — Enter one of the following:

\* — If you type \*, this means all of the following: **GET**, **POST**, **HEAD** and **PUT**.

**OPTIONS** — The OPTIONS method represents a request for information about the communication options available on the request/response chain identified by the URI. This method allows the client to determine the options and/or requirements associated with a resource, or the capabilities of a server, without implying a resource action or initiating a resource retrieval.



**PATCH** — The PATCH method is similar to PUT except that the entity contains a list of differences between the original version of the resource identified by the URI and the desired content of the resource after the PATCH action has been applied.

**COPY** — The COPY method requests that the resource identified by the URI be copied to the location(s) given in the request's URI header field.

**DELETE** — The DELETE method requests that the origin server delete the resource identified by the URI.

**MOVE** — The MOVE method requests that the resource identified by the URI be moved to the location(s) given in the request's URI header field. This method is equivalent to a COPY immediately followed by a DELETE, but enables both to occur within a single transaction.

**LINK** — The LINK method establishes one or more Link relationships between the existing resource identified by the URI and other existing resources.

**UNLINK** — The UNLINK method removes one or more Link relationships from the existing resource identified by the URI. These relationships may have been established using the LINK method or by any other method supporting the Link header.

**TRACE** — The TRACE method requests that the server identified by the URI reflect whatever is received back to the client as the entity body of the response. In this way, the client can see what is being received at the other end of the request chain, and may use this data for testing or diagnostic information.

**Other** — Specify another method here. You may use wild card characters in the specification (see “Wild Cards” on page 205).

**Host** — the URI's host name

You may use wild card characters in specifying the host name (see “Wild Cards” on page 205). Functionality is dependent on the DNS setup of the addressed server.

The following restrictions apply when using wildcard characters in URI Host names:

- 1** Only the IP address or the full DNS name should be used.  
(For example: 191.81.23.\* or server.{paris,london}.com, but not {paris,london})
- 2** For expressions using a host name and port number, the port number must be explicitly specified.

For example, the expression paris\* matches requests on any port. It is recommended to restrict requests to a known HTTP server (for example, \*.paris:80, or paris:80).

**Path** — the URI's path name

You may use wild card characters in specifying the path name (see “Wild Cards” on page 205).

Path name matching is based on appending the file name in the request to the current working directory (unless the file name is already a full path name) and comparing the result to the path specified in the Resource definition.

The file path name must include the directory separator character /. For example, the request “/myfile” is matched to “/<current directory>/myfile”. If the Resource path name specifies only “myfile”, then the request will not be matched.

**Path** includes the file name (which can include wildcard characters). For example

- “/boys/bigboy/\*” includes all the files in the /boys/bigboy/ directory.
- “/boys/bigboy/” does not include any of the files in the /boys/bigboy/ directory.
- If /boys/bigboy were a file, it would be included in “/boys/bigboy/”.

When using wildcard characters, you must also specify either the full path name, or use the directory separator in the wildcard expression. For example, the path name “\*/myfile” will match “myfile” in all possible directories.



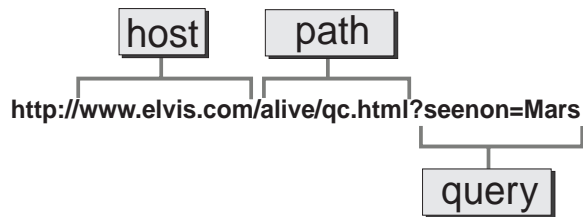
**Note** – Sometimes, the HTTP Security Server sees IP addresses instead of host names. In this case, the HTTP Security Server will attempt to reverse resolve the IP address to a host name, using reverse DNS. If the reverse DNS does not resolve correctly, the URI Resource will not match.

**Query** — the text following the ? symbol, if any

These are the parameters that are sent to the URI when it is accessed. You may use wild card characters in specifying the query text (see “Wild Cards” on page 205).

Example

For the URI shown in FIGURE 6-16, the components are listed in TABLE 6-8.



**FIGURE 6-16** URI components

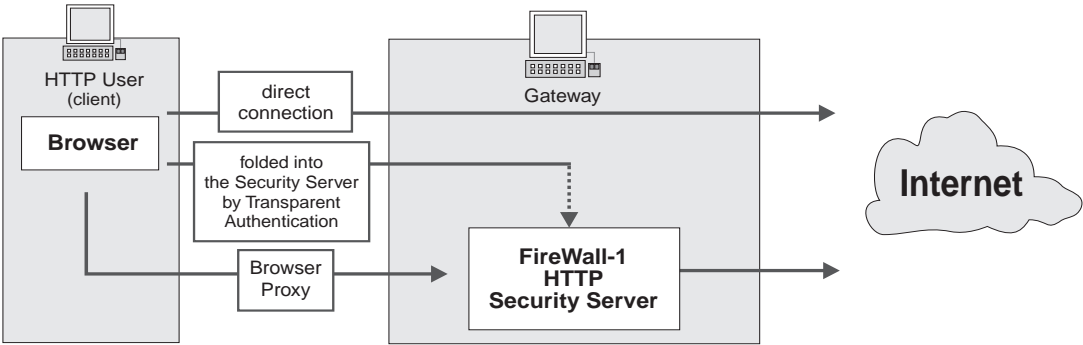
**TABLE 6-8** URI components

| component | value          |
|-----------|----------------|
| host      | www.elvis.com  |
| path      | /alive/qc.html |
| query     | seenon=Mars    |

## When Schemes Are Applied

The schemes checked in the **Schemes** field in the **Match** tab of the **URI Definition** window are not always applied.

FIGURE 6-17 shows three different ways that an HTTP browser can connect to the Internet through a FireWalled gateway (see “User Authentication and the HTTP Security Server” on page 497).



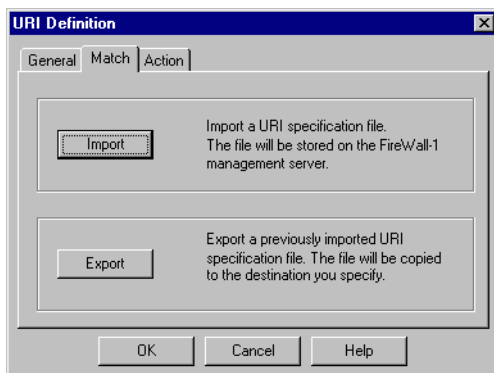
**FIGURE 6-17** HTTP Browser connecting through FireWalled Gateway

**TABLE 6-9** When Schemes Are Applied

| connection type                                                                                                                                                                                                                                                            | schemes applied     | comments                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------|
| directly, without the VPN-1/FireWall-1 HTTP Security Server                                                                                                                                                                                                                | none                | The schemes are not applied because the connection is not mediated by the VPN-1/FireWall-1 HTTP Security Server. |
| through the VPN-1/FireWall-1 HTTP Security Server, when the VPN-1/FireWall-1 HTTP Security Server is defined as the Proxy to the browser                                                                                                                                   | all checked schemes | The schemes are applied because the connection is mediated by the VPN-1/FireWall-1 HTTP Security Server.         |
| through the VPN-1/FireWall-1 HTTP Security Server, when the VPN-1/FireWall-1 HTTP Security Server is <i>not</i> defined as the Proxy to the browser, but the connection is folded into the VPN-1/FireWall-1 HTTP Security Server by the Transparent Authentication feature | HTTP only           | The schemes are applied because the connection is mediated by the VPN-1/FireWall-1 HTTP Security Server.         |

## URI Definition window — Match tab (file specification)

The **Match** tab of the **URI Definition** window (file specification) specifies additional parameters defining a URI resource.



**FIGURE 6-18** URI Definition window — Match tab (file specification)

Click on **Import** to import a URI Specification file (a list of URIs to which access will be denied or allowed, depending on the **Action** in the rule).

You will be asked to specify the file name.

Click on **Export** to export a previously imported URI Specification file.

You will be asked to specify a file name under which the file will be saved.

### URI Specification File Format

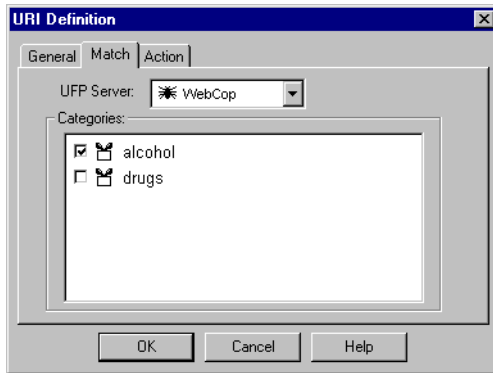
A URI Specification file is an ASCII file of records separated by \n, where each record consists of three fields, as described in TABLE 6-10. There should be no whitespace between the category and the \n. The last line in the file must also end in \n.

**TABLE 6-10** URI Specification File Format

| field             | explanation                                                         | example                                                                                          |
|-------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| IP address        | the URI's IP address                                                | 192.34.56.78                                                                                     |
| path              | the URI's path                                                      | /icecream (so it is possible to define a resource as everything under /icecream at 192.34.56.78) |
| category (in hex) | not currently used, but may not be blank, so enter "1" in all lines | 1                                                                                                |

## URI Definition window — Match tab (UFP)

The **Match** tab of the **URI Definition** window (UFP specification) specifies additional parameters defining a URI resource.



**FIGURE 6-19** URI Definition window — Match tab (UFP specification)

**Server** — Select the UFP server from the menu.

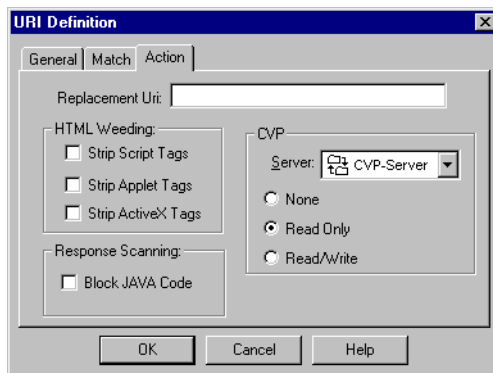
The UFP server should have already been defined in the Servers manager (see “UFP Servers” on page 320).

**Categories** — Check the categories you wish to include in the resource definition.

For information about retrieving the list of categories, see “UFP Server Properties window — Dictionary tab” on page 322.

## URI Definition window — Action tab

The **Action** tab of the **URI Definition** window specifies JAVA, ActiveX and CVP actions for a URI resource.



**FIGURE 6-20** URI Definition window — Action tab

**Replacement URI** — If the **Action** in a rule which uses this resource is **Drop** or **Reject**, then this URI is used instead of the one the user requested in the **Match** tab.

**Block JAVA Code** — If checked, JAVA applets are blocked by stripping JAVA code from incoming HTTP. JAVA applets already in the cache are not affected by this parameter.

When the HTTP Security Server encounters JAVA code in incoming HTTP, it strips the code and does not allow it to reach the browser. The user will see a message indicating that the applet cannot start (when the JAVA code is incorporated in an HTML document), or a message indicating that the document contains no data (if the JAVA code is directly fetched, that is, the link points to the class).

**Server** — Select the CVP server from the menu.

The CVP server should have already been defined in the Servers manager (see “CVP Servers” on page 322).

**CVP** — select one of the options:

- **None** - The file is not inspected.
- **Read Only** - The file is inspected by the CVP Server. If the CVP Server rejects the file, it is not retrieved.
- **Read/Write** - The file is inspected by the CVP Server. If the CVP Server detects that the file is invalid (perhaps because it contains a virus), the CVP Server corrects the file before returning it to the Inspection Module.

**HTML Weeding** — Check one of the options below to strip the specified code from the HTML page containing the reference to JAVA, JAVA Script or ActiveX code. In this way, the user will not be aware that the JAVA or ActiveX is available from the HTML page being viewed. JAVA applets already in the cache are not affected by this parameter.

Select any number of the following:

- **Strip Script Tags** — Strip JAVA Script tags from HTML code.
- **Strip Applet Tags** — Strip JAVA Applet tags from HTML code.
- **Strip ActiveX Tags** — Strip ActiveX tags from HTML code.

## SMTP Resources

### SMTP Security Server

The SMTP Security Server deals with the following conditions:

- badly formed header or pipe (send to program)

The mail is allowed but the offending field is stripped (if `smtp_rfc822 (true)` is defined under `:props` in `objects.C` — this is the default) and a warning message is sent to `asmtplib.log`.

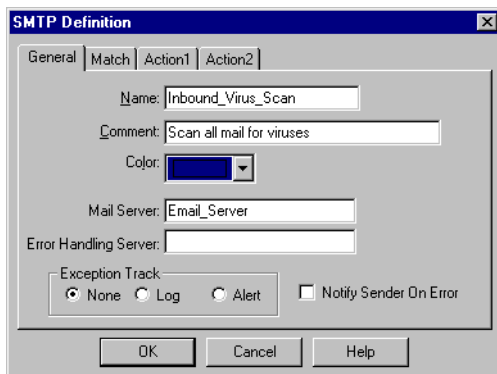
If `smtp_rfc822 (false)` is defined under `:props` in `objects.C`, the line is preserved as it is and not rewritten. A warning message is sent to `asmtplib.log`.

- source routing

If the envelope SMTP MAIL or RCPT commands contain source routing symbols, the SMTP Security Server replies with an error code.

## SMTP Definition window — General tab

The **General** tab of the **SMTP Definition** window specifies the basic parameters of an SMTP resource.



**FIGURE 6-21** SMTP Definition window — General tab

**Name** — the resource's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Resources** window when this resource is selected.

**Color** — the color of the resource's icon

Select the desired color from the drop-down list.

**Mail Server** — Mail is forwarded to this server.

If multiple servers are defined (see “Specifying Multiple Names” on page 219), then they are tried one after the other until successful.

If this field is empty, mail is forwarded to the server specified under `default_server` in `$FWDIR/conf/smtp.conf`. If this too is empty, then mail is forwarded to its original destination.

**Error Handling Server** — If **Notify Sender on Error** is checked, then:

- If **Error Handling Server** is empty, the error notification is sent to the server specified under `default_server` in `$FWDIR/conf/smtp.conf`.
- If `default_server` in `$FWDIR/conf/smtp.conf` is not specified, then the error notification is sent to the originator of the mail.

If **Notify Sender on Error** is not checked, then no error notification is generated.



If multiple servers are defined (see “Specifying Multiple Names” on page 219), then they are tried one after the other until successful.

**Exception Track** — This option determines if an action (specified in the **Action2** tab) taken as a result of a resource definition is logged.

Select one of the following:

- **None** — no logging or alerting
- **Log** — log the event
- **Alert** — issue an alert

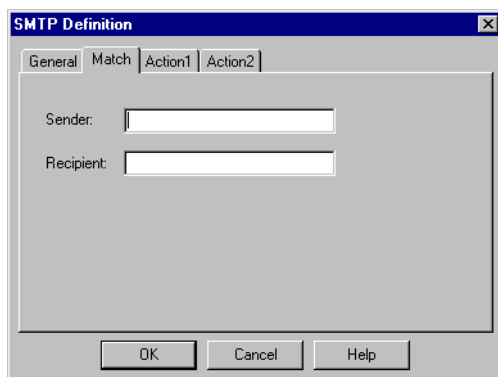
For example, if a virus is detected and **CVP** in the **Action2** tab (FIGURE 6-23 on page 218) is not set to **None**, or if the user attempts to send a message that is too long, the tracking specified here is taken.

**Notify Sender on Error** — Notify the sender if the message was not delivered.

See “Error Handling Server” on page 216 and “SMTP” on page 614.

## SMTP Definition window — Match tab

The **Match** tab of the **SMTP Definition** window specifies additional parameters defining an SMTP resource.



**FIGURE 6-22** SMTP Definition window — Match tab

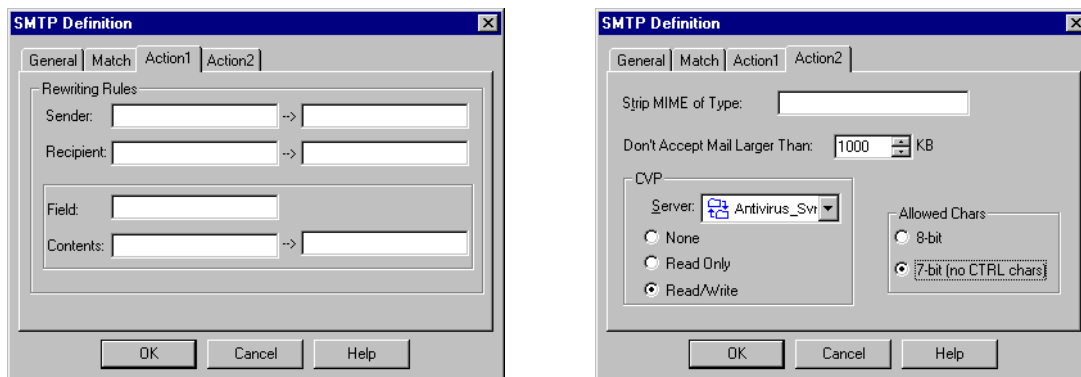
**Sender** — the From field in the envelope

**Recipient** — the To field in the envelope

You may use wild card characters in specifying these fields (see “Wild Cards” on page 205).

## SMTP Definition window — Action tabs

The **Action** tabs of the **SMTP Definition** window specify additional parameters of an SMTP resource.



**FIGURE 6-23** SMTP Definition window — Action tabs

### Action 1

This tab defines transformations to be performed on the given fields. The data in the field is modified in accordance with the defined transformation. The left part of the transformation is a match field (see “Wild Cards” on page 205). The right part specifies the form of the new transformed data. For information on specifying multiple names in some of these fields, see “Specifying Multiple Names” on page 219.

**Sender** — the **From** field in the header

You can also use the “&” wildcard character in specifying a field. For more information, see “Wild Cards” on page 205.

**Recipient** — the **To** field in the header

It’s recommended that the transformed data not include embedded spaces.

You can also use the “&” wildcard character in specifying a field. For more information, see “Wild Cards” on page 205.

**Field** — the name of a field in the SMTP header (for example, **cc** or **subject**)

**Contents** — the contents of the specified field



**Note** – Stripping fields such as **From** and **To** is discouraged, since it makes it impossible to deliver the mail message.

### Action 2

**Strip MIME of Type** — MIME attachments of the specified type will be stripped from the message.

## 1 Allowed types are (as defined in RFC 1521):

- text
- multipart
- message
- image
- audio
- video
- application

If you strip MIME of type text, the text in the body of the message is not stripped.

**Don't Accept Mail Larger Than** — Mail messages larger than this size will not be allowed to pass.

**Server** — Select the CVP server from the menu.

The CVP server should have already been defined in the Servers manager (see “CVP Servers” on page 322).

**CVP** — select one of the options:

- **None** — The file is not inspected.
- **Read Only** — The file is inspected by the CVP Server. If the CVP Server rejects the file, it is not retrieved.
- **Read/Write** — The file is inspected by the CVP Server. If the CVP Server detects that the file is invalid (perhaps because it contains a virus), the CVP Server corrects the file before returning it to the Inspection Module.

**Allowed Characters** — Select one of the following:

- **8 bit** — Allow 8 bit ASCII.
- **7 bit** — Allow only 7 bit ASCII (but no control characters).

## Specifying Multiple Names

In some fields, you can specify a list of names using the following syntax:

{name1 ,name2 }

Notes:

## 1 These rules apply to the following fields:

- **Mail Server**
- **Error Handling Server**
- **Sender**
- **Strip MIME of Type**
- **Recipient**
- **Field**
- **Contents**

- 2 There should be no whitespace before or after the names.
- 3 Write:  

```
{hostname1@domainname1,hostname2@domainname1}
```

 and not:  

```
{hostname1,hostname2}@domainname1
```
- 4 When rewriting, the number of names on the left side should be the same as the number of names on the right side. Rewrite:  

```
{name1,name2} to {newname1,newname2}
```

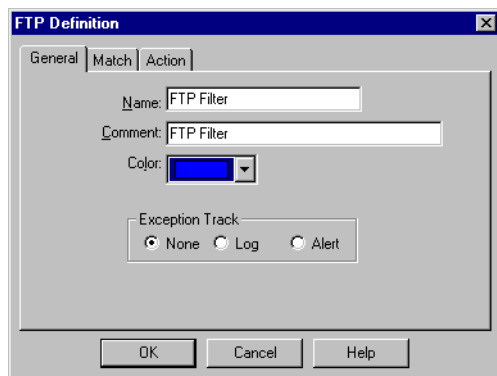
 However, if all the names of right side are to be rewritten to the same name on the left side, you can rewrite:  

```
{name1,name2} to newname1
```

## FTP Resources

### FTP Definition window — General tab

The **General** tab of the **FTP Definition** window specifies the basic parameters of an FTP resource



**FIGURE 6-24** FTP Definition window — General tab

**Name** — the resource's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Resources** window when this resource is selected.

**Color** — the color of the resource's icon

Select the desired color from the drop-down list.

**Exception Track** — This option determines if an action (specified in the **Action** tab) taken as a result of a resource definition is logged.

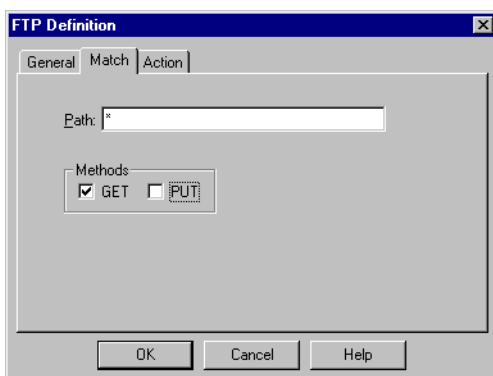
Select one of the following:

- **None** — no logging or alerting
- **Log** — log the event
- **Alert** — issue an alert

For example, if a virus is detected and **CVP** in the **Action** tab (FIGURE 6-26 on page 222) is not set to **None**, then the tracking specified here is taken.

## FTP Definition window — Match tab

The **Match** tab of the **FTP Definition** window specifies additional parameters defining an FTP resource.



**FIGURE 6-25** FTP Definition window — Match tab

**Path** — full path name of the file

File name matching is based on appending the file name in the command to the current working directory (unless the file name is already a full path name) and comparing the result to the path specified in the Resource definition.

The file path name must include the directory separator character /. For example, the FTP command “GET myfile” is matched to “/<current directory>/myfile”. If the Resource path name specifies only “myfile”, then the command “GET myfile” will not match this path.

**Path** includes the file name (which can include wildcard characters). For example

- “/boys/bigboy/\*” includes all the files in the /boys/bigboy/ directory.
- “/boys/bigboy/” does not include any of the files in the /boys/bigboy/ directory.
- If /boys/bigboy were a file, it would be included in “/boys/bigboy/”.

You may also use wildcard characters in **Path**. When using wildcard characters, you must also specify either the full path name, or use the directory separator in the wildcard expression. For example, the path name “\*/myfile” will match “myfile” in all possible directories.

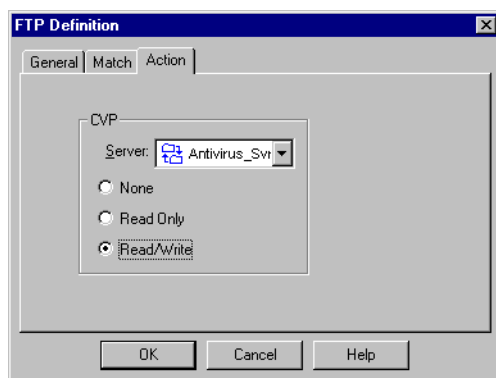
For more information on FTP file names, see Chapter 11, “Security Servers and Content Security.”

**Methods** — Select one of the following:

- **GET** — getting a file from the server to the client
- **PUT** — sending a file from the client to the server

## FTP Definition window — Action tab

The **Action tab** of the **FTP Definition** window specifies additional parameters of an FTP resource.



**FIGURE 6-26** FTP Definition window — Action tab

**Server** — Select the CVP server from the menu.

The CVP server should have already been defined in the Servers manager (see “CVP Servers” on page 322).

**CVP** — select one of the options:

- **None** - The file is not inspected.
- **Read Only** - The file is inspected by the CVP Server. If the CVP Server rejects the file, it is not retrieved.
- **Read/Write** - The file is inspected by the CVP Server. If the CVP Server detects that the file is invalid (perhaps because it contains a virus), the CVP Server corrects the file before returning it to the Inspection Module.

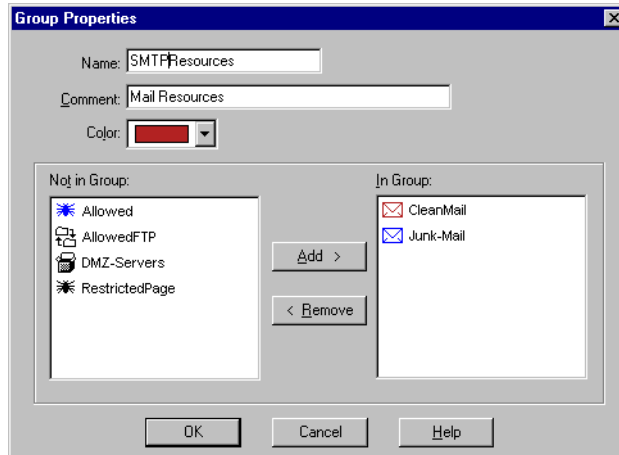
## Resource Groups

### Creating a Group

To create a new group, choose **Group** from the **Resource Type** menu (FIGURE 6-13 on page 204). The **Group Properties** window (FIGURE 6-27 on page 223) is then displayed.

## Adding a Resource or Group to a Group

To display and update a group's members, double-click on the group's name in the **Resources** window (FIGURE 6-12 on page 204). The **Group Properties** window (FIGURE 6-27) is then displayed.



**FIGURE 6-27** Group Properties window

**Name** — the group's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Resource** window when this group is selected.

**Color** — the color of the resource's icon

Select the desired color from the drop-down list.

In the left list box (labeled **Not in Group**), select the resources or groups you wish to include in the group and click on **Add**.



**Note** – You should not create resource groups of mixed types.

You can add a group to another group in one of two ways:

- 1** You can individually add all the resources in one group to another group, without nesting. Click on **Yes** in reply to the question in the window (FIGURE 6-28).

- 2 You can nest groups inside groups to create a group hierarchy of any desired complexity. Click on **No** in reply to the question in the window.

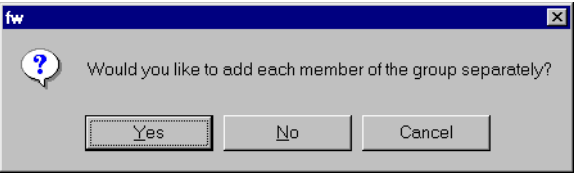


FIGURE 6-28 Adding a Group to a Group

Deleting a Resource or Group from a Group

To delete a resource or group from a group, double-click on the group’s name in the **Resources** window (FIGURE 6-12 on page 204). The **Group Properties** window (FIGURE 6-27 on page 223) is then displayed.

Select the resources or groups to be deleted from the right list box (labeled **In Group**), and then click on **Remove**.

List of Supported Services

TCP Services

TABLE 6-11 TCP Services

| Service Name            | normal port number | Description                                                                                                              | pre-defined in VPN-1/FireWall-1 | Comments                    |
|-------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------------------------|
| AOL (America OnLine)    | 5190               | protocol used by AOL clients to connect to AOL through a network connection, as opposed to a dial-up connection          | Yes                             |                             |
| chargen                 | 19                 | A TCP chargen server sends an unending stream of characters until the client terminates the connection.                  | No                              | This is also a UDP service. |
| Connected OnLine Backup | 16384              | PC agents that wake up occasionally and back up their encrypted data to the Connected backup server across the Internet. | Yes                             |                             |



**TABLE 6-11** TCP Services (continued)

| <b>Service Name</b> | <b>normal port number</b> | <b>Description</b>                                                                         | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>                                                                                                                                                                     |
|---------------------|---------------------------|--------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cooltalk            | 6499, 6500                | a voice communication protocol                                                             | Yes                                    | To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base. UDP is used for the voice connection. |
| daytime             | 13                        | A daytime server returns date and time of day in text format.                              | Yes                                    | This is also a UDP service.                                                                                                                                                         |
| discard             | 9                         | A discard server discards whatever it is sent by a client.                                 | Yes                                    | This is also a UDP service.                                                                                                                                                         |
| DNS                 | 53                        | Domain Name System — a distributed database used to map host names to IP addresses         | Yes                                    | This is also a UDP service. TCP DNS is used for Domain Name Download, while UDP DNS is used for Domain Name Queries.                                                                |
| echo                | 7                         | An echo server sends the client whatever the client sent the server.                       | Yes                                    | This is also a UDP service.                                                                                                                                                         |
| exec                | 512                       |                                                                                            | Yes                                    | see “rexec” on page 228                                                                                                                                                             |
| finger              | 79                        | a protocol that provides information about users on a specified host                       | Yes                                    |                                                                                                                                                                                     |
| ftp                 | 21                        | File Transfer Protocol — a protocol for copying files between hosts                        | Yes                                    | To enable auxiliary data connections, check <b>Enable FTP PORT Data Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.                               |
| gopher              | 70                        | a menu driven front end to other Internet services, such as Archie, anonymous FTP and WAIS | Yes                                    |                                                                                                                                                                                     |
| http                | 80                        | HyperText Transfer Protocol — a protocol used to implement the World Wide Web              | Yes                                    |                                                                                                                                                                                     |
| https               | 443                       | a version of HTTP that uses SSL for encryption                                             | Yes                                    |                                                                                                                                                                                     |

**TABLE 6-11** TCP Services (continued)

| Service Name | normal port number | Description                                                                         | pre-defined in VPN-1/FireWall-1 | Comments                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|--------------------|-------------------------------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H.323        | 1720               | client-to-client audio-visual application                                           | Yes                             | To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.<br><br>■ H.225 static connection sets up H.245 dynamic connection on dynamic TCP port, which opens two dynamic UDP connections with successive port numbers (that is, if first connection ports are A and B then second connection uses A+1 and B+1).<br><br>■ NAT Support |
| ident        | 113                | a protocol used for user identification                                             | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| imap         | 143                | Internet Mail Access Protocol                                                       | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| irc          | 6670, 6680         | Internet Relay Chat — a protocol for on-line “chat” conversations over the Internet | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| kerberos     | 750                | an authentication service                                                           | Yes                             | as <i>kerberos</i><br>This is also a UDP service. The Kerberos authentication scheme is <i>not</i> supported by VPN-1/FireWall-1.                                                                                                                                                                                                                                                                                        |
| ldap         | 389                | Lightweight Directory Access Protocol (simple X500 protocol).                       | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ldap-ssl     | 636                | Lightweight Directory Access Protocol over SSL.                                     | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LiveLan      | 1720               | H.323 based applications such as LiveLAN                                            | Yes                             | see “H.323” on page 226                                                                                                                                                                                                                                                                                                                                                                                                  |
| login        | 513                |                                                                                     | Yes                             | see “rlogin” on page 228                                                                                                                                                                                                                                                                                                                                                                                                 |
| Lotus Notes  | 1352               | a proprietary Lotus protocol                                                        | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |

**TABLE 6-11** TCP Services (continued)

| <b>Service Name</b>      | <b>normal port number</b> | <b>Description</b>                                             | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|---------------------------|----------------------------------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Conferencing   |                           | a voice conferencing and remote application sharing protocol   | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Microsoft Exchange       |                           | messaging center (mail, news, users directory)                 | Yes                                    | <p>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.</p> <ul style="list-style-type: none"> <li>■ The client requests service on DCE-RPC mapper (port 135), then initiates TCP connection to port it received from mapper.</li> <li>■ experimental support</li> <li>■ You must specifically allow DCE-RPC under <b>Services</b> in the Rule Base.</li> </ul> |
| Microsoft NetMeeting     | 1503                      | voice communication (one to one or conference) and application | Yes                                    | Uses H.323.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Microsoft NetShow        | 1755                      | streaming client-server multimedia                             | Yes                                    | <p>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.</p> <ul style="list-style-type: none"> <li>■ The client sends port command to server, and the server starts UDP on that port to the client.</li> <li>■ NAT support</li> </ul>                                                                                                                           |
| Microsoft SQL Server 6.0 | 1433                      | a data replication server                                      | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Mosaic                   |                           |                                                                | Yes                                    | a group consisting of archie, ftp, gopher and http                                                                                                                                                                                                                                                                                                                                                                                                |
| nbsession                | 139                       |                                                                | Yes                                    | belongs to the NBT group                                                                                                                                                                                                                                                                                                                                                                                                                          |
| NBT                      |                           | A NetBIOS extension defining an expanded application interface | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**TABLE 6-11** TCP Services (continued)

| <b>Service Name</b> | <b>normal port number</b> | <b>Description</b>                                                                                               | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>                                                                                                                                                 |
|---------------------|---------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| netstat             | 15                        |                                                                                                                  | Yes                                    |                                                                                                                                                                 |
| nntp                | 119                       | a protocol used to transmit news                                                                                 | Yes                                    |                                                                                                                                                                 |
| ntp                 | 123                       | time protocol with synchronization — a protocol providing access over to Internet to systems with precise clocks | Yes                                    | This is also a UDP service.                                                                                                                                     |
| Open Windows        | 2000                      |                                                                                                                  | Yes                                    |                                                                                                                                                                 |
| PointCast           | 80                        | a protocol for viewing news in TV like fashion                                                                   | No                                     |                                                                                                                                                                 |
| pop2                | 109                       | Post Office Protocol — a mail protocol that allows a remote mail client to read mail from a server               | Yes                                    |                                                                                                                                                                 |
| pop3                | 110                       | Post Office Protocol — a modified version of pop2                                                                | Yes                                    |                                                                                                                                                                 |
| RAS                 |                           | Remote Access Service                                                                                            | Yes                                    |                                                                                                                                                                 |
| RealAudio           | 7070                      | a protocol for the transmission of high quality sound on the Internet                                            | Yes                                    | To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.                   |
| rexec               | 512                       | a protocol that provides remote execution facilities with authentication                                         | Yes                                    | as <i>exec</i><br>To enable stderr, check <b>Enable RSH/REXEC Reverse stderr Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.  |
| rlogin              | 513                       | remote login — a protocol that enables remote login between hosts                                                | Yes                                    | as <i>login</i><br>To enable stderr, check <b>Enable RSH/REXEC Reverse stderr Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window. |

**TABLE 6-11** TCP Services (continued)

| Service Name | normal port number | Description                                                                                                 | pre-defined in VPN-1/FireWall-1 | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|--------------------|-------------------------------------------------------------------------------------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rsh          | 514                | remote shell — a protocol that allows commands to be executed on another system                             | Yes                             | as <i>shell</i><br>To enable stderr, check <b>Enable RSH/REXEC Reverse stderr Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.                                                                                                                                                                                                                                                                                                                                      |
| SecurID      |                    | a protocol used by an authentication service product of Security Dynamics Technologies, Inc.                | Yes                             | SecurID is a group consisting of the services required to implement SecurID.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| securidprop  | 5510               | a SecurID service                                                                                           | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| smtp         | 25                 | Simple Mail Transfer Protocol — a protocol widely used for the transmission of e-mail                       | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SQLNet       | 1521, 1525         | an Oracle protocol for transmission of SQL queries                                                          | Yes                             | To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base. This service can work in two modes:<br><br><ul style="list-style-type: none"> <li>■ In the first, the client connects to the server using TCP port 1521.</li> <li>■ In the second, the client connects to a manager server on TCP 1521 or 1525. This server sends the client a new server IP and port, then the client connects to the new server.</li> </ul> |
| Sybase SQL   | > 1024             | client-server database                                                                                      | No                              | uses a static TCP port (defined in the Sybase setup) above 1024                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| TACACS+      | 49                 | an authentication protocol                                                                                  | Yes                             | as <i>TACACSplus</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| telnet       | 23                 | Telecommunications Network Protocol — a remote terminal protocol enabling any terminal to login to any host | Yes                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**TABLE 6-11** TCP Services (continued)

| <b>Service Name</b> | <b>normal port number</b> | <b>Description</b>                                                                                                   | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| time                | 37                        | a service that returns the time of day as a binary number                                                            | Yes                                    | This is also a UDP service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| uucp                | 540                       | Unix to Unix Copy                                                                                                    | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Vosaic              | 1235                      | audio and video based on VDP (Video Datagram Protocol)                                                               | Yes                                    | also uses UDP ports 61801-61821                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| VDO-Live            | 7000                      | a protocol for the transmission of high quality video on the Internet                                                | Yes                                    | To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.                                                                                                                                                                                                                                                                                                                                                                 |
| wais                | 210                       | Wide Area Information Servers — a tool for keyword searches, based on database content, of databases on the Internet | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Webtheatre          | 12468                     | live audio & video streaming                                                                                         | Yes                                    | <p>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.</p> <ul style="list-style-type: none"> <li>■ Client opens TCP port 12468 by default for control. For each media stream request there is a port command from client to server including the RTP (UDP) port the client is waiting on. The audio passes on the RTP port and the control on the RTCP port (RTCP port = RTP port + 1).</li> <li>■ NAT support</li> </ul> |
| WinFrame            | 1494                      | remote LAN access                                                                                                    | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| X11                 | 6000 – 6063               | a windowing system protocol                                                                                          | Yes                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## UDP Services

**TABLE 6-12** UDP Services

| Service Name | normal port number | Description                                                                                                                   | pre-defined in VPN-1/FireWall-1 | Comments                                                                                                                                                  |
|--------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| archie       | 1525               | a tool for keyword searches, based on file names, of files on the Internet available through FTP                              | Yes                             |                                                                                                                                                           |
| BackWeb      | 370                | a UDP service similar to PointCast                                                                                            | Yes                             | source port 371<br>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base. |
| biff         | 512                |                                                                                                                               | Yes                             |                                                                                                                                                           |
| bootp        | 67                 | Bootstrap Protocol — a protocol for booting diskless systems                                                                  | Yes                             |                                                                                                                                                           |
| chargen      | 19                 | A UPD chargen server sends a datagram containing a random number of characters in response to each datagram sent by a client. | No                              | This is also a TCP service.                                                                                                                               |
| CU-SeeMe     | 7648 – 7652        | video, audio and chat (client to client); needs video camera                                                                  | Yes                             |                                                                                                                                                           |
| daytime      | 13                 | A daytime server returns date and time of day in text format.                                                                 | Yes                             | This is also a TCP service.                                                                                                                               |
| discard      | 9                  | A discard server discards whatever it is sent by a client.                                                                    | Yes                             | This is also a TCP service.                                                                                                                               |
| dns          | 53                 | Domain Name System — a distributed database used to map host names to IP addresses                                            | Yes                             | This is also a TCP service. TCP DNS is used for Domain Name Download, while UDP DNS is used for Domain Name Queries.                                      |
| echo         | 7                  | An echo server sends the client whatever the client sent the server.                                                          | Yes                             | This is also a TCP service.                                                                                                                               |

**TABLE 6-12** UDP Services (continued)

| <b>Service Name</b> | <b>normal port number</b> | <b>Description</b>                                                                                               | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>                                                                                                                        |
|---------------------|---------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| FreeTel             | 21300, 21301              | a voice communication protocol                                                                                   | Yes                                    | To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base. |
| InternetPhone       | 22555                     | a protocol for the transmission of voice quality sound over the Internet                                         | Yes                                    |                                                                                                                                        |
| ISAKMP              | 500                       | an encryption protocol                                                                                           | Yes                                    |                                                                                                                                        |
| kerberos            | 750                       | an authentication service                                                                                        | Yes                                    | This is also a TCP service. The Kerberos authentication scheme is <i>not</i> supported by VPN-1/FireWall-1.                            |
| name                | 42                        |                                                                                                                  | Yes                                    |                                                                                                                                        |
| nbdatagram          | 138                       |                                                                                                                  | Yes                                    | belongs to the NBT group                                                                                                               |
| nbname              | 137                       |                                                                                                                  | Yes                                    | belongs to the NBT group                                                                                                               |
| nfsd                | 2049                      |                                                                                                                  | Yes                                    | belongs to the NFS group                                                                                                               |
| ntp                 | 123                       | time protocol with synchronization — a protocol providing access over to Internet to systems with precise clocks | Yes                                    | This is also a TCP service.                                                                                                            |
| OnTime              | 1622                      | client/server calendar services                                                                                  | Yes                                    |                                                                                                                                        |
| RADIUS              | 1645                      | an authentication protocol                                                                                       | Yes                                    |                                                                                                                                        |
| RAS                 |                           | Remote Access Service                                                                                            | Yes                                    |                                                                                                                                        |
| RDP                 | 259                       | an internal VPN-1/FireWall-1 protocol used for establishing encrypted sessions                                   | Yes                                    |                                                                                                                                        |
| rip                 | 520                       | Routing Information Protocol — a protocol used to implement dynamic routing                                      | Yes                                    |                                                                                                                                        |
| SecurID             |                           | a protocol used by an authentication service product of Security Dynamics Technologies, Inc.                     | Yes                                    | SecurID is a group consisting of the services required to implement SecurID.                                                           |



**TABLE 6-12** UDP Services (continued)

| <b>Service Name</b> | <b>normal port number</b> | <b>Description</b>                                                                                                 | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>                                           |
|---------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----------------------------------------------------------|
| securid-udp         | 5510                      | a SecurID service                                                                                                  | Yes                                    |                                                           |
| snmp                | 161                       | a protocol used for managing network resources                                                                     | Yes                                    | See also Chapter 18, “SNMP and Network Management Tools”. |
| snmp-read           | 161                       | read only snmp                                                                                                     | Yes                                    |                                                           |
| snmp-trap           | 162                       | a notification to the manager by SNMP of some event of interest                                                    | Yes                                    |                                                           |
| StreamWorks         | 1558                      | a protocol for the transmission of high quality video (Xing)                                                       | Yes                                    |                                                           |
| syslog              | 514                       | a protocol that allows a computer to send logs to other computer                                                   | Yes                                    |                                                           |
| TACACS              | 49                        | an authentication protocol                                                                                         | Yes                                    |                                                           |
| TFTP                | 69                        | Trivial File Transfer Protocol — a small, simple file transfer protocol used primarily in booting diskless systems | Yes                                    |                                                           |
| time                | 37                        | a service that returns the time of day as a binary number                                                          | Yes                                    | This is also a TCP service.                               |
| traceroute          | >33000                    | a TCP/IP debugging application that shows the route followed by IP packets                                         | Yes                                    |                                                           |
| who                 | 513                       | a service that provides information on who is logged on to the local network                                       | Yes                                    |                                                           |

## RPC Services

**TABLE 6-13** RPC Services

| Service Name | program number | Description                                                                                                                             | pre-defined in VPN-1/FireWall-1 | Comments                                                                 |
|--------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------|
| DCE-RPC      |                | a protocol similar to Sun RPC Portmapper                                                                                                | Yes                             | Experimental support for use with Microsoft Exchange.                    |
| lockmanager  | 100021         | a protocol used for the transmission of lock requests                                                                                   | Yes                             | as <i>nlockmgr</i>                                                       |
| mountd       | 100005         | a protocol used for the transmission of file mount requests                                                                             | Yes                             | belongs to the NFS group                                                 |
| NFS          |                | Network File System — a protocol that provides transparent file access over a network                                                   | Yes                             | a group that includes all the services that are required for NFS.        |
| nfsprog      | 100003         |                                                                                                                                         | Yes                             | belongs to the NFS group                                                 |
| NIS          |                | Network Information System — a protocol that provides a network accessible system administration database, widely known as Yellow Pages | Yes                             | NIS is a group that includes all the services that are required for NIS. |
| nisplus      | 100300         |                                                                                                                                         | Yes                             |                                                                          |
| pcnfsd       | 150001         |                                                                                                                                         | Yes                             | belongs to the NFS group                                                 |
| rstat        | 100001         | a protocol used to obtain performance data from a remote kernel                                                                         | Yes                             |                                                                          |
| rwall        | 100008         | a protocol used to write to all users in a network                                                                                      | Yes                             |                                                                          |
| ypbind       | 100007         |                                                                                                                                         | Yes                             | belongs to the NIS group                                                 |
| yppasswd     | 100009         |                                                                                                                                         | Yes                             | belongs to the NIS group                                                 |

**TABLE 6-13** RPC Services (continued)

| <b>Service Name</b> | <b>program number</b> | <b>Description</b> | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b>          |
|---------------------|-----------------------|--------------------|----------------------------------------|--------------------------|
| ypserv              | 100004                |                    | Yes                                    | belongs to the NIS group |
| ypupdated           | 100028                |                    | Yes                                    | belongs to the NIS group |
| ypxfrd              | 100069                |                    | Yes                                    | belongs to the NIS group |

## ICMP Services

**TABLE 6-14** ICMP Services

| <b>Service Name</b>                  | <b>Description</b>                                                                                                                             | <b>pre-defined in VPN-1/FireWall-1</b> | <b>Comments</b> |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----------------|
| dest-unreach                         | an ICMP message indicating that the destination is unreachable                                                                                 | Yes                                    |                 |
| source-quench                        | an ICMP message indicating that the system cannot process datagrams at the rate at which they are being received                               | Yes                                    |                 |
| info-req                             | an obsolete ICMP message                                                                                                                       | Yes                                    |                 |
| info-reply                           | an obsolete ICMP message                                                                                                                       | Yes                                    |                 |
| mask-request                         | an ICMP message requesting a diskless system's subnet mask                                                                                     | Yes                                    |                 |
| mask-reply                           | an ICMP message in reply to a mask-request message                                                                                             | Yes                                    |                 |
| param-prblm                          | an ICMP message indicating invalid data in an earlier message                                                                                  | Yes                                    |                 |
| ping:<br>echo-request,<br>echo-reply | The ping program tests whether another host is available, and measures the time between the request (echo-request) and the reply (echo-reply). | Yes                                    |                 |

**TABLE 6-14** ICMP Services (continued)

| <b>Service Name</b>           | <b>Description</b>                                                                          | <b>pre-defined<br/>in VPN-1/FireWall-1</b> | <b>Comments</b> |
|-------------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------|-----------------|
| redirect                      | an ICMP error message sent by a router in response to a misdirected datagram                | Yes                                        |                 |
| time-exceeded                 | an ICMP error message indicating routing loops or reassembly failure                        | Yes                                        |                 |
| timestamp<br>(request, reply) | ICMP messages (request and reply) enabling systems to query each other for the current time | Yes                                        |                 |

## Other IP Protocol Services

**TABLE 6-15** Other IP Protocol Services

| <b>Service Name</b> | <b>IP protocol<br/>number</b> | <b>Description</b>                           | <b>pre-defined<br/>in VPN-1/FireWall-1</b> | <b>Comments</b> |
|---------------------|-------------------------------|----------------------------------------------|--------------------------------------------|-----------------|
| egp                 | 8                             | a protocol used to implement dynamic routing | Yes                                        |                 |
| ggp                 | 3                             | a protocol used to implement dynamic routing | Yes                                        |                 |
| igrp                | 9                             | a protocol used to implement dynamic routing | Yes                                        |                 |
| ospf                | 89                            | a protocol used to implement dynamic routing | Yes                                        |                 |


# Properties Setup

---

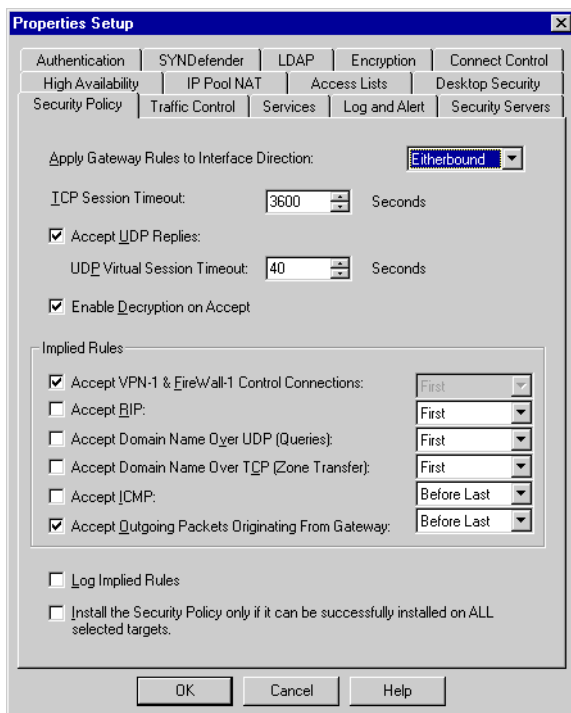
## In This Chapter

|                                  |                 |
|----------------------------------|-----------------|
| <i>Security Policy</i>           | <i>page 238</i> |
| <i>Services</i>                  | <i>page 242</i> |
| <i>Log and Alert</i>             | <i>page 243</i> |
| <i>Access Lists</i>              | <i>page 245</i> |
| <i>SYNDefender</i>               | <i>page 247</i> |
| <i>Security Servers</i>          | <i>page 248</i> |
| <i>LDAP (Account Management)</i> | <i>page 249</i> |
| <i>Authentication</i>            | <i>page 252</i> |
| <i>Encryption</i>                | <i>page 253</i> |
| <i>Connect Control</i>           | <i>page 254</i> |
| <i>High Availability</i>         | <i>page 255</i> |
| <i>IP Pool NAT</i>               | <i>page 256</i> |
| <i>Desktop Security</i>          | <i>page 257</i> |
| <i>Traffic Control</i>           | <i>page 258</i> |

A Security Policy is defined not only by the Rule Base, but also by the properties specified in the various tabs of the **Properties Setup** window. These properties enable the user to control all aspects of a communication's inspection, while at the same time freeing the user of the need to specify repetitive detail in the Rule Base.

To display the **Properties Setup** window, choose **Properties** from the **Policy** menu, or click on  in the toolbar.

## Security Policy



**FIGURE 7-1** Properties Setup window — Security Policy tab

For information about the interaction between Properties and the Rule Base, see “Interaction between Rule Base and Properties” on page 281.”

**Apply Gateway Rules to Interface Direction** — This property specifies the communication direction in which a rule will be enforced when Gateways is specified in its **Install On** column.

- **Inbound** — Enforce the Security Policy only on packets entering the gateway.

Packets will be allowed to leave the gateway only if the **Accept Outgoing Packets** property (see page 241) is checked.

- **Outbound** — Enforce the Security Policy only on packets leaving the gateway.

You can still enforce a rule in the incoming direction by choosing **Destination** under **Install On**, and specifying the gateway. You must have at least one rule like this that allows packets to enter the gateway, otherwise no packets will be allowed to enter the gateway.

- **Eitherbound** — Enforce the Security Policy on packets entering and leaving the gateway.

This is the default setting. This option gives added protection, as packets passing through the gateway are examined twice: once on the external interface and again on the internal interface.

**TCP Session Timeout** — A TCP session will be considered to have timed out after this time period.

For a detailed explanation of this parameter, see “Established TCP Connections” on page 308.

**Accept UDP Replies** — Accept reply packets in a two-way UDP communication.

A UDP communication sets up a two-way communication between the source and the destination; that is, when the communication is established between the source and the destination, a reply channel is also created between the destination and the source.

When a UDP communication is accepted on the destination and **Accept UDP Replies** is enabled, the reply channel is allowed. Only packets from the destination host going to the source host and source port are accepted as part of this communication.

- **UDP Virtual Session Timeout** — Specifies the amount of time a UDP reply channel may remain open without any packets being returned.

Since the communication is connectionless, there is no way to inform the reply channel when the communication has finished. VPN-1/FireWall-1 creates a connection context for UDP. Once the specified time has elapsed, the session is assumed to have ended and the reply channel is closed.

**Enable Decryption on Accept** — Decrypt incoming accepted packets even if the rule does not include encryption.

If this option is selected, then if a rule allows an unencrypted incoming connection, the rule will not reject the connection if it is encrypted. The motivation for this option is that encryption adds security, and a connection that would be accepted if it were not encrypted should not be rejected only because its security has been improved.

**Accept VPN-1 & FireWall-1 Control Connections** — VPN-1/FireWall-1 uses these connections for communications between FireWall daemons on different machines, and for connecting to external servers such as RADIUS, TACACS, *etc.*

If you enable this property, the fw1\_service service will be allowed between all workstations on which **VPN-1/FireWall Installed** is checked (**General** tab of the **Workstation Properties** window — see “Workstation Properties Window — General Tab” on page 102).

You can disable this option if the only FireWalled host is the Management Station and you have no external servers.



**Note** – In previous versions of VPN-1/FireWall-1, checking **Accept VPN-1 & FireWall-1 Control Connections** would allow the fw1\_service between all network objects defined in the VPN-1/FireWall-1 database. This new meaning of **Accept VPN-1 & FireWall-1 Control Connections** excludes, for example, an OPSEC server running on a machine on which VPN-1/FireWall-1 is not installed, and the `opsec_putkey` command would fail. To enable the fw1\_service for machines excluded by the new meaning, you must explicitly define a rule allowing the service.

Enabling this option opens the VPN-1/FireWall-1 daemon port and the Management Server port, allowing VPN-1/FireWall-1 GUI Clients to communicate with the Management Server. If you disable **Accept VPN-1 & FireWall-1 Control Connections** and you want VPN-1/FireWall-1 daemons to communicate with each other, you must explicitly allow these connections in the Rule Base.



**Note** – The Management Module trusts the IP addresses in the `$FWDIR/conf/gui_clients` file. This is not considered to be a security threat because the control connection is authenticated (and encrypted if the Encryption feature is installed), and anti-spoofing may be enforced.

**Accept RIP** — Accept Routing Information Protocol used by the routed daemon.

RIP maintains information about reachable systems and the routes to those systems.

**Accept Domain Name Over UDP (Queries)** — Accept Domain Name Queries used by named.

named resolves names by associating them with their IP address. If named does not know the IP address associated with a particular host name, it issues a query to the name server on the Internet. **Enable UDP Replies** must be enabled to receive the reply. Domain Name Queries are issued as needed. Make sure this property is not overridden by rules in the Rule Base.

**Accept Domain Name Over TCP (Zone Transfer)** — Allow uploading of domain name-resolving tables.

Tables of Internet host names and their associated IP addresses and other data can be uploaded from designated servers on the Internet. **Accept Established TCP Connections** must be enabled to receive a reply to a request for name-resolving tables.

**Accept ICMP** — Accept Internet Control Messages.

ICMP (Internet Control Message Protocol) is used by IP for control messages (for example, destination unreachable, source quench, route change) between systems.



The **Accept ICMP** property is set to **Before Last** to enable the user to define more detailed ICMP related rules that will be enforced before this property. If this property were **First**, then there would be no opportunity for the user to relate to ICMP in the Rule Base. If it were **Last**, then it would be enforced after the last rule (which typically rejects all packets) and would thus have no effect.

VPN-1/FireWall-1 maintains state information for ICMP. If **Accept ICMP** is enabled, VPN-1/FireWall-1 does not allow ICMP replies after one minute has passed since the corresponding ICMP request.

Enabling **Accept ICMP** does not enable ICMP Redirect. If you wish to enable ICMP Redirect, you must do so in the Rule Base.

**Accept Outgoing Packets Originating from Gateway** — Accept all outgoing packets (from the FireWall, not from the internal network).

When a packet passing through the gateway leaves the gateway, it will be allowed to pass only if one of the following conditions is true:

- The **Accept Outgoing Packets Originating from Gateway** property is checked.
- Rules are enforced both directions (eitherbound), and there is a rule which allows the packet to leave the gateway.

For additional information, see “How is a Security Policy enforced on a host’s different interfaces?” on page 625.

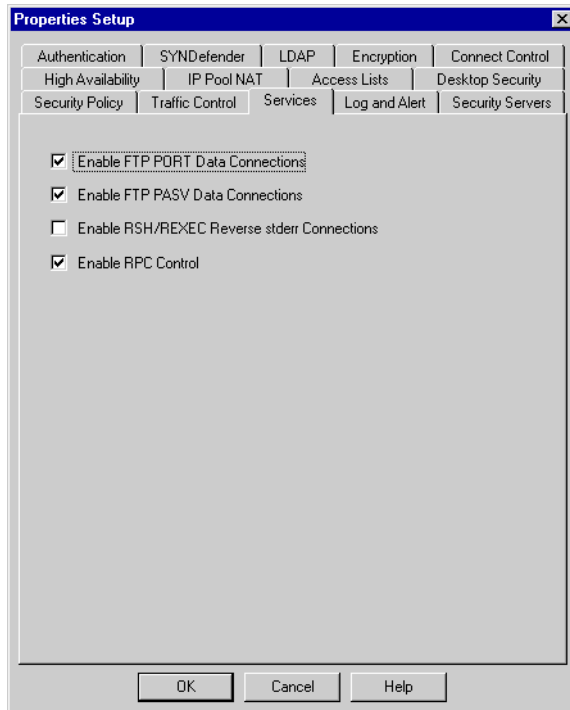
**Log Implied Rules** — Log the connections to which implied rules (the rules shown when **Implied Rules** has been selected in the **View** menu) are applied.

**Install the Security Policy only if it can be successfully installed on**

**ALL selected targets** — The Security Policy will be installed either on all selected VPN-1/FireWall-1 Version 4.1 and higher targets or on none of them.

This option enables a security administrator to ensure that the same Security Policy is being enforced at all enforcement points.

## Services



**FIGURE 7-2** Properties Setup window — Services tab

**Enable FTP PORT Data Connections** — Accept the FTP data connection of an accepted FTP control connection.

An FTP connection is established when the source (client) opens a control connection to the destination (server). After various FTP commands pass through the control connection, another connection, the data connection, may be opened to transfer files and data. When this property is enabled, the data connection from the destination to the source is allowed automatically as soon as the control connection is established. It is disabled as soon as the control connection is finished. The data connection is opened only for the port number specified in the control connection.

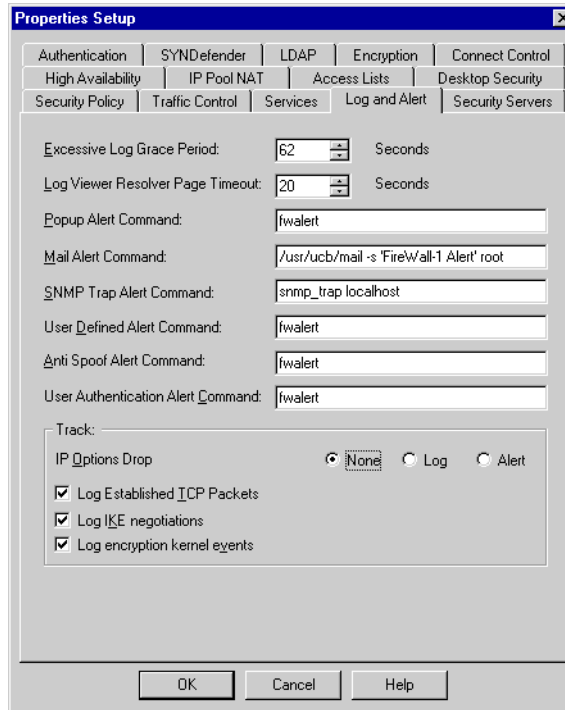
**Enable FTP PASV Connections** — Allow FTP PASV Connections.

Port numbers for FTP data connections are usually established by the FTP client binding to a random local port and then notifying the FTP server of the port number obtained. In contrast, with PASV (passive) connections, it is the server that binds to a port and then notifies the client of the port number.

**Enable RSH/REXEC Reverse stderr Connections** — Allow RSH and REXEC to open reverse connections for the `stderr` file.

**Enable RPC Control** — Enable the Inspection Module to handle the dynamic port numbers assigned by portmapper to RPC services.

## Log and Alert



**FIGURE 7-3** Properties Setup window — Log and Alert tab

**Excessive Log Grace Period** — Specifies the minimum amount of time between consecutive logs of similar packets.

Two packets are considered similar if they have the same source address, source port, destination address, and destination port; and the same protocol was used. After the first packet, similar packets encountered within the grace period will be acted upon according to the Security Policy, but only the first packet generates a log entry or an alert.

**Log Viewer Resolver Page Timeout** — After this amount of time, display the log page without resolving names and show only IP addresses.

For more information about this parameter, see Chapter 13, “Log Viewer.”

**Popup Alert Command** — Specifies the OS command (normally `$FWDIR/bin/alert`) to be executed on the Firewalled machine when an alert is issued.

It is recommended not to change this command, otherwise you may not become aware of the condition that caused the alert.

**Mail Alert Command** — Specifies the OS command(s) to be executed on the Firewalled machine when **Mail** is specified as the **Action** in a rule.

You can specify commands other than mail.

**SNMP Trap Alert Command** — Specifies the OS command to be executed on the Firewalled machine when **SNMP Trap** is specified as the **Action** in a rule.

**User Defined Alert Command** — Specifies the OS command (default is \$FWDIR/bin/alert) to be executed when **User-Defined** is specified as the **Action** in a rule.

**Anti Spoof Alert Command** — Specifies the OS command(s) to be executed (default is \$FWDIR/bin/alert) on the Firewalled machine when **Alert** is specified for Anti-Spoofing detection in the **Interface Properties** window (see “Interface Properties window — General and Security tabs” on page 105).

**User Authentication Alert Command** — Specifies the OS command(s) to be executed on the Firewalled machine when alert is specified for any of the following:

- **Authentication Failure Track** in the **Authentication** tab of the **Properties Setup** window
- **Successful Authentication Tracking** in the **General** tab of the **Client Authentication Action Properties** window.



**Note** – A message describing the event that triggered the alert is available in the command's `stdin` for all the alert commands listed above.

**IP Options Drop** — Specifies the action to take when a packet with IP Options is encountered.

VPN-1/FireWall-1 always drops these packets, but you can log them or issue an alert.

**Log Established TCP Packets** — This option controls logging TCP packets for previously established TCP connections, or packets whose connections have timed out (see “TCP Session Timeout” on page 239).

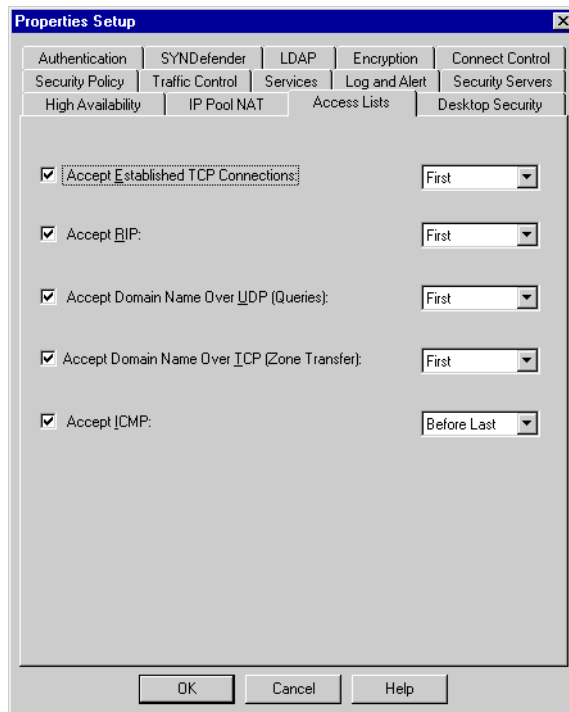
**Log IKE Negotiations** — This option controls logging IKE negotiation events.

For information about IKE events that are logged when this field is enabled, see “Properties Setup - Log and Alert” on page 104 of *Check Point Virtual Private Networks*.

**Log encryption kernel events** — This option controls logging encryption kernel events.

These events are usually errors, for example, scheme or method mismatch, checksum errors, clock synchronization mismatch, or rekey policy mismatch (SKIP).

## Access Lists



**FIGURE 7-4** Properties Setup — Access Lists tab

The **Access Lists** tab of the **Properties Setup** window is similar to the **Security Policy** tab (see “Security Policy” on page 238), but only options relevant for routers are enabled.

**Accept Established TCP Connections** — Accept packets of established TCP connections.

**Accept RIP** — Accept Routing Information Protocol used by the routed daemon.

RIP maintains information about reachable systems and the routes to those systems.

**Accept Domain Name Over UDP (Queries)** — Accept Domain Name Queries used by named.

named resolves names by associating them with their IP address. If named does not know the IP address associated with a particular host name, it issues a query to the name server on the Internet. **Enable UDP Replies** must be enabled to receive the reply. Domain Name Queries are issued as needed. Make sure this property is not overridden by rules in the Rule Base.

**Accept Domain Name Over TCP (Zone Transfer)** — Allow uploading of domain name-resolving tables.

Tables of Internet host names and their associated IP addresses and other data can be uploaded from designated servers on the Internet. **Accept Established TCP Connections** must be enabled to receive a reply to a request for name-resolving tables.

**Accept ICMP** — Accept Internet Control Message Protocol messages.

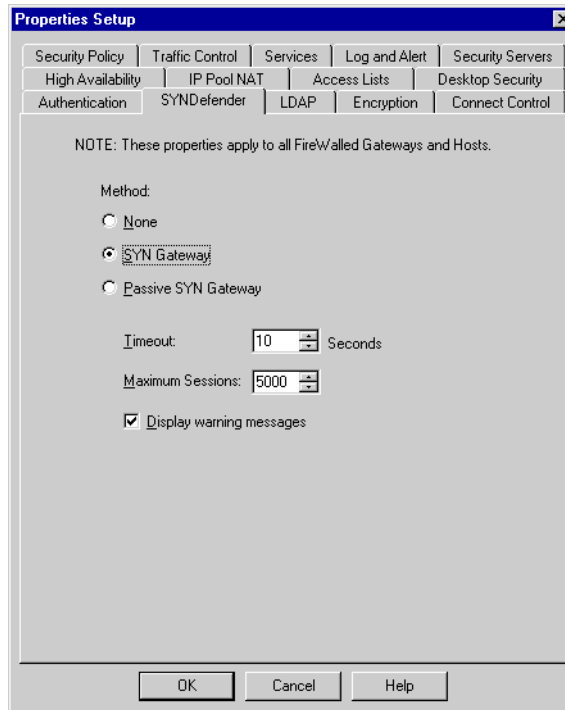
The IP on each system uses ICMP (Internet Control Message Protocol) to send control messages (for example, destination unreachable, source quench, route change) to other systems. This protocol is commonly used to assure proper and efficient operation of IP.

This property is set to **Before Last** to enable the user to define more detailed ICMP related rules that will be enforced before this property. If this property were **First**, then there would be no opportunity for the user to relate to ICMP in the Rule Base. If it were **Last**, then it would be enforced after the last rule (which typically rejects all packets) and would thus have no effect.

Enabling this option does not enable ICMP Redirect. If you wish to enable ICMP Redirect, you must do so in the Rule Base.

# SYNDefender

The **SYNDefender** tab of the **Properties Setup** window defines the parameters of the VPN-1/FireWall-1 SYNDefender feature, which protects against SYN attacks.



**FIGURE 7-5** Properties Setup window — SYNDefender tab

For information about SYNDefender, see “What is the TCP SYN Flooding Attack?” on page 617.

**Method** — Choose one of the following:

- **None** — SYNDefender is not deployed.  
If you choose this option, your network will not be protected from SYN attacks.
- **SYN Gateway** — Deploy the SYN Gateway method.
- **Passive SYN Gateway** — Deploy the Passive SYN Gateway method.

**Timeout** — Specifies how long SYNDefender waits for an acknowledgment before concluding that the connection is a SYN attack.

**Maximum Sessions** — Specifies the maximum number of protected sessions.

This number specifies the number of entries in an internal connection table maintained by SYNDefender. If the table is full, SYNDefender will not examine new connections.

If you change this value, the new value will take effect as follows:

- IBM AIX — The new value takes effect after you install the Security Policy, stop and restart the FireWall/VPN Module.
- on all other platforms — The new value takes effect after you install the Security Policy and reboot.

**Display Warning Messages** — If set, SYNDefender will print console messages regarding its status.

## Security Servers

**Properties Setup**

|                   |                  |                 |                  |
|-------------------|------------------|-----------------|------------------|
| High Availability | IP Pool NAT      | Access Lists    | Desktop Security |
| Authentication    | SYNDefender      | LDAP            | Encryption       |
| Connect Control   | Security Policy  | Traffic Control | Services         |
| Log and Alert     | Security Servers |                 |                  |

Telnet Welcome Message File:

FTP Welcome Message File:

Rlogin Welcome Message File:

Client Authentication Welcome File:

SMTP Welcome Message:

HTTP Next Proxy: Host:  Port:

HTTP Servers:

| Logical Name | Host | Port | Reauthentication |
|--------------|------|------|------------------|
|              |      |      |                  |

New... Edit Remove

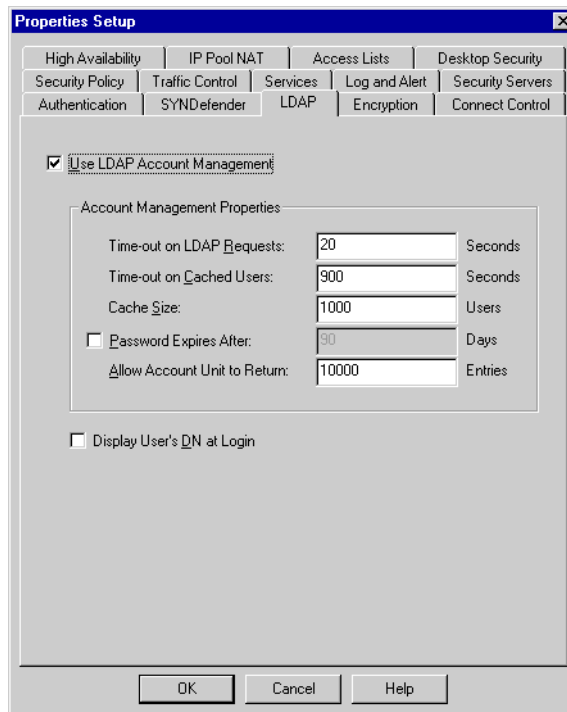
OK Cancel Help

**FIGURE 7-6** Properties Setup window — Security Servers tab

For information about Security Servers, see “Security Servers” on page 341.



## LDAP (Account Management)



**FIGURE 7-7** Properties Setup window — LDAP tab

The **LDAP** tab defines the properties related to communications with LDAP Servers (see “VPN-1/FireWall-1 LDAP Account Management” on page 174).

**Use LDAP Account Management** — Check this field if User Authentication will use LDAP Account Units, in addition to the VPN-1/FireWall-1 internal User Database.

- If this field is checked, the other fields in the window are enabled.
- If this field is not checked, User Authentication will use only the VPN-1/FireWall-1 internal User Database.

**Time-out on LDAP Requests** — An LDAP request will be considered to have timed out after this period (specified in seconds).

**Time-out on Cached Users** — A cached user will be considered to be out-of-date after this period (specified in seconds), and will be fetched again from the LDAP Server.

**Cache Size (Users)** — This field specifies the number of users that will be cached.

The cache is FIFO (first-in, first-out). When a new user is added to a full cache, the first user is deleted to make room for the new user. VPN-1/FireWall-1 does not query the LDAP Server for users already in the cache, unless the cache has timed out.

**Password Expires After** — The number of days for which a user's password is valid.

After this period has passed, the user must define a *new* password. This is not to be confused with the case when the user is asked to re-authenticate after an FWZ SecuRemote connection has been open for a certain period of time. The re-authentication period is defined in the **FWZ Encryption** window (see "FWZ Properties" on page 136 of *Check Point Virtual Private Networks*).



**Note** – This field does not apply IKE pre-shared secrets and certificates, which do not expire.

If a user's password is modified using a tool other than the Check Point Account Management Client, `fw1pwdLastMod` attribute is not updated, and the new password will expire on the day the old one would have expired.

To specify that a password never expires, set **Password Expires After** to 0 (zero) days.

### Example

Suppose that for user Alice, **Days before Password Expires** is 15. On January 1<sup>st</sup>, Alice modifies her password using the Check Point Account Management Client. `fw1pwdLastMod` is set to January 1<sup>st</sup>, so her password will expire on January 16<sup>th</sup>.

Suppose that on January 10<sup>th</sup>, Alice modifies her password again.

- If she uses the Check Point Account Management Client to modify her password, then:
  - `fw1pwdLastMod` is changed to January 10<sup>th</sup>.
  - Her new password is valid for 15 days from January 10<sup>th</sup>, and will expire on January 26<sup>th</sup>.
- If she uses a different LDAP Client to modify her password, then:
  - `fw1pwdLastMod` is not changed, and is still January 1<sup>st</sup>.
  - Her new password is valid for 15 days from January 1<sup>st</sup>, and will expire on January 16<sup>th</sup>.

When an user defined on an LDAP Account Unit enters a password, VPN-1/FireWall-1 checks whether the password has expired. If the password has expired, the user is prompted to enter a new password.

The new password must be different from the old one, and must also satisfy the following conditions :

- minimum length
- minimum number of lowercase letters (a-z)
- minimum number of uppercase letters (A-Z)
- minimum number of symbols (non-letters and non-numbers)
- minimum number of digits (0-9)

The default values for these conditions are given in the `objects.C` file by the following parameters (the default setting is in parenthesis):

```
:props (
:psswd_min_length (0)
:psswd_min_num_of_lowercase (0)
:psswd_min_num_of_uppercase (0)
:psswd_min_num_of_symbols (0)
:psswd_min_num_of_numbers (0)
```

**Allow Account Unit to Return** — This field specifies the number of users that the Account Unit may return in response to a single query.

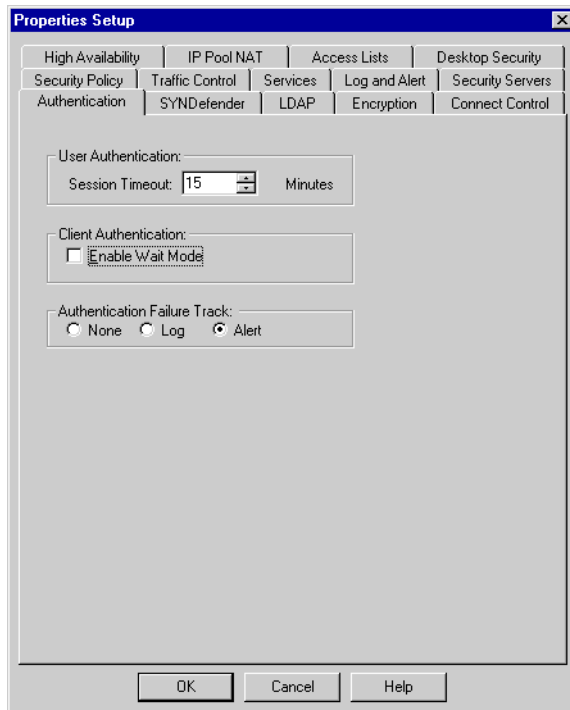
**Display user's DN at login** — If checked, then when an LDAP user logs in, his or her DN will be displayed before he or she is prompted for a password.

This property is a useful diagnostic tool when there is more than one user with the same name in an Account Unit. In this case, the first one is chosen and any others are ignored. If this property is enabled, the user can verify that the correct entry is being used.



**Note** – A user can log in either with a user name or with a DN.

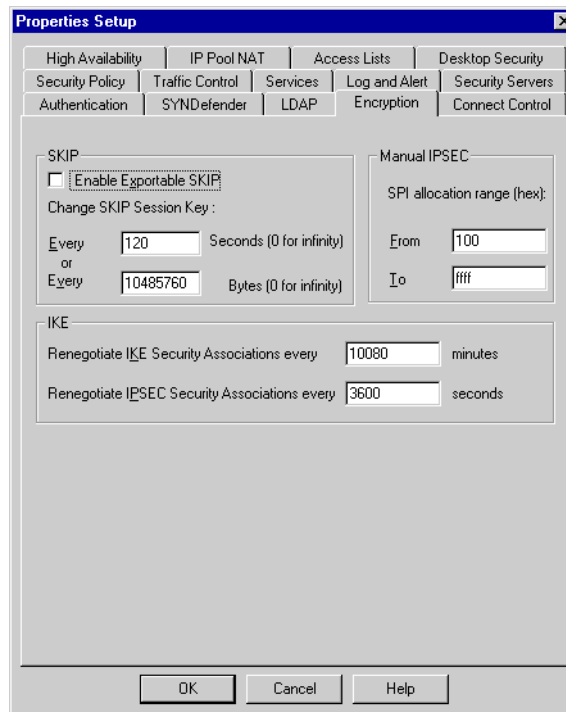
## Authentication



**FIGURE 7-8** Properties Setup — Authentication tab

For information about authentication, see Chapter 15, “Authentication.”

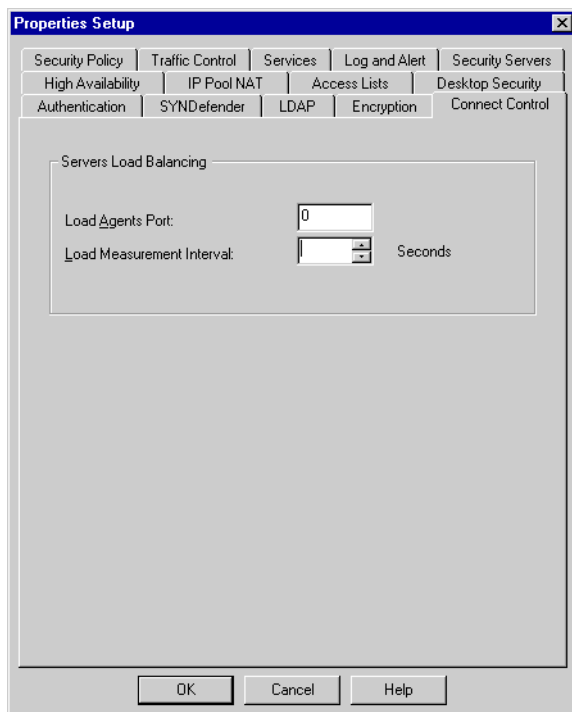
# Encryption



**FIGURE 7-9** Properties Setup — Encryption tab

For information about encryption, see *Check Point Virtual Private Networks*.

## Connect Control



**FIGURE 7-10** Properties Setup — Connect Control tab

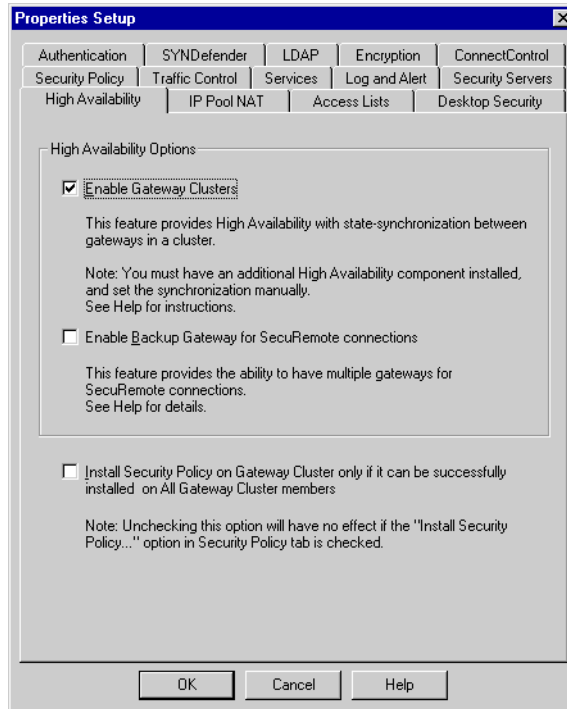
### Server Load Balancing Parameters

**Load Agents Port** — the port on which the Load Measurement Agent communicates

**Load Measurement Interval** — the intervals at which the Load Measuring Agent measures the load

For more information about these parameters, see “Server Load Balancing” on page 581.

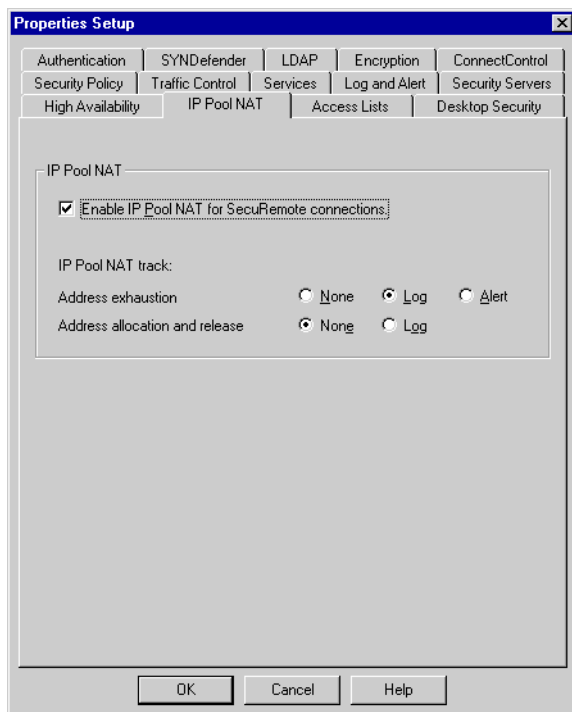
## High Availability



**FIGURE 7-11** Properties Setup — High Availability tab

See Chapter 12, “High Availability for Encrypted Connections” of *Check Point Virtual Private Networks* for information about these parameters.

## IP Pool NAT

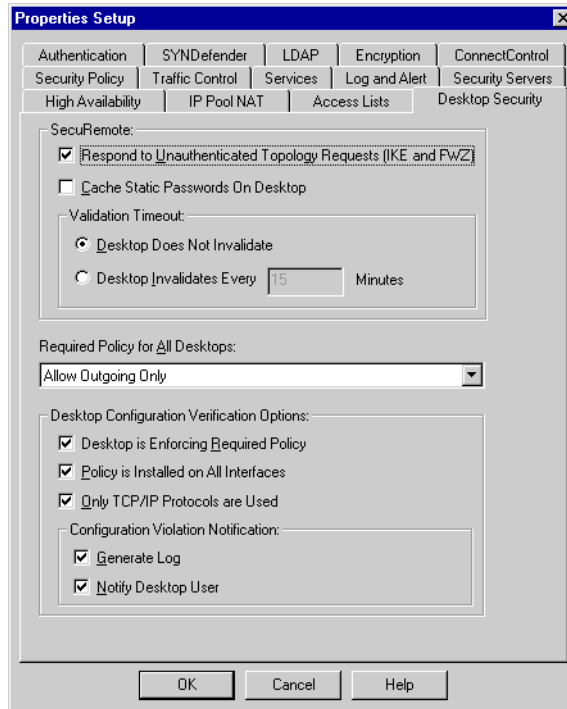


**FIGURE 7-12** Properties Setup window — IP Pool NAT tab

For information about the **IP Pool NAT** tab, see “IP Pools” on page 249 of *Check Point Virtual Private Networks* for information about these parameters.



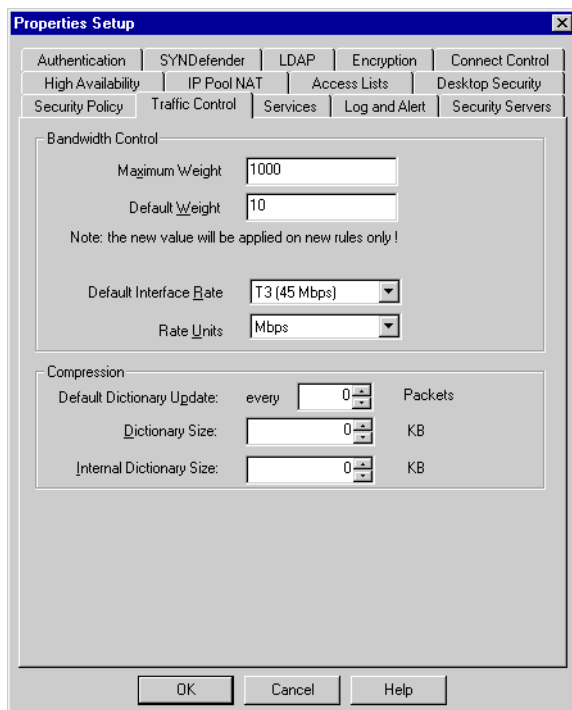
## Desktop Security



**FIGURE 7-13** Properties Setup window — Desktop Security tab

For information about the **Desktop Security** tab, see Chapter 11, “VPN-1 SecureClient” of *Check Point Virtual Private Networks*.

## Traffic Control



**FIGURE 7-14** Properties Setup window — Traffic Control tab

### Bandwidth Control

**Maximum Weight** — the maximum rate that can be assigned to a rule

**Default Weight** — the default rate assigned to a new rule and to **Default** rules

**Default Interface Rate** — the default bandwidth capacity for interfaces

**Rate Units** — the unit specified by default for transmission rates

### Compression



**Note** – The compression feature is not available in this release.

**Default Dictionary Update: every** — the frequency (in number of packets) with which the dictionary is updated

**Dictionary Size** — the size of the transmitted dictionary

**Internal Dictionary Size** — the size of the internal dictionary



# Security Policy Rule Base

---

## In This Chapter

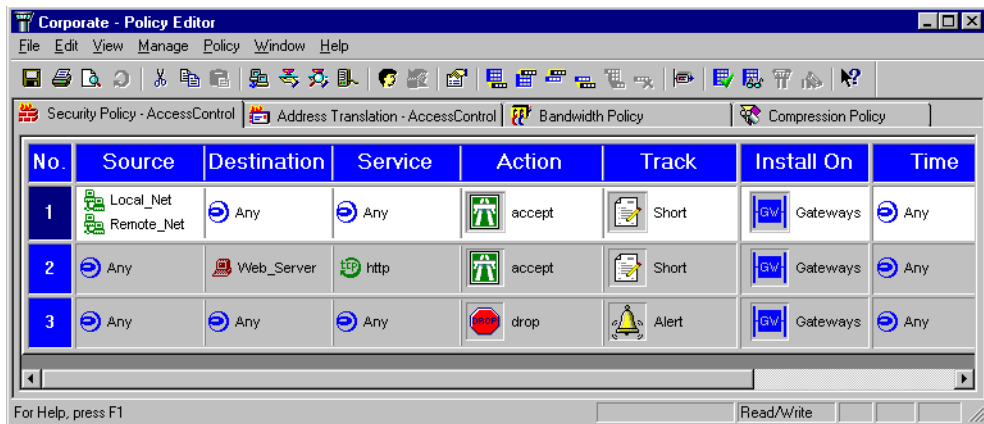
|                                                        |                 |
|--------------------------------------------------------|-----------------|
| <i>Rule Base — Basic Concepts</i>                      | <i>page 261</i> |
| <i>Editing a Policy</i>                                | <i>page 263</i> |
| <i>Masking Rules</i>                                   | <i>page 283</i> |
| <i>Querying the Rule Base</i>                          | <i>page 288</i> |
| <i>Disabling Rules</i>                                 | <i>page 298</i> |
| <i>Installing and Uninstalling the Security Policy</i> | <i>page 298</i> |
| <i>Installing Access Lists</i>                         | <i>page 302</i> |
| <i>Default Security Policy</i>                         | <i>page 305</i> |
| <i>Auxiliary Connections</i>                           | <i>page 307</i> |
| <i>Established TCP Connections</i>                     | <i>page 308</i> |

## Rule Base — Basic Concepts

A VPN-1/FireWall-1 Policy consists of network objects, users, services, properties and a Rule Base.

Each rule in a Rule Base defines the packets that match the rule (based on **Source**, **Destination** and **Service** and the **Time** at which the packet is inspected by the FireWall or Inspection Module enforcing the rule). The first rule that matches a packet is applied, and the specified **Action** is taken. The communication may be logged or an alert may be issued, depending on the value of the **Track** field.

VPN-1/FireWall-1 follows the principle “That Which Is Not Expressly Permitted is Prohibited.” To enforce this principle, VPN-1/FireWall-1 implicitly adds a rule at the end of the Rule Base that drops all communication attempts not described by the other rules.



**FIGURE 8-1** Policy Editor window with Rule Base

The **Policy Editor** window’s title shows the name of the Security Policy currently displayed.

Depending on your license (the VPN-1/FireWall-1 features your Management Station is licensed to implement), you may see as many as four tabs in the **Policy Editor** window:

- Security Policy — Access Control

The Security Policy Rule Base is described in this chapter.

- Address Translation — Access Control

The Address Translation Rule Base is described in Chapter 14, “Network Address Translation.”

- Bandwidth Policy

The Bandwidth Policy is described in the book *Check Point FloodGate-1 Architecture and Administration*.

- Compression Policy

This feature will be implemented in a future release.

Because rules are examined sequentially for each packet, only packets not described by the earlier rules are examined by the implicit rule. However, if you rely on the implicit rule to drop these packets, there is no way to log them. In order to log these packets, you must explicitly define a “none of the above” rule, as follows:



**FIGURE 8-2** “None of the Above” Rule

If you do not explicitly define such a rule, VPN-1/FireWall-1 will implicitly define one for you, and the packets will be dropped. In no case will VPN-1/FireWall-1 allow these packets to pass. The advantage of defining such a rule explicitly is that you can then specify logging for these packets.



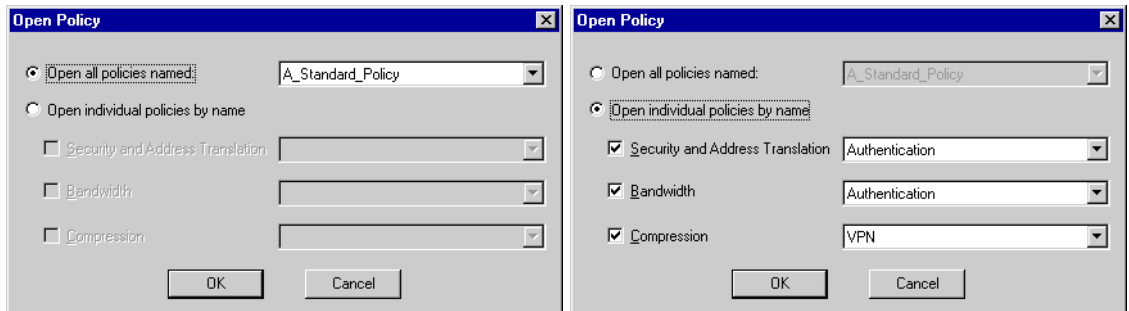
**Note** – It’s best to organize lists of objects (sources, destinations, or services) in groups rather than in long lists. Using groups will give you a better overview of your Security Policy and will lead to a more readable Rule Base. In addition, objects added to groups will be automatically included in the rules.

Logged events are recorded in the Log File. For information about the Log File, see Chapter 13, “Log Viewer.” Alerts and important system events are automatically recorded in the Log File, even when not explicitly requested by the user.

## Editing a Policy

### Opening a Policy

If the policy you wish to edit is not the one currently displayed, then choose **Open** from the **File** menu and specify the policy to open in the **Open Policy** window (FIGURE 8-3).



**FIGURE 8-3** Open Policy window

To open all the tabs of one policy, choose **Open all policies named** and then select a policy from the list.

To open individual tabs of different policies, choose **Open individual policies by name**, check the policy type and select a policy from the list. If you do not open a specific tab, then the tab of the last displayed policy continues to be displayed.



**Note** – A policy's **Security Policy** and **Address Translation** tabs are always displayed together. It is not possible to display the **Security Policy** tab of one policy and the **Address Translation** tab of another policy.

Alternatively, you can retrieve a policy installed on another VPN/FireWall Module by choosing **Open** from the **File** menu and selecting a FireWall in the **Open Policy** window (FIGURE 8-3).

To open a policy, select it from the list in **Available Security Policies**.

Select the **Security Policy** tab to display and edit the Security Policy rules. To display and edit the Address Translation rules, select the **Address Translation** tab. For information about Address Translation rules, see Chapter 14, “Network Address Translation.”

## Retrieving a Policy

To retrieve a policy installed on another VPN/FireWall Module, select the VPN/FireWall Module from the list in **Security Policies on Targets**. The policy (including all the objects defined at the time the policy was installed) will be retrieved, and you will be able to view the policy in read-only mode. You will not be able to modify the policy.

## Creating a New Policy

To create a new policy, choose **New** from the **File** menu. Use **Save As** in the **File** menu to save the Security Policy to a new file.

## Saving a Policy

When you save a policy (by choosing **Save** from the **File** menu), all the displayed tabs are saved in their own policies. For example, if you are displaying the **Security Policy** and **Address Translation** tabs of PolicyA, the **Bandwidth Policy** tab of PolicyB and the **Compression** tab of PolicyC, and choose **Save** from the **File** menu, then:

- The **Security Policy** and **Address Translation** tabs are saved in PolicyA
- The **Bandwidth Policy** tab is saved in PolicyB
- The **Compression** tab is saved in PolicyC

When you choosing **Save As** from the **File** menu, only the current tab is saved in the policy you specify. For example, if you are displaying the **Security Policy** and **Address Translation** tabs of PolicyA, the **Bandwidth Policy** tab of PolicyB and the **Compression** tab of PolicyC, and choose **Save As** from the **File** menu and specify PolicyD while the current tab is the **Security Policy** tab, then:

- The **Security Policy** and **Address Translation** tabs are saved in PolicyD
- The **Bandwidth Policy** tab is not saved







- The **Compression** tab is not saved

## Adding a Rule

You can add a rule at any point in the Rule Base.

**TABLE 8-1** Adding a Rule

| To add a rule           | Select from menu             | Toolbar Button                                                                     |
|-------------------------|------------------------------|------------------------------------------------------------------------------------|
| after the last rule     | <b>Rule&gt;Add&gt;Bottom</b> |  |
| before the first rule   | <b>Rule&gt;Add&gt;Top</b>    |  |
| after the current rule  | <b>Rule&gt;Add&gt;After</b>  |  |
| before the current rule | <b>Rule&gt;Add&gt;Before</b> |  |



**Note** – The current rule is the one that is highlighted. To select a rule, click on its number.

A new rule will be added to the Rule Base, and default values will appear in all the data fields. You can modify the default values as needed.

Alternatively, right-click on the rule’s number to display the Rule menu.



**FIGURE 8-4** Rule menu

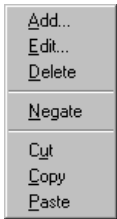
**TABLE 8-2** Rule menu items

| Menu Item                | Action                                                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Insert Rule Above</b> | Insert a rule above the current rule.                                                                                                        |
| <b>Add Rule Below</b>    | Add a rule below the current rule.                                                                                                           |
| <b>Delete Rule</b>       | Delete the current rule.                                                                                                                     |
| <b>Copy Rule</b>         | Copy the current rule to the clipboard.                                                                                                      |
| <b>Cut Rule</b>          | Delete the current rule and put it on the clipboard.                                                                                         |
| <b>Paste Rule</b>        | Paste the rule on the clipboard (a menu will be displayed where you can specify whether to paste the rule before or after the current rule). |
| <b>Hide Rule</b>         | Hide the current rule (see “Masking Rules” on page 283).                                                                                     |
| <b>Disable Rule</b>      | Disable the current rule (see “Disabling Rules” on page 298).                                                                                |

## Modifying a Rule

To modify a rule, add, modify, or delete data field values until the rule is as desired.

Right-click in the data field to open the Policy Editor Object menu (FIGURE 8-5).



**FIGURE 8-5** Policy Editor Object Menu

The choices displayed in the menu depend on the field in which you right-clicked.

**TABLE 8-3** Modifying Network Objects

| for a description of how to modify ... | ... see                   |
|----------------------------------------|---------------------------|
| <b>Source</b>                          | "Source" on page 267      |
| <b>Destination</b>                     | "Destination" on page 269 |
| <b>Service</b>                         | "Service" on page 270     |
| <b>Action</b>                          | "Action" on page 271      |
| <b>Track</b>                           | "Track" on page 273       |
| <b>Install On</b>                      | "Install On" on page 273  |
| <b>Time</b>                            | "Time" on page 275        |
| <b>Comments</b>                        | "Comments" on page 276    |

Items in the **Source**, **Destination**, **Services**, **Install On** and **Time** data fields are not exclusive. When you select one of these items, open the menu of that option. Choose the desired option: **Add**, **Delete**, **Negate** (**Negate** is not available for **Install On**).

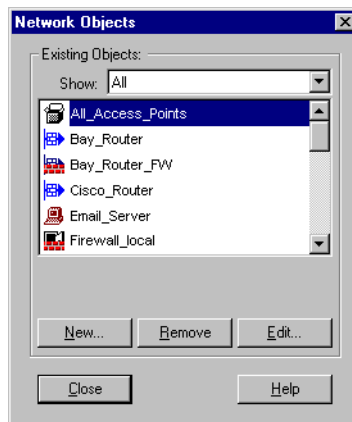


**Note** – You can view the properties of a network object or service object by double-clicking on its icon.

## Source

**Add** — The **Network Objects** window (FIGURE 8-6) is displayed, from which you can select network objects to add to the rule's **Source**.

You can define any number of items in **Source**.



**FIGURE 8-6** Network Objects window

**Add Users Access** — The **Users Access** window (FIGURE 8-7) is displayed, from which you can select user group(s) to add to the rule's **Source**.



**FIGURE 8-7** User Access window

You must choose **Add Users Access** for a rule whose **Action** is one of the following:

- Client Authentication
- Session Authentication
- User Authentication
- Client Encryption (SecuRemote)

- 1** Choose one of the user groups.
- 2** Make the appropriate choice under **Location**.

If you check **No Restriction**, then there will be no restriction on the source of the users. For example, if you choose **AllUsers** and check **No Restriction**, then **AllUsers@Any** will be inserted under **Source** in the rule.

If you check **Restrict To**, then the source will be restricted to the network object you select in the list box. For example, in FIGURE 8-7, the source object in the rule will be **AllUsers@Local\_Net**.

- 3** Click on **OK**.

**Edit** — Edit the selected object.

You must first select one of the objects already defined under **Source**. The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

Alternatively, you can double-click on an object to edit it.

**Delete** — Delete the selected object.

You must first select one of the objects already defined under **Source**.

**Negate** — Negate the selected object.

All the objects defined under **Source** will be negated. Negation means that the rule applies when the communication's **Source** is *not* one of the **Source** objects in the rule.

When more than one object is listed under **Source**, it is not possible to negate some but not others. Either all are negated or none are negated.

**Cut** — Delete the selected object and put it on the clipboard.

You must first select one of the objects already defined under **Source**.

**Copy** — Copy the selected object to the clipboard.

You must first select one of the objects already defined under **Source**.

**Paste** — Paste the object on the clipboard in the rule's **Source**.

## Destination

**Add** — The **Object Manager** window (FIGURE 8-6 on page 267) is displayed, from which you can select network objects to add to the rule's **Destination**.

You can define any number of items in **Destination**.

**Edit** — Edit the selected object.

You must first select one of the objects already defined under **Destination**. The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

Alternatively, you can double-click on an object to edit it.

**Delete** — Delete the selected object.

You must first select one of the objects already defined under **Destination**.

**Negate** — Negate the selected object.

All the objects defined under **Destination** will be negated. Negation means that the rule applies when the communication's **Destination** is *not* one of the **Destination** objects in the rule.

When more than one object is listed under **Destination**, it is not possible to negate some but not others. Either all are negated or none are negated.

**Cut** — Delete the selected object and put it on the clipboard.

You must first select one of the objects already defined under **Destination**.

**Copy** — Copy the selected object to the clipboard.

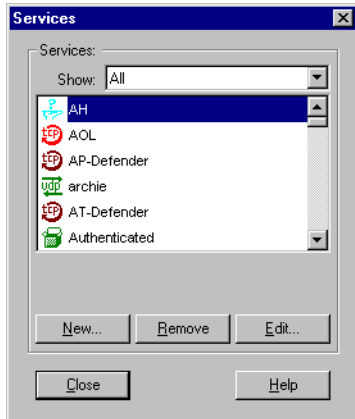
You must first select one of the objects already defined under **Destination**.

**Paste** — Paste the object on the clipboard in the rule's **Destination**.

## Service

**Add** — The **Services** window (FIGURE 8-8) is displayed, from which you can select network objects to add to the rule's **Services**.

You can define any number of items in **Services** in the rule.



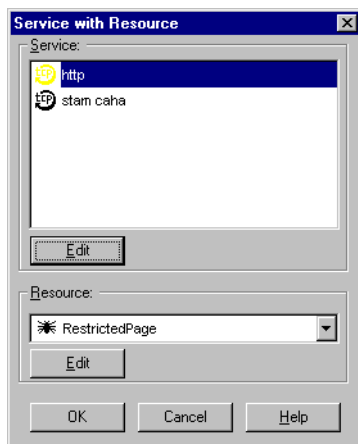
**FIGURE 8-8** Services window



**Note** – Some services must be explicitly defined in the rule, otherwise they will not function properly. For more information, see “Auxiliary Connections” on page 307.

**Add With Resource** — Add a resource.

The **Services with Resource** window (FIGURE 8-9) is displayed.



**FIGURE 8-9** Services with Resource window

For additional information about resources, see “Content Security” on page 360.

**Edit** — Edit the selected object.

You must first select one of the objects already defined under **Service**. The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

Alternatively, you can double-click on an object to edit it.

**Delete** — Delete the selected object.

You must first select one of the objects already defined under **Service**.

**Negate** — Negate the selected object.

All the objects defined under **Service** will be negated. Negation means that the rule applies when the communication's **Service** is *not* one of the services in the rule.

When more than one object is listed under **Service**, it is not possible to negate some but not others. Either all are negated or none are negated.

**Cut** — Delete the selected object and put it on the clipboard.

You must first select one of the objects already defined under **Service**.

**Copy** — Copy the selected object to the clipboard.

You must first select one of the objects already defined under **Service**.

**Paste** — Paste the object on the clipboard in the rule's **Service**.

## Action


You can only select one **Action**.

**Edit Properties** — Edit the properties of the rule's **Action**.

This choice is available for a rule whose existing **Action** is User Authentication, Client or Session Authentication, and opens the appropriate **Authentication Action Properties** window (see Chapter 15, "Authentication.")

If you wish to modify the Encryption parameters of a rule to which Encryption has been added, select **Edit Encryption** from the menu rather than **Edit Properties**.


**Add Encryption** — Add **Encryption** to the **Action** for this rule.

This choice is available for a rule whose existing **Action** is User Authentication, Client or Session Authentication, and to which Encryption has not already been added. An envelope icon () is superimposed on the existing **Action** icon in the rule.

You can modify the Encryption parameters by displaying the menu again and selecting **Edit Encryption**.

For additional information about VPN-1/FireWall-1's encryption features, see *Check Point Virtual Private Networks*.

**Remove Encryption** — Remove **Encryption** from the **Action** for this rule.

This choice is available for a rule whose existing **Action** is User Authentication, Client or Session Authentication, and to which Encryption has already been added. The envelope icon () is removed from the existing **Action** icon in the rule.









**Edit Encryption** — Edit this rule’s Encryption parameters.

This choice is available for a rule whose existing **Action** is Encrypt, and for a rule whose existing **Action** is User Authentication, or Session Client Authentication, and to which **Encryption** has already been added. The **Encryption Properties** window is displayed.

For additional information about the **Encryption Properties** window, see “Rule Encryption Properties” on page 117 of *Check Point Virtual Private Networks*.

TABLE 8-4 lists the choices available from the **Action** menu.

**TABLE 8-4** Action Menu

| Action                                                                              | Meaning                                                                      | Action                                                                              | Meaning                                                                                       |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|    | <b>Accept</b> — Accept the connection.                                       |    | <b>Client Authentication</b> — Invoke Client Authentication for this connection.              |
|    | <b>Reject</b> — Reject the connection.                                       |    | <b>Session Authentication</b> — Invoke Session Authentication for this connection.            |
|   | <b>Drop</b> — Drop the connection; do not notify the sender.                 |   | <b>Encrypt</b> — Encrypt outgoing packets. Accept incoming encrypted packets and decrypt them |
|  | <b>User Authentication</b> — Invoke User Authentication for this connection. |  | <b>Client Encryption</b> — Accept only SecuRemote communications.                             |

When a **Drop** action is taken, the sender is not notified.

TABLE 8-5 describes what happens when a **Reject** action is taken.








**TABLE 8-5** Difference between Reject and Drop

| service | Reject                                              |
|---------|-----------------------------------------------------|
| TCP     | The sender is notified.                             |
| UDP     | Sends an ICMP port unreachable error to the sender. |
| other   | Same as <b>Drop</b> .                               |



## Track

**TABLE 8-6** Track Menu

| Track                                                                              | Meaning                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                    | no logging or alerting for this communication                                                                                                                                                                                  |
|   | <b>Short Log</b> — Log in short format.                                                                                                                                                                                        |
|   | <b>Long Log</b> — Log in long format.                                                                                                                                                                                          |
|   | <b>Accounting</b> — Log in Accounting format.                                                                                                                                                                                  |
|   | <b>Alert</b> — Issue an alert (as defined in the <b>PopUp Alert Command</b> field in the <b>Logging and Alerting</b> tab of the <b>Properties Setup</b> window - see Chapter 7, “Properties Setup”).                           |
|   | <b>Mail</b> — Send a mail alert (as defined in the <b>Mail Alert Command</b> field in the <b>Logging and Alerting</b> tab of the <b>Properties Setup</b> window - see Chapter 7, “Properties Setup”).                          |
|   | <b>SNMP Trap</b> — Issue an SNMP trap (as defined in the <b>Snmp Trap Alert Command</b> field in the <b>Logging and Alerting</b> tab of the <b>Properties Setup</b> window - see Chapter 7, “Properties Setup”).               |
|  | <b>User Defined</b> — Issue a User Defined Alert (as defined in the <b>User Defined Alert Command</b> field in the <b>Logging and Alerting</b> tab of the <b>Properties Setup</b> window - see Chapter 7, “Properties Setup”). |

## Install On







The **Install On** field specifies which FireWalled objects will enforce the rule. You can select any number of **Install On** objects.

The **Install On** object is not necessarily the packet's destination, but the FireWalled object through which the packet will pass on its way to its destination.



**Note** – The entire Security Policy is installed on all of the **Install On** objects, but each object enforces only that part of the Security Policy which is relevant to it.

**TABLE 8-7** Install On Menu

| Install On                                                                        | Meaning                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Enforce on all network objects defined as gateways, in the direction specified in the <b>Apply Gateway Rules to Interface Direction</b> property in the <b>Security Policy</b> tab of the <b>Properties Setup</b> window (see Chapter 7, “Properties Setup”). |
|  | Enforce in the inbound direction on the FireWalled network objects defined as <b>Destination</b> (typically servers) in this rule.                                                                                                                            |
|  | Enforce in the outbound direction on the FireWalled network objects defined as <b>Source</b> (typically clients —initiators of traffic) in this rule.                                                                                                         |
|  | Enforce on all routers.                                                                                                                                                                                                                                       |
|  | Enforce on all Integrated FireWalls.                                                                                                                                                                                                                          |
|  | Enforce on the specified target object(s) only, in the inbound and outbound (eitherbound) directions.                                                                                                                                                         |

## Gateways

If you specify **Gateways**, the rule is enforced on all the hosts that are defined as gateways (in the **Host Properties** window). The rule is enforced in the direction specified in **Apply Gateway Rules to Interface Direction** property in the **Security Policy** tab of the **Properties Setup** window (see Chapter 7, “Properties Setup”).



**Note** – If you are enforcing a Security Policy on a gateway, there is no need for Access Lists on routers, except when you wish to protect the router itself.

A Bay Networks router can function in either of two modes: as a packet filter (in which case VPN-1/FireWall-1 installs an Access List), or as a FireWalled router (in which case VPN-1/FireWall-1 installs a Security Policy).

### Source

If you specify **Source**, the rule is enforced on the FireWalled network objects specified under **Source** in that rule. The icon for **Source** shows arrows pointing away from the object, to indicate that the rule is enforced for outgoing communications only.

For example, consider the following rule:

| Source          | Destination | Services | Action | Track     | Install On |
|-----------------|-------------|----------|--------|-----------|------------|
| mailsrvr,london | Any         | Any      | Accept | Short Log | Src        |

The rule is enforced only on london, because mailsrvr is not FireWalled. However, the rule is applied to communications originating either on mailsrvr or london.

#### Destination

If you specify **Destination**, the rule is enforced on the FireWalled network objects specified under **Destination** in that rule. The icon for **Destination** shows arrows pointing to the object, to indicate that the rule is enforced for incoming communications only.

#### Routers

If you specify **Routers**, the rule is enforced on the appropriate interfaces on all routers, using VPN-1/FireWall-1's auto-scoping feature. For example, a rule specifying **Source** as localnet is enforced on the router's localnet interface. VPN-1/FireWall-1 generates an Access List for the router (except for Bay Networks routers on which VPN/FireWall Module is installed, in which case a Security Policy is installed). It should be noted that with Access Lists only a subset of VPN/FireWall Module functionality can be implemented. For example, it is not possible to secure FTP back connections.

#### Targets

If you specify an object by name, then the rule is enforced for both incoming and outgoing communications (eitherbound).

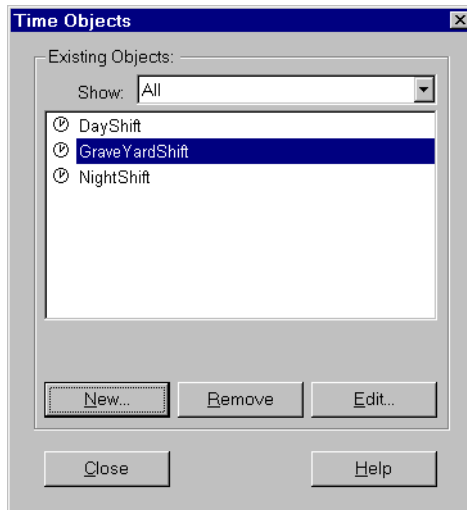
**TABLE 8-8** Rule Enforcement Directions

| Install On      | Enforced on Packets in this Direction                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination     | Inbound                                                                                                                                                                    |
| Source          | Outbound                                                                                                                                                                   |
| Gateways        | Based on the direction specified in the <b>Apply Gateway Rules to Interface Direction</b> property in the <b>Security Policy</b> tab of the <b>Properties Setup</b> window |
| Specific Target | Inbound and Outbound (Eitherbound)                                                                                                                                         |

## Time

**Add** — The **Time Objects** window (FIGURE 8-10) is displayed, from which you can select time objects to add to the rule's **Time**.

You can define any number of items in **Time**.



**FIGURE 8-10** Time Objects window

**Edit** — Edit the selected object.

You must first select one of the objects already defined under **Time**. The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

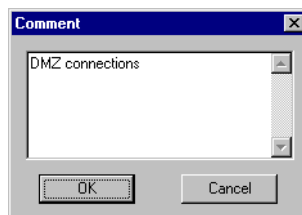
Alternatively, you can double-click on an object to edit it.

**Delete** — Delete the selected object.

You must first select one of the objects already defined under **Time**.

## Comments

To add a comment to a rule, double-click on the **Comment** field to open the **Comment** window (FIGURE 8-11).



**FIGURE 8-11** Comment window

Type any text you wish in the text box and click on **OK**.






**Note** – In this window, a carriage return is not interpreted as clicking on **OK**, so there can be more than one line in a comment.

## Copying, Cutting and Pasting Rules

To copy, cut or paste, select a rule or rules by selecting their numbers.

**TABLE 8-9** Copying, Cutting and Pasting Rules



| Action | Select from menu | Toolbar Button                                                                      |
|--------|------------------|-------------------------------------------------------------------------------------|
| Cut    | Edit>Cut         |  |
| Copy   | Edit>Copy        |  |
| Paste  | Edit>Paste       |  |

If you choose **Paste**, then the **Paste** menu will be opened. You must then select **Before**, **After**, **Top**, or **Bottom** to specify where in the Rule Base to paste the rule.

## Deleting a Rule

To delete a rule, select a rule or rules by selecting their numbers.

**TABLE 8-10** Deleting a Rule

| Action | Select from menu | Toolbar Button                                                                                                                                                              |
|--------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cut    | Edit>Cut         |  or  |

## Completing the Rule Base

### Verifying and Viewing the Security Policy

When you have defined the desired rules, open the **Policy** menu and select **Verify** to perform a heuristic check on the Rule Base. Verification will check that the rules are consistent and that no rule is redundant. If a Rule Base fails the verification, an appropriate message will appear.

To view the INSPECT code before installing the Security Policy, open the **Policy** menu and select **View**. Verification is automatically performed every time you view the Rule Base, and before the Security Policy is installed.

## “Silently” Dropping an Application

It is common practice for the last rule in a Rule Base to reject packets that fail to match any of the preceding rules and to log these rejections. If you would like to “silently” drop a specific application or group of applications, simply add a rule (before the last rule) that drops the application(s) without logging.

## Installing and Enforcing

Installing a Security Policy consists of generating an Inspection Script from the rule base and properties, compiling the Inspection Script to generate Inspection Code, and installing the Inspection Code on all the network objects specified in the **Install On** window.

The **Install On** window specifies the network object on which the Security Policy is installed. In contrast, the **Install On** column in the Policy Editor specifies the network object that is to enforce a specific rule.

In principle, the Security Policy should be installed on all the network objects which are to enforce it. However, VPN-1/FireWall-1 will allow you to not install the Security Policy on one or more of the objects that are to enforce it. This capability is useful for debugging purposes, but in all other cases you should take care to correctly deploy your Security Policy.

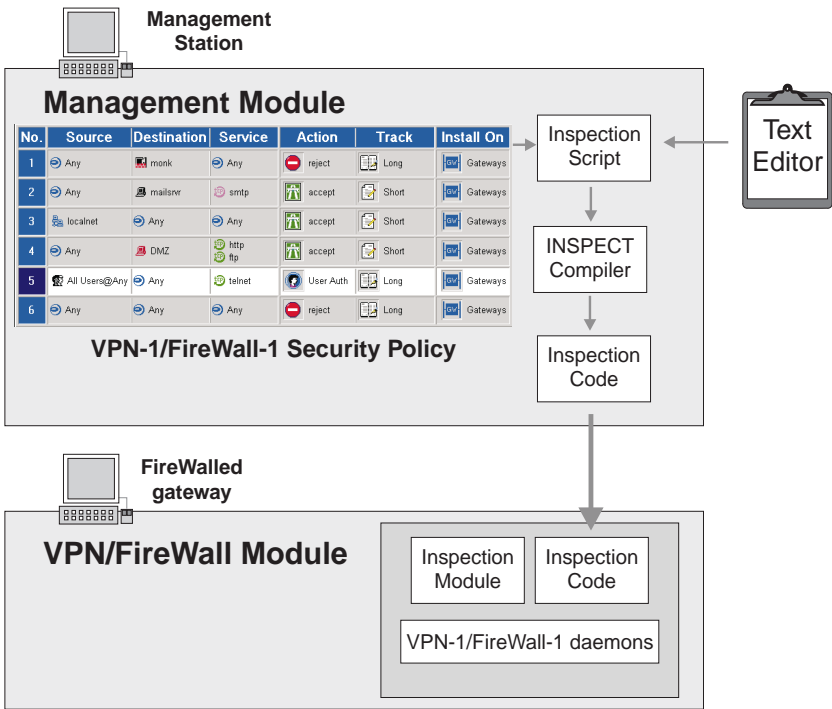
If you fail to install a Security Policy on a network object on which it should be installed, the VPN/FireWall Module will improperly monitor traffic through that object. If you install a Security Policy on a network object that does not enforce any part of that policy, the VPN/FireWall Module will block all traffic through that object (because only the implicit drop rule will be applied). See “Rule Base — Basic Concepts” on page 261.

## Inspection Scripts and Inspection Code

The rules that comprise a Security Policy are stored in an ASCII file named `$FWDIR/conf/rule_base.w`. Manually editing this file affects the GUI representation of rules and properties.

An Inspection Script (named `$FWDIR/conf/rule_name.pf`) is generated from the rules file (`$FWDIR/conf/rule_base.w`) and properties ASCII file (`$FWDIR/conf/objects.c`). An Inspection Script can be viewed and even manually edited, but editing an Inspection Script does *not* affect the GUI representation of rules and properties. On the other hand, it does affect the Inspection Code compiled from the Inspection Script and thus introduces inconsistencies between the GUI representation and the Inspection Code. For this reason, directly editing an Inspection Script should be avoided. If you edit the `$FWDIR/lib/*.def` files instead, you will avoid these inconsistencies.

Inspection Code (named \$FWDIR/temp/rule\_base.fc) is compiled from an Inspection Script. It is this Inspection Code that is installed on network objects and used by the VPN/FireWall Module to enforce a Security Policy.



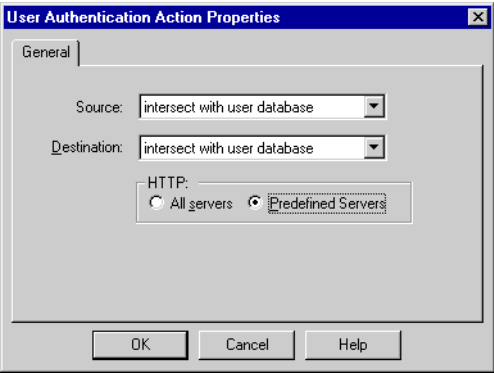
**FIGURE 8-12** VPN-1/FireWall-1 Inspection Components - flow of information

When a Security Policy is installed on a network object, the object receives the entire Inspection Code but executes only those rules with matching scope. If there are no rules with matching scope, the VPN/FireWall Module will drop all traffic, by the default rule (“That Which Is Not Expressly Permitted is Prohibited”). Installing what is essentially an empty Security Policy (no rules with matching scope) effectively bars all traffic.

## Rule Authentication Properties

If **User Authentication**, **Client Authentication**, **Session Authentication** or **Client Encryption** is specified as a rule’s **Action**, the rule’s properties are specified in the **Authenticate Action Properties** window.

To display the **Authenticate Action Properties** window, right-click on the **Action** field in the rule and choose **Edit Properties** from the menu.



**FIGURE 8-13** Authenticate Action Properties window for a User Authentication Rule

**TABLE 8-11** Authenticate Action Properties window

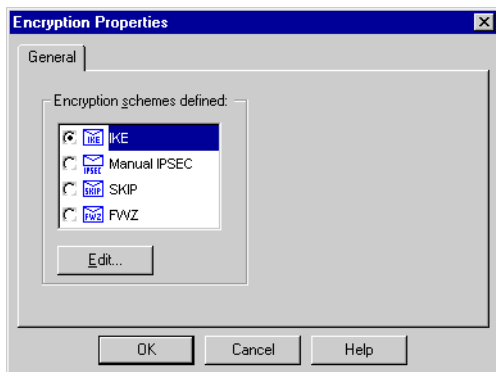
| For information about the Authenticate Action Properties window for | see ...                                                                       |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------|
| User Authentication rules                                           | “User Authentication” on page 484                                             |
| Client Authentication rules                                         | “Client Authentication” on page 526                                           |
| Session Authentication rules                                        | “Session Authentication” on page 515                                          |
| Client Encryption rules                                             | Chapter 9, “SecuRemote Server” of <i>Check Point Virtual Private Networks</i> |

## Encryption Properties

If **Encrypt** is specified as a rule's **Action**, the **Encryption Properties** window (FIGURE 8-14) defines the rule's encryption properties.

To display the **Encryption Properties** window, double click on the rule's Encrypt action.





**FIGURE 8-14** Encryption Properties window

For information about the **Encryption Properties** window, see “Rule Encryption Properties” on page 117 of *Check Point Virtual Private Networks*.

## Interaction between Rule Base and Properties

A Security Policy is defined not only by the Rule Base, but also by parameters specified in the **Security Policy** tab of the **Properties Setup** window. These parameters enable the user to control all aspects of a packet’s inspection, while at the same time freeing the user of the need to specify repetitive detail in the Rule Base.

Packets are matched in the following sequential order:

- 1** The anti-spoofing rules are applied.
- 2** Checked properties in the **Security Policy** tab of the **Properties Setup** window labeled **First** are matched first.  
If a property is not checked, then it is not included in the Security Policy.
- 3** Rules are matched according to their order in the Rule Base, except for the last rule in the Rule Base.
- 4** Properties in the **Security Policy** tab of the **Properties Setup** window labeled **Before Last** are matched after all but the last rule in the Rule Base.
- 5** The last rule in the Rule Base is matched.
- 6** The property in the **Properties Setup** window labeled **Last** is matched.
- 7** The implicit drop rule is matched.

In the Rule Base, the principle of “That Which Is Not Expressly Permitted is Prohibited” applies. For example, if the Rule Base does not expressly permit ICMP traffic, then ICMP traffic will be dropped.

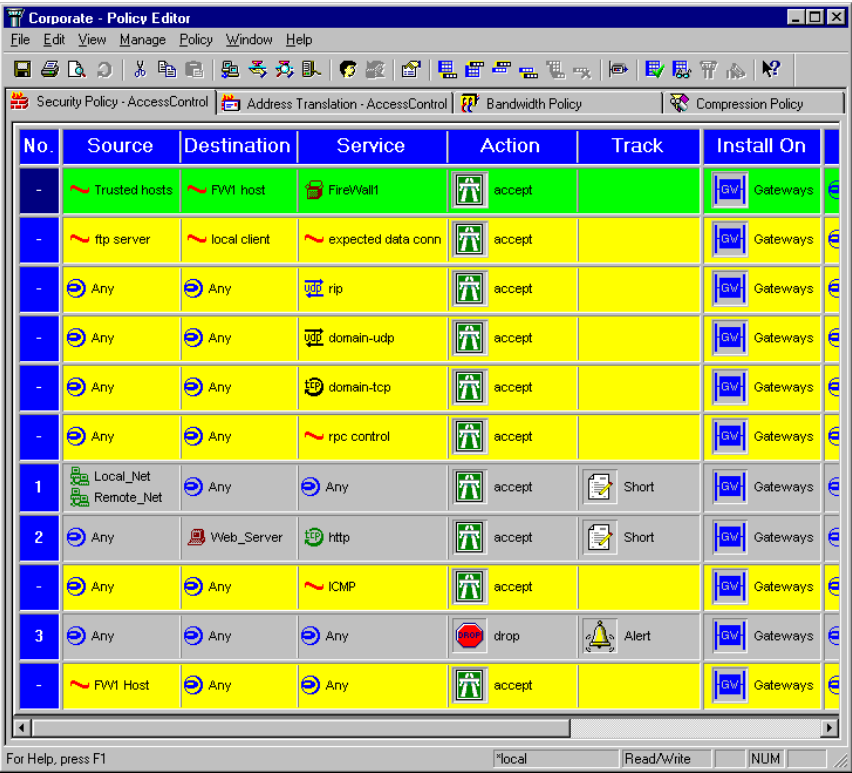
However, if the **Accept ICMP** option in the **Properties Setup** window is checked, and **Last** is not selected for the option, then ICMP traffic will be permitted.

Also, if **Apply Gateway Rules to Interface Direction** is set to **Inbound** and **Accept Outgoing Packets** is not checked, then no outgoing traffic will be allowed, no matter what the Rule Base indicates.

The settings in the **Security Policy** tab of the **Properties Setup** window are translated into macros and compiled in the Inspection Code.

## Implied Rules

You can see how the properties and rules interact by checking **Implied Rules** in the **View** menu. The explicit rules (those you have defined) will be displayed together with the implicit rules (those derived from the properties) in the correct sequence (see FIGURE 8-15).



**FIGURE 8-15** Policy Editor showing implied rules

The numbered rules are those you have explicitly defined. The implicit rules are not numbered.

For additional information about Properties, see Chapter 7, “Properties Setup.”

## Masking Rules

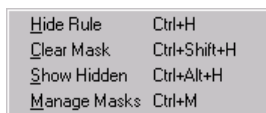
You can view only part of the Rule Base by hiding rules you do not want to see. This feature is useful when you have a large complex Rule Base and you want to view only a few of the rules without being distracted by other rules. Hidden rules remain part of the Rule Base and are installed when the Security Policy is installed.

### Hiding Rules

To hide a rule, proceed as follows:

- 1** Select the rule by clicking on its number.
- 2** Select **Mask (hiding rules)** from the **View** menu.

The Mask menu (FIGURE 8-16) is displayed.



**FIGURE 8-16** Mask menu

- 3** Select **Hide Rule**.

The rule is now hidden, but it is still part of the Rule Base and will be installed when the Security Policy is installed.

Alternatively, right-click on the rule number to open the Rule menu (FIGURE 8-4 on page 266) and select **Hide Rule**.

### Viewing Hidden Rules

If **Show Hidden** in the Mask menu is checked, then all the hidden rules are displayed in the Rule Base together with the other rules. Hidden rules are colored differently from other rules, making it easy to identify them so that you can unhide them.

If **Show Hidden** is not checked, the hidden rules are not displayed. A thick colored horizontal line indicates the presence of hidden rules.



**FIGURE 8-17** Rule Base with a hidden rule not displayed

In FIGURE 8-17, there is a hidden rule between rules 2 and 4. The gap in the numbering indicates how many rules are hidden.

Whether they are displayed or not, hidden rules are installed when the Security Policy is installed.

### Unhiding Hidden Rules

To unhide all the hidden rules, select **Clear Mask** from the Mask menu (FIGURE 8-16 on page 283).

# Masks

## Defining a Mask

Consider the Rule Base in FIGURE 8-18 below.

| No. | Source   | Destination | Service | Action | Track | Install On |
|-----|----------|-------------|---------|--------|-------|------------|
| 1   | Any      | mailserver  | smtp    | accept | Short | Gateways   |
| 2   | Any      | London      | Any     | drop   | Long  | Gateways   |
| 3   | localnet | DMZ         | ftp     | accept | Short | Gateways   |
| 4   | localnet | DMZ         | http    | accept | Short | Gateways   |
| 5   | localnet | DMZ         | ftp     | accept |       | Gateways   |
| 6   | localnet | DMZ         | http    | accept |       | Gateways   |
| 7   | Any      | Any         | Any     | reject | Long  | Gateways   |

**FIGURE 8-18** Rule Base before defining masks

Suppose that you want to sometimes hide all the FTP rules and at other times you want to hide all the HTTP rules. You can do this as follows:

- 1 Select the first FTP rule (rule 3).
- 2 Hide the selected rule as described in “Hiding Rules” on page 283.
- 3 Select the second FTP rule (rule 5).
- 4 Hide this rule as well.

The Rule Base now looks like this (FIGURE 8-19):

| No. | Source   | Destination | Service | Action | Track | Install On |
|-----|----------|-------------|---------|--------|-------|------------|
| 1   | Any      | mailserver  | smtp    | accept | Short | Gateways   |
| 2   | Any      | London      | Any     | drop   | Long  | Gateways   |
| 4   | localnet | DMZ         | http    | accept | Short | Gateways   |
| 6   | localnet | DMZ         | http    | accept |       | Gateways   |
| 7   | Any      | Any         | Any     | reject | Long  | Gateways   |

**FIGURE 8-19** Rule Base with FTP rules (rules 3 and 5) hidden

- 5 Select **Mask (hiding rules)** from the **View** menu.

The **Mask** menu (FIGURE 8-16 on page 283) is displayed.

- 6** Select **Manage Masks** from the **Mask** menu.

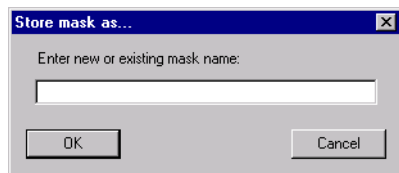
The **Named Masks** window (FIGURE 8-20) is displayed.



**FIGURE 8-20** Named Masks window

- 7** Click on **Store As**.

The **Store Mask As** window (FIGURE 8-21) is displayed.



**FIGURE 8-21** Store Mask As window

- 8** Enter a name for the mask (for example, **FTPRules**).
- 9** Select **Mask (hiding rules)** from the **View** menu.
- 10** Select **Clear Masks** from the Mask menu (FIGURE 8-16 on page 283).

The hidden rules are unhidden and the Rule Base once again is displayed as in FIGURE 8-18 on page 285.

## Reapplying a Mask

You can now reapply the FTPRules mask and in one action hide all the FTP rules as follows:

**1** Select **Mask (hiding rules)** from the **View** menu.

**2** Select **Manage Masks** from the Mask menu.

The **Named Masks** window (FIGURE 8-20 on page 286) is displayed.

**3** Select **FTPRules**.

**4** Click on **Fetch**.

The FTP rules (rules 3 and 5) are once again hidden, as in FIGURE 8-19 on page 285.

## Defining Another Mask

To define a mask for the HTTP rules (rules 4 and 6), proceed as follows:

**1** Unhide all the hidden rules, as described in “Unhiding Hidden Rules” on page 284.

**2** Define a mask for the HTTP rules (named “HTTPRules”) in the same way that you defined the FTPRules mask.

## Applying Masks

You can apply masks one after another using the **Fetch** command in the **Named Masks** window. When you apply a mask, any other mask that is currently applied is first “unapplied”. So, for example, if you apply the FTPRules mask, the FTP rules are hidden. If you then apply the HTTPRules mask, the FTP rules are unhidden and the HTTP rules are hidden.

## Querying the Rule Base

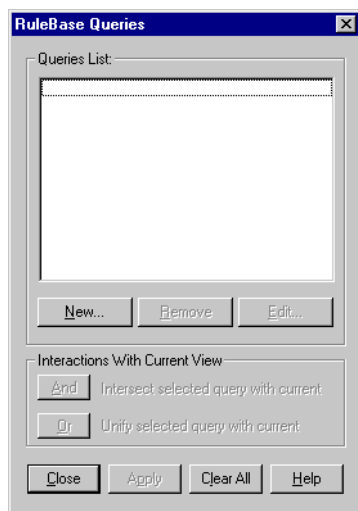
You can query the Rule Base and display only the rules that satisfy the criteria specified in the query, hiding all the other rules.

### Example

Consider once again the Rule Base depicted in FIGURE 8-18 on page 285. Suppose that you want to display only rules whose **Source** includes localnet.

- 1 From the **View** menu, select **Queries**.

The **Rule Base Queries** window (FIGURE 8-22) is displayed, showing all the defined queries (in this case there are none).



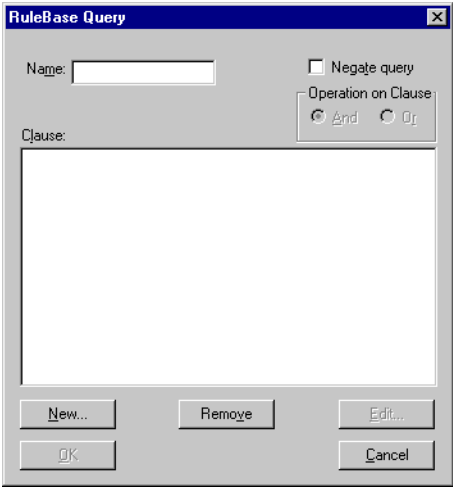
**FIGURE 8-22** Rule Base Queries window

For a detailed explanation of the **Rule Base Queries** window, see “Rule Base Queries window” on page 295.

- 2 Click on **New**.



The **Rule Base Query** window (FIGURE 8-23) is displayed.

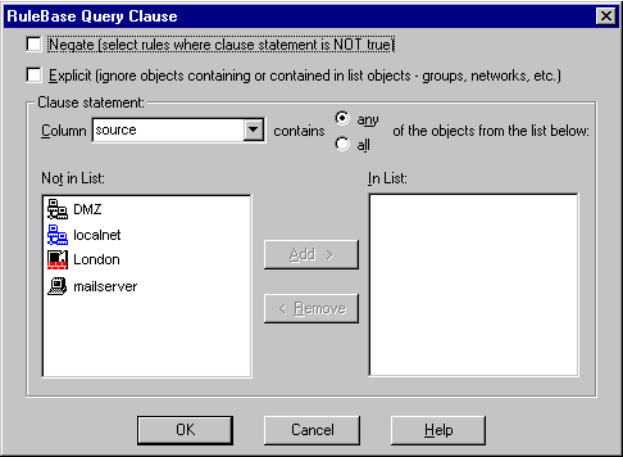


**FIGURE 8-23** Rule Base Query window

For a detailed explanation of the **Rule Base Query** window, see “Rule Base Query Clause window” on page 297.

- 3** Enter a name for the query in **Name**.
- 4** Click on **New**.

The **Rule Base Query Clause** window (FIGURE 8-24) is displayed.



**FIGURE 8-24** Rule Base Query Clause window

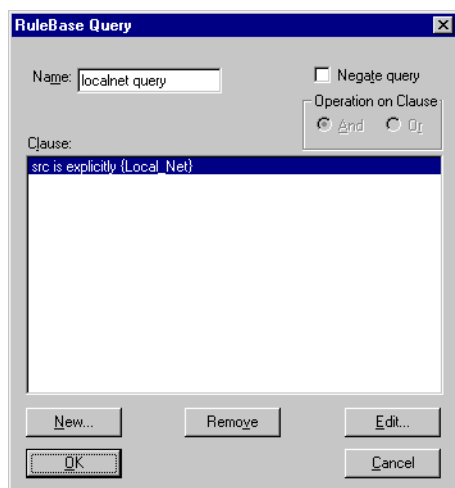
For a detailed explanation of the **Rule Base Query Clause** window, see “Rule Base Query Clause window” on page 297.

- 5** Check **Explicit**.

This specifies that only rules in which localnet explicitly appears (in contrast to rules where localnet is a member of a group explicitly appearing in the rule) will be considered as satisfying the query.

- 6** In **Column**, select **source**.  
This is the default.
- 7** In the **Not In List** box, select localnet.
- 8** Click on **Add**.  
localnet is moved to the **In List** box.
- 9** Click on **OK**.

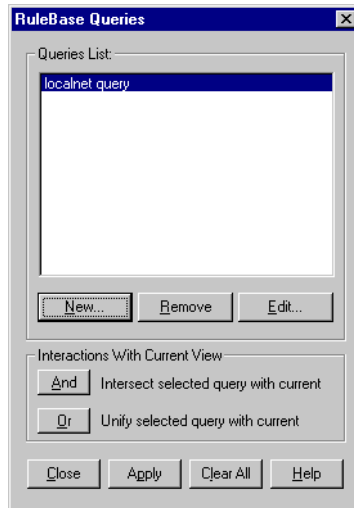
The **Rule Base Query** window (FIGURE 8-25 on page 290) is displayed, and the query clause just defined is listed.



**FIGURE 8-25** Rule Base Query window showing one query clause

- 10** Click on **OK**.

The **Rule Base Queries** window (FIGURE 8-26) is displayed, and the query just defined is listed.



**FIGURE 8-26** Rule Base Queries window showing one query

### 11 Click on **Apply**.

The query is used as a mask for hiding the rules that do not satisfy the query criteria. The Rule Base is displayed as in FIGURE 8-27.

| No. | Source   | Destination | Service | Action | Track | Install On |
|-----|----------|-------------|---------|--------|-------|------------|
| 3   | localnet | DMZ         | ftp     | accept | Short | Gateways   |
| 4   | localnet | DMZ         | http    | accept | Short | Gateways   |
| 5   | localnet | DMZ         | ftp     | accept |       | Gateways   |
| 6   | localnet | DMZ         | http    | accept |       | Gateways   |

**FIGURE 8-27** Rule Base after being masked by the query

The only rules that are displayed (that is, the only rules that are not hidden), are those whose **Source** includes localnet.

Note that the **Rule Base Queries** window is still open, allowing you to continue to define or use additional queries.

### 12 Click on **Close** to close the **Rule Base Queries** window.

## Refining the Query

Suppose that you want to refine the query so that the only rules displayed are those that satisfy the following criteria:

- **Source** includes localnet
- **Service** includes FTP

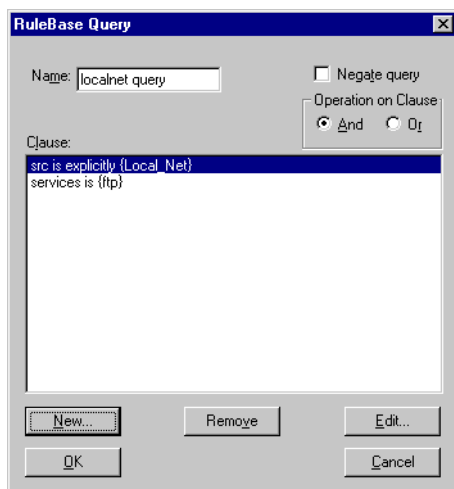
There are two ways to do this:

- Modify the query (by adding an additional clause) to specify both of the above criteria (see “To Modify the Query below).
- Define a new query that specifies only the second criterion and apply both queries, one after the other (see “To Define a New Query” on page 293).

## ▼ To Modify the Query

- 1** In the **Rule Base Queries** window (FIGURE 8-26), select the query.
  - 2** Click on **Edit**.
  - 3** In the **Rule Base Query** window (FIGURE 8-25), click on **New**.
  - 4** The **Rule Base Query Clause** window (FIGURE 8-24) is displayed.
  - 5** In **Column**, select **services**.
  - 6** In the **Not In List** box, select FTP.
  - 7** Click on **Add**.
- FTP is moved to the **In List** box.
- 8** Click on **OK**.

The **Rule Base Query** window (FIGURE 8-28) is displayed, and both query clauses are listed.



**FIGURE 8-28** Rule Base Query window showing two query clauses

**9** Click on **OK**.

The **Rule Base Queries** window (FIGURE 8-26) is displayed.

**10** Click on **Apply**.

The modified query is used as a mask for hiding the rules that do not satisfy the query criteria. The Rule Base is displayed as in FIGURE 8-29.

| No. | Source                                                                                     | Destination                                                                           | Service                                                                               | Action                                                                                   | Track                                                                                   | Install On                                                                                   |
|-----|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 3   |  localnet |  DMZ |  ftp |  accept |  Short |  Gateways |
| 5   |  localnet |  DMZ |  ftp |  accept |                                                                                         |  Gateways |

**FIGURE 8-29** Rule Base after being masked by the modified query

## ▼ To Define a New Query

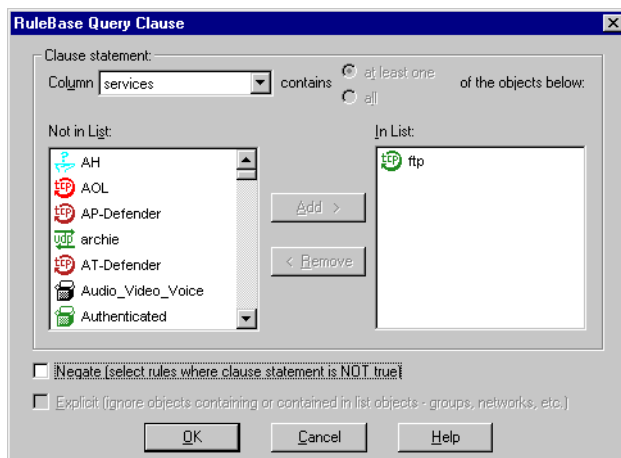
**1** In the **Rule Base Queries** window (FIGURE 8-26), click on **New**.**2** In the **Rule Base Query** window (FIGURE 8-25), enter a name for the query in **Name**.**3** Click on **New**.

The **Rule Base Query Clause** window (FIGURE 8-24) is displayed.

**4** In **Column**, select **services**.**5** In the **Not In List** box, select FTP.**6** Click on **Add**.

FTP is moved to the **In List** box.

FIGURE 8-30 show the **Rule Base Query Clause** window with the FTP service selected.



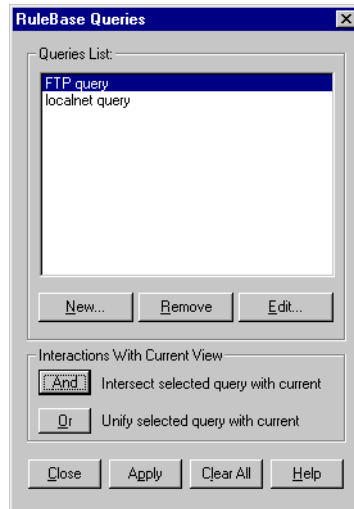
**FIGURE 8-30** Rule Base Query Clause window showing FTP selected

- 7** Click on **OK**.
- 8** In the **Rule Base Query** window, click on **OK**.
- 9** In the **Rule Base Queries** window, select the query just defined.
- 10** Click on **And**.

The newly defined query is applied in addition to the previous query, and the result is shown in FIGURE 8-29 on page 293.

## Rule Base Queries window

The **Rule Base Queries** window lists all the defined queries, and allows you to add edit, delete, and apply queries.



**FIGURE 8-31** Rule Base Queries window

**New** — Add a new query.

The **Rule Base Query** window (FIGURE 8-32 on page 296) is displayed.

**Edit** — Edit the selected query.

The **Rule Base Query** window (FIGURE 8-32 on page 296) is displayed.

**Remove** — Delete the selected query.

**And** — Apply the selected query as a mask, ANDing it with any masks currently applied.

The selected query is intersected with the current view. If another query is currently applied, only rules that match both queries are displayed.

**Or** — Unify the selected query with the current view. If another query is currently applied, rules that match either query are displayed.

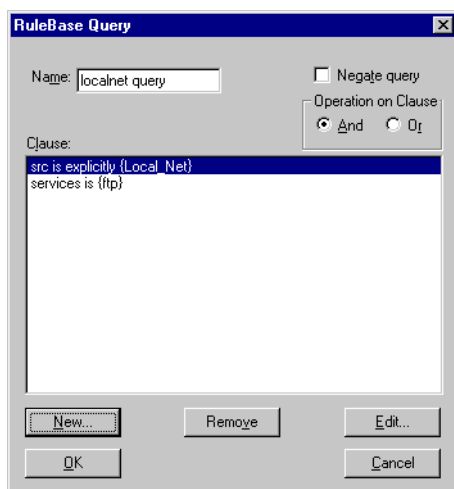
**Close** — Close the **Rule Base Queries** window.

**Apply** — Apply the selected query.

This has the same effect as **And** if a query is selected. Double-clicking on a query is equivalent to clicking on **Apply**.

**Clear all** — Unhide all rules.

## Rule Base Query window



**FIGURE 8-32** Rule Base Query window

**Name** — Enter the query's name.

**Negate Query** — The query is understood to be the negation of all its clauses.

For example, if the query specifies that **Source** is localnet, then the negated query specifies that **Source** is *not* localnet.

**Operation On Criteria** — Select one of the choices.

- **And** — the query's clauses are ANDed together
- **Or** — the query's clauses are ORed together

For example, suppose one query clause specifies that **Source** is localnet and another query clause specifies that **Service** is FTP. Then:

- If you select **And**, then the query specifies (**Source** is localnet) AND (**Service** is FTP).
- If you select **Or**, then the query specifies (**Source** is localnet) OR (**Service** is FTP).

If **Negate Query** is checked, then the meaning of **And** and **Or** is:

- If you select **And**, then the query specifies NOT ((**Source** is localnet) AND (**Service** is FTP)).
- If you select **Or**, then the query specifies NOT ((**Source** is localnet) OR (**Service** is FTP)).

**New** — Define a new query clause.

The **Rule Base Query Clause** window (FIGURE 8-33 on page 297) is displayed.

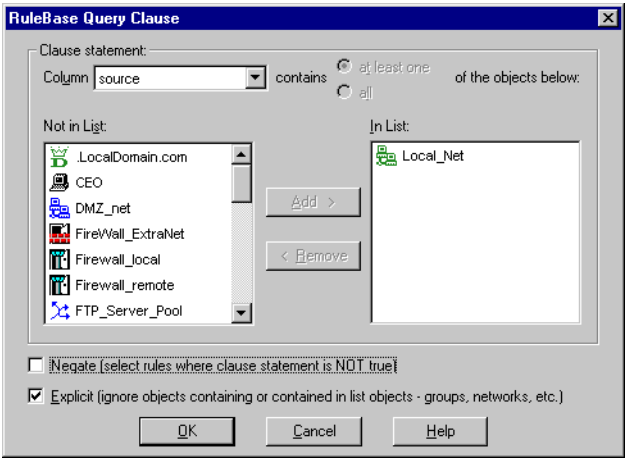
**Edit** — Edit the currently selected query clause.



The **Rule Base Query Clause** window (FIGURE 8-33 on page 297) is displayed.

**Remove** — Delete the currently selected query clause.

## Rule Base Query Clause window



**FIGURE 8-33** Rule Base Query Clause window

**Column** — Select a Rule Base column.

**Not in List** — objects not included in the query.

**In List** — objects included in the query clause.

To add an object to the query clause, click on the object in the **Not in List** box, and then click on **Add**.

To remove an object from the query clause, click on the object in the **In List** box, and then click on **Remove**.

**Negate** — If you check this box, then the criteria specified in the query clause are negated.

For example, if the query clause specifies **Service** is FTP, then if you check **Negate**, the clause is taken to specify “NOT (**Service** is FTP)”.

**Explicit** — If checked, only rules that explicitly include the object satisfy the criteria.

If the rule includes a group of which the object is a member, then the rule does not satisfy the criteria. Also, if the rule includes an object which is a member of a group specified in the criteria, then the rule does not satisfy the criteria.

For example, the standard VPN-1/FireWall-1 service definitions include a group named “Authenticated”, of which FTP and HTTP are members. If **Explicit** is checked, then a rule does *not* satisfy the criteria in the following two cases:

- The query clause specifies Authenticated and the rule includes FTP.
- The query clause specifies FTP and the rule includes Authenticated.

## Disabling Rules

When you disable a rule, the rule is no longer part of the Rule Base and is not installed when the Security Policy is installed. However, the rule is still displayed in the Rule Base, and you can re-enable it at any time.

This feature is useful for experimenting with the Rule Base. For example, you can disable a rule (or rules), install the Security Policy, analyze the effects of the new Security Policy and then re-enable the rule without having to re-enter it.


To disable a rule, select the rule by clicking on its number and then select **Disable Rule** from the **Edit** menu.

When a rule is disabled, a large red cross is drawn over its rule number.

To enable a disabled rule, select the rule and then select **Disable Rule** from the **Edit** menu.

Alternatively, right-click on the rule number to open the Rule menu (FIGURE 8-4 on page 266) and select **Disable Rule**.

FIGURE 8-34 shows a Rule Base with two rules (rule 1 and rule 3) disabled.

| No.                                                                               | Source   | Destination | Service | Action | Track | Install On |
|-----------------------------------------------------------------------------------|----------|-------------|---------|--------|-------|------------|
|  | Any      | mailserver  | smtp    | accept | Short | Gateways   |
| 2                                                                                 | Any      | London      | Any     | drop   | Long  | Gateways   |
|  | localnet | DMZ         | ftp     | accept | Short | Gateways   |
| 4                                                                                 | localnet | DMZ         | http    | accept | Short | Gateways   |
| 5                                                                                 | localnet | DMZ         | ftp     | accept |       | Gateways   |
| 6                                                                                 | localnet | DMZ         | http    | accept |       | Gateways   |
| 7                                                                                 | Any      | Any         | Any     | reject | Long  | Gateways   |

**FIGURE 8-34** Rule Base with rule 1 and rule 3 disabled

## Installing and Uninstalling the Security Policy

### Verifying the Rule Base and Security Policy

Installing the Security Policy does the following:

- performs heuristic verification on rules, and checks that rules are consistent and that every rule does something
- confirms that each of the **Install On** objects enforces some part of the Rule Base

If an **Install On** object does not enforce at least one rule, then the only rule it enforces is the default rule, which rejects all communications.

- converts the Rule Base to an Inspection Script and compiles the Inspection Script to generate Inspection Code
- distributes the Inspection Code to the selected target hosts
- distributes the User Database to the selected target hosts

Installing a Security Policy means downloading it to the FireWalled objects (gateways, hosts, and routers) which will enforce it. Except in the case of routers, there must be a VPN/FireWall Module running on the object which is receiving the Security Policy. In addition, the control channel between the machine that is installing the Security Policy and the object that is receiving the Security Policy must be enabled (see “Distributed Configurations” on page 69 for a detailed description of this control channel and how to enable it).

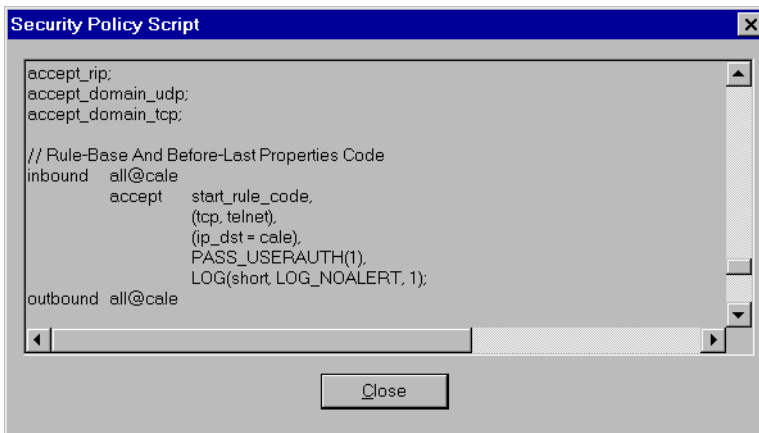
When installing Access Lists to a router, the router must be accessible and you must have permission to install the Access List. See the documentation for your router on how to define the appropriate permissions.

## Viewing the Inspection Script

To view the Inspection Script, choose **View** from the **Policy** menu. While viewing the text of the Inspection Script, you can save it to a file (on the server) by using the **File** menu. You can then edit the file and use the command-line interface from the server to load it in the VPN/FireWall Module. The Inspection Script is automatically verified when you load it for viewing.

For additional information about the INSPECT language, see Chapter 3, “The INSPECT Language” of *Check Point Reference Guide*.

FIGURE 8-35 shows an example of an Inspection Script.



**FIGURE 8-35** View Inspection Script Text

## Installing the Security Policy

When you have completed defining the Rule Base, choose **Install** from the **Policy** menu to install the Security Policy on the selected hosts. The **Install Policy** window (FIGURE 8-36) is then displayed. By default, all FireWalled hosts and routers are already selected.



**FIGURE 8-36** Install Policy window

Click on **Clear** to uncheck all the objects in the list, or **All** to check all the objects in the list.

You may unselect specific items, if you wish. The Security Policy will not be installed on unselected items.

Click on **OK** to install the Security Policy on all selected hosts. Installation progress is displayed.

Installing the Security Policy does the following:

- performs heuristic verification on rules, and checks that rules are consistent and that every rule does something
- confirms that each of the **Install On** objects enforces some part of the Rule Base  
If an **Install On** object does not enforce at least one rule, then the only rule it enforces is the default rule, which rejects all communications.
- converts the Rule Base to an Inspection Script and compiles the Inspection Script to generate Inspection Code
- distributes the Inspection Code to the selected target hosts
- distributes the User and Encryption databases to the selected target hosts

VPN-1/FireWall-1 issues a warning if there is an inconsistency in the Rule Base or if there is a rule that does nothing.

## Uninstalling the Security Policy

Choose **UnInstall** from the **Policy** menu to install the Security Policy on the selected hosts. The **Install Policy** window (FIGURE 8-36 on page 300) is then displayed.

## Inspection Code Loading

When you install or uninstall a Security Policy from the GUI (by choosing **Install** or **UnInstall** from the **Policy** menu), the VPN-1/FireWall-1 Management Server runs the `fw` command with the `load` or `unload` argument (see “`fw load`” on page 9 of and “`fw unload`” on page 11 of *Check Point Reference Guide* for more information).

You can modify this behavior so that choosing **Install** or **UnInstall** from the **Policy** menu runs a program or shell script (batch file) of your choice. For example, to run `bigapple`, add the following statement to the `setup.C` file:

```
load_program ("bigapple")
```

`bigapple` will be run with the same argument list that `fw` would have received (where the first argument is either `load` or `unload`). It is then your responsibility to ensure that `bigapple` correctly processes its arguments and installs or uninstalls the Security Policy. Of course, `bigapple` can also perform any other functions you wish.

## Installing Access Lists

When you install a rule on a router, VPN-1/FireWall-1 generates Access Lists and loads them to the router. Access Lists are also enforced by the PIX Integrated Firewall. VPN-1/FireWall-1 also allows you to import Access Lists for Cisco, 3Com and Microsoft RRAS routers, enabling the integration of existing filter configurations. You can also import Access Lists from a PIX Integrated Firewall. Access Lists for routers and for PIX can be viewed and verified.

When installing Access Lists to a router, the router must be accessible and you must have permission to install the Access List. See the documentation for your router on how to define the appropriate permissions. You must also define the correct access permissions in the **Setup** tab of the **Router Properties** window.



**Note** – A Bay Networks router can function in either of two modes: as a packet filter (in which case you can install an Access List on the router by choosing **Access Lists** from the **Policy** menu), or as a FireWalled router (in which case you can install a Security Policy on the router by choosing **Install** from the **Policy** menu). Bay Networks routers cannot implement VPN-1/FireWall-1's encryption, authentication or Network Address Translation features.

## Importing Access Lists

The VPN-1/FireWall-1 Open Security Extension feature enables you to import existing Access Lists from the following routers and security devices:

- Steelhead routers (Microsoft RRAS)
- Cisco routers
- 3Com routers
- PIX integrated firewalls

Access Lists can be imported to a Rule Base or as ASCII files. Access Lists imported to a Rule Base are displayed in terms of source, destination, service, the router interface and direction to which each rule applies. Imported Access Lists can be modified in the Rule Base and installed on the appropriate router interface.

ASCII files display Access Lists as simple text files and include additional details that are not represented in the Rule Base. You cannot modify the imported ASCII files.

Imported Access Lists can also be viewed and verified. Verification checks Access Lists for inconsistencies and redundant rules. For more information, see “Verifying and Viewing Access Lists” on page 304.



**Note** – Router or integrated firewall properties are not part of an imported policy.

## ▼ To Import Router Access Lists

- 1 From the **Policy** menu, choose **Access Lists**.

The **Router Access Lists Control** window (FIGURE 8-37 on page 303) is displayed.

- 2 Check **Import Access Lists**. Specify the following parameters:

**Router** — Select a router from the drop-down list.

**Interface** — Select an interface.

The drop-down list displays all the interfaces available for the selected router.

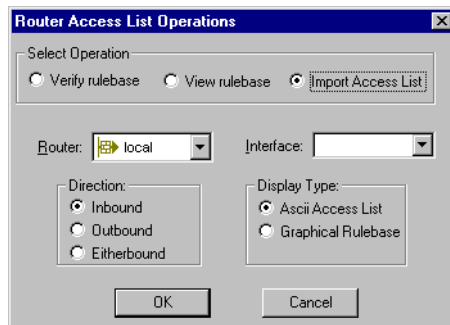
**Direction** — Check a direction.



**Note** – Eitherbound means both inbound and outbound.

**Display Type** — Check one of the following:

- **Ascii Access Lists**
- **Graphical Rule Base**



**FIGURE 8-37** Router Access Lists Operations window with import options

## Managing Imported Access Lists in the Rule Base

VPN-1/FireWall-1 opens a new Security Policy when you import Access Lists to the Rule Base. The Security Policy title displays the name of the imported Rule Base in the following format:

```
<router name>_<inbound/outbound/eitherbound>_Imported_Policy
```

Each filter rule is displayed as a rule in the Rule Base. The Rule Base specifies the **Source**, **Destination** and **Service** for each imported filter rule. The **Install On** field displays the router interface and direction to which each rule applies, using the following format:

```
<inbound/outbound/eitherbound>.<interface name>@<router name>
```

The Rule Base **Comment** displays additional filter information.

## Modifying Imported Rules

You can modify an imported rule's **Source**, **Destination**, and **Service** fields, but you cannot modify the **Install On** field. You can delete, copy, cut, and paste imported rules. You cannot add a new rule on a specific router interface. You must first copy and paste a rule that specifies the router interface and direction under **Install On** and then modify the other data fields in that rule.

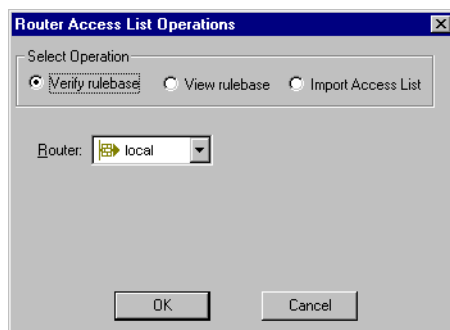
## Unknown Network Objects and Services

**Unknown** network objects or services indicate objects that you have not yet defined to VPN-1/FireWall-1. You can complete the object or service definition based on properties imported from the Access Lists, such as IP addresses or service port numbers. To view the imported properties of an **Unknown** object, double-click on the object to open the appropriate **Properties** window.

## Verifying and Viewing Access Lists

VPN-1/FireWall-1 allows you to view and verify Access Lists generated from the Rule Base. Verification checks that the rules are consistent and that no rule is redundant. If a Rule Base fails the verification, an appropriate message will appear. You can also view and verify imported Access Lists.

To verify or view router Access Lists, choose **Access Lists** from the **Policy** menu. The **Router Access List Operations** window is displayed.

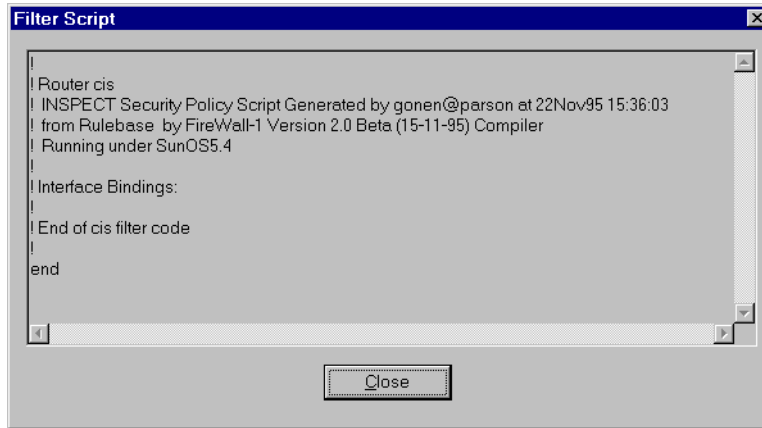


**FIGURE 8-38** Router Access List Operations window

To verify Access Lists, check **Verify** and select the appropriate router from the drop-down list.



To view Access Lists, check **View** and select the appropriate router from the drop-down list. VPN-1/FireWall-1 verifies the Access List before displaying it.



**FIGURE 8-39** View of a Cisco Access List

## Installing Access Lists

For instructions on installing Access Lists to routers, see “Installing the Security Policy” on page 300.

## Default Security Policy

### Overview

During the boot process, there is a short period of time (measured in seconds) between the point when the gateway becomes able to communicate and the point when the VPN-1/FireWall-1 Security Policy is loaded and is enforced. During this time (the period of vulnerability) both the gateway and networks behind the gateway are vulnerable to attack, unless you take measures to protect them.

You can protect networks behind the gateway by disabling IP Forwarding in the OS kernel and allowing VPN-1/FireWall-1 to control IP Forwarding. If you do this, there will never be a time when IP Forwarding is on but your Security Policy is not being enforced, so networks behind the gateway are safe.

Disabling IP Forwarding protects networks behind the gateway, but it does not protect the gateway itself. For this purpose, VPN-1/FireWall-1 enables you to implement a minimal default Security Policy during the period of vulnerability.



**Note** – If you stop VPN-1/FireWall-1 (`fwstop`) while the Default Security Policy is active, then no Security Policy will be enforced until you start VPN-1/FireWall-1 again (`fwstart`).

## Default Security Policies

### Standard Default Security Policies

When you install the VPN/FireWall Module, you are asked to choose between two default Security Policies:

**1** accept

The accept default Security Policy allows:

- all outgoing communications
- incoming communications on ports through which there were previous outgoing communications
- ICMP packets
- broadcast packets

**2** drop

The drop default Security Policy drops all communications in and out of the gateway during the period of vulnerability.

If the boot process requires that the gateway communicate with other hosts, then the drop default Security Policy should not be used.

### User-Defined Default Security Policies

You can define your own default Security Policy as follows:

**1** Create an INSPECT script named `defaultfilter.pf` in `$FWDIR/conf`.

The script may not perform any of the following functions:

- logging
- authentication
- encryption
- content security

**2** Run `fw defaultgen`.

You must ensure that your Security Policy does not interfere with the boot process.

### Verifying the Default Policy

You can verify that the default Security Policy is indeed loaded as follows:

**1** Boot the system.

**2** Before installing another Security Policy, type the following command:

```
$FWDIR/bin/fw stat
```

The command's output should show that `defaultfilter` is installed.

## Auxiliary Connections

A number of services establish auxiliary connections that require special handling by VPN-1/FireWall-1. For example, an FTP data connection from the FTP server to the client will be allowed only if the **Enable FTP PORT Data Connections** property in the **Services** tab of the **Properties Setup** window is enabled.

Consider the following Rule Base

| Source    | Destination | Services | Action | Track    | Install On |
|-----------|-------------|----------|--------|----------|------------|
| FTPClient | FTPServer   | Any      | Accept |          | Gateways   |
| Any       | Any         | Any      | Reject | Long Log | Gateways   |

If the **Enable FTP PORT Data Connections** property is not enabled, the data connection from FTPServer to FTPClient will not be allowed, because there is no rule that allows connections from FTPServer to FTPClient.

If the auxiliary connection is from the client to the server (as with FTP PASV), the auxiliary connection may be improperly handled in some cases (for example, if the server's IP address is translated).

Before a back connection is opened (for example, for FTP), the back connection's destination port is checked against a list of known TCP and UDP services. If the requested port "belongs" to a well known service, the back connection is rejected.

Services that open back connections fall into two categories in VPN-1/FireWall-1 (assuming that there is a rule that allows the initial connection):

- VPN-1/FireWall-1 allows auxiliary connections only if the appropriate property is enabled. These services are:
  - FTP PORT
  - RSH/REXEC
  - FTP PASV
  - RPC Control
- VPN-1/FireWall-1 allows auxiliary connections only if the service is specifically listed under **Services** in the rule that allows the initial connection. These services are:
  - VDOLive
  - H.323
  - BackWeb
  - FreeTel
  - NetShow
  - WebTheatre
  - CoolTalk
  - RealAudio
  - MS Exchange services (requires DCE-RPC)
  - sqlnet2

# Established TCP Connections

## Overview

VPN-1/FireWall-1 inspects *all* IP packets against the Security Policy. The first packet of each TCP connection or UDP session is checked against the Rule Base. If the first packet is accepted, VPN-1/FireWall-1 adds the connection to an internal table of open connections (the connections table), in the format:

```
<src-addr,src-port,dst-addr,dst-port,ip-p;enc-key,type,flags>
```

Subsequent packets of an established TCP connection (or UDP session) are checked against the table rather than against the Rule Base.

VPN-1/FireWall-1 considers a packet to be part of an established TCP connection if it is not a SYN/NO-ACK packet, that is, if it is not the first packet of a TCP connections.

You can see the connections table by typing:

```
fw tab -t connections -u
```

on the FireWalled gateway.

One of the first things VPN-1/FireWall-1 does for each packet is to determine whether the packet's TCP connection (or UDP session) is listed in the connections table. If it is, the packet is immediately accepted (and possibly encrypted or decrypted).

There are several advantages to using this method:

- 1** VPN-1/FireWall-1 needs some way of accepting replies to valid TCP connections. Suppose the Rule Base allows connections from A to B, but rejects connections from B to A. If A initiates a connection to B, the replies to that connection must be accepted even though connections from B to A are rejected. By using the connections table, VPN-1/FireWall-1 is able to differentiate between replies to the original A to B connection (which are allowed to pass) and B to A connections (which are rejected).
- 2** It is very inefficient to scan each packet against the entire Rule Base. It is much more efficient to accept all packets of previously approved connections.

Entries are removed from the connections table when one of the following happens:

- for TCP connections:
  - 20 to 50 seconds after VPN-1/FireWall-1 sees two FIN packets, *or*
  - after the connection is idle for more than TCP\_TIMEOUT seconds
- for UDP sessions, after the connection is idle for more than UDP\_TIMEOUT seconds

These values are set by the user in the **Security Policy** tab of the **Properties Setup** window (Windows GUI).

In addition, the `connections` table is cleared when a Security Policy is re-loaded (as are as most of the other tables). The new Security Policy is then enforced on the already active connections and sessions.

It may happen that an entry for a connection still taking place is removed, either because the connection was idle for a long time and has been re-activated, or because a new Security Policy was loaded.

For example, suppose your Security Policy accepts allows connections from A to B, but rejects connections from B to A. Suppose you do the following:

**1** TELNET from A to B.

**2** Type the command:

```
sleep 100; echo "hello"
```

**3** Reload the same Security Policy.

After 100 seconds, a packet returns from B to A, carrying the word “hello”. Although this packet is part of a valid connection, VPN-1/FireWall-1 rejects it.

To solve this problem, VPN-1/FireWall-1 drops TCP packets that claim to belong to established TCP connections (that is, non-SYN and ACK packets) in a special way. The packet is not actually dropped, but instead all the data is removed from the packet, leaving only the IP and TCP headers, which renders the packet harmless. In addition, the SEQ number of the TCP header is mangled.

When A receives the mangled packet, A immediately responds, because of the mangled SEQ number. If the connection is still valid, this response is matched against the Rule Base, and the connection is re-recorded in the `connections` table. If the Rule Base indicates that the connection is to be logged, then the packet is logged if **Log Established TCP Packets** in the **Logging and Alerting** tab of the **Security Policy** window is checked. VPN-1/FireWall-1 then restarts the timeout clock.

If the connection has become invalid, the packet is dropped. VPN-1/FireWall-1 notices that it is dropping a reply to a mangled TCP packet and so does not mangle it again but drops it for good.

In rare cases, VPN-1/FireWall-1 logs the mangled packets if the rule that dropped the packet specified a log action. This means that even if a connection is legal, you might see a drop log entry even though the connection continues. To eliminate these spurious log entries, uncheck **Log Established TCP Packets** in the **Logging and Alerting** tab of the **Properties Setup** window and reload the Security Policy.

## Example

Suppose the Rule Base allows host A to initiate an FTP connection with host B, and specifies that the connection be logged. The log then shows an entry for the first packet, but not for subsequent packets (because the Rule Base is checked only for the first packet). Suppose also that the connection times out.

**If the First Packet After the Timeout is Sent by A** — If the first packet after the timeout is sent by A, it is handled as though it were the first packet of the connection. The packet is accepted and the timeout clock is restarted. If the Rule Base specifies logging, the packet is logged.

**If the First Packet After the Timeout is Sent by B** — If the first packet after the timeout is sent by B, VPN-1/FireWall-1 checks the Rule Base. Even if the Rule Base specifies that the packet be dropped or rejected, VPN-1/FireWall-1 mangles the packet and passes it to A. This forces A to request a re-transmission, upon which the Rule Base is checked again as described in “If the First Packet After the Timeout is Sent by A” above.

TABLE 8-12 summarizes the logging options for re-established TCP connections.

**TABLE 8-12** Logging a Re-Established TCP Connections

| <b>Log Established TCP Packets</b> | <b>first packet after timeout sent by A</b>                                                                           | <b>first packet after timeout sent by B</b>                                                    |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| checked                            | packet is logged only if specified by Rule Base — packet is handled just as the connection’s first packet was handled | packet is logged only if specified by Rule Base (possibly under last “None of the Above” rule) |
| not checked                        | packet is not logged                                                                                                  | packet is not logged                                                                           |

# Time Objects

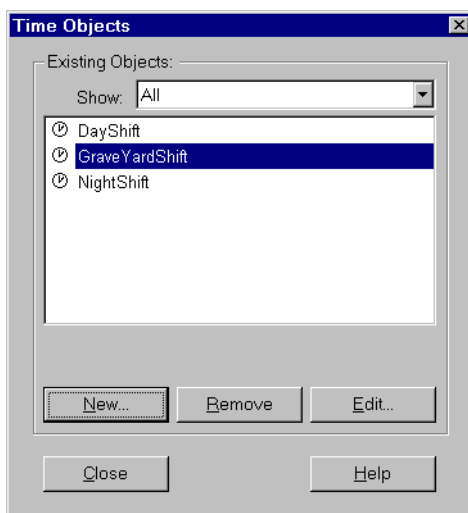
## In This Chapter

|                            |                 |
|----------------------------|-----------------|
| <i>Time Object Windows</i> | <i>page 313</i> |
| <i>Time Object Groups</i>  | <i>page 315</i> |

## Overview

Time objects are used to specify time periods during which rules are in effect.

To define a time object, open the **Time Objects** window (FIGURE 9-1 on page 311) by choosing **Time Objects** from the **Manage** menu. The **Time Objects** window appears (FIGURE 9-1 on page 311).



**FIGURE 9-1** Time Objects window

The objects displayed depend on what you have selected from the **Show** dropdown list.

**TABLE 9-1** Time Object Actions

| for a description of how to ... | ... see                                  |
|---------------------------------|------------------------------------------|
| create a time object            | “Creating a New Time Object” on page 312 |
| modify a time object            | “Modifying an Object” on page 312        |
| delete a time object            | “Deleting an Object” on page 312         |

▼ **Creating a New Time Object**

To create a new object, click on **New**. A menu appears, listing the types of objects you can create.



**FIGURE 9-2** Add Time Object menu

Choose a type from the menu. A window appears prompting you to enter the properties of the selected object type.

▼ **Deleting an Object**

To delete an object, select the object and click on **Remove**.

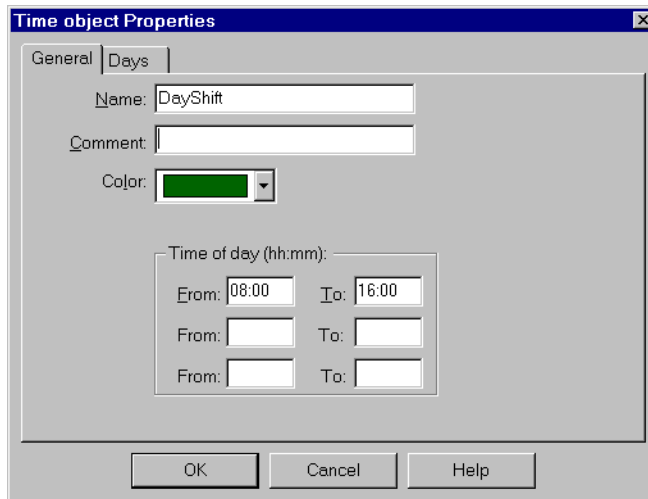
▼ **Modifying an Object**

To modify an object, select the object and click on **Edit**, or double-click on the object.



# Time Object Windows

## Time Object Properties Window — General Tab



**FIGURE 9-3** Time Object Properties window — General tab

**Name** — the object's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Time Object** window when this item is selected.

**Color** — the color of the object's icon

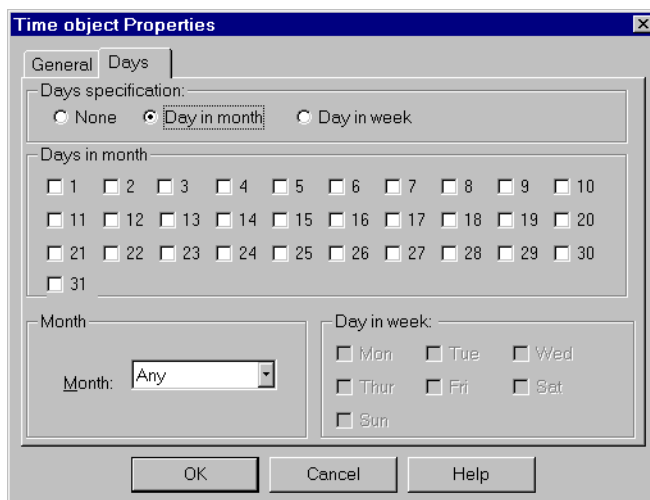
Select the desired color from the drop-down list.

**Time of Day** — Enter up to three **From–To** pairs in 24-hour notation.

To specify all day, set **From** to 00:00 and **To** to 23:59.

A rule in which a time object is used is applied only to connections which begin during the time period defined by the time object. If an allowed connection extends past the time period, it will be allowed to continue.

## Time Object Properties Window — Days Tab



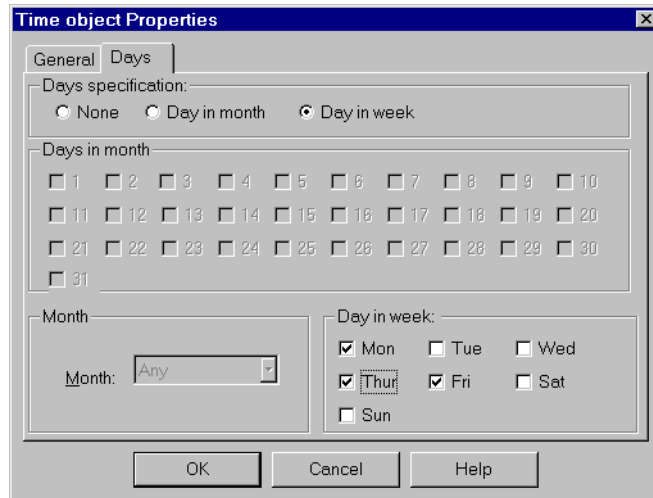
**FIGURE 9-4** Time Object Properties window — Days tab (Days in Month)

**Days Specification** — Choose one of the following:

**None** — The times of day specified in the **General** tab of the **Time Object Properties** window apply on all days.

**Day in Month** — The times of day specified in the **General** tab of the **Time Object Properties** window apply only on the days of the month checked under **Days in Month** (FIGURE 9-4).

**Day in Week** — The times of day specified in the **General** tab of the **Time Object Properties** window apply on the days of the month checked under **Days in Week** (FIGURE 9-5 on page 315).



**FIGURE 9-5** Time Object window — Days tab (Days in Month)

**Month** — The times of day specified in the **General** tab of the **Time Object Properties** window apply only during the month specified. This field is enabled only if **Days Specification** is **Days in Month**.

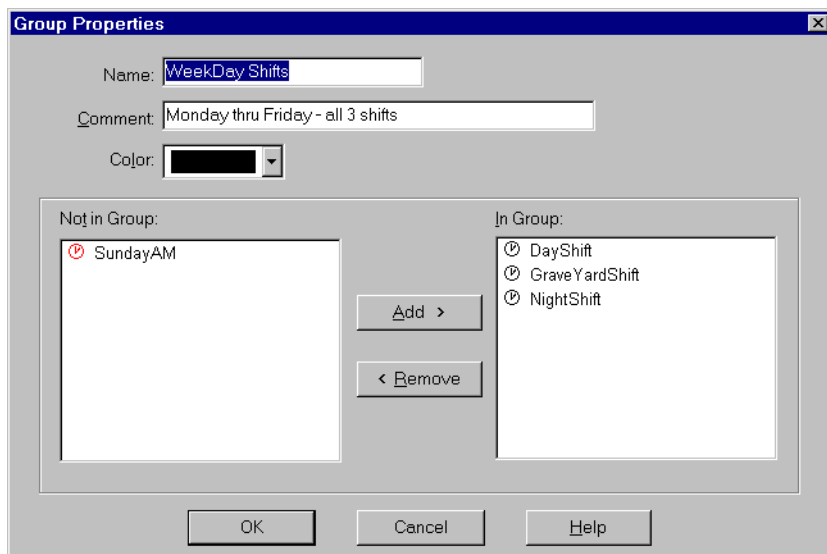
## Time Object Groups

You can simplify the Rule Base by defining a group of time objects and using the group in rules.

### Creating a Group

To create a group, create an object of type Group using the Time Object Manager (see “Creating a New Time Object” on page 312). Next, add objects to the group using the **Group Properties** window (FIGURE 9-6 on page 316).

To display the **Group Properties** window, double-click on the group’s name in the **Time Object Manager** window.



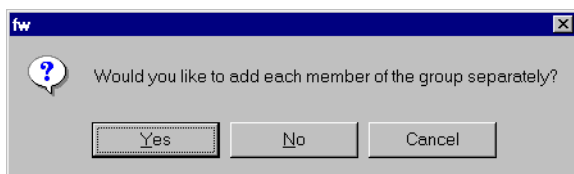
**FIGURE 9-6** Group Properties window

## Adding an Object to a Group

In the left listbox (labeled **Not in Group**), select the objects you wish to include in the group. Use the **Add** button to add individual objects and to add groups to the group.

You can add a group to another group in one of two ways:

- 1** You can individually add all the objects in one group to another group, without nesting. Click on **Yes** in reply to the question in the window (FIGURE 9-7).
- 2** You can nest groups inside groups to create a group hierarchy of any desired complexity. Click on **No** in reply to the question in the window.



**FIGURE 9-7** Adding a Group to a Group

## Deleting an Object from a Group

Select the objects to be deleted from the right listbox (labeled **In Group**), and then click on **Remove**.

# Server Objects

---

## In This Chapter

|                                        |                 |
|----------------------------------------|-----------------|
| <i>Server Objects</i>                  | <i>page 317</i> |
| <i>UFP Servers</i>                     | <i>page 320</i> |
| <i>CVP Servers</i>                     | <i>page 322</i> |
| <i>CVP Manager</i>                     | <i>page 323</i> |
| <i>RADIUS Servers</i>                  | <i>page 329</i> |
| <i>TACACS Servers</i>                  | <i>page 332</i> |
| <i>AXENT Pathways Defender Servers</i> | <i>page 333</i> |
| <i>Policy Servers</i>                  | <i>page 334</i> |
| <i>LDAP Account Units</i>              | <i>page 334</i> |

## Server Objects

A server object represents a server running on a specific host. The available server objects are:

### 1 URL Filtering Protocol (UFP)

A UFP server can be used in defining a URI Resource. For information about URI Resources, see “URI Resources” on page 205.

### 2 Content Vectoring Protocol (CVP)

A CVP server examines the contents of a file or data stream. For examples of how to use CVP servers in a resource definition, see Chapter 6, “Services and Resources.”

See “Implementing CVP Inspection” on page 366 for information about the CVP protocol.

### 3 RADIUS

A RADIUS Server is used to provide authentication services. For information about defining an Authentication scheme for a user, see “User Properties Window — Authentication tab” on page 158.

### 4 RADIUS Server group

A RADIUS Server group consists of RADIUS Servers.

### 5 TACACS

A TACACS Server is used to provide authentication services. For information about defining an Authentication scheme for a user, see “User Properties Window — Authentication tab” on page 158.

### 6 AXENT Defender

An AXENT Defender Server is used to provide authentication services. For information about defining an Authentication scheme for a user, see “User Properties Window — Authentication tab” on page 158.

### 7 LDAP Account Unit

The VPN-1/FireWall-1 Account Management system is an independent module that enables the Security Manager to integrate an LDAP-compliant user database with VPN-1/FireWall-1 User Authentication. An LDAP Server can contain multiple branches (for example, “o=University of Michigan,c=UK”). An LDAP Server and a subset of its branches constitute a VPN-1/FireWall-1 Account Unit.

For information about Account Units, see “Account Units” on page 177.

### 8 Certificate Authority

For information about Certificate Authorities, see Chapter 3, “Certificate Authorities” of *Check Point Virtual Private Networks*.

### 9 Policy Server


For information about Policy Servers, see the book *SecureClient Administration*.

For information about Authentication schemes in general, see “Authentication Schemes” on page 484.

For information on how to obtain third-party servers, see <http://www.checkpoint.com>.

## Defining Server Objects

To define a Server object, open the **Server Objects** window (FIGURE 10-1 on page 319) by:

- choosing **Servers** from the **Manage** menu, or
- selecting  from the toolbar.

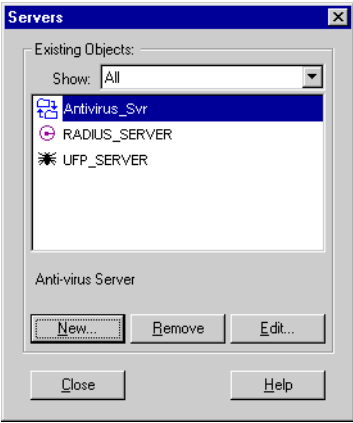


FIGURE 10-1 Server Objects window

The objects displayed depend on what you have selected from the **Show** dropdown list.

TABLE 10-1 Server Object Actions

| for a description of how to ... | ... see                             |
|---------------------------------|-------------------------------------|
| create a server object          | “Creating a New Server” on page 319 |
| modify a server object          | “Modifying a Server” on page 320    |
| delete a server object          | “Deleting a Server” on page 320     |

▼ **Creating a New Server**

To create a new server, click on **New**. A menu appears, listing the types of servers you can create.

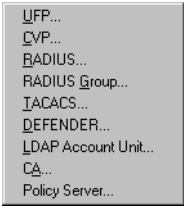


FIGURE 10-2 New Server Object menu

Choose a type from the menu and click on **OK**. A window appears prompting you to enter the properties of the selected server type.

**TABLE 10-2** Server Types

| to create an server of type .... | ... which is used for ...                                | ... see                                                                             |
|----------------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------------|
| UFP                              | URI resources                                            | “UFP Servers” on page 320                                                           |
| CVP                              | Anti-Virus checking (for example) for all resource types | “CVP Servers” on page 322                                                           |
| RADIUS                           | RADIUS authentication                                    | “RADIUS Servers” on page 329                                                        |
| RADIUS Group                     | RADIUS authentication                                    | “RADIUS Server Groups” on page 331                                                  |
| TACACS                           | TACACS authentication                                    | “TACACS Servers” on page 332                                                        |
| DEFENDER                         | AXENT Defender authentication                            | “AXENT Pathways Defender Servers” on page 333                                       |
| LDAP Account Unit                | maintaining an LDAP user database                        | “LDAP Account Units” on page 334                                                    |
| CA                               | defining a Certificate Authority                         | Chapter 3, “Certificate Authorities” of <i>Check Point Virtual Private Networks</i> |
| Policy Server                    | defining a SecureClient Policy Server                    | Chapter 11, “VPN-1 SecureClient” of <i>Check Point Virtual Private Networks</i>     |

### ▼ Deleting a Server

To delete a server, select the server and click on **Remove**.

### ▼ Modifying a Server

To modify a server, select the server and click on **Edit**, or double-click on the server.

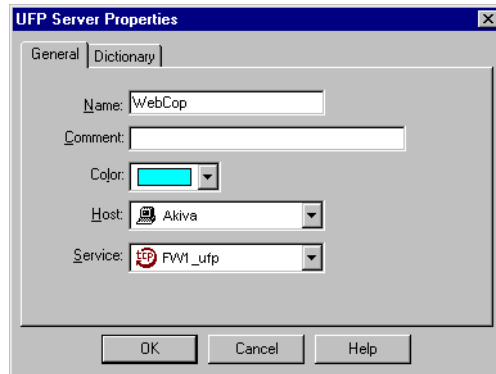
## UFP Servers

UFP servers are used in URI Resource definitions. For information about URI Resources, see “URI Resources” on page 205.

A UFP server is used to specify a list of URLs. A UFP server has a pre-defined list of categories, which can be downloaded (see “UFP Server Properties Window — Dictionary Tab” on page 322).



## UFP Server Properties Window — General Tab



**FIGURE 10-3** UFP Server Properties window — General tab

**Name** — the object's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Server Object** window when this item is selected.

**Color** — the color of the object's icon

Select the desired color from the drop-down list.

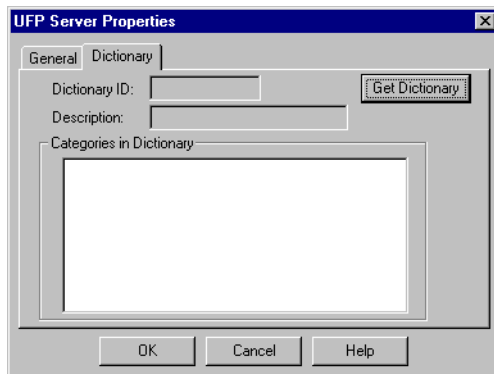
**Host** — Select the host on which the server is running from the menu.

The host should have already been defined as a network object (see “Defining Network Objects” on page 97).

**Service** — From the menu, select the service for communication with the server.

For UFP servers, the service is FW1\_ufp.

## UFP Server Properties Window — Dictionary Tab



**FIGURE 10-4** UFP Server Properties window — Dictionary tab

**Get Dictionary** — Click on this to fetch the category list from the server.

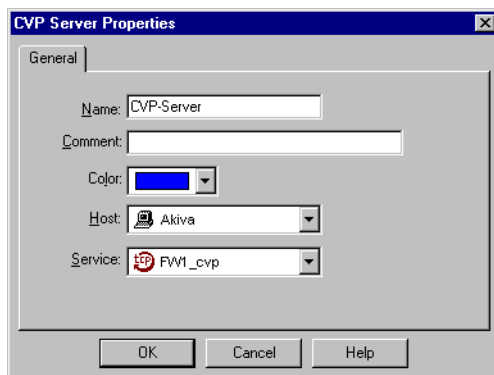
You can select individual categories from the list in the definition of the resource that uses this UFP server. For information, see “URI Definition window — Match tab (UFP)” on page 214.

## CVP Servers

CVP servers are used to inspect files before their retrieval, for example, to provide Anti-Virus services. For information about CVP, see “Implementing CVP Inspection” on page 366.

For examples of how to use CVP servers in a resource definition, see Chapter 6, “Services and Resources.”

## CVP Server Properties Window — General Tab



**FIGURE 10-5** CVP Server Properties window — General tab

**Name** — the server’s name

**Comment** — descriptive text

This text is displayed on the bottom of the **Server Object** window when this item is selected.

**Color** — the color of the server's icon

Select the desired color from the drop-down list.

**Host** — Select the host on which the server is running from the menu.

The host should have already been defined as a network object (see “Defining Network Objects” on page 97).

**Service** — From the menu, select the service for communication with the server.

For CVP servers, the service is FW1\_cvp.

## CVP Manager

### Overview

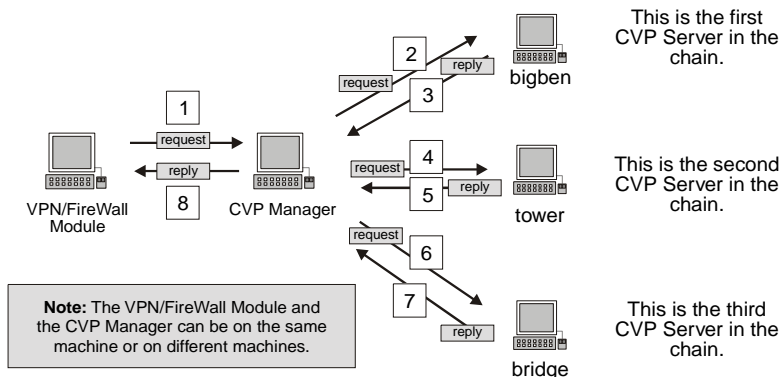
The CVP Manager application enables a Resource to invoke any number of CVP Servers. This capability is useful when each of the CVP Servers performs a different function.

In addition, identical CVP Servers can be configured to share the load among themselves.

The CVP Manager is defined on the VPN/FireWall Module as a CVP Server (see FIGURE 10-8 on page 325). The CVP Manager's configuration file (see “CVP Manager Configuration File” on page 325) specifies the sequence in which the CVP Servers are invoked, as well as other parameters.

### Different Functionality

In the configuration shown in FIGURE 10-6, the CVP Manager invokes the CVP Servers on bigben, tower and bridge, one after the other.

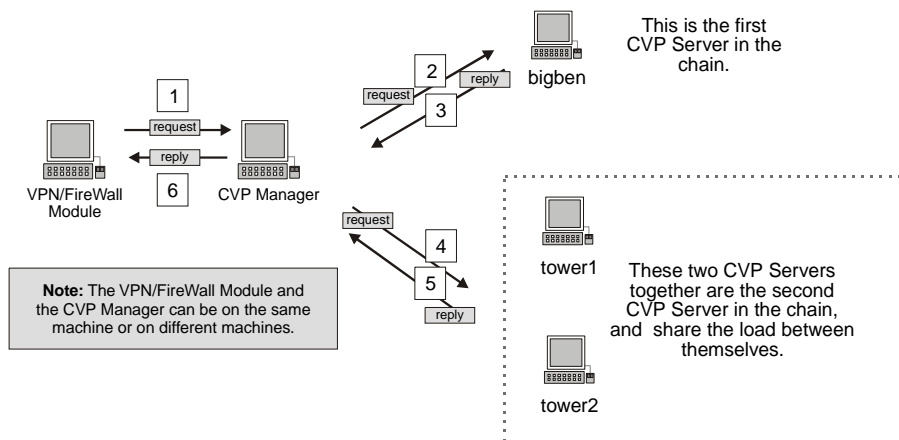


**FIGURE 10-6** Three CVP Servers invoked one after the other

The configuration in FIGURE 10-6 is specified in the configuration file in FIGURE 10-9 on page 326.

## Load Sharing

In the configuration shown in FIGURE 10-7, the CVP Manager invokes the CVP Server on bigben and then invokes either the CVP Server on tower1 or the CVP Server on tower2.



**FIGURE 10-7** Three CVP Servers with load sharing

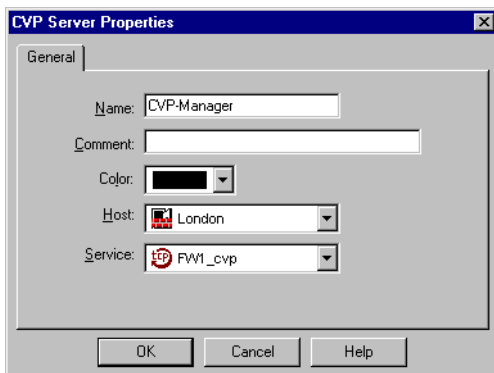
The configuration in FIGURE 10-7 is specified in the configuration file in FIGURE 10-10 on page 327.

## Configuration

To configure multiple CVP Servers using the CVP Manager, proceed as follows:

- 1** Install the CVP Manager, either on the same machine as a VPN/FireWall Module that will be invoking it or on a different machine.

- 2 On the VPN-1/FireWall-1 Management Station, define the CVP Manager as a CVP Server in the **CVP Server Properties** window (FIGURE 10-8).



**FIGURE 10-8** CVP Server Properties window

- 3 Configure the chained CVP Servers and specify the sequence in which they are invoked and other parameters.

The chained CVP Servers are configured in the `cvpm.conf` file on the machine on which the CVP Manager is installed (see “CVP Manager Configuration File” on page 325).

- 4 Define a Resource that specifies the CVP Manager as the CVP Server.
- 5 Use the Resource in a rule.
- 6 Install the Security Policy.

## Installation

The CVP Manager is an executable file and is available for the Windows NT and Solaris platforms. The CVP Manager can be installed when VPN-1/FireWall-1 is installed or at a later time.

## CVP Manager Configuration File

The configuration is specified in the file `cvpm.conf`, in the directory in which the CVP Manager is installed.

If there are syntax errors in the configuration file, then whenever the CVP Manager is invoked, an error message (“Request could not be handled on Content Security Server”) will be displayed on the CVP Manager machine and the user application (Web browser, FTP Client etc.). In addition, the error will be logged to the VPN-1/FireWall-1 Log.

## Example

The following configuration file describes the configurations shown in FIGURE 10-6 on page 323 and in FIGURE 10-7 on page 324.



**Note** – Words in **bold** are keywords. In some cases, a number is appended at the end of a keyword (for example, **chained\_server\_1**). The numbers must be consecutive.

The following configuration file describes the configuration shown in FIGURE 10-6 on page 323 (no load sharing).

```
CVP Configuration file
The port for FW-1-to-CVP-M communications
cvpm port 18181

Chain configuration
#####
0=continue processing after server replies "unsafe", 1=stop (drop)
drop_on_unsafe 1

Recovery time in minutes for load sharing
recovery_time 1

Number of servers on the chain
num_of_servers 3

chained_server_1 cvp_on_bigben
chained_server_2 tower_cvp_server
chained_server_3 cvp_srv_bridge

Server definitions
#####
cvp_on_bigben port 18181
cvp_on_bigben ip 195.024.205.243

tower_cvp_server port 18181
tower_cvp_server ip 195.024.205.154

cvp_srv_bridge port 18181
cvp_srv_bridge ip 195.024.205.157
```

**FIGURE 10-9** CVP Mannager Configuration - No Load Sharing Example

The following configuration file describes the configuration shown in FIGURE 10-7 on page 324 (with load sharing).

```
CVP Configuration file

The port for FW-1-to-CVP-M communications
cvpm port 18181

Chain configuration
#####
Number of servers in the chain
num_of_servers 2
chained_server_1 cvp_on_bigben
chained_server_2 tower_servers

0=continue processing after server replies "unsafe", 1=stop (drop)
drop_on_unsafe 1
Recovery time in minutes for load sharing
recovery_time 1

Server definitions
#####

cvp_on_bigben port 18181
cvp_on_bigben ip 195.024.205.243

Number of servers of Load-Sharing
tower_servers num_of_servers 2

The method can be random / round_robin
tower_servers method round_robin
tower_servers server1 av_on_tower1
tower_servers server2 av_on_tower2

av_on_tower1 port 18303
av_on_tower1 ip 195.024.205.154

av_on_tower2 port 18304
av_on_tower2 ip 195.024.205.154
```

**FIGURE 10-10** CVP Manager Configuration - Load Sharing Example

## Authenticated Communications (Control Channel)

You can establish a non-SSL authenticated communication (control) channel between the VPN/FireWall Module, the CVP Manager and the CVP Servers by using the `cvpm_putkey` command.

Syntax

```
cvpm_putkey [-port port_number | fw | none] [-p password] <target>
```

Options

| parameter   | meaning                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port        | One of the following (see the example for details): <ul style="list-style-type: none"><li>■ port_number — the port number on the CVP Manager (for the connection between the CVP Server and the CVP Manager)</li><li>■ fw — for the connection between the CVP Manager and the VPN/FireWall Module</li><li>■ none — for the connection between the CVP Manager and a CVP Server</li></ul> |
| -p password | The key (password). You will be prompted for this field if you do not enter it in the command line.                                                                                                                                                                                                                                                                                       |
| target      | The IP address of the other machine (with which the control channel will be established)                                                                                                                                                                                                                                                                                                  |

Example

In the configuration shown in FIGURE 10-6 on page 323, if you wish to establish authenticated control channels between the machines, proceed as follows:

- 1** On the VPN/FireWall Module, enter the following command:

```
fw putkey -p <password> <IP address of CVP Manager>
```

This command, together with the first `cvpm_putkey` command in step 2, establishes the authenticated control channel between the VPN/FireWall Module and the CVP Manager.

- 2** On the CVP Manager, enter the following commands:

```
cvpm_putkey -port fw -p <password> <IP address of VPN/FireWall Module>
cvpm_putkey -port none -p <password> <IP address of bigben>
cvpm_putkey -port none -p <password> <IP address of tower>
cvpm_putkey -port none -p <password> <IP address of bridge>
```

The last three `cvpm_putkey` commands, together with the individual `cvpm_putkey` commands in step 3 through step 5, establish the authenticated control channels between the CVP Manager and each of the CVP Servers.



- 3** On bigben, enter the following command:

```
cvpm_putkey -port 18181 -p <password> <IP address of CVP Manager>
```

- 4** On tower, enter the following command:

```
cvpm_putkey -port 18181 -p <password> <IP address of CVP Manager>
```

- 5** On bridge, enter the following command:

```
cvpm_putkey -port 18181 -p <password> <IP address of CVP Manager>
```

- 6** In the configuration files on all the machines (see FIGURE 10-9 on page 326, for example) use the `auth_port` parameter instead of the `port` parameter.

## Installation

To install the CVP Manager, proceed as follows:

- **NT** — Run `setup.exe` in the `windows\CPcvpm-41` directory on the CD.
- **Solaris** — Run `pkgadd` to install the `CPcvpm-41` package.

After the installation is complete, edit the `cvpm.conf` file (see “CVP Manager Configuration File” on page 325).

To start the CVP Manager, proceed as follows:

- **NT** — Start the CVP Manager Service using the Services Manager in the Control Panel.
- **Solaris** — Run the script `S99cvpm_d` in the `/etc/rc3.d` directory.

Alternatively, reboot the machine.

To remove CVP Manager, proceed as follows:

- **NT** — Use Add/Remove programs in the Control Panel.
- **Solaris** — Run `pkgrm CPcvpm-41`.

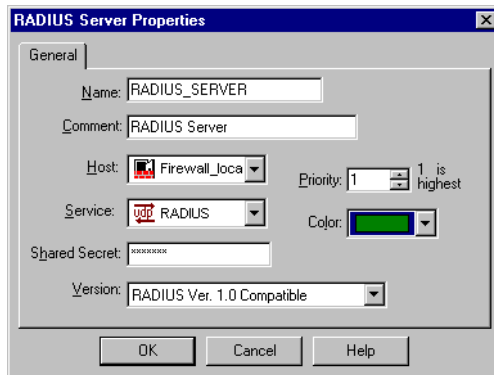
The target directory is not removed by this command.

## RADIUS Servers

RADIUS servers are used for authenticating users. For information about defining an Authentication scheme for a user, see “User Properties Window — Authentication tab” on page 158.

For information about Authentication schemes in general, see “Authentication Schemes” on page 484.

## RADIUS Server Properties Window — General Tab



**FIGURE 10-11** RADIUS Server Properties window — General tab

**Name** — the server’s name

**Comment** — descriptive text

This text is displayed on the bottom of the **Server Object** window when this item is selected.

**Color** — the color of the server’s icon

Select the desired color from the drop-down list.

**Priority** — When more than one RADIUS server is contacted (that is, when a group of RADIUS servers or **Any** is specified for a RADIUS user) then they are contacted in the sequence defined by their priorities, where a lower number specifies a higher priority.

**Host** — From the menu, select the host on which the server is running.

The host should have already been defined as a network object (see “Defining Network Objects” on page 97).

**Shared Secret** — enter a string of up to 15 nonspace characters.

The shared secret is a key that authenticates communication between the FireWalled machine and the RADIUS server. You must use the same shared secret you defined in the `clients` file on the RADIUS server.

**Service** — From the menu, select the service for communication with the server.

For RADIUS servers, the service is RADIUS.

**Version** — Select the version from the dropdown list.

The items in the list are given under `radius_versions` in the file `$FWDIR/lib/setup.C`.

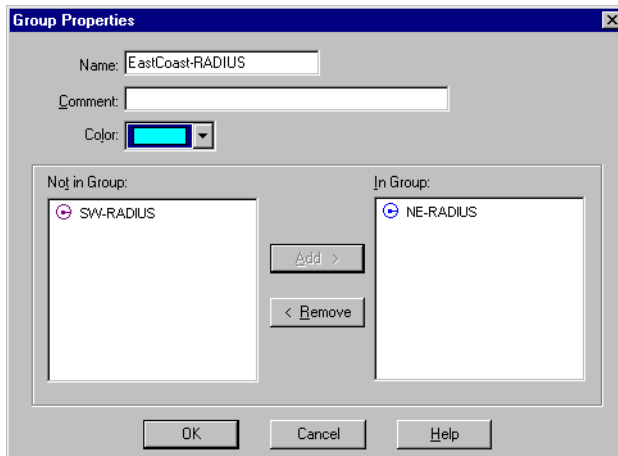
## RADIUS Server Groups

You can simplify the Rule Base by defining a group of RADIUS servers and using the group in rules. If a RADIUS server group is defined in a user's Authentication properties, VPN-1/FireWall-1 sends authentication requests to the servers in the group according to their priority, as defined in the **General Tab** of the **RADIUS Server Properties** window (FIGURE 10-11 on page 330). If two servers have the same priority, their order is determined arbitrarily.

### Creating a RADIUS Server Group

To create a group, create an object of type **RADIUS Group** using the Server Object Manager (see "Creating a New Server" on page 319). Next, add objects to the group using the **Group Properties** window (FIGURE 10-12 on page 331).

To display the **Group Properties** window, double-click on the group's name in the **Server Object Manager** window.



**FIGURE 10-12** Group Properties window

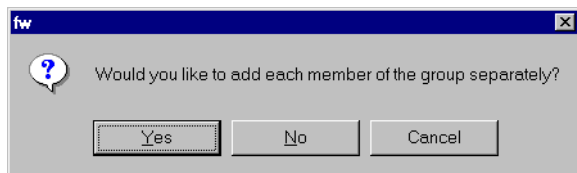
### Adding a Server to a RADIUS Server Group

In the left listbox (labeled **Not in Group**), select the servers you wish to include in the group. Use the **Add** button to add individual objects and to add groups to the group.

You can add a group to another group in one of two ways:

- 1** You can individually add all the objects in one group to another group, without nesting. Click on **Yes** in reply to the question in the window (FIGURE 10-13).

- 2 You can nest groups inside groups to create a group hierarchy of any desired complexity. Click on **No** in reply to the question in the window.



**FIGURE 10-13** Adding a Group to a Group



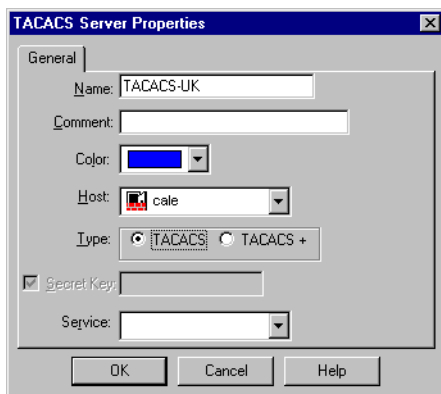
**Note** – All the servers in a server group must be of the same type.

## Deleting a Server from a RADIUS Server Group

Select the servers to be deleted from the right listbox (labeled **In Group**), and then click on **Remove**.

## TACACS Servers

### TACACS Server Properties Window — General Tab



**FIGURE 10-14** TACACS Server Properties window — General tab

**Name** — the server's name

**Comment** — descriptive text

This text is displayed on the bottom of the **Server Object** window when this item is selected.

**Color** — the color of the server's icon

Select the desired color from the drop-down list.

**Host** — From the menu, select the host on which the server is running.

The host should have already been defined as a network object (see “Defining Network Objects” on page 97).

**Type** — Select **TACACS** or **TACACS +**.

**Secret Key** — For more information on this field, see the TACACS server documentation.

**Service** — From the menu, select the service for communication with the server **Type**.

For TACACS+ Servers, for example, the service is “TACACS+”.

## AXENT Pathways Defender Servers

### Defender Server Properties Windows—General Tab



**FIGURE 10-15** Defender Server Properties window — General tab

**Name** — the server’s name

**Comment** — descriptive text

This text is displayed on the bottom of the **Server Object** window when this server is selected.

**Color** — the color of the server’s icon

Select the desired color from the drop-down list.

**Host** — the host on which the primary Axent Defender server is running

Select the host from the drop-down list. The host should have already been defined as a workstation.

**Backup Host** — the host of the backup Axent Defender server

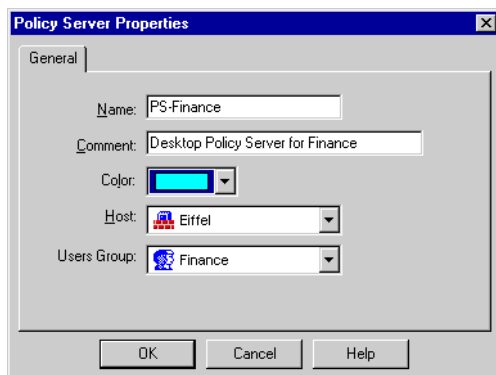
The **Backup Host** is not a separate Axent server, but is a backup server to the primary server defined under **Host**. Because it is not a separate server, it does not have its own **Agent Name** and **Agent ID**.

**Agent ID** — the Agent ID of the VPN/FireWall Module, as defined on the Axent Pathways Defender Server

**Agent Key** — a 16 hexadecimal digit key

This key is defined on the Axent Pathways Defender Server and is used to encrypt communication between the VPN/FireWall Module and the Axent Pathways Defender Server.

## Policy Servers



**FIGURE 10-16** Defender Server Properties window — General tab

## LDAP Account Units

In VPN-1/FireWall-1, users can be managed on an LDAP (Lightweight Directory Access Protocol) Server. The LDAP Server and VPN-1/FireWall-1 Management Server usually reside on different hosts and are maintained by different people. Separating the functionality of the two systems provides the following benefits:

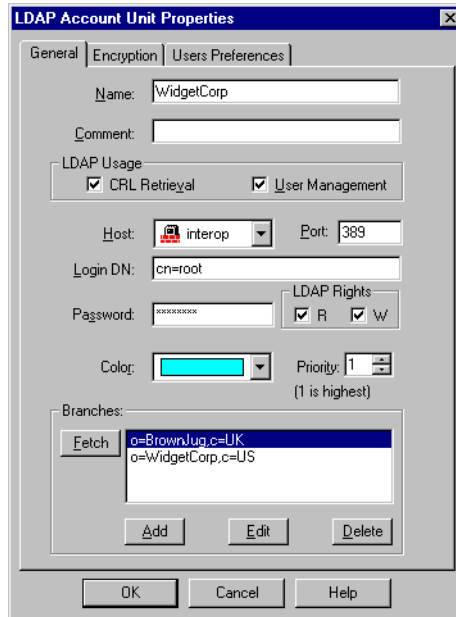
- The system administrator can use existing LDAP-compliant directories.
- A single VPN-1/FireWall-1 Management Server can be used by several departments or customers, each of which can manage its own users independently.
- Users can maintain and change their own passwords.

There is no limit to the number of users that can be defined on an LDAP Server.

An LDAP Server can contain multiple branches ("o=University of Michigan,c=UK", for example, is a branch). A Check Point Account Unit consists of a subset of the branches defined on an LDAP Server. A user database can be made up of more than one Account Unit. Any number of Account Units can be defined to VPN-1/FireWall-1.

For information about how LDAP Account Units are used in VPN-1/FireWall-1, see “VPN-1/FireWall-1 LDAP Account Management” on page 174.

## LDAP Account Unit Properties Window — General Tab



**FIGURE 10-17** LDAP Account Unit Properties window — General tab

**Name** — the Account Unit’s name

**Comment** — descriptive text

This text is displayed on the bottom of the **Server Object** window when this LDAP Server is selected.

**Host** — the host on which the LDAP Server is running

Select the host from the drop-down list. The host should have already been defined as a network object (see “Defining Network Objects” on page 97).

**Port** — the port on which the LDAP Server is listening for non-encrypted communication

**CRL Retrieval** — This Account Unit is used for CRL retrieval, that is, it is the CRL depository for OPSEC PKI-enabled Certificate Authorities (see Chapter 3, “Certificate Authorities” of *Check Point Virtual Private Networks*).

If you check **CRL Retrieval**, you only need to specify **Host**, **Port**, and server **Branches** in this window.

**User Management** — This Account Unit is used for managing users in an LDAP directory.

**User Management** is enabled only if **Use LDAP Account Management** is checked in the **LDAP** tab of the **Properties Setup** window (FIGURE 7-7 on page 249).

**Login DN** — the DN that will be used to bind (login) to the Account Unit

**Password** — the password for binding

**LDAP Rights** — the VPN/FireWall Module's access privileges on the LDAP Server

Check **R**(ead) or **W**(rite) or both.

If **Write** is checked, users can update their VPN-1/FireWall-1 passwords on the LDAP Server.

If the LDAP Server is a slave, uncheck **W**.

**Color** — the color of the server's icon

Select the desired color from the drop-down list.

**Priority** — this Account Unit's priority in relation to other Account Units

For an explanation of how this parameter is used, see "Enforcing a Security Policy" on page 180.

**Branches** — the branches of the LDAP directory which will be searched when querying to this LDAP Server

## Branches



**Note** – It is recommended that the same branches be defined for an Account Unit both in the VPN-1/FireWall-1 GUI and in the Account Management Client (if you are running the Account Management Client directly rather than from within the Windows GUI).

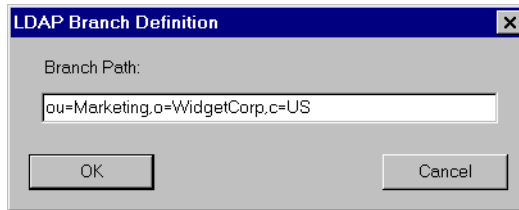
## Fetching All Branches

If your LDAP Server is Version 3.0 or higher, you can fetch all the branches (suffixes) supported by the LDAP Server by clicking on **Fetch**.



## Adding a New Branch

To add a new branch, click on **Add**. The **LDAP Branch Definition** window is displayed.



**FIGURE 10-18** LDAP Branch Definition

Enter the branch and click on **OK**.

## Changing a Branch

To change a branch definition, select the branch and click on **Edit**.

## Deleting a Branch

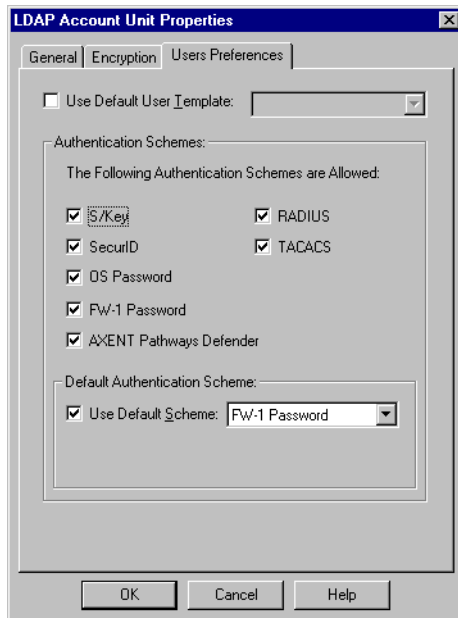
To delete a branch from the list, select the branch and click on **Delete**.

## LDAP Account Unit Properties Window — User Preferences Tab

The **User Preferences** tab specifies the following:

- the default template that will be used to provide VPN-1/FireWall-1-specific attributes to LDAP users maintained with a third-party LDAP Client

- the authentication schemes that will be supported by the VPN/FireWall Module for users defined on this LDAP Account Unit.



**FIGURE 10-19** LDAP Account Unit Properties window — User Preferences tab

**Use Default User Template** — Specifies the VPN-1/FireWall-1 user template from which to obtain VPN-1/FireWall-1-specific attributes for LDAP users for whom these attributes are not defined, that is, users maintained with a third-party LDAP Client.

When users are maintained with a third-party LDAP Client in which VPN-1/FireWall-1-specific attributes are not defined, the missing VPN-1/FireWall-1-specific attributes are retrieved at run-time from the VPN-1/FireWall-1 template specified in **Use Default User Template**. This template should not define attributes that vary from user to user, because there is no way to define these values — they don't appear in the LDAP Client and the user is not defined in the VPN-1/FireWall-1 User Database.

For example, the template should not specify IKE with shared-secret (because the secret is different for each user), but it can specify IKE with certificates. Note that the template can specify internal (VPN-1/FireWall-1) password authentication scheme, even though this is different for each user, because all LDAP servers support password authentication.



**Warning** – VPN-1/FireWall-1-specific attributes will not be visible in the LDAP Client for users to whom the default user template is applied.

This option is not supported by VPN-1/FireWall-1 Modules prior to Version 4.1, but Use Default Scheme is supported.

**Authentication Schemes** — Specifies the authentication schemes enabled on the LDAP Account Unit.

**Use Default Scheme** — Specifies the authentication scheme to be used when no authentication scheme is defined for the user on the Account Unit, for example, when users are maintained with a third-party LDAP Client in which VPN-1/FireWall-1-specific attributes are not defined.

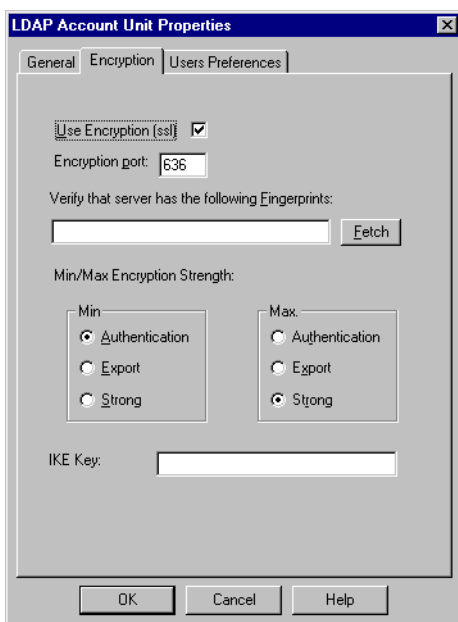
This option is enabled only if **Use Default User Template** is not checked, because the template specified in **Use Default User Template** includes an authentication scheme.

See “fw1auth-method” on page 185 for more information.

If you select TACACS or RADIUS, you will be prompted to enter the server name.

S/Key is not available here, because it includes user-specific information, and there is no way to define user-specific information in this case (see **Use Default User Template** above).

## LDAP Account Unit Properties Window — Encryption Tab



**FIGURE 10-20** LDAP Account Unit Properties window — Encryption tab

**Use Encryption (SSL)** — whether to connect to this Server using SSL

**Server’s fingerprint** — the Server’s fingerprint

VPN-1/FireWall-1 does not use a Certificate Authority to obtain or confirm LDAP Server keys. Before your first SSL connection, you should fetch its fingerprint and then confirm the fingerprint by fax or telephone or some other non-network means. You can also enter the data in this field manually.

On subsequent SSL connections to the LDAP Server, VPN-1/FireWall-1 requests the Server's key, computes its fingerprint and compares it to the one it previously obtained and stored. If there is a discrepancy, all access to the LDAP Server is aborted.

**Encryption Port** — the port on the LDAP Server to which to connect

The default port numbers is 636 for an LDAP SSL connection.

**Min/Max Encryption Strength** — Select the weakest (under **Min**) and strongest (under **Max**) encryption method the Account Unit is prepared to use.

TABLE 10-3 lists the methods used for each Strength. Note that **Strong** in the GUI corresponds to Very Strong in the table.

**TABLE 10-3** Encryption Method Parameters

| <b>Strength</b>                                                    | <b>Authentication Method</b> | <b>Encryption and Data Integrity Methods</b>                                                                                                                                             |
|--------------------------------------------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication</b>                                              | RSA (512 bit)                | no encryption<br>data integrity: MD5 or SHA-1, depending on the other side                                                                                                               |
| <b>Export</b>                                                      | RSA (512 bit)                | <ul style="list-style-type: none"> <li>■ RC4 (40 bit) and MD5, <i>or</i></li> <li>■ DES (40 bit) and SHA-1</li> </ul>                                                                    |
| Strong (this cannot be specified in the GUI but can be negotiated) | RSA (1024 bit)               | <ul style="list-style-type: none"> <li>■ RC4 (64 bit) and MD5, <i>or</i></li> <li>■ DES (40 bit) and MD5 or SHA-1, depending on the other side</li> </ul>                                |
| Very Strong (this is indicated in the GUI by <b>Strong</b> )       | RSA (1024 bit)               | <ul style="list-style-type: none"> <li>■ RC4 (128 bit) and MD5 or SHA-1, depending on the other side, <i>or</i></li> <li>■ 3DES and MD5 or SHA-1, depending on the other side</li> </ul> |

**IKE Key** — the key with which users' IKE pre-shared secrets are encrypted on the Account Unit

# Security Servers and Content Security

---

## In This Chapter

|                         |                 |
|-------------------------|-----------------|
| <i>Security Servers</i> | <i>page 341</i> |
| <i>Content Security</i> | <i>page 360</i> |

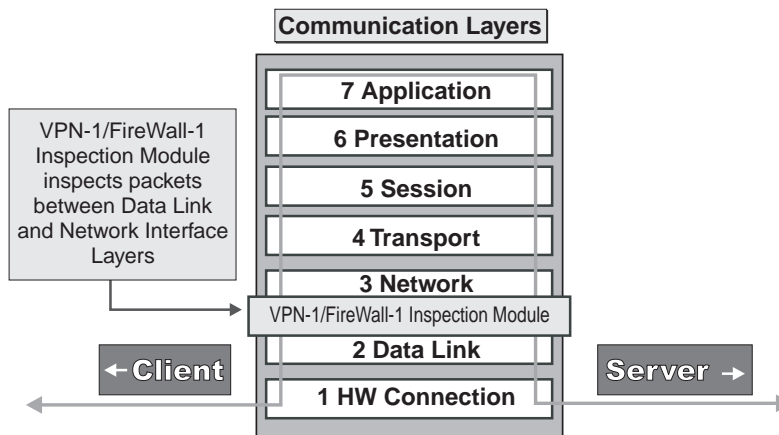
## Security Servers

### Overview

When the first packet of a new connection arrives at a VPN/FireWall Module (a gateway or host with FireWall-1 installed), the Inspection Module examines the Rule Base to determine whether or not the connection is to be allowed. VPN-1/FireWall-1 applies the first rule that describes the connection (**Source**, **Destination** and **Service**); if this rule's **Action** is **Accept** or **Encrypt**, then the connection is allowed.

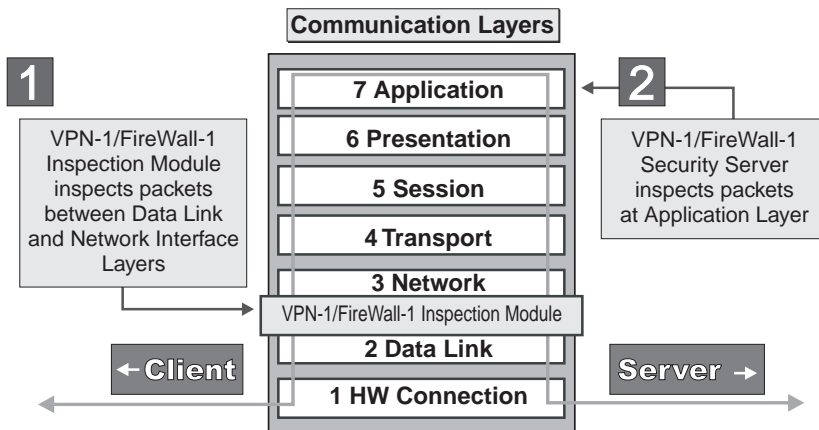
Once a connection is established, VPN-1/FireWall-1 adds the connection to the `connections` table (see “Auxiliary Connections” on page 307). Subsequent packets of the connection are verified against the `connections` table rather than against the Rule Base. The packet is allowed to pass only if the connection is listed in the `connections` table.

In a connection such as this, the entire connection is handled by the VPN-1/FireWall-1 Inspection (Kernel) Module (FIGURE 11-1).



**FIGURE 11-1** A connection handled by the VPN-1/FireWall-1 Inspection (Kernel) Module

When the relevant rule specifies a **Resource** under **Service**, or **User Authentication** under **Action**, the corresponding VPN-1/FireWall-1 Security Server is invoked in order to mediate the connection (FIGURE 11-2).



**FIGURE 11-2** A connection mediated by a VPN-1/FireWall-1 Security Server

The VPN-1/FireWall-1 Security Servers provide two features:

**1** Authentication

For information about Authentication, see Chapter 15, “Authentication.”

**2** Content Security

For information about Content Security, see “Content Security” on page 360.

When a VPN-1/FireWall-1 Security Server is invoked, the Inspection (Kernel) Module diverts all the packets in the connection to the Security Server, which performs the required authentication and/or Content Security inspection. If the connection is allowed, then the Security Server opens a second connection to the final destination. Altogether, there are two connections: one from the client to the Security Server, and another from the Security Server to the final destination (the server, from the client's point of view). Both of these connections are maintained in the `connections` table.

There are five VPN-1/FireWall-1 Security Servers, as described in TABLE 11-1.

**TABLE 11-1** VPN-1/FireWall-1 Security Servers — features

| Server | Authentication | Content Security | Comments        |
|--------|----------------|------------------|-----------------|
| TELNET | yes            | no               |                 |
| RLOGIN | yes            | no               |                 |
| FTP    | yes            | yes              |                 |
| HTTP   | yes            | yes              |                 |
| SMTP   | no             | yes              | secure sendmail |

#### TELNET

The TELNET Security Server provides Authentication services, but not Content Security.

#### RLOGIN

The RLOGIN Security Server provides Authentication services, but not Content Security.

#### FTP

The FTP Security Server provides Authentication services, and Content Security based on FTP commands (PUT/GET), file name restrictions, and CVP checking (for example, for viruses).

In addition, the FTP Security Server logs FTP `get` and `put` commands, as well as the associated file names, if the rule's **Track** is **Long Log**.

#### HTTP

The HTTP Security Server provides Authentication services, and Content Security based on schemes (HTTP, FTP, GOPHER etc.), methods (GET, POST, etc.), hosts (for example, "\*.com"), paths and queries. Alternatively, a file containing a list of IP addresses and paths to which access will be denied or allowed can be specified.

#### SMTP

The SMTP Security Server provides Content Security based on **From** and **To** fields in the envelope and header and attachment types. In addition, it provides a secure sendmail application that prevents direct online connection attacks.

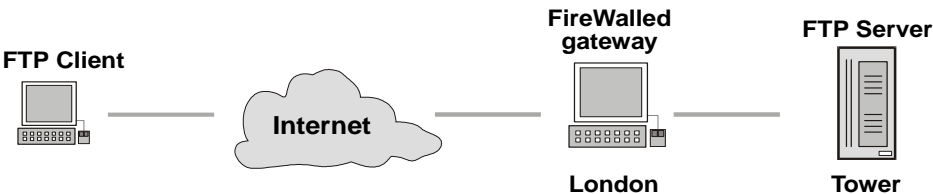
The SMTP Security Server also serves as an SMTP address translator, that is, it can hide real user names from the outside world by rewriting the **From** field, while maintaining connectivity by restoring the correct addresses in the response.

## Security Servers and the Rule Base

### The ‘Insufficient Information’ Problem

At the time the Rule Base is examined, it is not always possible for VPN-1/FireWall-1 to know which rule applies to a connection. This is because the connection’s first packet, on the basis of which VPN-1/FireWall-1 must determine whether to allow or disallow the connection, does not contain all the information VPN-1/FireWall-1 needs in order to determine which rule applies to the connection.

For example, consider the following network configuration and Rule Base:



**FIGURE 11-3** Protected FTP Server

| Source         | Destination | Services         | Action   | Track     | Install On |
|----------------|-------------|------------------|----------|-----------|------------|
| Professors@Any | tower       | ftp              | UserAuth | Short Log | Gateways   |
| Any            | tower       | ftp->GetResource | Accept   | Long Log  | Gateways   |
| Any            | Any         | Any              | Reject   | Long Log  | Gateways   |

Suppose the user Alice FTPs to Tower. Should VPN-1/FireWall-1 authenticate her (in accordance with the first rule) or accept the connection without authentication (in accordance with the second rule)? The answer depends on whether Alice belongs to the group **Professors@Any**, but VPN-1/FireWall-1 can only find out who she is (and on the basis of who she is, to which user groups she belongs) by invoking the Authentication process.

However, VPN-1/FireWall-1 cannot first authenticate Alice (to find out who she is) and then decide which rule to apply, because this can lead to the absurd situation where a user fails the Authentication process but the connection is still allowed.

### The Solution

The VPN-1/FireWall-1 Authentication procedure, depicted in FIGURE 11-4 on page 346, solves this problem. The procedure prevents an Authentication rule from being applied when another less restrictive rule (that is, a rule without Authentication) can also be applied to the connection.



## Examples

Consider the following Rule Base:

| Source         | Destination | Services         | Action   | Track     | Install On |
|----------------|-------------|------------------|----------|-----------|------------|
| Professors@Any | tower       | ftp              | UserAuth | Short Log | Gateways   |
| Teachers@Any   | tower       | ftp->GetResource | UserAuth | Long Log  | Gateways   |
| Any            | Any         | Any              | Reject   | Long Log  | Gateways   |

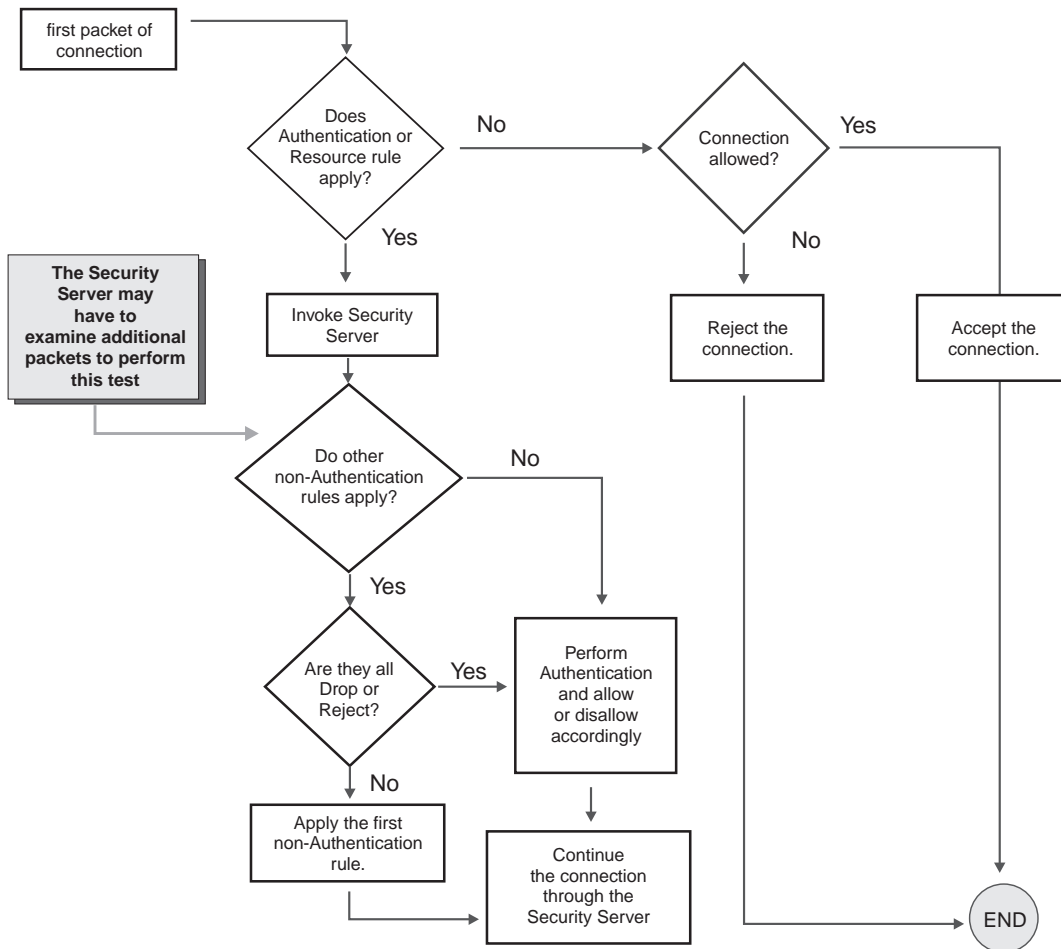
Suppose a user FTPs to Tower. VPN-1/FireWall-1 matches the first rule, and invokes the FTP Security Server and authentication process. However, if the user belongs to **Teachers@Any**, then the second rule is the one which applies to the connection. Since both rules specify Authentication, it doesn't matter that the Authentication was invoked by a rule other than the one that was applied to the connection. This is because Authentication scheme and password are attributes of the user, not of the group, and are the same whether the user is being authenticated as a member of **Professors@Any** or of **Teachers@Any**. Next, consider this Rule Base:

| Source         | Destination | Services         | Action   | Track     | Install On |
|----------------|-------------|------------------|----------|-----------|------------|
| Professors@Any | tower       | ftp              | UserAuth | Short Log | Gateways   |
| Any            | tower       | ftp->GetResource | Accept   | Long Log  | Gateways   |
| Any            | Any         | Any              | Reject   | Long Log  | Gateways   |

Suppose a user FTPs to Tower. The first matching rule is the first rule (whose **Action** is **UserAuth**), but it is the second rule that is applied, because it also matches but its **Action** is **Accept**. In this case, it is important that the original rule was not applied, that is, that there was no Authentication even though the Security Server was invoked.



**Note** – In this case, the connection is mediated by the Security Server, even though there was no Authentication.



**FIGURE 11-4** Authentication Procedure

You can verify this by stepping through the Authentication procedure depicted in FIGURE 11-4 on page 346.

## Outgoing Connections

User Authentication and Resource rules are applied only to connections incoming to a FireWalled machine. An outgoing connection originating on a FireWalled machine will not be folded into a Security Server on that machine, but will be dropped (because of the third rule).

## FTP Security Server

When an FTP connection is mediated by the VPN-1/FireWall-1 FTP Security Server, then the user's requested FTP commands and file names are matched against the FTP Resource defined in the relevant rule.

The FTP Security Server is invoked when a rule specifies an FTP Resource in the **Service** field and/or User Authentication in the **Action** field. If no FTP Resource is specified in the rule (that is, if the Security Server is invoked because the **Action** is User Authentication), then an FTP Resource of GET and PUT allowed for all files is applied.

## FTP Resource Matching

FTP Resource matching consists of matching methods and file names to the Resource definition.

### Methods

TABLE 11-2 lists the FTP commands that correspond to the methods specified in the FTP Resource definition.

**TABLE 11-2** FTP actions and commands

| method (defined in the FTP Resource) | applies to these FTP commands | meaning          |
|--------------------------------------|-------------------------------|------------------|
| GET                                  | RETR                          | retrieve         |
|                                      | RNFR                          | rename from      |
|                                      | XMD5                          | MD5 signature    |
| PUT                                  | STOR                          | store            |
|                                      | STOU                          | store unique     |
|                                      | APPE                          | append           |
|                                      | RNFR                          | rename from      |
|                                      | RNTO                          | rename to        |
|                                      | DELE                          | delete           |
|                                      | MKD                           | make directory   |
|                                      | RMD                           | remove directory |

The VPN-1/FireWall-1 FTP Security Server passes all other FTP commands to the FTP server for execution.

### File Names

File name matching is based on the concatenation of the file name in the command and the current working directory (unless the file name is already a full path name) and comparing the result to the path specified in the FTP Resource definition.

When specifying the path name in the FTP Resource definition, only lower case characters and a directory separator character / can be used.

The Security Server modifies the file name in the command as follows:

- for DOS, the drive letter and the colon (:) is stripped for relative paths
- the directory separator character (/ or \) is replaced, if necessary, with the one appropriate to the FTP server's OS

In some cases, the Security Server is unable to resolve the file name, that is, it is unable to determine whether the file name in the command matches the file name in the resource.

Example - DOS

Suppose the current directory is d:\temp and the file name in the resource is c:x. Then the Security Server is unable to determine the absolute path of the file name in the command because the current directory known to the Security Server is on disk D: and the file is on disk C:, which may have a different current directory.

Example - Unix

If the file name in the command contains . . references which refer to symbolic links, then it's possible that the file name in the command matches the resource's path, but that the two in fact refer to different files.

When the Security Server cannot resolve a file name, the action it takes depends on the **Action** specified in the rule being applied:

- If the rule's **Action** is Reject or Drop, then the rule is applied and its **Action** taken.
- If the rule's **Action** is Accept, Encrypt or Authenticate, then:

If the resource path is \* or there is no resource, the rule is applied.

Otherwise, the rule is not applied. Instead, VPN-1/FireWall-1 scans the Rule Base and applies the next matching rule (which may be the default rule that drops everything). In this case, a potential problem is that the rules may specify different entries in their **Track** fields. For example, it may happen that the original rule specifies **Accounting** in the **Track** field while the rule that is applied does not.

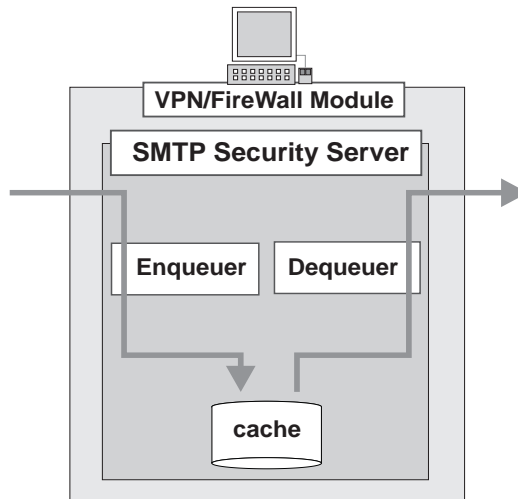
## SMTP Security Server

The SMTP Security Server does not provide Authentication, because there is no human user at a keyboard who can be challenged for authentication data. However, the SMTP Security Server provides Content Security that enables a Security Administrator to:

- provide mail address translation by hiding outgoing mail's **From** address behind a standard generic address that conceals internal network structure and real internal users
- drop mail from given addresses

- strip MIME attachments of specified types from mail
- strip the **Received** information from outgoing mail, in order to conceal internal network structure
- drop mail messages above a given size
- CVP checking (for example, for viruses)

In addition, the SMTP Security Server provides additional security over standard sendmail applications. Its functionality is split between two separate modules (FIGURE 11-5), so there is no direct path connecting mail servers, preventing direct online connections to the real sendmail application.



**FIGURE 11-5** VPN-1/FireWall-1 SMTP Security Server

One process writes incoming messages to a disk cache, and the other process empties the cache.

#### Functionality

The VPN-1/FireWall-1 SMTP Security Server supports the following SMTP commands:

- |        |        |        |
|--------|--------|--------|
| ■ RCPT | ■ QUIT | ■ HELP |
| ■ MAIL | ■ DATA | ■ RSET |
| ■ HELO | ■ NOOP | ■ VRFY |

The VRFY command always returns USEROK, to prevent repeated messages from automatic mailers.

SMTP Security Server Configuration

The SMTP Security Server configuration file is `$FWDIR/conf/smtp.conf`.

**TABLE 11-3** Fields in `$FWDIR/conf/smtp.conf`

| parameter      | meaning                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| timeout        | number of seconds after which connection times out                                                              |
| scan_period    | how frequently the spool directory is scanned                                                                   |
| resend_period  | number of seconds after which the SMTP Security Server resends the message after failing to deliver the message |
| abandon        | number of seconds after which the SMTP Security Server abandons attempts to resend                              |
| rundir         | SMTP Security Server files are written at and below this directory                                              |
| postmaster     | to whom to send error messages                                                                                  |
| default_server | the actual sendmail application resides here                                                                    |
| error_server   | the server to be notified in the event of an error                                                              |

Alerts

The SMTP Security Server can be configured to issue alerts in the event of various SMTP-related system error conditions, such as insufficient disk space (possibly caused by a denial-of-service attack).

HTTP Security Server

Support for FTP

The HTTP Security Server supports FTP requests through a web browser. The HTTP Security Server must be defined as the HTTP proxy to the user's Web browser. This is done in the user's Web browser proxy settings.

FIGURE 11-6 shows the proxy configuration windows for Netscape and Internet Explorer.

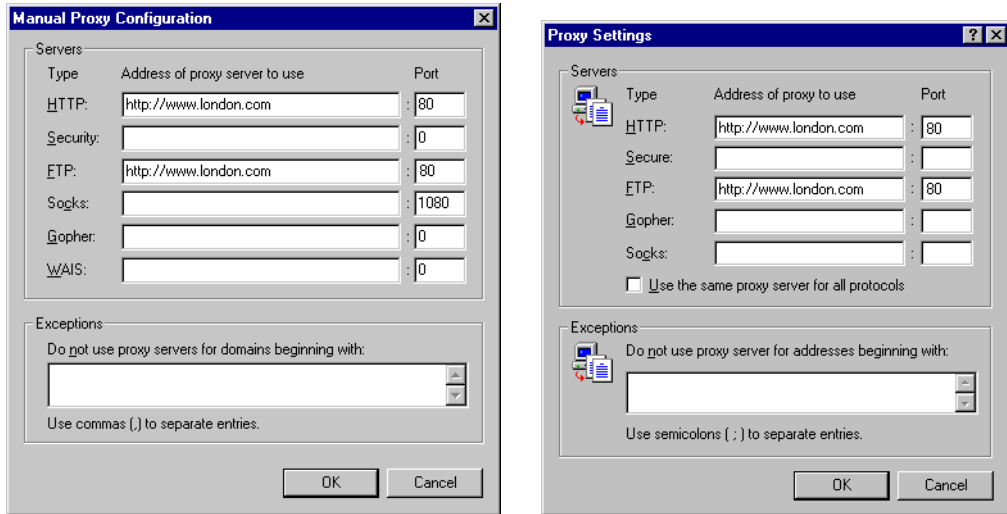


FIGURE 11-6 Proxy Configuration — Netscape 4.0 and Internet Explorer 3.0x

When a user requests an FTP URL through a browser:

- 1 The browser connects to the Security Server and sends an HTTP request with FTP as the method.
- 2 The Security Server opens an FTP session with the requested server.
- 3 The Security Server sends the FTP request to the server and formats all responses as HTTP messages, which it sends to the browser. These messages are listed in the file `/conf/f2ht-msgs`.

The Security Server sends a RETR request to the FTP server to determine whether the requested URL specifies a directory or plain file. If the FTP server returns an error message with a text line indicating the request is not a plain file, the Security Server assumes the requested URL is a directory. The Security Server then sends the directory listing to the browser as an HTML page.

If the requested URL is a file, the Security Server determines whether it is a text file or a binary file. If the requested file ends with one of the suffixes listed in the file `/conf/f2ht-bin-sfxs`, it is considered a binary file.

FTP requests through a web browser are enabled by both User Authentication and URI Resource rules. If the relevant rule specifies a URI Resource, then **ftp** must be defined as one of the enabled **Schemes** in the **URI Definition** window.

For more information on URI Resources, see “URI Resources” on page 205.

## Support for HTTPS

HTTPS (HTTP encrypted by SSL) connections are handled by the HTTP Security Server in the following ways:

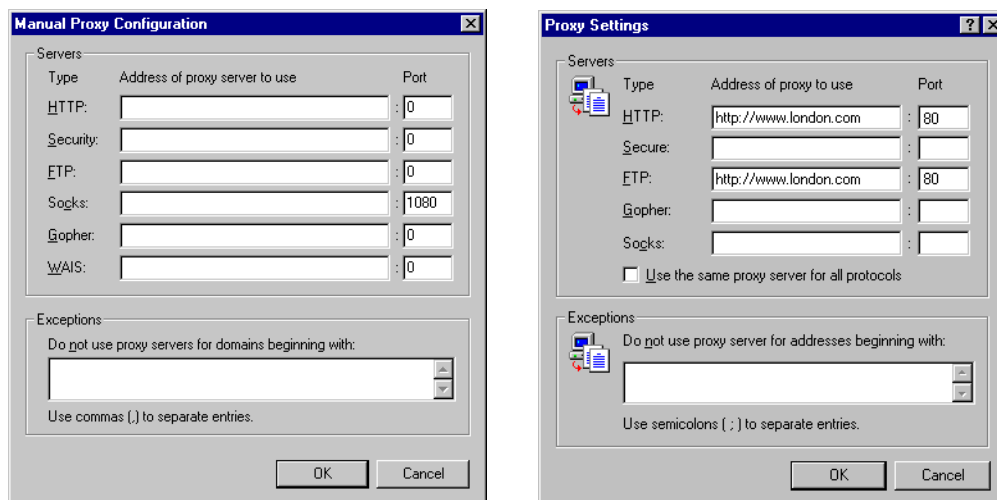
- **Security Proxy Mode** — In Security Proxy mode, the HTTP Security Server is defined as the “security proxy” in the user’s Web browser settings. The HTTP Security Server acts as a proxy for HTTPS connections, but does not inspect content.
- **Non-transparent Mode** — The HTTP Security Server is configured to encrypt and decrypt HTTPS connections. This option is known as “Non-transparent”, because the user of HTTPS must initiate the connection on the gateway before connecting to the target server.

### Security Proxy Mode

HTTPS (HTTP encrypted by SSL) connections can be handled by the HTTP Security Server when it is defined as the Security Proxy to the local user’s Web browser. The HTTP Security Server proxies outgoing HTTPS connections, but does not inspect content. This option can be used with User Authentication rules to authenticate outgoing HTTPS, and with Resource rules. User Authentication and Resource rules can be used together.

The user can configure a Security Proxy for the following Web browsers:

- Internet Explorer version 3.0x and higher
- Netscape version 4.0x and higher



**FIGURE 11-7** HTTP Proxy and Security Proxy Settings — Netscape 4.0x and Internet Explorer 3.0x

HTTPS requests generally use the HTTP “CONNECT” method (tunneling mode). Because the CONNECT method only specifies a hostname and port, the HTTP Security Server does not have access to the content of the communication, not even the URL. In addition, the Security Server does not verify that the connections are really using



HTTPS — it only checks the requested hostname and port number. All communication between the client and the target server is encrypted — the HTTP Security Server mediates the connection. This is useful if internal users want to send encrypted information over the Internet.



**Note** – Although the connection is encrypted between the local client and the external server, the authentication session between the local client and the HTTP Security Server is clear (unencrypted).

### User Authentication Rules

In Security Proxy mode, you can provide security by requiring internal users to authenticate before accessing external HTTPS servers. For more information, see “Authenticating Internal Users Accessing External HTTPS (Security Proxy Mode)” on page 505.

### URI Resource rules

The **URI Definition** window must specify the following:

**Connection Methods** (on the **General** tab) — check **Tunneling**

When **Tunneling** is checked, HTTP requests using the CONNECT method are matched. The HTTP Security Server does not inspect the content of the request, not even the URL. Only the host and port number can be checked. Therefore, when **Tunneling** is checked, some Content Security options in the URI Resource specification, (for example, CVP options, HTML weeding) are disabled.

If you check **Tunneling**, you may still use the URI File or UFP specifications. A URI File specification must define a file that lists only server names and their port numbers. The UFP specification must use a UFP server that maintains a list of only server names and port numbers.

**Host** (on the **Match** tab)— Specify the host and port of a known HTTPS server, for example:

```
https server host:443
```

The field to the left of the colon specifies the URI’s host. The field to the right of the colon specifies the port.

A wildcard character (“\*”) indicates any host or any port. For example, you can specify “\*:443” or “\*:\*”. For HTTPS, “\*” (a single wildcard character) is not a valid entry, though “\*” is a valid entry for HTTP or FTP resources.

For more information on URI Resources, see “URI Resources” on page 205.

## Non-transparent Mode and HTTPS

To enable the HTTP Security Server to inspect the contents of HTTPS connections, you can configure the HTTP Security Server to encrypt and decrypt HTTPS connections. This requires the implementation of Non-transparent Authentication.

This option is known as “Non-transparent Mode” because the user of HTTPS must request the gateway before being allowed to continue to the target host. Because the HTTP Security Server is not defined as a Security Proxy to the user’s Web browser, Non-transparent Mode is best used to authenticate external users accessing internal servers.

For information on configuring support for HTTPS in Non-transparent Mode, see “HTTP Security Server and Non-Transparent Authentication” on page 509 in Chapter 15, “Authentication.”

## Interaction with OPSEC Products

The VPN-1/FireWall-1 Security Servers support third-party products working with Check Point’s OPSEC SDK. In the OPSEC framework, the enterprise security system is composed of several components, each of which is provided by a different vendor and may be installed on a different machine. FireWall-1 distributes security tasks to the OPSEC components. Transactions between FireWall-1 and OPSEC security components take place using open, industry standard protocols.

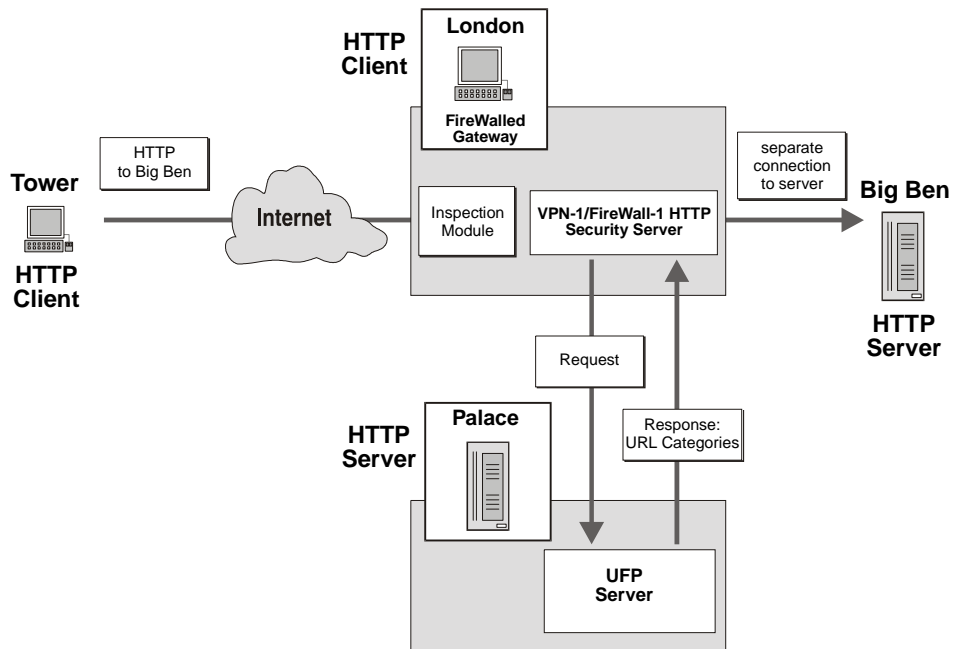
Information about OPSEC is available at [www.opsec.com](http://www.opsec.com).

Example OPSEC components are:

- a CVP (Content Vectoring Protocol) server that examines files for content
- a UFP (URL Filtering Protocol) server that categorizes URLs

In a common OPSEC model, a VPN-1/FireWall-1 Security Server acts as a client sending requests to an OPSEC server. The Security Server intercepts a connection and generates a request to the OPSEC server. The server processes the request and sends a reply to the Security Server, which processes the original connection based on the reply.

FIGURE 11-8 shows how the HTTP Security Server handles a connection request to a URL:



**FIGURE 11-8** Connection invoking a UFP Server

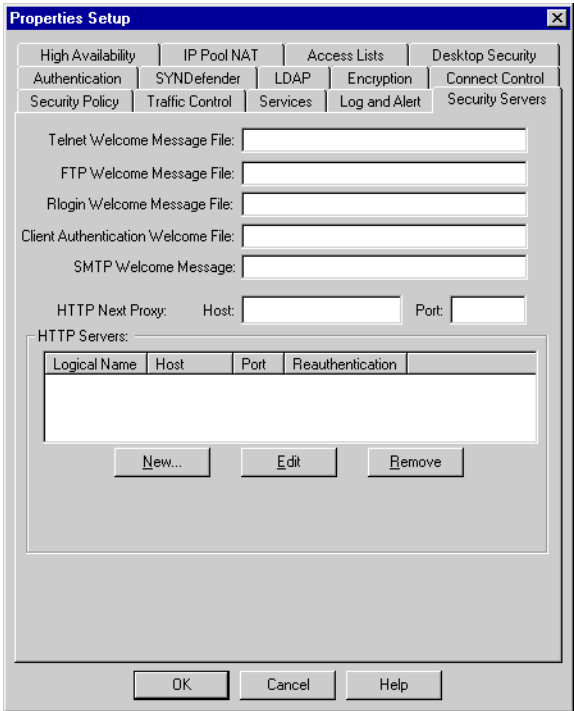
- 1** VPN-1/FireWall-1 intercepts a connection request to a URL.  
The connection matches a rule which specifies a URI Resource under the Rule Base **Service** field. The Resource definition specifies a UFP server which maintains a list of URLs and their categories. VPN-1/FireWall-1 determines that the UFP server must be invoked.
- 2** VPN-1/FireWall-1 diverts the connection to the HTTP Security Server. The Security Server connects to the UFP server and initiates the URL Filtering Protocol.
- 3** The HTTP Security Server sends a request containing the name of the URL.
- 4** The UFP server checks the URL against lists of URLs and their categories. The UFP server returns a message notifying the HTTP Security Server of the categories to which the URL belongs.
- 5** The HTTP Security Server takes the action defined for the resource, either allowing or disallowing the connection attempt.

For information on defining UFP or CVP Servers, see Chapter 10, “Server Objects.”

For more information on OPSEC-certified products see <http://www.opsec.com>.

## Defining Security Servers

The properties of the VPN-1/FireWall-1 Security Servers are specified in the **Security Servers** tab of the **Properties Setup** window (FIGURE 11-9).



**FIGURE 11-9** Properties Setup window - Security Servers tab

**Telnet Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated TELNET session (optional)

**SMTP Welcome Message File** — the name of a file whose contents are to be displayed when the SMTP Security Server starts (optional)

**FTP Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated FTP session (optional)

**Rlogin Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated RLOGIN session (optional)

**Client Authentication Welcome Message File** — the name of a file whose contents are to be displayed when a user begins a Client Authenticated session (optional)



**Note** – Client Authenticated sessions initiated through the Manual Sign On method are not mediated by a Security Server.

For more information, see “Client Authentication” in Chapter 15, “Authentication”.

The following fields specify parameters for the HTTP Security Server:

**HTTP Next Proxy** — For information about this field, see “HTTP Security Server Configuration” on page 498 of Chapter 15, “Authentication.”

**HTTP Servers:** — You can define HTTP Servers to restrict HTTP access to specific hosts and ports. For more information, see “HTTP Servers List (Security Servers tab)” on page 499 .

## Security Server Configuration

### fwauthd.conf file

Each line in the Security Server configuration file `$FWDIR/conf/fwauthd.conf` corresponds to a Security Server.

|       |                  |      |     |
|-------|------------------|------|-----|
| 21    | bin/in.aftpd     | wait | 0   |
| 80    | bin/in.ahttpd    | wait | 0   |
| 513   | bin/in.arlogind  | wait | 0   |
| 25    | bin/in.asmtpd    | wait | 0   |
| 23    | bin/in.atelnetd  | wait | 0   |
| 259   | bin/in.aclientd  | wait | 259 |
| 900   | bin/in.ahclientd | wait | 900 |
| 10081 | bin/in.lhttpd    | wait | 0   |

**FIGURE 11-10** `$FWDIR/conf/fwauthd.conf` – example

**TABLE 11-4** `$FWDIR/conf/fwauthd.conf` fields

| field number | meaning                        |
|--------------|--------------------------------|
| 1            | standard service’s port number |
| 2            | Security Server executable     |
| 3            | wait flag (always set to wait) |
| 4            | Security Server port number    |

The Security Service executables are listed in TABLE 11-5.

**TABLE 11-5** Security Service binaries

| Service               | binary name                                                                                                                                                                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TELNET                | bin/in.atelnetd                                                                                                                                                                                                                 |
| FTP                   | bin/in.aftpd                                                                                                                                                                                                                    |
| HTTP                  | bin/in.ahttpd                                                                                                                                                                                                                   |
| SMTP                  | bin/in.asmtpd                                                                                                                                                                                                                   |
| RLOGIN                | bin/in.arlogind                                                                                                                                                                                                                 |
| client authentication | <div><div>■ bin/in.aclientd (This is not a Security Server.)</div><div>■ bin/in.ahclientd (This is not a Security Server, but the executable for when a user initiates client authentication through a Web browser.</div></div> |
| logical servers       | bin/in.lhttpd (This is not a Security Server.)                                                                                                                                                                                  |

The wait flag is always set to wait.

The Security Server port number is one of the following:

- 0 — specifies that FireWall will choose a random high port for the Security Server
  - positive value — specifies a real port number
- If this option is chosen, the standard service’s port number (the first field) should be the real port number for the service secured by this Security Server. For example, for TELNET this would usually be port 23.
- negative value — indicates that FireWall-1 randomly chooses multiple ports for the Security Server.

The absolute value indicates the number of random selected ports that will be chosen. The example below specifies that FireWall-1 will randomly select four high ports for the HTTP Security Server:

|    |               |      |    |
|----|---------------|------|----|
| 80 | bin/in.ahttpd | wait | -4 |
|----|---------------|------|----|

This option is especially useful for HTTP because it enables several HTTP Security Servers to run concurrently. If you configure a negative port number, the HTTP client will initially connect to a randomly selected port. If the client

connects again before the **Authorization Timeout** specified in the **Control Properties/Security Servers** window, the same port will be chosen. If the client connects again after the **Authorization Timeout**, another port will be chosen.



**Note** – Configuring a negative port value is recommended only for gateway machines with more than one CPU. Configuring this option on a gateway machine with one CPU can result in a performance degradation.

## Configuring Multiple HTTP Security Servers

You can modify the Security Server configuration to enable multiple HTTP Security Servers to run concurrently. Multiple HTTP clients connecting concurrently can be handled by several HTTP Security Servers.



**Note** – This option is recommended for gateway machines with more than one CPU. Using this option on a gateway machine with only one CPU will result in a performance degradation.

The file `$FWDIR/conf/fwauthd.conf` lists the Security Server executables and their assigned port numbers. The example line below shows the HTTP Security Server assigned to a dynamically allocated port:

|    |               |      |   |
|----|---------------|------|---|
| 80 | bin/in.ahttpd | wait | 0 |
|----|---------------|------|---|

The last field indicates the Security Server port number.

A negative port value indicates that VPN-1/FireWall-1 randomly chooses multiple ports for the HTTP Security Server. The absolute value indicates the number of random ports that will be chosen. The number of random ports should correspond to the number of CPUs the gateway machine has.

The example below indicates that VPN-1/FireWall-1 will randomly select four high ports for the HTTP Security Server:

|    |               |      |    |
|----|---------------|------|----|
| 80 | bin/in.ahttpd | wait | -4 |
|----|---------------|------|----|

According to the above example, an HTTP client will initially connect to one of four randomly selected ports. If the same client connects again before the **Authorization Timeout** specified in the **Security Servers** tab of the **Properties Setup** window, the same port will be chosen. If the same client connects again after the **Authorization Timeout**, another port will be chosen.

Another concurrent HTTP client will connect to one of the remaining free ports.

## Using a Security Server to Authenticate Other Services

You can use the TELNET, RLOGIN and FTP Security Servers to authenticate any interactive service. The user starts the interactive service as usual, but instead of being immediately connected to the interactive service's server (assuming the Rule Base allows such a connection), the user is first prompted for authentication data by the TELNET Security Server. If the authentication is successful, the user is then connected to the interactive service's server in a normal session.

To do this, add a line in `$FWDIR/conf/fwauthd.conf` as follows:

```
port in.telnetd wait 0
```

where *port* is the normal port for the service you wish to authenticate using the TELNET Security Server.

## Content Security

### Resources and Security Servers

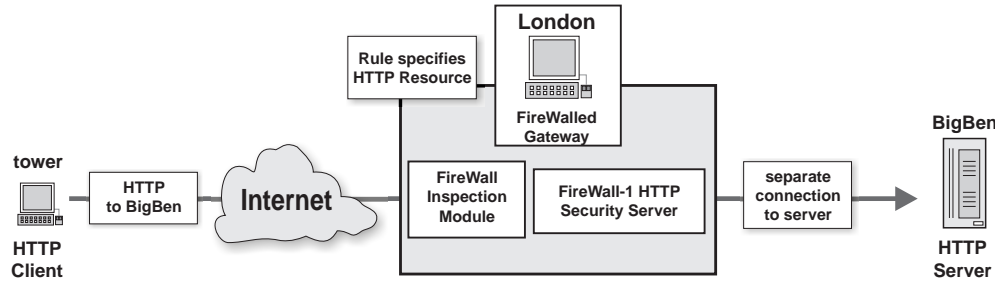
Content Security extends the scope of data inspection to the highest level of a service's protocol, achieving highly tuned access control to network resources. VPN-1/FireWall-1 provides content security for HTTP, SMTP and FTP connections using the VPN-1/FireWall-1 Security Servers and Resource object specifications.

A FireWall-1 Resource specification defines a set of entities which can be accessed by a specific protocol. You can define a Resource based on HTTP, FTP and SMTP. For example, you might define a URI resource whose attributes are a list of URLs and the HTTP and FTP schemes. The resource can be used in the Rule Base in exactly the same way a service can be used, and the standard logging and alerting methods are available to provide monitoring of resource usage.



When a rule specifies a Resource in the **Service** field of the Rule Base, the FireWall-1 Inspection Module diverts all the packets in the connection to the corresponding Security Server, which performs the required Content Security inspection. If the connection is allowed, the Security Server opens a second connection to the final destination.

FIGURE 11-11 depicts what happens when a rule specifies the use of an HTTP Resource.



**FIGURE 11-11** A connection mediated by the HTTP Security Server

For each connection established through a VPN-1/FireWall-1 Security Server, the Security Administrator is able to control specific access according to fields that belong to the specific service: URLs, file names, FTP PUT/GET commands, type of requests and others. Major security enhancements enabled by the Content Security feature are CVP checking (for example, for viruses) for files transferred and URL filtering.

When a Resource is specified, the Security Server diverts the connection to one of the following servers:

- Content Vectoring Protocol (CVP)

A CVP server examines and reports on the contents of files, for example, whether a file contains a virus.

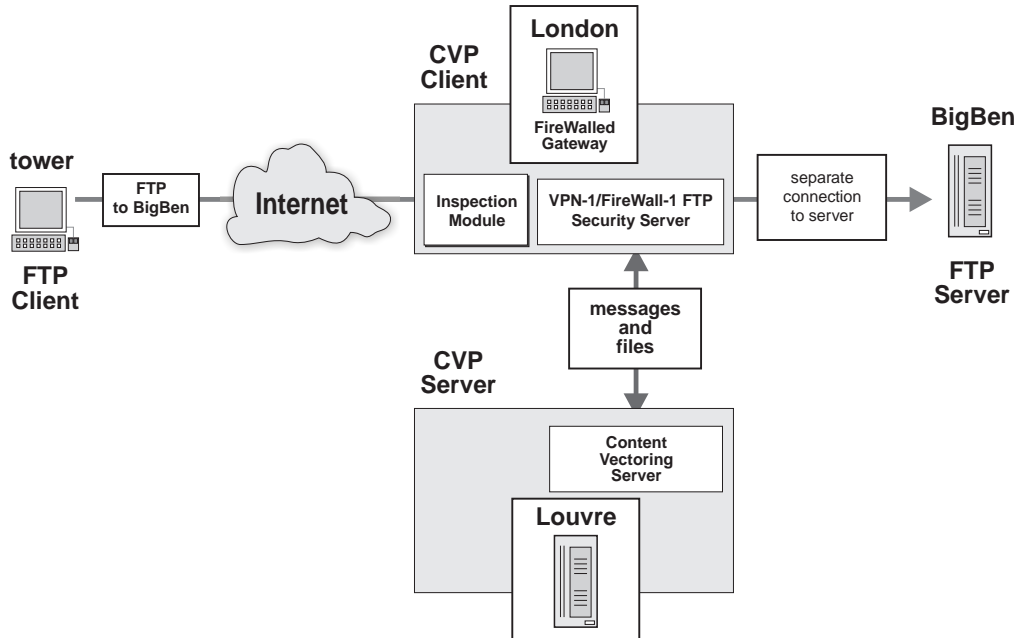
- URL Filtering Protocol (UFP)

A UFP server maintains a list of URLs and their categories.

The server performs the requested content inspection and returns the results to the Security Server. The Security Server allows or disallows the connection, depending on the results.

Communication between the Security Server and the CVP or UFP server is enabled through Check Point's OPSEC (Open Platform for Secure Enterprise Connectivity) framework. For more information about OPSEC integration within VPN-1/FireWall-1, see <http://www.checkpoint.com/opsec>.

FIGURE 11-12 shows what happens when a VPN-1/FireWall-1 Security Server passes a file to a Content Vectoring Server for inspection during an FTP connection.



**FIGURE 11-12** Content Vectoring Server

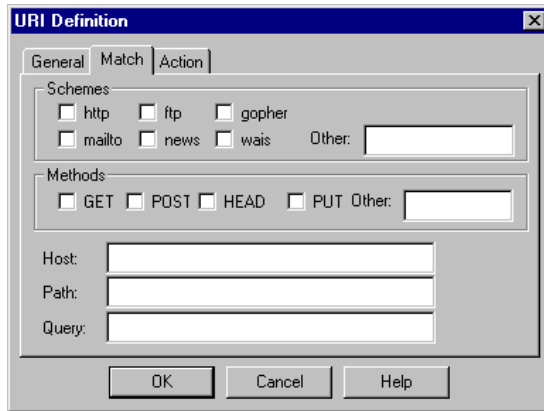
- 1** VPN-1/FireWall-1 determines that the Content Vectoring Server must be invoked. The relevant rule for the connection specifies a resource which includes CVP checking.
- 2** The FTP Security Server connects to the Content Vectoring Server and initiates the Content Vectoring Protocol.
- 3** The FTP Security Server sends the Content Vectoring Server the file to be inspected.
- 4** The Content Vectoring Server inspects the file, and returns a Validation Result message notifying the FTP Security Server of the result of the inspection.
- 5** The Content Vectoring Server optionally returns a modified version of the file to the FTP Security Server.
- 6** The FTP Security Server takes the action defined for the resource, either allowing or disallowing the file transfer.

For more information on CVP inspection, see “CVP Inspection” on page 365.

## Web (HTTP)

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific case. URI resources can define schemes (HTTP, FTP, GOPHER etc.), methods (GET, POST, etc.), hosts (for example, “\*.com”), paths and queries. Alternatively, a file containing a list of IP addresses of servers and paths can be specified.

In addition, the Security Administrator can define how to handle responses to allowed resources, for example, that JAVA applets not be allowed even on resources that are allowed. JAVA applets, JAVA scripts and ActiveX can be removed from HTML. A customizable replacement URL, for example a page containing a standardized error message, can be displayed when access to a response is denied.



**FIGURE 11-13** URI Resource Definition

## URL Filtering

URL filtering provides precise control over Web access, allowing administrators to define undesirable or inappropriate Web pages. FireWall-1 checks Web connection attempts using URL Filtering Protocol (UFP) servers. UFP servers maintain lists of URLs and their appropriate categories (i.e. permitted or denied). URL databases can be updated to provide a current list of blocked sites. All communication between FireWall-1 and the URL Filtering server is in accordance with the URL Filtering Protocol.

In order to implement URL filtering, proceed as follows:

- 1** Define a UFP Server.
- 2** Define a URI Resource that specifies a list of URL categories from the UFP server.
- 3** Define rules that specify an action taken for the Resource.

Defining a UFP Server

UFP Servers are defined in the **UFP Server Properties** window (see Chapter 10, “Server Objects”).

Defining a Resource

The URI resource is defined in the **URI Definition** window (UFP Specification). The URI Resource specifies the UFP server and a list of URL categories provided by the server. In the Resource depicted in FIGURE 11-14 on page 364, “WebCop” is the UFP Server, and the URL categories are “alcohol” and “drugs.” The “alcohol” category is selected. This means that if WebCop assigns the category “alcohol” to a URL, then the URL matches the resource’s definition, and the rule is applied.

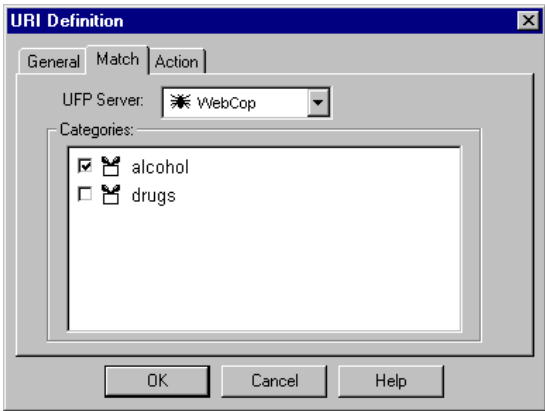


FIGURE 11-14 URI Definition window — Match tab (UFP specification)

Defining Rules

For example, suppose the Security Administrator defines two URI resources:

- **Allowed** — HTTP and FTP schemes, GET and POST methods
- **NotAllowed** — a list of “forbidden” URLs categories

Then the following rules prevent local users from accessing the **NotAllowed** resource and allow users access to the **Allowed** resource after authentication.

| No. | Source             | Destination | Service          | Action    | Track | Install On |
|-----|--------------------|-------------|------------------|-----------|-------|------------|
| 1   | All Users@localnet | Any         | http->Allowed    | User Auth | Short | Gateways   |
| 2   | localnet           | Any         | http->NotAllowed | reject    | Short | Gateways   |
| 3   | Any                | Any         | Any              | reject    | Alert | Gateways   |

FIGURE 11-15 Rule Base using Resources

When a Resource in a rule specifies a list of permitted or denied URLs, the HTTP Security Server sends a request to the UFP server containing the name of the URL in question. The UFP server checks the URL against lists of URLs and their categories. The UFP server returns a message notifying the HTTP Security Server of the categories to which the URL belongs.

For example, if a user requests a connection to a URL that belongs to a category specified in the Resource denied HTTP, FireWall-1 denies the connection request. If the URL does not belong to the categories defined by this Resource, the Security Server opens a separate connection to the destination.

For information on defining URI resources, see “Resources” on page 203.

## Mail (SMTP)

The SMTP protocol, designed to provide maximum connectivity between people all over the Internet, and enhanced to support file attachments, poses a challenge to the Security Administrator who wants to maintain connectivity but keep intruders out of the internal networks.

FireWall-1 offers an SMTP server that provides highly granular control over SMTP connections. The Security Administrator can:

- hide outgoing mail’s **From** address behind a standard generic address that conceals internal network structure and real internal users
- redirect mail sent to given **To** addresses (for example, to root) to another mail address
- drop mail from given addresses
- strip MIME attachments of given types from mail
- drop mail messages above a given size

For information on defining SMTP resources, see “SMTP Resources” on page 215.

## FTP

The FTP Security Server provides Content Security based on FTP commands (PUT/GET), file name restrictions, and CVP inspection for files.

For information on defining FTP resources, see “Resources” on page 203.”

## CVP Inspection

CVP inspection is an integral component of VPN-1/FireWall-1’s Content Security feature, and considerably reduces the vulnerability of protected hosts. CVP inspection examines all files transferred for all protocols. CVP configuration (which files to inspect, how to handle invalid files) is available for all Resource definitions. All VPN-1/FireWall-1 auditing tools are available for logging and alerting when these files are encountered.

CVP inspection is implemented by Content Vectoring Servers. The interaction between VPN-1/FireWall-1 and the Content Vectoring Server is defined by Check Point's OPSEC (Open Platform for Secure Enterprise Connectivity) framework. This interaction is depicted in FIGURE 11-12 on page 362.

For more information about OPSEC integration within VPN-1/FireWall-1, see <http://www.checkpoint.com/opsec>. If you would like to download evaluation versions of OPSEC-certified products, see <http://www.opsec.com>.

## Implementing CVP Inspection

In order to implement CVP inspection, proceed as follows:

- 1** Define a CVP Server.
- 2** Define Resource objects that specify CVP checking for the relevant protocols.
- 3** Define rules in the Rule Base that specify the action taken on connections that invoke each Resource.

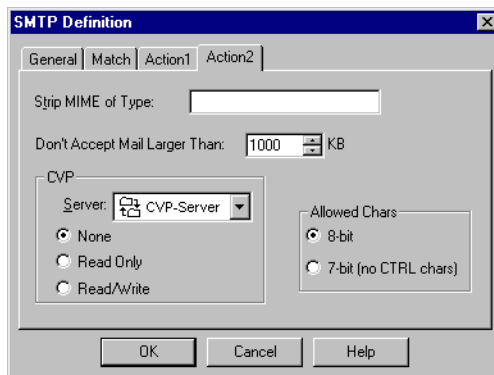
### Defining a CVP Server

Content Vectoring Servers are defined in the **CVP Server Properties** window (see "CVP Servers" on page 322).

### Defining Resources

The following CVP inspection options are available for all Resource definitions.

- **None** - The file is not inspected.
- **Read Only** - The file is inspected by the CVP Server. If the CVP Server rejects the file, it is not retrieved.
- **Read/Write** - The file is inspected by the CVP Server. If the CVP Server detects that the file is invalid (perhaps because it contains a virus), the CVP Server corrects the file before returning it to the Inspection Module.



**FIGURE 11-16** SMTP Resource with CVP properties

## Defining Rules

Rules that specify CVP inspection do not replace rules that allow FTP, HTTP, or SMTP connections. Since FireWall-1 examines the Rule Base sequentially, you must define rules in the appropriate order to prevent unwanted traffic from entering your network.

Resource rules which accept HTTP, SMTP, and FTP connections must be placed before other rules which accept these services. If you define a rule that allows all HTTP connections before a rule which specifies CVP inspection on a URI Resource, you may be allowing unwanted traffic.

Similarly, CVP rules must be placed after rules which reject FTP, HTTP or SMTP Resource connections. For example, a rule rejecting large e-mail messages must come before a CVP rule allowing specific SMTP connections.





# System Status Viewer

---

## In This Chapter

|                                     |                 |
|-------------------------------------|-----------------|
| <i>Monitoring System Status</i>     | <i>page 369</i> |
| <i>Displaying Objects</i>           | <i>page 382</i> |
| <i>Updating Object Status</i>       | <i>page 383</i> |
| <i>Options</i>                      | <i>page 384</i> |
| <i>Alerts</i>                       | <i>page 385</i> |
| <i>Menus</i>                        | <i>page 386</i> |
| <i>System Status Viewer Toolbar</i> | <i>page 388</i> |

## Monitoring System Status

The System Status Viewer displays a snapshot of all Check Point VPN/FireWall, FloodGate-1, Compression and High Availability modules in the enterprise, enabling real-time monitoring and alerting. Communication and traffic flow statistics are also displayed. Administrators can also use the System Status Viewer to specify the action to be taken if the status of a VPN/FireWall Module changes. For example VPN-1/FireWall-1 can issue an alert notifying system managers of any suspicious activity.

A proprietary VPN-1/FireWall-1 protocol is used for communication between the Check Point product modules and the Management Station.



**Note** – The Management Server retrieves the system status information and sends the data to the GUI Client. The GUI Client displays the data and, for VPN/FireWall Modules only, it may also issue transition notifications. For more information, see “Options” on page 384.

## Starting the System Status Viewer

To start the System Status Viewer, proceed as follows:

**TABLE 12-1** Starting the System Status Viewer

| Windows System | Action                                                                                                                                        |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Windows        | Double-click on the System Status Viewer icon, or choose <b>System Status</b> from the <b>Window</b> menu in the <b>Policy Editor</b> window. |
| X/Motif        | Run <code>\$FWDIR/bin/fwstatus</code> .                                                                                                       |

The **System Status Login** window (FIGURE 12-1) is displayed.



**FIGURE 12-1** System Status Login window

Enter your user name, password and the name of the Management Server to which you want to connect. Then click on **OK**.

## View

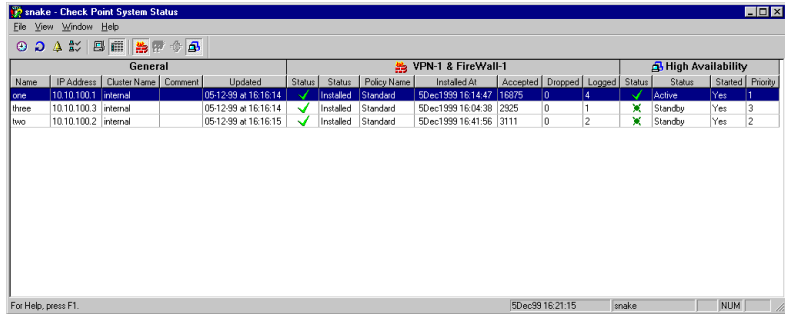
You can monitor your system using one of two views:

- Details View, described below.
- Icons View, described in “Icons View” on page 376.

### Details View

Details View is the default view in the System Status Viewer. Details View displays general information about network objects, data about the Check Point products installed on each object, as well as communication and packet flow statistics.

To switch to Details View, select **Details View** from the **View** menu, or click on  in the toolbar.



**FIGURE 12-2** System Status Details View

In Details View, columns are grouped into fields which display general information about each network object as well as specific information about each Check Point product running on the object. For example, in FIGURE 12-2 above, columns are grouped into three fields: **General**, **VPN-1 & FireWall-1**, and **High Availability**.


The columns displayed in the **General** field list general information about each network object in your system. This information is listed in TABLE 12-2.


**TABLE 12-2** General Information


| Column       | Explanation                                             |
|--------------|---------------------------------------------------------|
| Name         | The object's name.                                      |
| IP Address   | The object's IP address.                                |
| Cluster Name | The cluster to which the object belongs, if applicable. |
| Comment      | A descriptive comment about the object.                 |
| Update       | The last time the object's status was updated.          |


## Displaying Check Point Product Data

For every Check Point product you are licensed to use, the corresponding icon or menu item is enabled. Clicking on this icon collapses or expands the fields displaying information about the product.

To collapse/expand VPN-1/FireWall-1 data (TABLE 12-3 on page 372), click on  in the toolbar or choose **VPN-1/FireWall-1 Details** from the **View** menu.

To collapse/expand FloodGate-1 data (TABLE 12-4 on page 373), click on  in the toolbar or choose **FloodGate-1 Details** from the **View** menu.

To collapse/expand Compression data (TABLE 12-5 on page 374), click on  in the toolbar or choose **Compression Details** from the **View** menu.

To collapse/expand High Availability Module data (TABLE 12-6 on page 374), click on  in the toolbar or choose **High Availability Module Details** from the **View** menu.

For each network object, the System Status Viewer displays the following columns under the corresponding Check Point product fields:

**TABLE 12-3** VPN-1/FireWall-1 field





| Column       | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status       | <p>An icon representing the status of the VPN/FireWall Module installed on this object. There are four status levels:</p> <div><div><b>Installed</b> — A VPN/FireWall Module is installed on this object and is responding to status update requests from the Management Station.</div><div><b>Not installed</b> — A VPN/FireWall Module is not installed on this object.</div><div><b>Disconnected</b> — The VPN/FireWall module installed on this object is not responding to status update requests from the Management Station.</div><div><b>Untrusted</b> — The Management Station is not the Master of the VPN/FireWall Module on this object.</div></div> |
| Status       | <p>Text representing the status of the VPN/FireWall installed on the object: “Installed”, “Not Installed”, “Disconnected”, “Untrusted”. See above for meaning.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Policy Name  | <p>The name of the Security Policy.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Install Time | <p>The date and time the Security Policy was last installed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Accepted     | <p>The number of packets accepted by the VPN/FireWall Module.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Dropped      | <p>The number of packets rejected by the VPN/FireWall Module.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Logged       | <p>The number of packets logged by the VPN/FireWall Module.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

TABLE 12-4 FloodGate-1 Data





| Column          | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status          | <p>An icon representing the status of the Floodgate-1 Module installed on this object. There are four status levels:</p> <div><div><b>Installed</b> — a FloodGate-1 Module is installed on this object and is responding to status update requests from the Management Station.</div><div><b>Not installed</b> — a FloodGate-1 Module is not installed on this object</div><div><b>Disconnected</b> — the FloodGate-1 module installed on this object is not responding to status update requests from the Management Station.</div><div><b>Untrusted</b> — the Management Station is not the Master of the Floodgate-1 Module on this object.</div></div> |
| Status          | <p>Text representing the status of the FloodGate-1 Module installed on this object: “Installed”, “Not installed”, “Disconnected”, “Untrusted”. See above for meaning.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Policy Name     | <p>The name of the Bandwidth Policy installed on the object.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Conversations   | <p>The total number of conversations. Conversations are active connections and connections that are anticipated as a result of prior inspection. Examples are data connections in FTP, and the “second half” of UDP connections.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Pending Packets | <p>The number of packets waiting in FloodGate-1’s queues.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Pending Bytes   | <p>The number of bytes waiting in FloodGate-1’s queues.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

TABLE 12-5 Compression Data









| Column | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | <p>The status of the Compression Module installed on this object.<br/>There are four status levels:</p> <div><div><b>Installed</b> — the Compression Module is enabled on this object and is responding to status update requests from the Management Station.</div><div><b>Not installed</b> — a Compression Module is not installed on this object.</div><div><b>Disconnected</b> — the Compression Module is not responding to status update requests from the Management Station.</div><div><b>Untrusted</b> — the Management Station is not the Master of the Compression Module on this object.</div></div> |
| Status | <p>Text representing the status of the Compression Module:<br/>“Installed”, “Not Installed”, “Disconnected”, “Untrusted”. See above for meaning.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

TABLE 12-6 High Availability Data

| Column | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | <p>The status of the High Availability Module installed on this object:</p> <div><div><b>Active</b> — module installed and active</div><div><b>Active Attention</b> — This icon draws your attention to the fact that the module is active even though all the members of the cluster have some problem. Despite this, the gateway with the least problems and the next highest priority level is active and working as a backup until the highest priority level gateway can be restored.</div><div><b>Stand by</b> — module ready to replace an active module</div><div><b>Not Active</b> — module is down or there is a problem</div></div> |

**TABLE 12-6** High Availability Data

| Column   | Explanation                                                                                                                                                           |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status   | Text representing the status of the High Availability Module installed on this object: “Active”, “Active Attention”, “Stand by”, “Not Active”. See above for meaning. |
| Started  | “Yes” if the module is active. “No” if the module is inactive.                                                                                                        |
| Priority | The priority sequence number of the module.                                                                                                                           |

**Resizing Columns**


To change a column’s width in Details View, drag the column’s right border in the header, as follows:

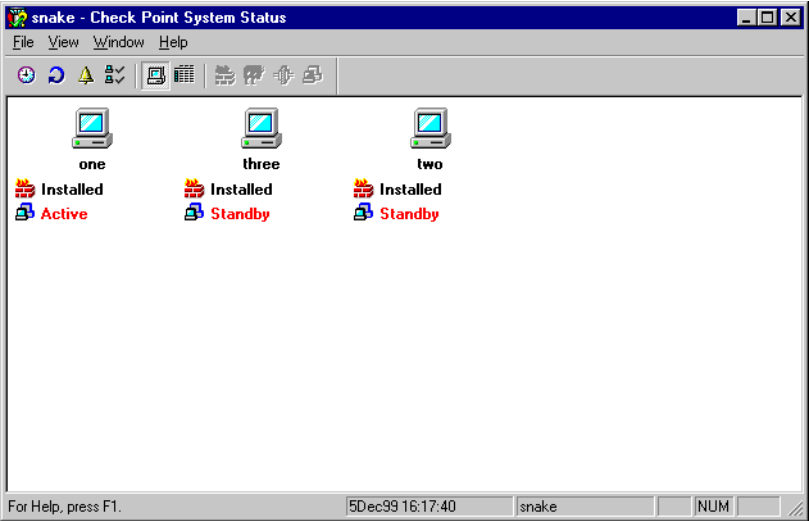
- 1** Move the cursor to the column’s right border in the header.
- 2** Click on the left mouse button without releasing it.
- 3** Move the column border without releasing it.
- 4** Release the left mouse button.

**Displaying Object Properties**

To display the properties of a specific object, double-click on the corresponding row or select the row and press **Enter**. For more information, see “Displaying Object Properties” on page 378.

## Icons View

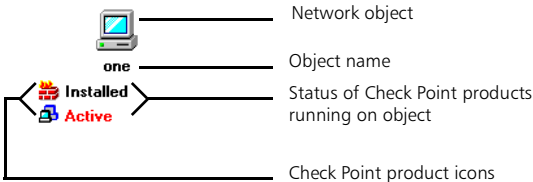
To use Icons View, click on  or choose **Icons View** from the **View** menu.



**FIGURE 12-3** System Status Icons View - VPN-1/FireWall-1 and High Availability

## Displaying Check Point Product Data

The System Status Viewer displays policy and communication data as follows:







**FIGURE 12-4** An object in Icons View

Each computer icon represents a FireWalled network object. The object name is listed under the icon. Under the object name is a list of all Check Point products currently enabled on that object. Each product is represented by an icon and the product's status. These are listed in TABLE 12-7 on page 377.



**TABLE 12-7** Icons View — Check Point Product Status

| Status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| For  VPN-1/FireWall-1,  FloodGate-1 and  Compression only:                                                                                                                                                                                                                                                                                     |
| <ul style="list-style-type: none"><li>■ <b>Installed</b> — this product is installed on object and is responding to status update requests from the Management Station.</li><li>■ <b>Not installed</b> — this product is not installed on this object.</li><li>■ <b>Disconnected</b> — this product is installed on this object but is not responding to status update requests from the Management Station.</li><li>■ <b>Untrusted</b> — the Management Station is not the Master of this product module on this object.</li></ul>                                                               |
| For  High Availability only:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <ul style="list-style-type: none"><li>■ <b>Active</b> — module installed and active</li><li>■ <b>Active Attention</b> — This icon draws your attention to the fact that the module is active even though all the members of the cluster have some problem. Despite this, the gateway with the least problems and the next highest priority level is active and working as a backup until the highest priority level gateway can be restored.</li><li>■ <b>Stand by</b> — module is ready to replace an active module</li><li>■ <b>Not Active</b> — module is down or there is a problem</li></ul> |

**Navigating in the Icons View**

In Icons View, you can navigate between icons using the arrow keys.

**Displaying Object Properties**

To display the properties of a specific object, double-click on the corresponding icon or select the icon and press **Enter**. For more information, see “Displaying Object Properties” on page 378.

**Hiding an Object**

To hide the icon corresponding to a specific object, right-click on the icon and choose **Hide** from the menu that is displayed.



**Note** – To redisplay the icon, choose **Show/Hide Objects...** and select the object name. For more information, see “Displaying Objects” on page 382.

## Updating Object Status

To update the status of a object, right-click on the corresponding icon and choose **Update** from the menu that is displayed. For more information, see “Updating Object Status” on page 383.

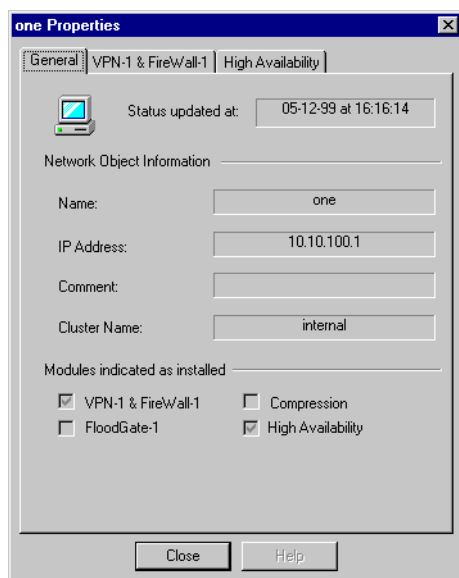
## Displaying Object Properties

You can display additional information about a network object and the Check Point products running on that object, as follows:

- In Details View, double-click on the row corresponding to the object, or select the row and press **Enter**.
- In Icons View, double-click on the icon corresponding to the object, or select the icon and press **Enter**.

The **Properties** window is displayed. The **Properties** window includes a **General** tab and a tab for each Check Point product installed on the object.

### Properties Window — General Tab



**FIGURE 12-5** Properties Window — General Tab

**Status updated at** — The date and time this object’s status was last updated.

#### **Network Object Information:**

**Name** – The object’s name.

**IP Address** — The IP address of the object.

**Comment** — Descriptive text.

**Cluster Name** — The cluster’s name, if applicable (High Availability only).

**Modules indicated as installed:**

**VPN-1 & FireWall-1** — If checked, a VPN/FireWall Module is installed on this object.

**FloodGate-1** — If checked, a FloodGate-1 Module is installed on this object.

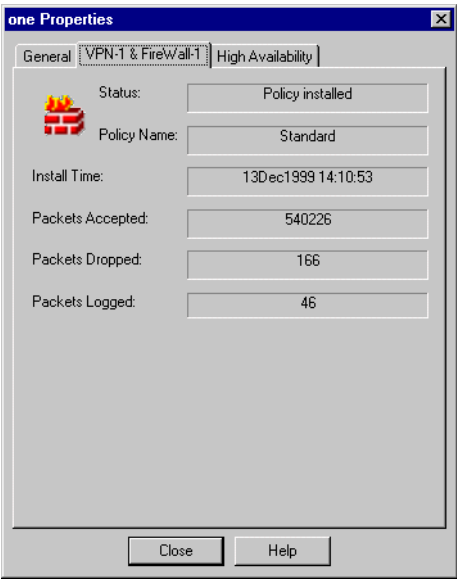
**Compression** — If checked, a Compression Module is installed on this object.

**High Availability** — If checked, a High Availability Module is installed on this object.



**Note** – The Compression Module is not available for this version.

**Properties Window — VPN-1 & FireWall-1 Tab**



**FIGURE 12-6** Properties Window — VPN-1&FireWall-1 Tab

**Status** — The status of the VPN/FireWall Module installed on this object.

For more information on status types, see TABLE 12-7 on page 377.

**Policy Name** — The name of the Security Policy installed on the VPN/FireWall Module.

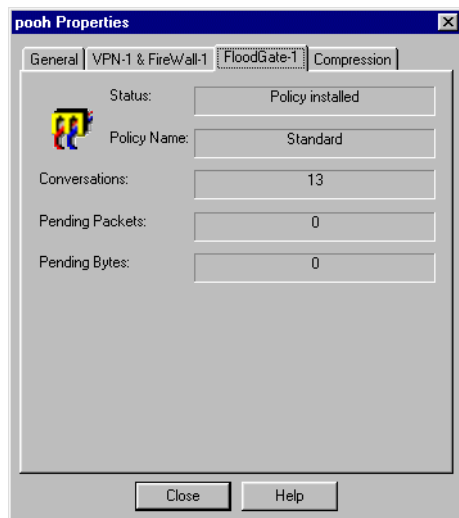
**Install Time** — The date and time the Security Policy was last installed.

**Packets Accepted** — The number of packets accepted by the VPN/FireWall Module.

**Packets Dropped** — The number of packets dropped by the VPN/FireWall Module.

**Packets Logged** — The number of packets logged by the VPN/FireWall Module.

### Properties Window — FloodGate-1 Tab



**FIGURE 12-7** Properties Window — FloodGate-1 Tab

**Status** — The status of the Floodgate-1 Module installed on this object.

For more information on status types, see TABLE 12-7 on page 377.

**Policy Name** — The name of the Bandwidth Policy installed.

**Conversations** — The total number of conversations.

Conversations are active connections and connections that are anticipated as a result of prior inspection. Examples are data connections in FTP, and the “second half” of UDP connections.

**Pending Packets** — The number of packets waiting in FloodGate-1’s queues.

**Pending Bytes** — The number of bytes waiting in FloodGate-1’s queues.

Properties Window Compression Tab



**FIGURE 12-8** Properties Window - Compression Tab

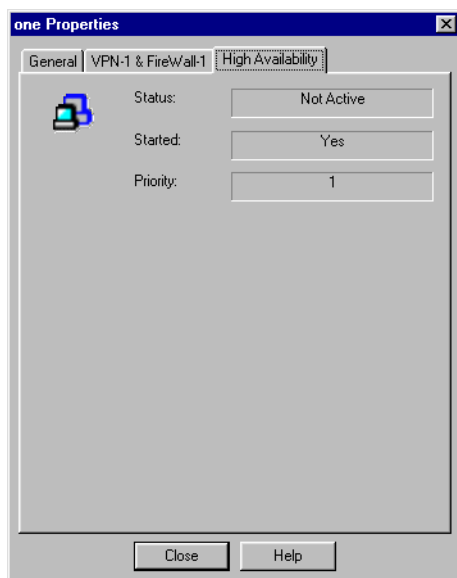
**Status** — The status of the Compression Module installed on this object.

For more information on status types, see TABLE 12-7 on page 377.



**Note** – The Compression Module is not available for this version.

## Properties Window —High Availability Tab



**FIGURE 12-9** Properties Window - High Availability Tab

**Status** — The status of the High Availability Module installed on this object.

For more information on status types, see TABLE 12-6 on page 374.

**Started** — **Yes** if the module is active. **No** if it is inactive.

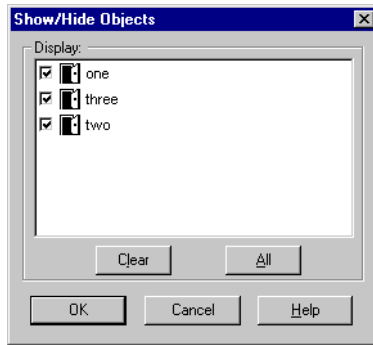
**Priority** — The priority sequence number of the module.

## Displaying Objects

In both Details View and Icons View, you can specify which network objects are to be displayed.

- 1** Choose **Show/Hide Objects...** from the **View** menu or click on  in the toolbar.


The **Show/Hide Objects** window (FIGURE 12-10) is displayed.



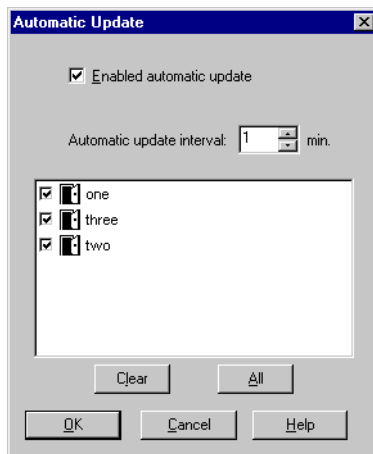
**FIGURE 12-10** Show/Hide Objects window

- 2** To display an object's status in the System Status Viewer, select the object's checkbox.
- 3** If you do not want to display an object's status in the System Status Viewer, clear the object's checkbox.  
Alternatively, in Icons View, right-click on the object that you want to hide and select **Hide** from the menu that is displayed.

## Updating Object Status

To update the status of all objects displayed in the System Status Viewer window, select  from the toolbar.

To enable or disable automatic updating of the status for specific objects, open the **Automatic Update** window by choosing **Automatic Update...** from the **View** menu.



**FIGURE 12-11** Automatic Update window

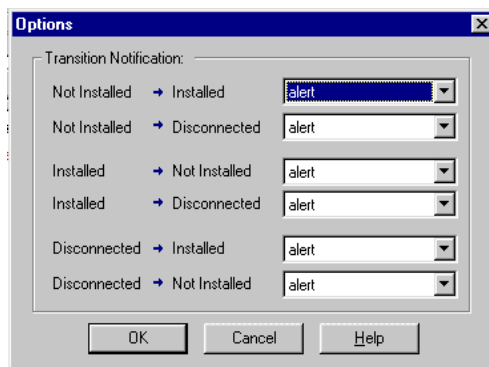
To enable automatic updating of the status of the the selected objects, check **Enabled automatic update** (this the default option). You can then specify the **Automatic update interval**, that is, how frequently the status of the selected objects is updated.

To disable automatic updating of an object's status in the System Status Viewer's main window, do not check **Enabled automatic update**. When **Enabled automatic update** is not checked, **Automatic update interval**, **Clear** and **All** will be disabled.

## Options

The **Options** window applies only to VPN-1/FireWall-1. In the **Options** window, you can specify the actions to be taken when the status of a FireWalled object changes.

To display the **Options** window, choose **Options...** from the **View** menu.



**FIGURE 12-12** Options window

Under **Transition Notification**, choose one of the following commands, or leave blank:

- **alert** — Issue an alert (as defined in the **Popup Alert Command** field in the **Log and Alert** tab of the **Properties Setup** window).
- **mail** — Send a mail alert (as defined in the **Mail Alert Command** field in the **Log and Alert** tab of the **Properties Setup** window).
- **Snmp Trap** — Issue an SNMP trap (as defined in the **SNMP Trap Alert Command** field in the **Log and Alert** tab of the **Properties Setup** window).
- **User Alert** — Issue a User Defined Alert (as defined in the **User Defined Alert Command** field in the **Log and Alert** tab of the **Properties Setup** window).


For information about the **Log and Alert** tab of the **Properties Setup** window, see “Log and Alert” on page 243.

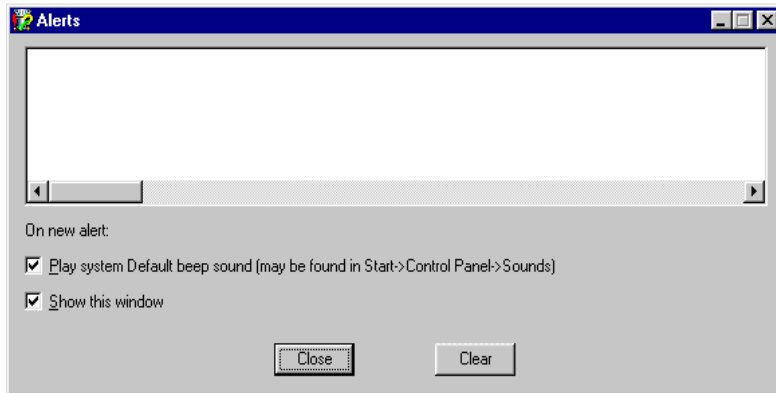
The text of a message describing the change of status is available to the `stdin` of the specified command.



## Alerts

The **Alerts** window applies only to VPN-1/FireWall-1. Alert commands are specified in the **Popup Alert Command** field in the **Log and Alert** tab of the **Properties Setup** window. For more information on Properties, see Chapter 7, “Properties Setup.”

To view the alerts, choose **Alerts...** from the **View** menu, or click on  in the toolbar. The **Alerts** window is displayed.



**FIGURE 12-13** Alerts window

To play a sound when an alert is received, check **Play system Default beep sound**.

To display the **Alerts** window the next time an alert is received, check **Show This Window**.

To clear alerts, select the alert(s) and then click on **Clear**.

To close the **Alerts** window, click on **Close**.



**Note** – Alerts are sent by VPN/FireWall Modules to the Management Station. The Management Station then forwards these alerts to all the System Status Viewer applications connected to the Management Station at that moment.

## Menus








### File Menu

**TABLE 12-8** File Menu Commands




| Menu Entry  | Toolbar Button | Description                    | See |
|-------------|----------------|--------------------------------|-----|
| <b>Exit</b> | none           | Exit the System Status Viewer. |     |

### View Menu

**TABLE 12-9** View Menu Commands

| Menu Entry                            | Toolbar Button                                                                      | Description                                                | See                                  |
|---------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------|--------------------------------------|
| <b>Toolbar</b>                        | none                                                                                | Toggle the display of the System Status Viewer Toolbar.    |                                      |
| <b>Status Bar</b>                     | none                                                                                | Toggle the display of the System Status Viewer Status Bar. |                                      |
| <b>Alerts</b>                         |    | Display the <b>Alerts</b> window.                          | “Alerts” on page 385                 |
| <b>Show/Hide Objects...</b>           |    | Display the <b>Show/Hide Objects</b> window.               | “Displaying Objects” on page 382     |
| <b>Automatic Update...</b>            |  | Display the <b>Automatic Update</b> window.                | “Updating Object Status” on page 383 |
| <b>Update Status</b>                  |  | Update the status of all objects displayed.                | “Updating Object Status” on page 383 |
| <b>Options...</b>                     | none                                                                                | Display the <b>Options</b> window.                         | “Options” on page 384                |
| <b>Icons View</b>                     |  | Toggle to Icons view.                                      | “Icons View” on page 376             |
| <b>Details View</b>                   |  | Toggle to Details view.                                    | “Details View” on page 370           |
| <b>VPN-1 &amp; FireWall-1 Details</b> |  | Toggle VPN-1/FireWall-1 details columns.                   | “Details View” on page 370           |

**TABLE 12-9** View Menu Commands

| Menu Entry                              | Toolbar Button                                                                    | Description                                                                                        | See                        |
|-----------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------|
| <b>FloodGate-1 Details</b>              |  | Toggle FloodGate-1 Module details columns.                                                         | “Details View” on page 370 |
| <b>Compression Details</b>              |  | Toggle Compression Module details columns. Note that this feature is not enabled for this version. | “Details View” on page 370 |
| <b>High Availability Module Details</b> |  | Toggle High Availability Module details columns.                                                   | “Details View” on page 370 |

## Window Menu

**TABLE 12-10** Window Menu Commands

| Menu Entry               | Toolbar Button | Description                 | See                                                            |
|--------------------------|----------------|-----------------------------|----------------------------------------------------------------|
| <b>Policy Editor</b>     | none           | Open the Policy Editor.     | Chapter 8, “Security Policy Rule Base”                         |
| <b>Log Viewer</b>        | none           | Open the Log Viewer.        | Chapter 13, “Log Viewer”                                       |
| <b>Real Time Monitor</b> | none           | Open the Real-Time Monitor. | <i>Check Point FloodGate-1 Architecture and Administration</i> |

## System Status Viewer Toolbar













**FIGURE 12-14** System Status Viewer Toolbar

The System Status Toolbar provides shortcuts for some **View** menu commands.

### Toolbar Buttons and Corresponding Menu Commands

**TABLE 12-11** Toolbar Buttons and Corresponding Menu Commands

| Toolbar Button                                                                      | Command on View Menu                    | Meaning                                                                                            |
|-------------------------------------------------------------------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------|
|    | <b>Automatic Update...</b>              | Display the <b>Automatic Update</b> window.                                                        |
|    | <b>Update Status</b>                    | Update the status of all objects displayed.                                                        |
|    | <b>Alerts</b>                           | Display the <b>Alerts</b> window.                                                                  |
|    | <b>Show/Hide Objects...</b>             | Display the <b>Show/Hide Objects</b> window.                                                       |
|    | <b>Icons View</b>                       | Toggle to Icons view.                                                                              |
|   | <b>Details View</b>                     | Toggle to Details view.                                                                            |
|  | <b>VPN-1/FireWall-1 Details</b>         | Toggle VPN-1/FireWall-1 details columns.                                                           |
|  | <b>FloodGate-1 Details</b>              | Toggle FloodGate-1 Module details columns.                                                         |
|  | <b>Compression Details</b>              | Toggle Compression Module details columns. Note that this feature is not enabled for this version. |
|  | <b>High Availability Module Details</b> | Toggle High Availability Module details columns.                                                   |



**Note** – The Check Point product icons are enabled only for those products you are licensed to use.

# Log Viewer

---

## In This Chapter

|                                        |                 |
|----------------------------------------|-----------------|
| <i>Viewing the Log</i>                 | <i>page 389</i> |
| <i>Navigation And Searching</i>        | <i>page 400</i> |
| <i>Displaying Selected Entries</i>     | <i>page 402</i> |
| <i>Log Viewer Options</i>              | <i>page 418</i> |
| <i>Active Connections</i>              | <i>page 393</i> |
| <i>Log Viewer Options</i>              | <i>page 418</i> |
| <i>Log File Management</i>             | <i>page 419</i> |
| <i>Printing and Saving Log Entries</i> | <i>page 420</i> |
| <i>Miscellaneous Functions</i>         | <i>page 420</i> |
| <i>Menus</i>                           | <i>page 421</i> |
| <i>Log Viewer Toolbar</i>              | <i>page 424</i> |

## Viewing the Log

The Log Viewer allows you to view entries in the Log File. Each entry in the Log File is a record of an event that, according to the Rule Base or the Properties, is to be logged. In addition, every event which caused an alert, as well as certain important system events (such as a Security Policy being installed or uninstalled on a host), are also logged. The format of log entries requested by a rule is determined by the log type specified in the rule.



**Note** – The Management Server reads the Log File and sends the data to the GUI Client for display. The GUI Client merely displays the data.

The Log Viewer gives you precise control over which information in the Log File is displayed. You can select which log entries and data fields to display. The Log Viewer also allows you to navigate through the Log File.

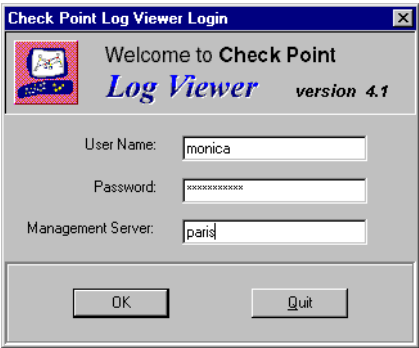
## Starting the Log Viewer

To start the Log Viewer, proceed as follows:

**TABLE 13-1** Starting the Log Viewer

| Windows System | Action                                                                                                                           |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Windows        | Double-click on the Log Viewer icon, or choose <b>Log Viewer</b> from the <b>Window</b> menu in the <b>Policy Editor</b> window. |
| X/Motif        | Run \$FWDIR/fwlog.                                                                                                               |

The **Log Viewer Login** window (FIGURE 13-1) is then displayed.



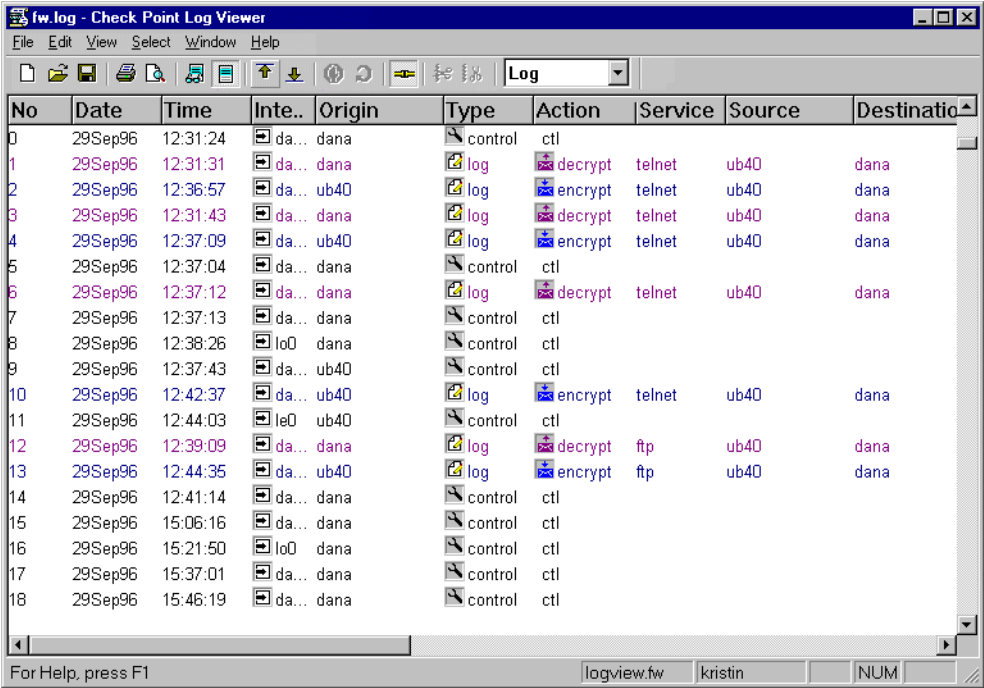
**FIGURE 13-1** Log Viewer Login window

Enter your user name, password and the name of the Management Server to which to connect. Then click on **OK**.

For information about how to define users on the Management Server, see “Access Control” on page 62.

A Log Server is a machine to which log events are sent by one or more VPN/FireWall Modules. One of these VPN/FireWall Modules may be running on the Log Server. For more information, see “Redirecting Logging to Another Master” on page 420.

After a brief delay, the **Check Point Log Viewer** window is displayed.



**FIGURE 13-2** Log Viewer

The name of the Log File is displayed in the Log Viewer's title bar. The status bar shows the name of the format file and the server name.

## Mode

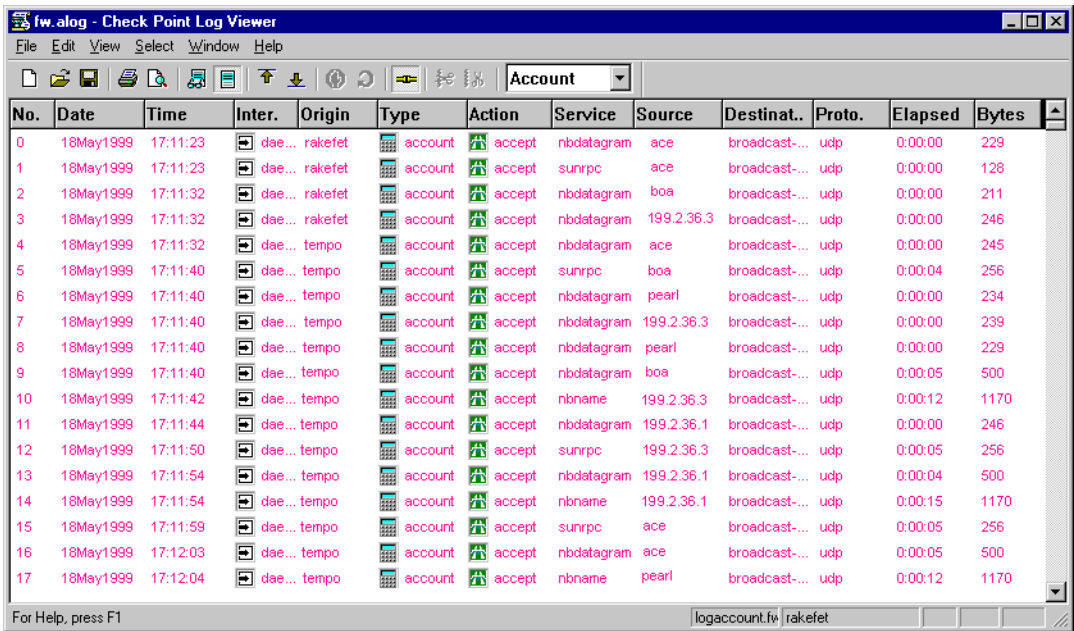
You can display one of three different logs by making the appropriate selection from the listbox in the toolbar:

### Security Log

This is the familiar log (see FIGURE 13-2), showing all security-related events. To view this log, select **Log** in the listbox.

## Accounting Entries

To show accounting entries only in the Log Viewer (FIGURE 13-3), select **Account** from the list box in the toolbar.



| No. | Date      | Time     | Inter. | Origin  | Type    | Action | Service   | Source     | Destinat.     | Proto. | Elapsed | Bytes |
|-----|-----------|----------|--------|---------|---------|--------|-----------|------------|---------------|--------|---------|-------|
| 0   | 18May1999 | 17:11:23 | dae... | rakefet | account | accept | nbdtagram | ace        | broadcast-... | udp    | 0:00:00 | 229   |
| 1   | 18May1999 | 17:11:23 | dae... | rakefet | account | accept | sunrpc    | ace        | broadcast-... | udp    | 0:00:00 | 128   |
| 2   | 18May1999 | 17:11:32 | dae... | rakefet | account | accept | nbdtagram | boa        | broadcast-... | udp    | 0:00:00 | 211   |
| 3   | 18May1999 | 17:11:32 | dae... | rakefet | account | accept | nbdtagram | 199.2.36.3 | broadcast-... | udp    | 0:00:00 | 246   |
| 4   | 18May1999 | 17:11:32 | dae... | tempo   | account | accept | nbdtagram | ace        | broadcast-... | udp    | 0:00:00 | 245   |
| 5   | 18May1999 | 17:11:40 | dae... | tempo   | account | accept | sunrpc    | boa        | broadcast-... | udp    | 0:00:04 | 256   |
| 6   | 18May1999 | 17:11:40 | dae... | tempo   | account | accept | nbdtagram | pearl      | broadcast-... | udp    | 0:00:00 | 234   |
| 7   | 18May1999 | 17:11:40 | dae... | tempo   | account | accept | nbdtagram | 199.2.36.3 | broadcast-... | udp    | 0:00:00 | 239   |
| 8   | 18May1999 | 17:11:40 | dae... | tempo   | account | accept | nbdtagram | pearl      | broadcast-... | udp    | 0:00:00 | 229   |
| 9   | 18May1999 | 17:11:40 | dae... | tempo   | account | accept | nbdtagram | boa        | broadcast-... | udp    | 0:00:05 | 500   |
| 10  | 18May1999 | 17:11:42 | dae... | tempo   | account | accept | nbdtagram | 199.2.36.1 | broadcast-... | udp    | 0:00:12 | 1170  |
| 11  | 18May1999 | 17:11:44 | dae... | tempo   | account | accept | nbdtagram | 199.2.36.1 | broadcast-... | udp    | 0:00:00 | 246   |
| 12  | 18May1999 | 17:11:50 | dae... | tempo   | account | accept | sunrpc    | 199.2.36.3 | broadcast-... | udp    | 0:00:05 | 256   |
| 13  | 18May1999 | 17:11:54 | dae... | tempo   | account | accept | nbdtagram | 199.2.36.1 | broadcast-... | udp    | 0:00:04 | 500   |
| 14  | 18May1999 | 17:11:54 | dae... | tempo   | account | accept | nbdtagram | 199.2.36.1 | broadcast-... | udp    | 0:00:15 | 1170  |
| 15  | 18May1999 | 17:11:59 | dae... | tempo   | account | accept | sunrpc    | ace        | broadcast-... | udp    | 0:00:05 | 256   |
| 16  | 18May1999 | 17:12:03 | dae... | tempo   | account | accept | nbdtagram | ace        | broadcast-... | udp    | 0:00:05 | 500   |
| 17  | 18May1999 | 17:12:04 | dae... | tempo   | account | accept | nbdtagram | pearl      | broadcast-... | udp    | 0:00:12 | 1170  |

FIGURE 13-3 Log Viewer showing Accounting Entries

The Accounting Log shows the following data (in addition to the data displayed in the Security Log):

- **Elapsed** — the duration of the connection  
**Elapsed** is calculated to the time of the last byte transferred.
- **Bytes** — the number of bytes transferred
- **Start Date** — the date on which the connection began



## Active Connections

To show Active Connections in the Log Viewer (FIGURE 13-4), that is, connections currently open through any of the VPN/FireWall Modules that are logging to the currently open Log File, select **Active** from the list box in the toolbar.

| No. | Date     | Time     | Conn. ID | Inter. | Orig.. | Type | Action | Service    | Source     | Destination          | Proto. |
|-----|----------|----------|----------|--------|--------|------|--------|------------|------------|----------------------|--------|
| 7   | 7Jun1999 | 15:45:40 | 242      | dae... | dana   | log  | accept | nbname     | 199.23.6.3 | broadcast-199.20...  | udp    |
| 8   | 7Jun1999 | 15:45:40 | 243      | dae... | dana   | log  | accept | bootp      | prnsrv     | 255.255.255.255      | udp    |
| 9   | 7Jun1999 | 15:45:40 | 244      | dae... | dana   | log  | accept | lotus      | sage       | gold.checkpoint.c... | tcp    |
| 10  | 7Jun1999 | 15:45:40 | 245      | dae... | dana   | log  | accept | sunrpc     | 199.23.6.3 | broadcast-199.20...  | udp    |
| 11  | 7Jun1999 | 15:45:40 | 246      | dae... | dana   | log  | accept | 135        | sage       | broadcast-199.20...  | udp    |
| 12  | 7Jun1999 | 15:45:40 | 247      | dae... | dana   | log  | accept | nbssession | prnsrv     | netapp.checkpoin...  | tcp    |
| 13  | 7Jun1999 | 15:46:06 | 248      | dae... | dana   | log  | accept | FW1_mgmt   | 199.23.6.3 | rakefet              | tcp    |
| 14  | 7Jun1999 | 15:45:40 | 249      | dae... | dana   | log  | accept | FW1_mgmt   | art        | rakefet              | tcp    |
| 15  | 7Jun1999 | 15:45:40 | 250      | dae... | dana   | log  | accept | nbdatagram | art        | broadcast-199.20...  | udp    |
| 16  | 7Jun1999 | 15:45:40 | 251      | dae... | dana   | log  | accept | domain-udp | hank       | joni.checkpoint.com  | udp    |
| 17  | 7Jun1999 | 15:45:51 | 253      | dae... | dana   | log  | accept | nbname     | hank       | broadcast-199.20...  | udp    |
| 18  | 7Jun1999 | 15:45:54 | 254      | dae... | dana   | log  | accept | nbdatagram | 199.23.6.3 | broadcast-199.20...  | udp    |
| 19  | 7Jun1999 | 15:45:54 | 255      | dae... | dana   | log  | accept | nbdatagram | hank       | broadcast-199.20...  | udp    |
| 20  | 7Jun1999 | 15:45:58 | 256      | dae... | dana   | log  | accept | nbname     | sage       | broadcast-199.20...  | udp    |
| 21  | 7Jun1999 | 15:46:01 | 257      | dae... | dana   | log  | accept | domain-udp | 199.23.6.3 | joni.checkpoint.com  | udp    |
| 22  | 7Jun1999 | 15:46:14 | 259      | dae... | dana   | log  | accept | nbdatagram | sage       | broadcast-199.20...  | udp    |
| 23  | 7Jun1999 | 15:46:15 | 260      | dae... | dana   | log  | accept | nbdatagram | prnsrv     | broadcast-199.20...  | udp    |

**FIGURE 13-4** Log Viewer showing Active Connections

The Active Connections window displays the following data (in addition to the data displayed in the Security Log):

- **Elapsed** — the duration of the connection  
**Elapsed** is calculated to the time of the last byte transferred.
- **Bytes** — the number of bytes transferred
- **Start Date** — the date on which the connection began
- **Conn. ID** — the connection ID, a fixed number (in contrast to the **No** field which changes dynamically).


## Blocking Connections

You can terminate an active connection and block further connections from and to specific IP addresses. There are two ways to terminate a connection:

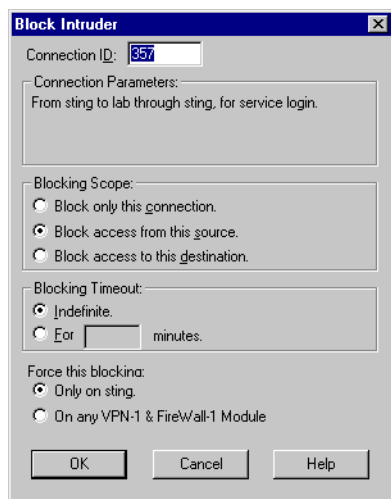
- using the **Block Intruder** window (see “From the Block Intruder Window” on page 394)
- using the **Block Request** window (see “From the Block Request Window” on page 395)

### ▼ From the Block Intruder Window

To terminate a connection using the **Block Intruder** window, proceed as follows:

- 1 Select the connection you want to block by clicking on it.
- 2 Select **Block Intruder** from the **Select** menu, or click on  in the toolbar.

The **Block Intruder** window (FIGURE 13-5) is displayed.



**FIGURE 13-5** Block Intruder window

**Connection ID** and **Connection Parameters** are those of the selected connection.

- 3 In **Blocking Scope**, select one of the options:

- **Block only this connection** — The selected connection is terminated, and all further attempts to establish a connection from the same source IP address to the same destination IP address and port will be blocked.
- **Block access from this source** — The selected connection is terminated, and all further attempts to establish connections from the source IP address of the selected connection will be denied.

- **Block access to this destination** — The selected connection is terminated, and all further attempts to establish connections to the destination IP address of the selected connection will be denied.

**4** In **Blocking Timeout**, select one of the options:

- **Indefinite** — Block all further access.
- **For ... minutes** — Block all further access attempts for the specified number of minutes.

**5** In **Force this blocking**, select one of the options:

- **Only on ...** — Block access attempts through the indicated VPN/FireWall Module.
- **On any VPN-1 & FireWall-1 Module** — Block access attempts through all FireWall Modules which are defined as gateways or hosts on the Log Server.

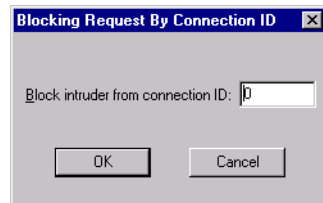
**6** Click on **OK**.

## ▼ From the Block Request Window

If you select **Block Intruder** using the **Block Request** window, proceed as follows:

**1** Select from the **Select** menu when no connection is selected.

The **Block Request** window (FIGURE 13-6) is displayed.



**FIGURE 13-6** Block Request window

**2** Enter the **Connection ID** of the connection you want to terminate.

**3** Click on **OK**.

## Clearing Blocked Connections

To clear blocked connections choose **Clear Blocking** from the **Select** menu, or click on  in the toolbar.










## Log Viewer Data

You can specify which of the available data fields (columns) to display in the Log Viewer. In addition, you can change the width of columns, and define selection criteria based on the columns. Only entries matching the selection criteria will be displayed.

The available columns are (in alphabetical order):

**Action** — action carried out on this connection (see TABLE 13-2)

**TABLE 13-2** Actions

| Icon                                                                              | Action                                                                 | Icon                                                                              | Action                                            |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------|
|  | <b>Accept</b> — The connection was allowed to proceed.                 |  | <b>Decrypt</b> — The connection was decrypted.    |
|  | <b>Reject</b> — The connection was blocked.                            |  | <b>Key Install</b> — encryption keys were created |
|  | <b>Drop</b> — The connection was dropped without notifying the source. |  | <b>Authorize</b> — Client Authentication logon    |
|  | <b>Encrypt</b> — The connection was encrypted.                         |  | <b>Deauthorize</b> — Client Authentication logoff |
|  | <b>Authcrypt</b> — SecuRemote user logon                               |                                                                                   |                                                   |

**Bytes** — the number of bytes transferred

**Conn. ID** — an ID uniquely identifying the connection (Active Connections only)

**Date** — the date the event occurred

**Destination** — the destination of the communication

**DstKeyID** — the KeyID of the destination of an encrypted communication

**Elapsed** — the duration of the connection

**Info.** — additional information (for example, messages generated during Inspection Code installation, etc.) not included in other fields

For authenticated FTP sessions, the **Info.** field shows each get and put operation as well as the file names.

**Inter.** — hardware interface at which the logged event occurred

**No.** — number of the log entry (a sequential number assigned by VPN-1/FireWall-1)

**Origin** — name of the host enforcing the rule that caused the logged event

**Product** — the product installed on the host (VPN-1/FireWall-1, FloodGate-1)

**Proto.** — the communication protocol used

**Rule** — the number of the rule in the Rule Base that was applied to this packet

Rule 0 (zero) means the action was not taken because of a rule but rather for some other reason (for example, anti-spoofing or authentication was applied).

**S\_Port** — the source port

**Service** — the service (destination port) requested by this communication





**Source** — the source of the communication

**SrcKeyID** — the KeyID of the source of an encrypted communication

**Time** — the time of day the event occurred

**Type** — the type of tracking that caused the event to be logged (TABLE 13-3)

**TABLE 13-3** Action Types

| Icon                                                                                | Action Type                                                                                                                           |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>Alert</b> — The Security Policy specified to issue an alert.                                                                       |
|    | <b>Log</b> — The Security Policy specified to log the event.                                                                          |
|   | <b>Control</b> — This type of event is logged automatically (for example, installation of a Security Policy is logged automatically). |
|  | <b>Accounting</b> — The Security Policy specified to generate an accounting log for the connection.                                   |

**User** — the user name

**XlateDport** — translated destination port number

**XlateDst** — translated destination address

**XlateSport** — translated source port number

**XlateSrc** — translated source address

## Hiding a Column

### From the Column Menu

To hide a column, right-click anywhere in the column, displaying the **Column** menu (FIGURE 13-7), and choose **Hide**.

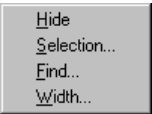


FIGURE 13-7 Column Menu

### From the View Menu

Another way to hide a column is to choose **Hide/Unhide** from the **View** menu. The **Hide/Unhide** menu is displayed (FIGURE 13-8).

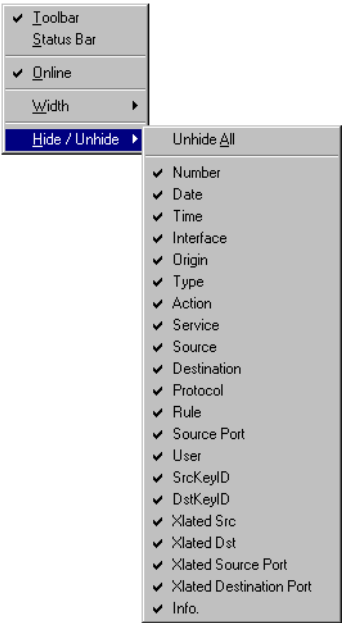


FIGURE 13-8 Hide/Unhide menu

To display a column, check it. To hide a column, uncheck it. To display all the columns, choose **Unhide All**.

### Unhiding a Hidden Column

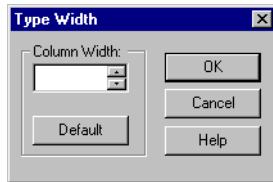
To display a column which is currently hidden, choose **Hide/Unhide** from the **View** menu and check the column you wish to display (unhide).

## Changing a Column's Width

### From the Column Menu

To change a column's width, right-click anywhere in the column, displaying the **Column** menu (FIGURE 13-7 on page 398), and choose **Width**.

The **Width** window (similar to FIGURE 13-9) is displayed, in which you can specify a width in pixels, or reset the column's width to its default value.

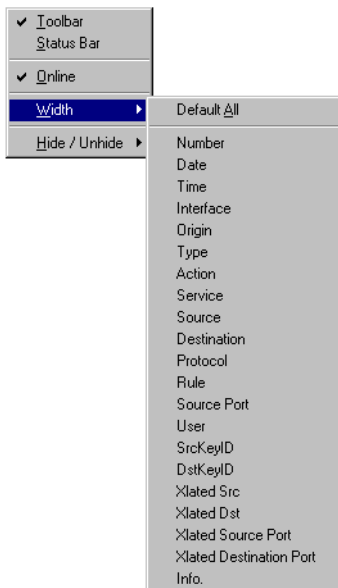


**FIGURE 13-9** Width window

The title of the window depends on the column whose width is being changed.

### From the View Menu

Another way of changing a specific column's width is to select **Width** from the **View** menu. The **Width** menu is displayed.



**FIGURE 13-10** Width Menu

Select **Default All** to reset the width of all columns to their default values.

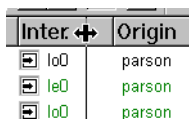
To set the width of a specific column, select that column from the menu. The **Width** window (similar to FIGURE 13-9 on page 399) is displayed, in which you can specify a width in pixels, or reset the column's width to its default value.

## By Dragging the Column's Border

Another way of changing a specific column's width is to drag the column's right border in the header, as follows:

- 1 Move the cursor to the column's right border in the header.

The cursor changes to the column resize cursor (see FIGURE 13-11).



**FIGURE 13-11** Dragging the Vertical Column Header Border

- 2 Click on the left mouse button without releasing it.
- 3 Move the column border to the desired position while you keep the left mouse button down.
- 4 Release the left mouse button.

## Navigation And Searching

### Scrolling through the Log File



To scroll through the entries in the Log Viewer, use the scrollbars on the side and bottom of the Log Viewer. You can also use the arrow, **PageUp** and **PageDown** keys.

### Navigating to a Specific Location in the Log File

To go to a specific location in the log file, open the **Edit** menu and select the desired option:

**Go To Top** — to go to the beginning of the Log File

**Go To Bottom** — to go to the end of the Log File

Alternatively, you can select  from the toolbar to go to the top of the Log File, or  to go to the bottom.

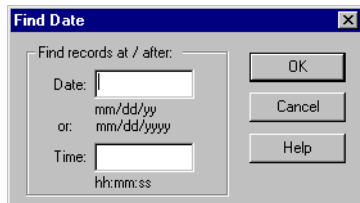


## Finding a Specific Record

### From the Column Menu

To find a specific record in the Log File based on a value in a specific column, right-click anywhere in that column, displaying the **Column** menu (FIGURE 13-7 on page 398), and then choose **Find**. The **Find** window (similar to FIGURE 13-12) is displayed.

For example, if you wish to find the first log entry after a specific date, right-click in the **Date** column and then choose **Find**. The **Find Date** window (FIGURE 13-12) is then displayed.

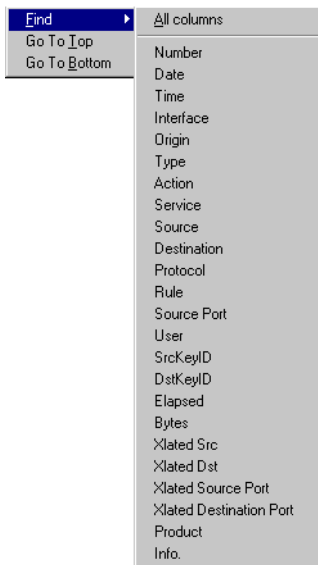


**FIGURE 13-12** Find Date window

Enter the desired criteria and click on **OK** to go to the specified location.

### From the Edit Menu

Another way to find a specific record in the Log File is to select **Find** from the **Edit** menu. The **Find** menu (FIGURE 13-13) is then displayed.



**FIGURE 13-13** Find menu

For example, to find the first log entry after a specific date, select **Find** from the **Edit** menu and then select **Date**. The **Find Date** window (FIGURE 13-12) is then displayed.

To search all the columns for a specific value, choose **All Columns** (see “All Columns” below).

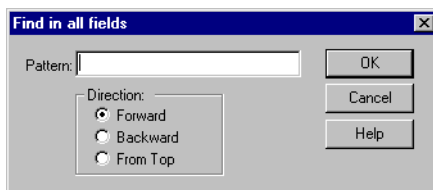
## All Columns

The **All Columns** option allows you to search for a text string in any specified data column in the Log File.

For example, to search for a text string in all the columns, proceed as follows:

- 1 Choose **All Columns**.

The **Find in all Fields** window is displayed.



**FIGURE 13-14** Find in all Fields window

- 2 In the **Pattern** field, enter the text string to search for.  
You can specify a regular expression in this field.
- 3 Select one of the **Direction** options to specify the desired search direction:
  - **Forward** — to search forward from the current entry (toward the end of the Log File)
  - **Backward** — to search backwards from the current entry toward the beginning of the Log File
  - **From Top** — to search forward from the beginning of the Log File
- 4 Click on **OK** to go to the specified log entry.

## Displaying Selected Entries

### Selection Criteria

To display only entries of interest in the Log Viewer and to hide other entries, you can specify selection criteria.

### From the Column Menu

To specify selection criteria, proceed as follows:

- 1 Right-click anywhere in the column.

The **Column** menu (FIGURE 13-7 on page 398) is displayed.

## 2 Choose **Selection**.

The appropriate **Selection Criterion** window for that column will be displayed (see “Specifying Selection Criteria” on page 404).

## From the **Select** Menu

Another way to specify selection criteria is to select **By columns** from the **Select** menu. The **Column Selection** menu is then displayed (FIGURE 13-15).



**FIGURE 13-15** Column Selection Menu

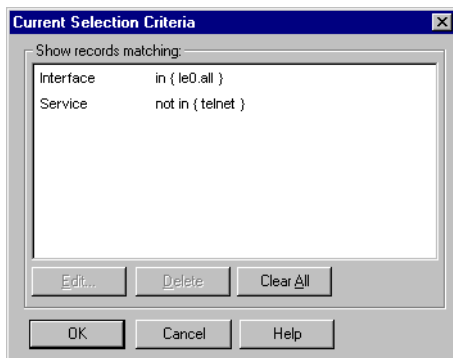


**Note** – Selection criteria are in effect only if **Apply Selection** (in the **General** tab of the **Options** window) is checked. To display the **Options** window, choose **Options...** from the **Select** menu (see “Log Viewer Options” on page 418).

You may now do one of the following:

- Choose the column for which you wish to define selection criteria.  
The appropriate **Selection Criterion** window for that column will be displayed (see “Specifying Selection Criteria” on page 404).
- Choose **Current** to display the **Current Selection Criteria** window (FIGURE 13-16).

## Current Selection Criteria window



**FIGURE 13-16** Current Selection Criteria window

To modify one of the selection criteria displayed, select it and then click on **Edit**, or double-click on the criterion. A window will be displayed in which you will be prompted to specify the properties of the selection.

To delete a criterion, select it and click on **Delete**.

## Specifying Selection Criteria

Only the log entries that match the selection criteria will be displayed in the Log Viewer.

A description of the specific selection criteria follows. You can specify as many selection criteria as you wish. The selection criteria are logically ANDed, that is, a log entry is displayed only if it matches all the selection criteria.

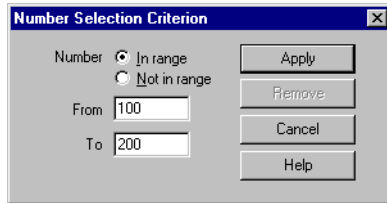
All selection criteria are saved when you exit the Log Viewer, and the same selection criteria will be available the next time you enter the Log Viewer. If the check box is checked, selection criteria will be in effect.

## ▼ To Select By Number, Port, Rule, Date or Time

- 1 Choose **Select** from the Log Viewer Menu and specify the selection criterion from the **By columns** menu, or right-click on the column corresponding to the selection criterion and then choose **Selection** from the **Column** menu.

The appropriate **Selection Criterion** window is displayed.

For example, choose **Select** from the Log Viewer Menu and select **Number** from the **By columns** menu, or right-click on **Number** column and then choose **Selection** from the **Column** menu. The **Number Selection Criterion** window (FIGURE 13-17) is displayed.



**FIGURE 13-17** Number Selection Criterion window

The default is to include log entries, that is, to display only log entries that are within the specified range. To exclude log entries, that is, to display only log entries that are not in the specified range, select **Not in range**.

- 2 Specify the range you wish to include or exclude by entering **From** and **To** criteria.
- 3 Click on **Apply** to apply the specified criteria.

The criterion will be displayed in the **Current Selection Criteria** window.

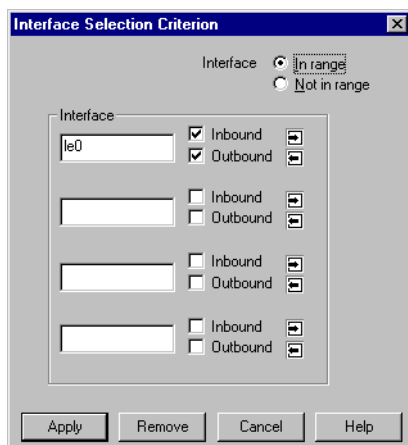
- 4 Click on **Remove** to delete the specified criterion.

The criterion will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select By Interface

- 1 Choose **Select** from the Log Viewer Menu and select **Interface** from the **By columns** menu, or right-click on **Interface** column and then choose **Selection** from the **Column** menu.

The **Interface Selection Criterion** window (FIGURE 13-18) appears.



**FIGURE 13-18** Interface Selection Window

The default is to include the specified interfaces in the selection. To exclude the interfaces specified, select **Not in range**.

In each **Interface** field, you may specify one interface (for example, sl0, le0, all) to be included in (or excluded from) the selection criteria. The list is logically ORed (added); that is, all interfaces specified will be included (or excluded).

- 2** To select inbound packets, check **Inbound**. To select outbound packets, check **Outbound**. To select eitherbound packets, check both **Inbound** and **Outbound**.

- 3** Click on **Apply** to apply the specified criteria.

The criteria will be displayed in the **Current Selection Criteria** window.

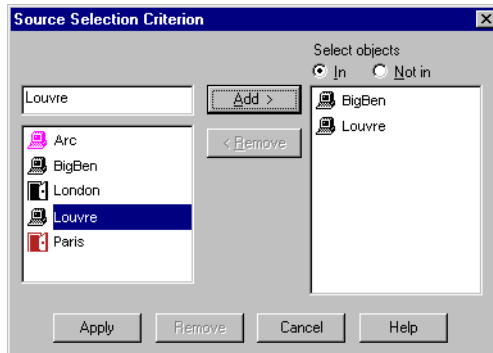
- 4** Click on **Remove** to delete the specified criteria.

The criteria will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select By Origin, Source, Destination, User or Service

- 1 Choose **Select** from the Log Viewer Menu and specify the selection criterion from the **By columns** menu, or right-click on the column corresponding to the selection criterion and then choose **Selection** from the **Column** menu.

The window for the appropriate selection criterion appears.



**FIGURE 13-19** Source Object Selection Criterion window

The default is to include the specified items in the selection. To exclude the specified items, select **Not In**.

- 2 In the left listbox, select the items you wish to include or exclude. Use the **Add** button to add individual items and groups.

Use the **Add** data entry field (to the left of the **Add** button) to add an item by typing its name. Click on **Add** to add the name you typed. In this way, you can, for instance, add external **Source** or **Destination** hosts which do not appear in the listbox. You may specify a host by entering its name or by entering its address in conventional IP dot notation.



**Note – Origin** is the origin of the log entry, that is, the host that generated the log entry and on which the rule is enforced. **Origin** can only be an internal object (see “Location: Internal/External” on page 103). **Source** and **Destination** are the source and destination of the packet, either of which may be internal or external.

The Objects and Group elements that you added are displayed in the right listbox. These elements are the selection criteria.

- 3 If you wish to delete an item in the right listbox (the list of selection criteria), select it and click on **Remove**.

- 4 Select **Apply** to apply the specified criteria.

The criteria will be displayed in the **Current Selection Criteria** window.

- 5 Click on **Remove** to delete the specified criteria.

The criteria will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select By Address Translation Parameter

- 1 Choose **Select** from the Log Viewer Menu and specify the selection criterion from the **By columns** menu, or right-click on the column corresponding to the selection criterion and then choose **Selection** from the **Column** menu.

Address translation parameters include the following:

**XlateSrc** — the translated source IP address

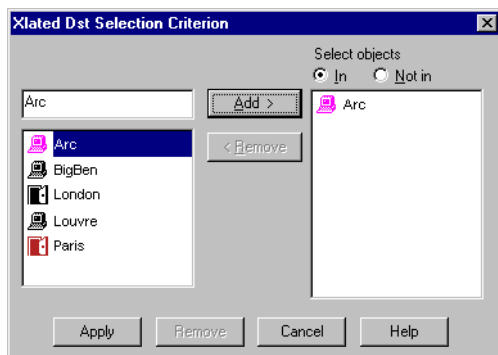
**XlateDst** — the translated destination IP address

**XlateSPort** — the translated source port number

**XlateDPort** — the translated destination port number

## ▼ XlateSrc or XlateDst

If you selected **XlateSrc** or **XlateDst**, then the **Xlated Src Selection Criterion** window or the **Xlated Dst Selection Criterion** window is displayed.



**FIGURE 13-20** Xlated Dst Selection Criterion window

The default is to include the specified items in the selection. To exclude the specified items, select **Not In**.

- 1 In the left listbox, select the items you wish to include or exclude. Use the **Add** button to add individual items and groups.

Use the **Add** data entry field (to the left of the **Add** button) to add an item by typing its name. Click on **Add** to add the name you typed. In this way, you can, for instance, add external **Source** or **Destination** hosts, which do not appear in the listbox. You may specify a host by entering its name or by entering its address in conventional IP dot notation.

- 2 Select **Apply** to apply the specified criteria.

The criteria will be displayed in the **Current Selection Criteria** window.

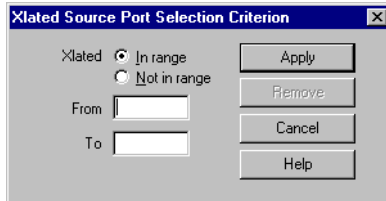
- 3 Click on **Remove** to delete the specified criteria.

The criteria will no longer be displayed in the **Current Selection Criteria** window.



## ▼ XlateSPort or XlateDPort

If you selected **XlateSPort** or **XlateDPort**, then the **Xlated Source Port Selection Criterion** window or the **Xlated Destination Port Selection Criterion** window is displayed.



**FIGURE 13-21** Xlated Source Port Selection Criterion window

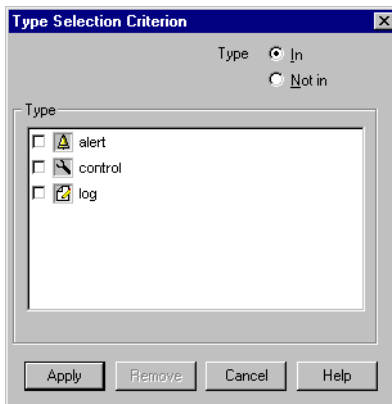
The default is to include the specified items in the selection. To exclude the specified items, select **Not In**.

- 1** Select **Apply** to apply the specified criteria.  
The criteria will be displayed in the **Current Selection Criteria** window.
- 2** Click on **Remove** to delete the specified criteria.  
The criteria will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select by Type

- 1** Choose **Select** from the Log Viewer Menu and select **Type** from the **By columns** menu, or right-click on **Type** column and then choose **Selection** from the **Column** menu.

The **Type Selection Criterion** window is displayed.







**FIGURE 13-22** Type Selection Criterion Window

The default is to include the specified types in the selection. To exclude the specified types, select **Not In**.

- 2 Select the types you wish to include or exclude (TABLE 13-4).

**TABLE 13-4** Entry Types

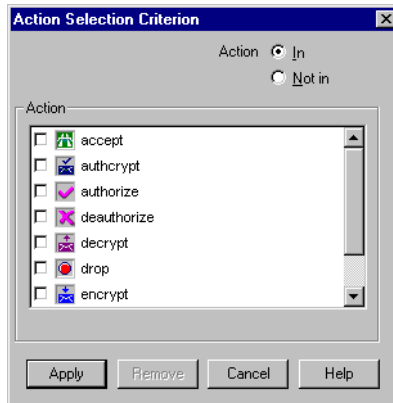
| icon                                                                              | meaning                                                                                                                                                    |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Alert</b> — an event that generated an alert. Available only in <b>Log</b> and <b>Active</b> modes.                                                     |
|  | <b>Control</b> — an event that was logged automatically (for example, installing a Security Policy). Available only in <b>Log</b> and <b>Active</b> modes. |
|  | <b>Log</b> — an event that was logged as specified by the Security Policy. Available only in <b>Log</b> and <b>Active</b> modes.                           |
|  | <b>Accounting</b> — an accounting log for the connection. Available only in <b>Account</b> mode.                                                           |

- 3 Click on **Apply** to apply the specified criteria.  
The criteria will be displayed in the **Current Selection Criteria** window.
- 4 Click on **Remove** to delete the specified criteria.  
The criteria will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select by Action

- 1 Choose **Select** from the Log Viewer Menu and select **Action** from the **By columns** menu, or right-click on **Action** column and then choose **Selection** from the **Column** menu.

The **Action Selection Criterion** window is displayed.



**FIGURE 13-23** Action Selection Criterion window

The default is to include the specified actions in the selection. To exclude the specified actions, select **Not In**.

- 2 Select the actions you wish to include or exclude (TABLE 13-5).

**TABLE 13-5** Action icons

| Icon | Action                                                                 | Icon | Action                                            |
|------|------------------------------------------------------------------------|------|---------------------------------------------------|
|      | <b>Accept</b> — The connection was allowed to proceed.                 |      | <b>Decrypt</b> — The connection was decrypted.    |
|      | <b>Reject</b> — The connection was blocked.                            |      | <b>Key Install</b> — encryption keys were created |
|      | <b>Drop</b> — The connection was dropped without notifying the source. |      | <b>Authorize</b> — Client Authentication logon    |
|      | <b>Encrypt</b> — The connection was encrypted.                         |      | <b>Deauthorize</b> — Client Authentication logoff |
|      | <b>Authcrypt</b> — SecuRemote user logon                               |      |                                                   |

- 3 Select **Apply** to apply the specified criteria.

The criteria will be displayed in the **Current Selection Criteria** window.

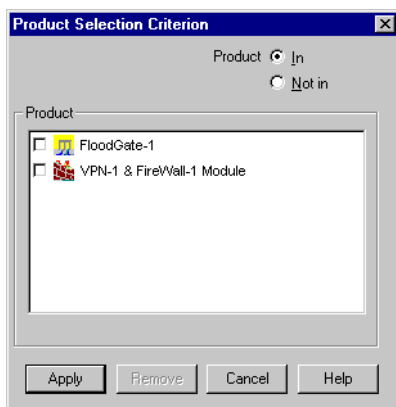
- 4 Click on **Remove** to delete the specified criteria.

The criteria will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select by Product

- 1 Choose **Select** from the Log Viewer Menu and select **Product** from the **By columns** menu, or right-click on **Product** column and then choose **Selection** from the **Column** menu.

The **Product Selection Criterion** window is displayed.



**FIGURE 13-24** Product Selection window

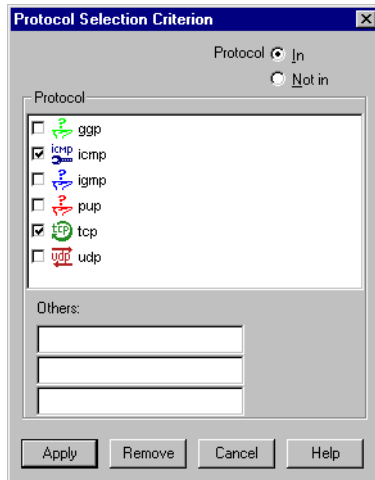
The default is to include the specified actions in the selection. To exclude the specified actions, select **Not In**.

- 2 Select the products (**VPN-1&FireWall-1**, **FloodGate-1**) you wish to include or exclude.

## ▼ To Select By Protocol

- 1 Choose **Select** from the Log Viewer Menu and select **Protocol** from the **By columns** menu, or right-click on **Protocol** column and then choose **Selection** from the **Column** menu.

The **Protocol Selection Criterion** window (FIGURE 13-25) is displayed.



**FIGURE 13-25** Protocol Selection Criterion Window

The default is to include the specified protocols in the selection. To exclude the specified selections, select **Not In**.

- 2 Select the protocols you wish to include or exclude.

You may also add other protocols by typing the name or the number of the desired protocol in the **Others** field.

- 3 Click on **Apply** to apply the specified criteria.

The criteria will be displayed in the **Current Selection Criteria** window.

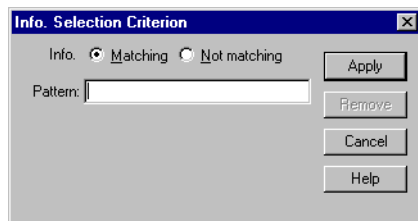
- 4 Click on **Remove** to delete the specified criteria.

The criteria will no longer be displayed in the **Current Selection Criteria** window.

## ▼ To Select By Info., SrcKeyID or DstKeyID

- 1 Choose **Select** from the Log Viewer Menu and select **Info.**, **SrcKeyID** or **DstKeyID** from the **By columns** menu, or right-click on appropriate column and then choose **Selection** from the **Column** menu.

The corresponding **Selection Criterion** window is displayed.



**FIGURE 13-26** Information Selection Criterion Window

The default is to include the specified additional information in the selection. To exclude the specified information, select **Not Matching**.

- 2 In the **Pattern** field, type the string to be included (or excluded).

- 3 Click on **Apply** to apply the specified criteria.

The criteria will be displayed in the **Current Selection Criteria** window.

- 4 Click on **Remove** to delete the specified criteria.

The criteria will no longer be displayed in the **Current Selection Criteria** window.

## Example

Assume a Log File as displayed in FIGURE 13-27.

| No | Date    | Time     | Inte.. | Origin | Type    | Action  | Service | Source | Destination |
|----|---------|----------|--------|--------|---------|---------|---------|--------|-------------|
| 0  | 29Sep96 | 12:31:24 | da...  | dana   | control | ctl     |         |        |             |
| 1  | 29Sep96 | 12:31:31 | da...  | dana   | log     | decrypt | telnet  | ub40   | dana        |
| 2  | 29Sep96 | 12:36:57 | da...  | ub40   | log     | encrypt | telnet  | ub40   | dana        |
| 3  | 29Sep96 | 12:31:43 | da...  | dana   | log     | decrypt | telnet  | ub40   | dana        |
| 4  | 29Sep96 | 12:37:09 | da...  | ub40   | log     | encrypt | telnet  | ub40   | dana        |
| 5  | 29Sep96 | 12:37:04 | da...  | dana   | control | ctl     |         |        |             |
| 6  | 29Sep96 | 12:37:12 | da...  | dana   | log     | decrypt | telnet  | ub40   | dana        |
| 7  | 29Sep96 | 12:37:13 | da...  | dana   | control | ctl     |         |        |             |
| 8  | 29Sep96 | 12:38:26 | lo0    | dana   | control | ctl     |         |        |             |
| 9  | 29Sep96 | 12:37:43 | da...  | ub40   | control | ctl     |         |        |             |
| 10 | 29Sep96 | 12:42:37 | da...  | ub40   | log     | encrypt | telnet  | ub40   | dana        |
| 11 | 29Sep96 | 12:44:03 | le0    | ub40   | control | ctl     |         |        |             |
| 12 | 29Sep96 | 12:39:09 | da...  | dana   | log     | decrypt | ftp     | ub40   | dana        |
| 13 | 29Sep96 | 12:44:35 | da...  | ub40   | log     | encrypt | ftp     | ub40   | dana        |
| 14 | 29Sep96 | 12:41:14 | da...  | dana   | control | ctl     |         |        |             |
| 15 | 29Sep96 | 15:06:16 | da...  | dana   | control | ctl     |         |        |             |
| 16 | 29Sep96 | 15:21:50 | lo0    | dana   | control | ctl     |         |        |             |
| 17 | 29Sep96 | 15:37:01 | da...  | dana   | control | ctl     |         |        |             |
| 18 | 29Sep96 | 15:46:19 | da...  | dana   | control | ctl     |         |        |             |

**FIGURE 13-27** Log File — Selection Criteria Not Applied

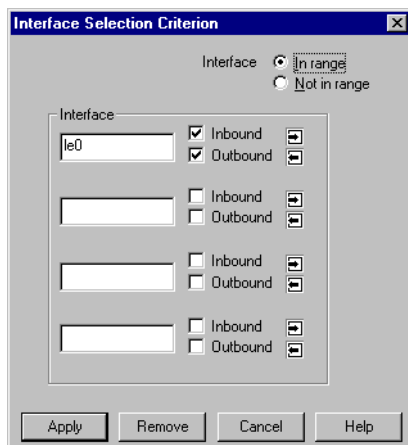
To display only log entries relating to the leO interface and to non-TELNET services, proceed as follows:

- 1 Choose **Select** from the Log Viewer menu and **Interface** from the **By columns** menu, or right-click in the **Inte.** column and then choose **Selection** from the **Column** menu.

The **Interface Selection Criterion** window is displayed (FIGURE 13-28).

- 2 Type leO on the first line.

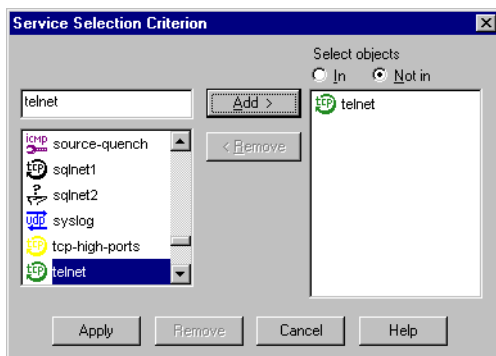
- 3 Select **Inbound** and **Outbound** on the first line.



**FIGURE 13-28** Interface Selection window

- 4 Click on **Apply** to close the window.
- 5 Choose **Select** from the Log Viewer menu and **Service** from the **By columns** menu, or right-click in the **Service** column and then choose **Selection** from the **Column** menu.

The **Service Selection Criterion** window (FIGURE 13-29) is displayed.

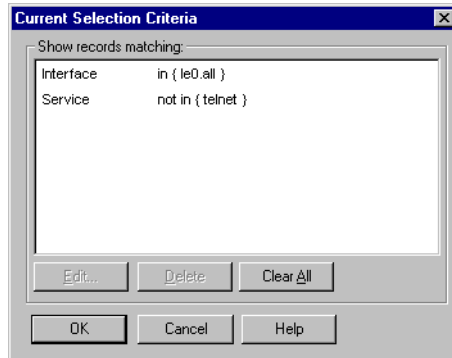


**FIGURE 13-29** Service Selection Criterion window

- 6 Select **telnet** and add it to the list on the right by selecting **Add**.
- 7 Select **Not In** under **Select Objects**.
- 8 Click on **Apply** to close the window.



The **Current Selection Criteria** window (FIGURE 13-30) now shows the specified criteria.



**FIGURE 13-30** Log Viewer Selection Manager Showing Two Criteria

Only Log entries matching the criteria (le0 interface and to non-TELNET services) are displayed in the Log Viewer (FIGURE 13-31).

| No   | Date    | Time     | Inter. | Origin | Type | Action | Service | Source  |
|------|---------|----------|--------|--------|------|--------|---------|---------|
| 1715 | 10Mar96 | 20:26:19 | le0    | parson | log  | accept | http    | mitchel |
| 1716 | 10Mar96 | 20:28:06 | le0    | parson | log  | accept | http    | mitchel |
| 1717 | 10Mar96 | 20:28:26 | le0    | parson | log  | accept | http    | mitchel |
| 1718 | 10Mar96 | 20:31:44 | le0    | parson | log  | accept | http    | mitchel |
| 1723 | 11Mar96 | 13:17:26 | le0    | parson | log  | accept | http    | parson  |
| 1724 | 11Mar96 | 13:17:38 | le0    | parson | log  | accept | http    | parson  |
| 1725 | 11Mar96 | 13:17:41 | le0    | parson | log  | accept | http    | parson  |
| 1726 | 11Mar96 | 13:18:09 | le0    | parson | log  | accept | http    | parson  |
| 1733 | 3Apr96  | 14:15:42 | le0    | parson | log  | accept | http    | natasha |
| 1734 | 3Apr96  | 14:15:46 | le0    | parson | log  | accept | http    | parson  |
| 1735 | 3Apr96  | 14:16:05 | le0    | parson | log  | accept | http    | natasha |
| 1736 | 3Apr96  | 14:16:05 | le0    | parson | log  | accept | http    | parson  |
| 1737 | 3Apr96  | 14:17:14 | le0    | parson | log  | accept | http    | parson  |

**FIGURE 13-31** Log File — Selection Criteria Applied

## Saving and Reusing Selection Criteria

### ▼ To save selection criteria in a file

To save selection criteria in a file, proceed as follows:

- 1 Choose **New Selection** from the **Select** menu.
- 2 Modify the selection criteria as required.

- 3 Choose **Save Selection** from the **Select** menu and specify a file name for the selection criteria.

### ▼ To re-use selection criteria that you have saved in a file

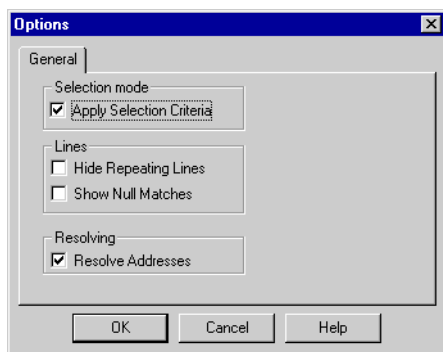
- 1 Choose **Open Selection** from the **Select** menu.
- 2 Specify the file name for the selection criteria.

Entries in the Log Viewer will be displayed in accordance with the selection criteria in the file you have opened.

## Log Viewer Options

### Options window — General tab


To display the Log Viewer **Options** window (FIGURE 13-32), choose **Options** from the **Select** menu.



**FIGURE 13-32** Options window — General tab

**Apply Selection Criteria**— This option controls whether the selection criteria are applied or not.

If this option is checked, all selection criteria in the **Current Selection Criteria** window are applied to the Log Viewer and only log entries that match the criteria are displayed. If it is cleared, no selection criteria are applied, and all log entries are displayed in the Log Viewer. This option allows you to display the selection criteria in the **Current Selection Criteria** window without applying them to the Log Viewer.

Checking this option is equivalent to selecting  in the toolbar.

**Hide Repeating Lines**— This option controls the display of log entries that differ only by date and time.

If two or more consecutive log entries are identical, you may hide all but the first entry by checking **Hide Repeating Lines**. The **Hide Repeating Lines** option does not affect entries that are not consecutive.

VPN-1/FireWall-1 automatically eliminates duplicate log entries within a user-specified time limit. For instance, if the same entry is logged twice within a short period of time, the system will automatically suppress the second entry. The time limit for suppressing successive identical log entries is set in the **Excessive Log Grace Period** field of the **Log and Alert** tab of the **Properties Setup** window (see “Log and Alert” on page 243).

**Show Null Matches** — This option controls the display of Null Matches, that is, log entries that are neither included nor excluded by the current selection criteria.

For instance, if you choose to display only log entries whose **Action** is either **Reject** or **Drop**, control logs are null matches because **Action** is not relevant to a control log. They are neither included nor excluded. If **Show Null Matches** is checked, the null matches are displayed.

**Resolve Addresses** — This option controls the display of source and destination host names.

If **Resolve Address** is checked, the name of the host and the domain are displayed. If not checked, the source and destination hosts are identified by their addresses in conventional IP dot notation.

## Online Update

The Log Viewer shows the Log File as it was when the Log Viewer was started. In order to update the Log Viewer online as new entries are added to the Log File, check **Online** in the **View** menu.

This option controls displaying additions to the Log File as they occur. This option is only relevant if the current Log File, is displayed in the log viewer. If **OnLine** is checked and the Log Viewer is at the end of the Log File, new log records will be displayed as they are added to the Log File.

## Log File Management

### Opening a Different Log File

To open a different Log File, choose **Open** from the **File** menu and specify the file to open.

### Starting A New Log File

To start a new Log File, choose **New** from the **File** menu.

When you create a new Log File, the current Log File is closed and written to disk with a name that contains the current date and time. The new Log File receives the default Log File name, `$FWDIR/log/fw.log`. This operation actually performs a Log File switch.

Only one Log File can be open in the Log Viewer at a time.

## Deleting The Currently Displayed Log File

To delete the currently displayed Log File, choose **Delete** from the **File** menu.

The Log File currently displayed in the Log Viewer will be deleted.

## Printing and Saving Log Entries

The **File** menu allows you to load Log Files and save and print log entries.

When printing or saving, only the log entries that match the selection criteria will be printed or saved.

### Saving the Currently Displayed Log Entries

To save the currently displayed Log File entries to a file, choose **Save** from the **File** menu and specify the name to assign to the file.

The current log entries will be written to file. Only the records that match the selection criteria will be saved to the file (both those that are visible in the window and those that are not).

### Printing the Currently Displayed Log Entries

To print the currently displayed Log File entries, choose **Print** from the **File** menu.

You can print log entries that are currently displayed in the Log Viewer or all the entries in the file that match the Selection Criteria.

You can print to a file or to a printer in ASCII (text) format by selecting the appropriate options in the **Print** window.

## Miscellaneous Functions

### Redirecting Logging to Another Master


A Master is a machine to which VPN/FireWall Modules direct logging. The file `$FWDIR/conf/masters` contains a list of IP addresses (or network object names), one per line. When the VPN/FireWall Module starts working, it reads this file to determine where to direct logging.

Logs can also be directed to a Customer Log Module (CLM). A CLM is a Management Station that only perform logging and collect alerts if the `$FWDIR/conf/loggers` exists and identifies the CLM. For more information see “Loggers File” on page 79.


### Exporting Log Data to Another Application

To create a comma delimited ASCII file which can be input to other applications, choose **Export** from the **File** menu.

## Stop Update

To stop loading Log data from the server, click on  in the toolbar.





## Reload Log Data

To reload the Log Viewer with new data, click on  in the toolbar.

## Menus



### File Menu

**TABLE 13-6** File Menu Commands

| Menu Entry           | Toolbar Button                                                                      | Description                                                                    | See                                                        |
|----------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------|
| <b>New</b>           |    | Create a new Log File.                                                         | “Starting A New Log File” on page 419                      |
| <b>Open</b>          |    | Close the currently open Log File and open another Log File.                   | “Opening a Different Log File” on page 419                 |
| <b>Save As</b>       | none                                                                                | Save the currently selected records in the open Log File in a file.            | “Saving the Currently Displayed Log Entries” on page 420   |
| <b>Purge</b>         | none                                                                                | Delete the currently open Log File.                                            | “Deleting The Currently Displayed Log File” on page 420    |
| <b>Print</b>         |   | Print the current Log File.                                                    | “Printing the Currently Displayed Log Entries” on page 420 |
| <b>Print Preview</b> |  | Print Preview the currently open Log File.                                     |                                                            |
| <b>Print Setup</b>   | none                                                                                | Print Setup                                                                    |                                                            |
| <b>Export</b>        | none                                                                                | Export the currently selected records in to a comma delimited ASCII text file. | “Exporting Log Data to Another Application” on page 420    |
| <b>Exit</b>          | none                                                                                | Exit the Log Viewer application.                                               |                                                            |


## Edit Menu

**TABLE 13-7** Edit Menu Commands

| Menu Entry          | Toolbar Button                                                                    | Description                          | See                                                             |
|---------------------|-----------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------|
| <b>Find</b>         | none                                                                              | Open the Find menu.                  | "Finding a Specific Record" on page 401                         |
| <b>Go To Top</b>    |  | Go to the beginning of the Log File. | "Navigating to a Specific Location in the Log File" on page 400 |
| <b>Go To Bottom</b> |  | Go to the end of the Log File.       | "Navigating to a Specific Location in the Log File" on page 400 |




## View Menu

**TABLE 13-8** View Menu Commands

| Menu Entry         | Toolbar Button                                                                    | Description                                                                   | See                         |
|--------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-----------------------------|
| <b>Toolbar</b>     | none                                                                              | Toggle the display of the Log Viewer Toolbar.                                 |                             |
| <b>Status Bar</b>  | none                                                                              | Toggle the display of the Log Viewer Status Bar.                              |                             |
| <b>Online</b>      |  | Toggle the periodic automatic updating of the Log Viewer.                     | "Online Update" on page 419 |
| <b>Width</b>       | none                                                                              | Set width of specific columns or restore all columns to their default widths. |                             |
| <b>Hide/Unhide</b> | none                                                                              | Hide or unhide (show) specific columns or all columns.                        |                             |

## Select Menu

**TABLE 13-9** Select Menu Commands

| Menu Entry               | Toolbar Button                                                                     | Description                                                                    | See                                                 |
|--------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>By columns</b>        | none                                                                               | Open a menu listing all the columns                                            |                                                     |
| <b>Options</b>           | none                                                                               | Open the <b>Options</b> window — <b>General</b> tab (FIGURE 13-32 on page 418) | “Options window — General tab” on page 418          |
| <b>Current</b>           |   | Open the <b>Current Selection Criteria</b> window (FIGURE 13-16 on page 404)   | “Selection Criteria” on page 402                    |
| <b>New Selection</b>     | none                                                                               | Create new selection criteria.                                                 | “Saving and Reusing Selection Criteria” on page 417 |
| <b>Open Selection</b>    | none                                                                               | Open a selection criteria file.                                                | “Saving and Reusing Selection Criteria” on page 417 |
| <b>Save Selection</b>    | none                                                                               | Save the current selection criteria in a file.                                 | “Saving and Reusing Selection Criteria” on page 417 |
| <b>Save Selection As</b> | none                                                                               | Specify a new name for the current selection criteria file.                    | “Saving and Reusing Selection Criteria” on page 417 |
| <b>Block Intruder</b>    |   | Open the <b>Block Intruder</b> window (FIGURE 13-5 on page 394).               | “Blocking Connections” on page 394                  |
| <b>Clear Blocking</b>    |  | Clear blocked connections.                                                     | “Clearing Blocked Connections” on page 395          |

## Window Menu

**TABLE 13-10** Window Menu Commands

| Menu Entry           | Toolbar Button | Description                    | See                                    |
|----------------------|----------------|--------------------------------|----------------------------------------|
| <b>System Status</b> | none           | Open the System Status Viewer. | Chapter 12, “System Status Viewer”     |
| <b>Policy Editor</b> | none           | Open the Policy Editor.        | Chapter 8, “Security Policy Rule Base” |

## Help Menu

**TABLE 13-11** Help Menu Commands

| Menu Entry              | Toolbar Button | Description                       |
|-------------------------|----------------|-----------------------------------|
| <b>Help Topics</b>      | none           | Display Log Viewer Help.          |
| <b>About Log Viewer</b> | none           | Display the Log Viewer About box. |

## Log Viewer Toolbar

















**FIGURE 13-33** Log Viewer Toolbar

Some of the toolbar buttons are shortcuts for menu commands (see TABLE 13-12). Other buttons have no corresponding menu commands.

## Toolbar Buttons and their corresponding menu commands

**TABLE 13-12** Toolbar Buttons and their corresponding menu commands

| Toolbar Button                                                                      | Menu Command                 | Meaning                                            | Toolbar Button                                                                      | Menu Command                    | Meaning                                       |
|-------------------------------------------------------------------------------------|------------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------|-----------------------------------------------|
|    | <b>File&gt;New</b>           | Open a new Log File.                               |    | <b>Edit&gt;Go To Top</b>        | Go to the top of the Log File.                |
|   | <b>File&gt;Open</b>          | Open an existing Log File.                         |   | <b>Edit&gt;Go To Bottom</b>     | Go to the bottom of the Log File.             |
|  | <b>File&gt;Save</b>          | Save the current Log File.                         |  | none                            | Stop retrieving data from the Log File.       |
|  | <b>File&gt;Print</b>         | Print the current Log File.                        |  | none                            | Reload data from the Log File.                |
|  | <b>File&gt;Print Preview</b> | Print Preview the current Log File.                |  | <b>View&gt;Online</b>           | Toggle the online updating of the Log Viewer. |
|  | <b>Select&gt;Current</b>     | Open the <b>Current Selection Criteria</b> window. |  | <b>Select&gt;Block Intruder</b> | Open the <b>Block Intruder</b> window.        |
|  | none                         | Apply current selection criteria.                  |  | <b>Select&gt;Clear Blocking</b> | Clear blocked connections                     |



# Network Address Translation

---

## In This Chapter

|                                                           |                 |
|-----------------------------------------------------------|-----------------|
| <i>Introduction</i>                                       | <i>page 425</i> |
| <i>Translation Modes</i>                                  | <i>page 428</i> |
| <i>Address Translation and Routing</i>                    | <i>page 435</i> |
| <i>IANA Recommendations</i>                               | <i>page 439</i> |
| <i>Supported Services</i>                                 | <i>page 439</i> |
| <i>Generating Address Translation Rules Automatically</i> | <i>page 440</i> |
| <i>Configuring Address Translation — Windows GUI</i>      | <i>page 442</i> |
| <i>Address Translation Examples</i>                       | <i>page 457</i> |
| <i>Address Translation Examples</i>                       | <i>page 457</i> |
| <i>Managing PIX Address Translation</i>                   | <i>page 464</i> |
| <i>Advanced Topics</i>                                    | <i>page 470</i> |
| <i>Frequently Asked Questions</i>                         | <i>page 475</i> |

## Introduction

### The Need for Address Translation

The need for IP address translation — replacing one IP address in a packet by another IP address — arises in two cases:

- 1** The network administrator wishes to conceal the network's internal IP addresses from the Internet.

The administrator may reason that there is nothing to be gained, from a security point of view, by making a network's internal addresses public knowledge.

- 2** An internal network's IP addresses are invalid Internet addresses (that is, as far as the Internet is concerned, these addresses belong to another network).

This situation may have arisen for historical reasons: an internal network was originally not connected to the Internet and its IP addresses were chosen without regard to Internet conventions. If such a network is then connected to the Internet, its long-established internal IP addresses cannot be used externally. Changing these addresses may be impractical or unfeasible.

In both cases, the internal IP addresses cannot be used on the Internet. However, Internet access must still be provided for the internal hosts with the invalid or secret IP addresses.

Application gateways (proxies) have historically served as a partial solution to these problems. For example, to hide his or her internal IP addresses, a user can TELNET to a gateway and from there continue to the Internet through a proxy. VPN-1/FireWall-1 can be easily set up to provide and enforce such a scheme for a wide variety of services (FTP, TELNET, HTTP, and almost all other TCP, UDP and RPC services). Moreover, VPN-1/FireWall-1 supplements this scheme by providing user authentication on the gateway.

On the other hand, proxies do have drawbacks:

- Proxies are tailored per application, so it is impossible to use applications that are not proxied, inbound or outbound.
- Proxies are not transparent, so that even authorized outbound users need to go through the application on the gateway, and impose a large overhead on the gateway host. Once a connection is accepted by a proxy, it functions as a packet forwarder at the application layer, which is an inefficient use of resources.
- It is difficult to provide good proxies for protocols other than TCP.

In contrast, VPN-1/FireWall-1's generic and transparent fully RFC 1631 compliant Address Translation feature provides a complete and efficient solution. The administrator can determine which internal addresses are to be concealed (that is, mapped to the FireWalled host's IP address) and which are to be mapped to a range of IP addresses visible to the Internet. At the same time, internal hosts can be configured to be accessible from the Internet even though their internal IP addresses are invalid Internet addresses. VPN-1/FireWall-1 achieves full Internet connectivity for internal clients at the maximum bandwidth possible through a standard workstation.

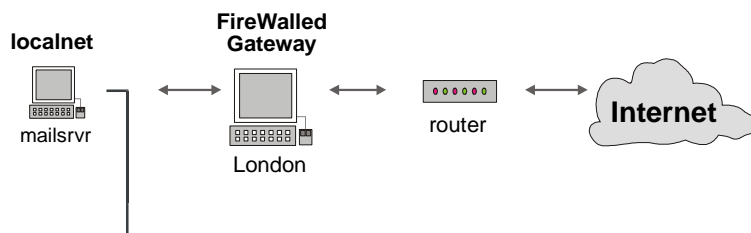
Address Translation can be used to implement "one way routing," so that there is no route from the outside to an internal network or to hosts.



**Note** – Address Translation changes IP addresses in the packet, so it is almost always necessary to make some changes in the routing tables to ensure that packets with translated addresses reach their proper destinations.

## Example

Consider the following network configuration:



**FIGURE 14-1** Example Network Configuration

Suppose the administrator of this network wishes to provide mail services to the internal (private) hosts, but the internal IP addresses cannot be used, for one of the reasons stated above (see “The Need for Address Translation” on page 425.)



**Note** – The gateway has a valid IP address which cannot be concealed.

One possible solution is to move the mail server (which is currently on one of the internal hosts) to the gateway. This solution is not optimal, because of:

- the significant overhead the mail server imposes on the gateway
- reduced security
- the administrative overhead incurred when modifying the configuration

A better solution might be to implement Address Translation on the gateway, as follows, using the Static Destination Mode of Address Translation (see “Static Destination Mode” on page 434):

- The mail server is assigned a valid IP address (its public IP address), which is exposed to the Internet. However, internally, the mail server retains its existing (private) IP address.
- Incoming mail arrives at the gateway, where the destination IP address (the mail server’s public IP address) is translated to its private address. The source IP address of outgoing mail is translated from the mail server’s private IP address to its public IP address.

Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” on page 435).

## Configuring Address Translation

There are two methods of configuring Address Translation:

**Automatic Configuration** — Address Translation is configured as a property of a machine, network or Address Range.

This is the recommended method. Under this method, rules for an Address Translation Rule Base are automatically generated, and the object's properties are applied whenever the object is used in the Security Policy. In addition, numerous implementation details are automatically handled correctly (for example, Anti-Spoofing). If you use one of the other methods, you must account for these implementation details manually.

Automatic configuration is the simplest method to use, but it is somewhat inflexible: the generated rules cannot be modified, but you can add rules (with the second method — see below) before and after the automatically generated rules.

For information on this method, see “Generating Address Translation Rules Automatically” on page 440.

**Address Translation Rules** — The System Administrator defines an Address Translation Rule Base, in many ways similar to a Security Policy Rule Base.

This method is available only under the VPN-1/FireWall-1 Windows GUI (Windows and X/Motif only). You can also add Address Translation rules before and after the rules generated automatically by the previous method, but you cannot modify or delete the automatically generated rules.

This method is more difficult to use than the previous method, but is more powerful and more flexible.

For information on this method, see “Configuring Address Translation — Windows GUI” on page 442.

## Translation Modes

VPN-1/FireWall-1 supports two kinds of Address Translation:

**Dynamic (Hide)** — Many invalid addresses are translated to a single valid address, and dynamically assigned port numbers are used to distinguish between the invalid addresses.

Dynamic Address Translation is called Hide Mode, because the invalid addresses are “hidden” behind the valid address. For details of this mode, see “Hide Mode” on page 429.

**Static** — Each invalid address is translated to a corresponding valid address.

There are two modes of Static Address Translation:

- Static Source Mode (see “Static Source Mode” on page 432)
- Static Destination Mode (see “Static Destination Mode” on page 434)

## In This Section

|                                |                 |
|--------------------------------|-----------------|
| <i>Hide Mode</i>               | <i>page 429</i> |
| <i>Static Source Mode</i>      | <i>page 432</i> |
| <i>Static Destination Mode</i> | <i>page 434</i> |

## Hide Mode

Hide Mode is used for connections initiated by hosts in an internal network, where the hosts' IP addresses are invalid. In Hide Mode, the invalid internal addresses are hidden behind a single valid external address, using dynamically assigned port numbers to distinguish between them.



**Note** – The IP address of a gateway's external interface must *never* be hidden.

## Assigning Port Numbers

Port numbers are dynamically assigned from two pools of numbers:

- from 600 to 1023
- from 10,000 to 60,000

If the original port number is less than 1024, then a port number is assigned from the first pool. If the original port number is greater than 1024, then a port number is assigned from the second pool. VPN-1/FireWall-1 keeps track of the port numbers assigned, so that the original port number is correctly restored for return packets. A port number currently in use is not assigned again to a new connection.

## Limitations

Hide Mode has several limitations:

- Hide Mode does not allow access to the “hidden” hosts to be initiated from the outside, that is, an external machine cannot connect to any of the hosts whose addresses have been translated. For example, in the configuration in FIGURE 14-3 on page 430, if you run your HTTP server on 200.0.0.108 (one of the internal machines with an invalid address), external machines will not be able to connect to your HTTP server using 199.203.145.35 (the gateway's valid address) as the destination.

This limitation can also be considered an advantage of Hide Mode.

- Hide Mode cannot be used for protocols where the port number cannot be changed.
- Hide Mode cannot be used when the external server must distinguish between clients on the basis of their IP addresses, since all clients share the same IP address under Hide Mode.

Example

Suppose localnet is an internal network with invalid addresses are as follows:

| Valid IP address | Invalid IP addresses      |
|------------------|---------------------------|
| 199.203.145.35   | 200.0.0.100 - 200.0.0.200 |

199.203.145.35 is the address of gateway’s external interface.

You can hide the invalid addresses behind the valid address by specifying Address Translation in the **NAT** tab of localnet’s **Network Properties** window as follows:

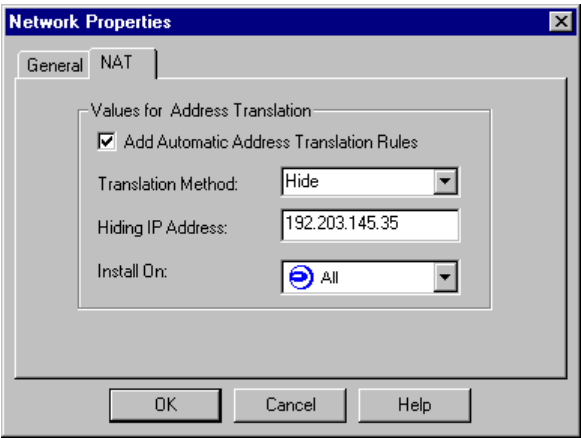


FIGURE 14-2 NAT tab for localnet

Source addresses of outbound packets from hosts in localnet will be translated to 199.203.145.35, as illustrated in FIGURE 14-3. The source port number serves to direct reply packets to the correct host.

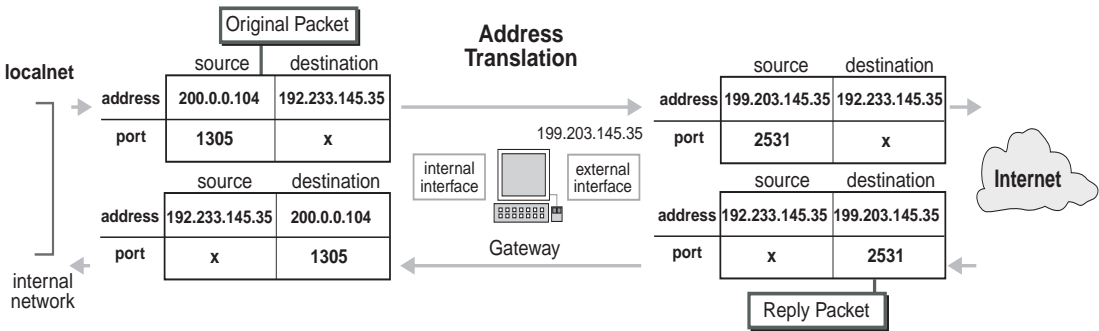
















FIGURE 14-3 Hide Mode Address Translation

The following two Address Translation rules (FIGURE 14-4) are automatically generated from the above definition (FIGURE 14-2 on page 430):

| No. | Original Packet                                                                            |                                                                                            |                                                                                       | Translated Packet                                                                                           |                                                                                            |                                                                                              | Install On                                                                              |
|-----|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
|     | Source                                                                                     | Destination                                                                                | Service                                                                               | Source                                                                                                      | Destination                                                                                | Service                                                                                      |                                                                                         |
| 1   |  localnet |  localnet |  Any |  Original                  |  Original |  Original |  All |
| 2   |  localnet |  Any      |  Any |  localnet (Hiding Address) |  Original |  Original |  All |

**FIGURE 14-4** Hide Mode Automatically Generated Rules

The first rule (which does not translate anything) applies to connections from the gateway to localnet and prevents the address of the gateway's internal interface from being translated<sup>1</sup>.

The second rule expresses the Address Translation defined in the **NAT** tab (FIGURE 14-2 on page 430) and illustrated in FIGURE 14-3. Note the small letter **H** under **localnet**'s icon, which indicates Hide Mode translation.

For a detailed description of the meaning of the fields in an Address Translation Rule Base, see "Structure of an Address Translation Rule" on page 442.



**Note** – Routing tables on the gateway and router may have to be modified to implement this scheme (see "Address Translation and Routing" on page 435).

## Choosing the Valid External Address for Hide Mode

You can choose to hide the internal IP addresses either behind the IP address of the gateway's external interface, or behind an imaginary IP address.

If you hide the internal IP addresses behind the IP address of the gateway's external interface ...

You will not have to make any changes to your routing tables (see "Address Translation and Routing" on page 435), because presumably the routing tables are already correctly configured for the gateway's external interface.

On the other hand, you may have problems when a hidden connection shadows a connection originating on the gateway itself. For example, suppose a user on the gateway TELNETs to an external server, and is allocated the local TCP port 10001 by the gateway's TCP module. Next, a user on one of the internal hosts also TELNETs to the external server and, because the connection is hidden, it is allocated the same TCP port 10001 by the VPN/FireWall Module on the gateway. In this event, packets returning from the external TELNET server to the first TELNET client will be (incorrectly) diverted to the internal host, where they will be ignored.

1. For an explanation of why this rule is necessary, see "Can I translate the gateway's internal address?" on page 476.

If you hide the internal IP addresses behind an imaginary IP address ...

You will probably have to change the routing tables (see “Address Translation and Routing” on page 435) so that replies to the imaginary IP address are directed to the gateway, but you will not have problems with shadowed connections as described above.

## Statically Translating Addresses

### Static Source Mode

Static Source Mode translates invalid internal IP addresses to valid IP addresses, and is used when the connection is initiated by internal clients with invalid IP addresses. Static Source Mode ensures that the originating hosts have unique, specific valid IP addresses, and is usually used together with Static Destination Mode.

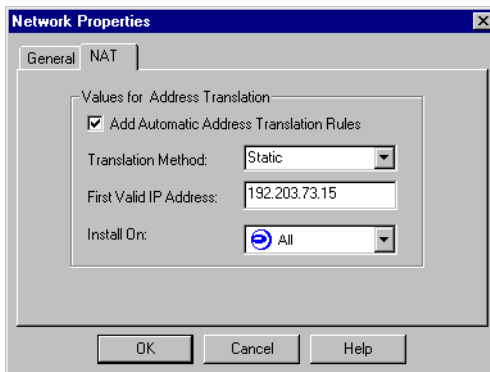
When you generate Address Translation rules automatically, Static Source Mode and Static Destination Mode rules are always generated in pairs.

### Example

Suppose localnet is an internal network with invalid addresses, but a corresponding set of valid addresses is available, as follows:

| Valid IP addresses             | Invalid IP addresses      |
|--------------------------------|---------------------------|
| 199.203.73.15 – 199.203.73.115 | 200.0.0.100 – 200.0.0.200 |

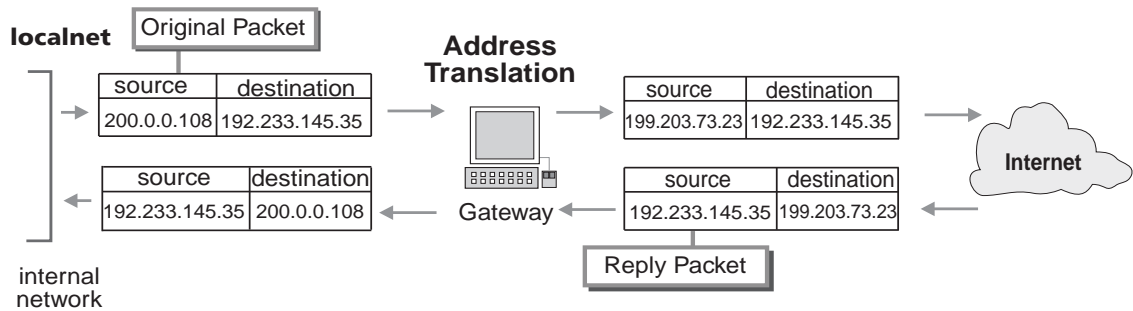
You can translate the invalid addresses to the valid addresses by specifying Address Translation in the **NAT** tab of localnet’s **Workstation Properties** window as follows:



**FIGURE 14-5** Static Address Translation



The invalid addresses of hosts in localnet will be translated to the valid addresses starting at 199.203.73.15.



**FIGURE 14-6** Address Translation using Static Source Mode

The following three Address Translation rules (FIGURE 14-7) are automatically generated from the above definition (FIGURE 14-5 on page 432):

| No. | Original Packet |                            |         | Translated Packet          |             |          | Install On |
|-----|-----------------|----------------------------|---------|----------------------------|-------------|----------|------------|
|     | Source          | Destination                | Service | Source                     | Destination | Service  |            |
| 1   | localnet        | localnet                   | Any     | Original                   | Original    | Original | All        |
| 2   | localnet        | Any                        | Any     | localnet (Valid Addresses) | Original    | Original | All        |
| 3   | Any             | localnet (Valid Addresses) | Any     | Original                   | localnet    | Original | All        |

**FIGURE 14-7** Automatically Generated Address Translation rules for Static Translation

The first rule (which does not translate anything) applies to connections from the gateway to localnet and prevents the address of the gateway’s internal interface from being translated<sup>1</sup>.

Note that two static translation rules are generated:

- The first static translation rule (rule number 2) is a Static Source Mode rule, and expresses the Address Translation illustrated in FIGURE 14-6.
- The second static translation rule (rule number 3) is the corresponding Static Destination rule and expresses the Address Translation illustrated in FIGURE 14-8 on page 434 (see “Static Destination Mode” on page 434).

1. For an explanation of why this rule is necessary, see “Can I translate the gateway’s internal address?” on page 476.

For a detailed description of the meaning of the fields in an Address Translation Rule Base, see “Structure of an Address Translation Rule Base” on page 442.



**Note** – Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” on page 435).

Static Destination Mode

Static Destination Mode translates valid addresses to invalid addresses for connections initiated by external clients. Static Destination Mode is used when servers inside the internal network have invalid IP addresses, and ensures that packets entering the internal network arrive at their proper destinations. Static Destination Mode is usually used together with Static Source Mode.

When you generate Address Translation rules automatically, Static Source Mode and Static Destination Mode rules are always generated in pairs.

Example

Suppose localnet is an internal network with invalid addresses, but a corresponding set of valid addresses is available, as follows:

| Valid IP addresses             | Invalid IP addresses      |
|--------------------------------|---------------------------|
| 199.203.73.15 – 199.203.73.115 | 200.0.0.100 – 200.0.0.200 |

The second static translation rule (rule number 3) in FIGURE 14-7 on page 433 (generated from the **NAT** tab in FIGURE 14-5 on page 432) translates the valid addresses starting at 199.203.73.15 to the corresponding invalid addresses starting at 200.0.0.100. This is illustrated in FIGURE 14-8.

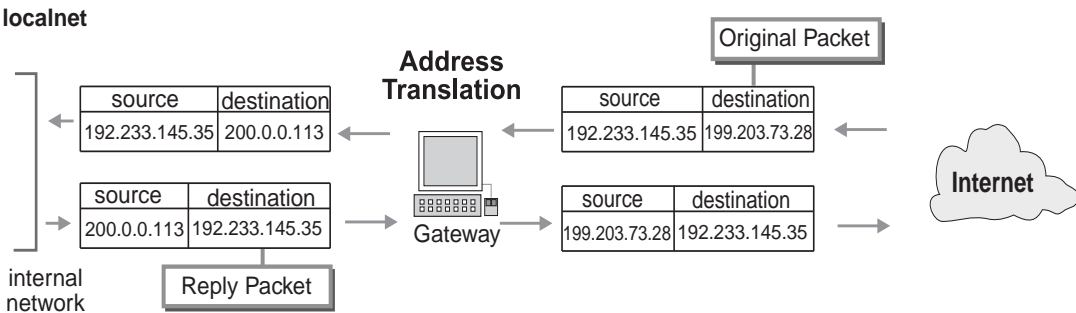


FIGURE 14-8 Address Translation using Static Destination Mode



**Note** – Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” below).

# Address Translation and Routing

## Configuring Routing on the Gateway

To correctly implement Address Translation, you must ensure that a return packet intended for a host whose address has been translated is routed back to that host. There are two routing issues involved:

- ensuring that the packet reaches the gateway
- ensuring that the gateway forwards the packet to the correct interface and host



**Note** – You will usually have to reconfigure your routing tables on the gateway (and on any intervening routers) to implement Address Translation.

## Ensuring That the Packet Reaches the Gateway

### From the Inside

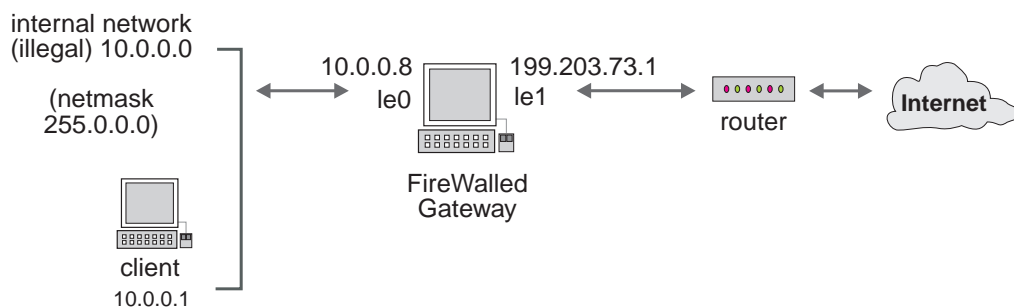
The internal hosts (whose addresses are being translated) need a default route to the gateway, just as they do without Address Translation.

### From the Outside

The translated (valid) addresses must be published, so that replies will be routed back to the gateway.

However, a router positioned between the gateway and the Internet may fail to route reply packets to the translating gateway. Instead, the router sends ARP requests, looking for the physical (MAC) address of the imaginary translated address.

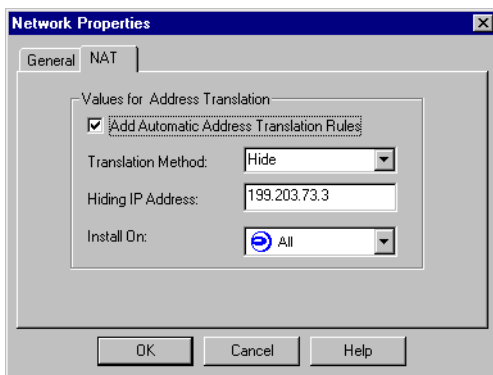
For example, consider the network configuration below (FIGURE 14-9), where the internal network's invalid addresses are hidden behind the non-existent IP address 199.203.73.3 (see FIGURE 14-10 on page 436).



**FIGURE 14-9** Hiding a Network

When the client (10.0.0.1) initiates a connection to the outside world, the gateway translates the packet's source address to 199.203.73.3, so when a reply packet arrives from the server, its destination address is 199.203.73.3. If no static route

exists, the router sees that the packet is destined for a directly attached network (199.203.73.x) and sends an ARP request querying for the physical address (MAC) of 199.203.73.3. But since 199.203.73.3 is an imaginary address, the router receives no response for its query and drops the packet.

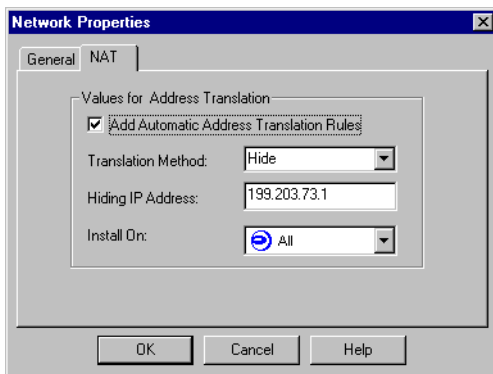


**FIGURE 14-10** Hiding a Network Behind a Non-Existent IP Address

There are three ways to solve this problem:

**1** Reconfigure the Address Translation.

Hide the invalid network behind the gateway's external address, as follows:



**FIGURE 14-11** Hiding a Network Behind a Real IP Address

**2** Another way of solving the problem is to change the routing on the router.

Define a static route on the router, using the equivalent of the Unix command:

```
route add 199.203.73.3 199.203.73.1 1
```

The route command can be added to the VPN-1/FireWall-1 startup script (fwstart) so that it is automatically executed each time VPN-1/FireWall-1 is started.

- 3** A third way of solving the problem is to change the routing on the gateway (proxy ARP method).

**Unix** — On the gateway, link the gateway’s external interface to its MAC address using the `arp` command, as follows:

```
arp -s <IP Address> <MAC Address> pub
```

where `<IP Address>` is the gateway’s external interface and `<MAC Address>` is that interface’s MAC address. For example,

```
arp -s 199.203.73.3 00:a0:c9:45:b5:78 pub
```

**NT** — Create a text file named `local.arp` in the `$FWDIR\state` directory. Each line in the file should be of the form:

```
<IP Address> <MAC Address>
```

where `<IP Address>` is the gateway’s external interface and `<MAC Address>` (in the format “xx-xx-xx-xx-xx”) is that interface’s MAC address. For example,

```
199.203.73.3 00-a0-c9-45-b5-78
```

## Ensuring That the Gateway Forwards the Packet to the Correct Host

When translating the destination address of a connection (Static Destination Mode), packets may be forwarded to the wrong gateway interface if there are no static routes on the gateway to the translated (new) destination IP address.

In this case, Address Translation takes place in the gateway only after internal routing but before transmission (see “Address Translation and Anti-Spoofing” on page 470), so the gateway’s routing sees an external destination address. To ensure that these packets are correctly routed to an internal host (and not bounced back out to the Internet), use static routing (the OS `route` command) to define the same “next hop” for both addresses.

For example, consider the following configuration:

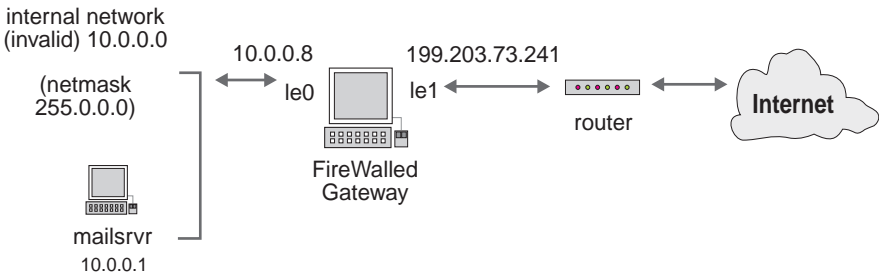


FIGURE 14-12 Static Address Translation

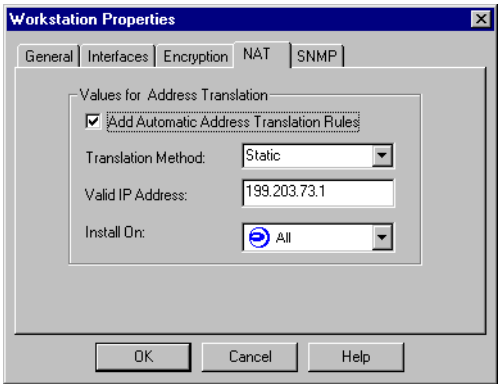


FIGURE 14-13 Static Address Translation for mailsrvr

This results in the rules below (FIGURE 14-16):

| No. | Original Packet |                          |         | Translated Packet        |             |          | Install On |
|-----|-----------------|--------------------------|---------|--------------------------|-------------|----------|------------|
|     | Source          | Destination              | Service | Source                   | Destination | Service  |            |
| 1   | mailsrvr        | Any                      | Any     | mailsrvr (Valid Address) | Original    | Original | All        |
| 2   | Any             | mailsrvr (Valid Address) | Any     | Original                 | mailsrvr    | Original | All        |

FIGURE 14-14 Static Address Translation rules

The second rule will work correctly only if the gateway knows that in order to reach the address 199.203.73.1, it should forward the packet to 10.0.0.1. To make this happen, add a static route on the gateway, using the command:

```
route add 199.203.73.1 10.0.0.1 1
```

The router also has to know that the packets to the translated address must be routed through the gateway. This can be achieved either by defining a static route on the router, or by having the gateway publish (to the router) the fact it has a route to the translated address. For additional information about this problem, see “Ensuring That the Packet Reaches the Gateway” on page 435.

## IANA Recommendations

RFC 1918 documents private address spaces for organizations that will not have hosts on the Internet.

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks:

**TABLE 14-1** Private Networks Address Space

| <b>class</b> | <b>from IP address ...</b> | <b>to IP address</b> |
|--------------|----------------------------|----------------------|
| A            | 10.0.0.0                   | 10.255.255.255       |
| B            | 172.16.0.0                 | 172.31.255.255       |
| C            | 192.168.0.0                | 192.168.255.255      |

An enterprise that decides to use IP addresses in the address spaces defined above can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise.

## Supported Services

### New Services

Network Address Translation now supports H.323, NetShow and VXTreme.

### Restrictions

TABLE 14-2 lists restrictions that apply to Address Translation when used with protocols that carry IP addresses or port numbers in the packet’s data portion, as opposed to the IP or TCP or UDP header.

TABLE 14-2 lists these restrictions.

**TABLE 14-2** Address Translation — Service Restrictions

| Service | Restrictions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Xing    | does not work with Address Translation                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| rshell  | does not work with Address Translation                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| sqlnet2 | If the listener and server are on two different hosts whose IP addresses are being translated, then the difference between their untranslated IP addresses must be the same as the difference between their translated IP addresses. For example, if their original IP addresses are 200.200.200.1 and 200.200.200.11 (a difference of 10), then their translated IP addresses can be 199.199.199.20 and 199.199.199.30 (also a difference of 10), but not 199.199.199.20 and 199.199.199.40 (a difference of 20). |

**FTP port command**

The FTP port command has been rewritten to support Address Translation, as specified in RFC 1631.

Generating Address Translation Rules Automatically

Overview

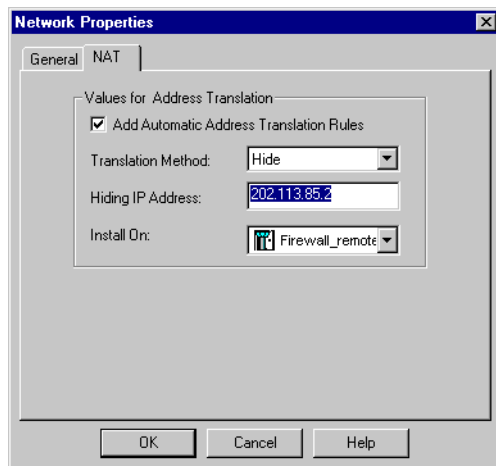
You can generate Address Translation rules for machines, networks and Address Ranges automatically, using the **NAT** tab of the network object’s **Properties** window (FIGURE 14-15 on page 441).

To generate Address Translation rules for a network object, proceed as follows:

- 1 Define the object whose address(es) will be translated using the Network Object Manager.  
  
For information on the Network Object Manager, see Chapter 4, “Network Objects” of *VPN-1/FireWall-1 Administration Guide*.
- 2 In the **NAT** tab of the object’s **Properties** window, check **Add Automatic Address Translation Rules**.

When this box is checked, the other fields in the window are enabled.





**FIGURE 14-15** Automatic Address Translation for a Network

- 3** Select a **Translation Method** from the drop-down menu.

For information about translation methods, see “Translation Modes” on page 428.

- 4** Enter an IP address for the translation.

If the **Translation Method** is **Hide**, then the IP address is the one behind which the object’s addresses will be hidden (see “Hide Mode” on page 429).

If the **Translation Method** is **Static**, then the IP address is the first one in the range to which the object’s addresses will be translated (see “Statically Translating Addresses” on page 432).

- 5** In **Install On**, select a FireWalled object on which to install the generated Address Translation rule.

**All** means all the FireWalled objects that are able to perform Address Translation.

- 6** Click on **OK** or on **Apply**.

To view the Address Translation Rule Base (including the automatically generated rules), select the **Address Translation** tab in the Rule Base Editor (Windows and X/Motif only) or examine the .pf file.

The automatically generated rules are colored differently from manually defined rules, and are positioned first in the Address Translation Rule Base. Automatically generated rules cannot be modified using the Rule Base Editor, nor can you change their sequence. The automatically generated rules themselves can only be modified by editing the fields in the **NAT** tabs.

However, you can add rules before and after the automatically generated rules (see “Configuring Address Translation — Windows GUI” on page 442). If you add rules before the automatically generated rules and then add more automatically generated rules, the new automatically generated rules will be positioned together with the other automatically generated rules.



**Note** – If a host for which Address Translation has been defined has more than one IP addresses (for example, if it is a gateway with multiple interfaces), the only IP address that will be translated is the IP address specified in the **General** tab of the **Workstation Properties** window.

## Configuring Address Translation — Windows GUI

### Overview

In the Windows GUI, Address Translation can be configured in the form of an Address Translation Rule Base. The Rule Base expression of an Address Translation rule enables you to:

- specify objects by name rather than by IP address
- restrict rules to specified destination IP addresses, as well as to the specified source IP Addresses
- translate both source and destination IP addresses in the same packet
- restrict rules to specified services (ports)
- translate ports

### Structure of an Address Translation Rule

An Address Translation rule, like a Security Policy rule, consists of two elements:

- conditions that specify when the rule is to be applied
- the action to be taken when the rule is applied (that is, when the conditions are satisfied)

In the Windows GUI (FIGURE 14-16), the Address Translation Editor is divided into four sections:

- **Original Packet**
- **Translated Packet**
- **Install On**
- **Comment**

| No. | Original Packet |                          |         | Translated Packet        |             |          | Install On | Comment                                       |
|-----|-----------------|--------------------------|---------|--------------------------|-------------|----------|------------|-----------------------------------------------|
|     | Source          | Destination              | Service | Source                   | Destination | Service  |            |                                               |
| 1   | mailsrvr        | Any                      | Any     | mailsrvr (Valid Address) | Original    | Original | All        | Automatic rule (see the network object data). |
| 2   | Any             | mailsrvr (Valid Address) | Any     | Original                 | mailsrvr    | Original | All        | Automatic rule (see the network object data). |

**FIGURE 14-16** Address Translation Rules in the Windows GUI

**Original Packet** and **Translated Packet** consist of, in turn:

- **Source**
- **Destination**
- **Service**

**Original Packet** specifies the conditions, that is, when the rule is applied.

**Translated Packet** specifies the action to be taken when the rule is applied.

The action is always the same:

- translate **Source** under **Original Packet** to **Source** under **Translated Packet**
- translate **Destination** under **Original Packet** to **Destination** under **Translated Packet**
- translate **Service** under **Original Packet** to **Service** under **Translated Packet**

If an entry under **Translated Packet** is **Original**, then the corresponding entry under **Original Packet** is not translated. TABLE 14-3 presents the various possibilities, using **Service** as an example.

**TABLE 14-3** Condition vs. Translation

| Original Packet Service is ... | Translated Packet Service is ...                                                                             |                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
|                                | Original                                                                                                     | <new service>                                                                                                            |
| Any                            | no conditions on <b>Service</b> , and <b>Service</b> is not translated                                       | invalid combination — Security Policy will not verify                                                                    |
| <old service>                  | the rule applies only to packets whose <b>Service</b> is <old service>, and <b>Service</b> is not translated | the rule applies only to packets whose <b>Service</b> is <old service>, and <old service> is translated to <new service> |

## Address Translation Rule Base Example

FIGURE 14-17 shows an example of an Address Translation Rule Base.

| No. | Original Packet  |                |               | Translated Packet |                  |                  | Install On | Comment         |
|-----|------------------|----------------|---------------|-------------------|------------------|------------------|------------|-----------------|
|     | Source           | Destination    | Service       | Source            | Destination      | Service          |            |                 |
| 1   | MyNetwork        | Any            | Any           | natasha           | Original         | Original         | All        | FWXT_HIDE       |
| 2   | IllegalAddresses | Any            | Any           | LegalAddresses    | Original         | Original         | All        | FWXT_SRC_STATIC |
| 3   | Any              | LegalAddresses | Any           | Original          | IllegalAddresses | Original         | All        | FWXT_DST_STATIC |
| 4   | Any              | DMZ-Servers    | StandardPorts | Original          | Original         | NonStandardPorts | All        | FWXT_DPORT      |

**FIGURE 14-17** Manually Added Address Translation Rules

#### Rule 1

The first rule in FIGURE 14-17 (a Hide Mode rule — note the small letter **H** under **natasha**'s icon) specifies that:

**Condition** — when the original packet's **Source** address belongs to the network object **MyNetwork**

**Action** — hide its **Source** address behind the address of the network object **natasha**

#### Rule 2

The second rule in FIGURE 14-17 (a Static Source Mode rule) specifies that:

**Condition** — when the original packet's **Source** address is in the address range **IllegalAddresses**

**Action** — translate its **Source** address to the corresponding address in the address range **LegalAddresses**

#### Rule 3

The third rule in FIGURE 14-17 (a Static Destination Mode rule) specifies that:

**Condition** — when the original packet's **Destination** address is in the address range **LegalAddresses**

**Action** — translate its **Destination** address to the corresponding address in the address range **IllegalAddresses**

#### Rule 4

The fourth rule in FIGURE 14-17 specifies that:

**Condition** — when the original packet's **Service** is in the service range **StandardPorts** and its **Destination** is **DMZ-Servers**

**Action** — translate its **Service** to the corresponding **Service** in the service range **NonStandardPorts**



**Note** – The first three rules in this example can be automatically generated by the method described in “Generating Address Translation Rules Automatically” on page 440. The last rule cannot be automatically generated.

## Compound Conditions

Conditions under **Original Packet** are ANDed together. For example, the fourth rule in FIGURE 14-17 has a compound condition, that is, there are two conditions to be met, both of which must be true in order for the rule to apply.

The two conditions are:








- 1 The original packet's service number is in the service range **StandardPorts**.
- 2 The original packet's **Destination** is **DMZ-Servers**.

It is not possible to express a compound condition in the command line representation.

## Multiple Translation

If the addresses in two internal networks are invalid, there may be problems in communications between the two networks (see “Gateway with Three Interfaces” on page 460 for further information), which arise because both the source and destination addresses of packets must be translated.

The Windows GUI allows the specification of multiple translations in a single rule. For example, FIGURE 14-18 shows a rule in which both the source and destination addresses of packets are translated.

| No. | Original Packet                                                                                   |                                                                                            |                                                                                       | Translated Packet                                                                         |                                                                                              |                                                                                            | Install On                                                                              | Comment |
|-----|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|---------|
|     | Source                                                                                            | Destination                                                                                | Service                                                                               | Source                                                                                    | Destination                                                                                  | Service                                                                                    |                                                                                         |         |
| 1   |  InvalidLocalNet |  ValidDMZ |  Any |  natasha |  InvalidDMZ |  Original |  All |         |

**FIGURE 14-18** Multiple Translation rule

For a detailed example of when a rule like this is necessary, see “Gateway with Three Interfaces” on page 460.

## Defining Address Translation Rules

To define an Address Translation rule using the Windows GUI, you must first define the objects that will be used in the rule.

Under **Source** and **Destination**, you can use any Machine or Network network object, including groups and **Address Range** objects.

Under **Service**, you can use any TCP or UDP **Services** object, including groups and **Port Range** objects.

## Address Range

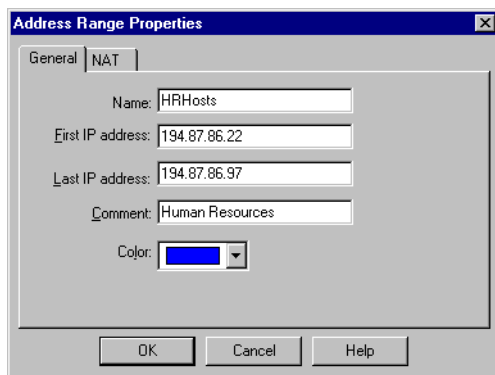
### Defining a Range of Addresses

To define a range of addresses, open the **Address Range Properties** window (FIGURE 14-20 on page 446) by selecting **Address Range** from the **Add Network Object** menu.



**FIGURE 14-19** Add Network Object menu

For information on how to display the **Add Network Object** menu, see “Defining Network Objects” on page 97.



**FIGURE 14-20** Address Range Properties window

**Name** — the object’s name

**First IP Address** — the first IP Address in the range

**Last IP Address** — the last IP Address in the range

**Comment** — descriptive text

This text is displayed on the bottom of the **Network Object** window when this item is selected.

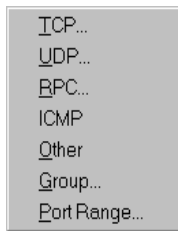
**Color** — the color of the object's icon

Select the desired color from the drop-down list.

## Port Range

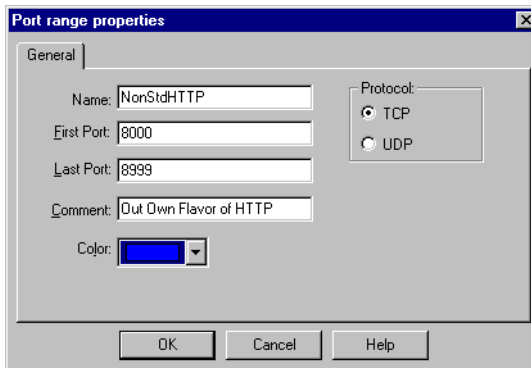
### Defining a Range of Ports

To define a range of services, open the **Port Range Properties** window (FIGURE 14-22 on page 447) by selecting **Port Range** from the **Add Service Object** menu.



**FIGURE 14-21** Add Service Object menu

For information on how to display the **Add Service Object** menu, see “Defining Network Objects” on page 97.



**FIGURE 14-22** Port Range Properties window

**Name** — the object's name

**First Port** — the first service in the range

**Last Port** — the last service in the range

**Comment** — descriptive text

This text is displayed on the bottom of the **Network Object** window when this item is selected.




































**Color** — the color of the object’s icon

Select the desired color from the drop-down list.

**Protocol** — select **TCP** or **UPD**

## Using the Address Translation Rules Editor

To display the Address Translation Rules Editor (FIGURE 14-23), select the **Address Translation** tab in the Rule Base Editor.

| No. | Original Packet                                                                                    |                                                                                                  |                                                                                                 | Translated Packet                                                                                |                                                                                                    |                                                                                                    | Install On                                                                             | Comment         |
|-----|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------|
|     | Source                                                                                             | Destination                                                                                      | Service                                                                                         | Source                                                                                           | Destination                                                                                        | Service                                                                                            |                                                                                        |                 |
| 1   |  MyNetwork        |  Any            |  Any           |  natasha        |  Original         |  Original         |  All | FWXT_HIDE       |
| 2   |  IllegalAddresses |  Any            |  Any           |  LegalAddresses |  Original         |  Original         |  All | FWXT_SRC_STATIC |
| 3   |  Any              |  LegalAddresses |  Any           |  Original       |  IllegalAddresses |  Original         |  All | FWXT_DST_STATIC |
| 4   |  Any              |  DMZ-Servers    |  StandardPorts |  Original       |  Original         |  NonStandardPorts |  All | FWXT_DPORT      |
| 5   |  InvalidLocalNet  |  ValidDMZ       |  Any           |  natasha        |  InvalidDMZ       |  Original         |  All |                 |

**FIGURE 14-23** Address Translation Rules Editor

To return to the Rule Base Editor, select the **Rule Base** tab.

An Address Translation Rule Base is part of a Security Policy. If you have more than one Security Policy, then each of them can have a corresponding Address Translation Rule Base. The Address Translation Rule Base is installed when the Security Policy is installed.







## Editing an Address Translation Rule Base

### Adding a Rule

You can add a rule at any point in the Address Translation Rule Base, except between automatically generated rules.

**TABLE 14-4** Adding a Rule

| To add a rule           | Select from menu             | Toolbar Button                                                                     |
|-------------------------|------------------------------|------------------------------------------------------------------------------------|
| after the last rule     | <b>Rule&gt;Add&gt;Bottom</b> |  |
| before the first rule   | <b>Rule&gt;Add&gt;Top</b>    |  |
| after the current rule  | <b>Rule&gt;Add&gt;Before</b> |  |
| before the current rule | <b>Rule&gt;Add&gt;After</b>  |  |

A new rule will be added to the Address Translation Rule Base, and default values will appear in all the data fields. You can modify the default values as needed.



**Note** – To select a rule or rules, select their numbers.

### Modifying a Rule's Data Fields

To modify a data field in a rule, right click on the value. A menu will be displayed, from which you can choose the new value.

### Original Packet — Source

**Source** can consist of only one object. The types of objects allowed for **Source** under **Original Packet** depend on what is specified for **Source** under **Translated Packet**, as listed in TABLE 14-5.

**TABLE 14-5** Original Packet - Source

|                                            | If Translated Packet - Source is ...                       |                                                            |                                                 |
|--------------------------------------------|------------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------|
|                                            | Original                                                   | Hide                                                       | Static                                          |
| <b>Original Packet - Source can be ...</b> | Machine, Network, Address Range or a group of one of these | Machine, Network, Address Range or a group of one of these | Machine, Network, Address Range but not a group |

**Add** — The **Object Manager** window (FIGURE 14-24) is displayed, from which you can select a network object.



**FIGURE 14-24** Object Manager window

**Replace** — The **Object Manager** window (FIGURE 14-24) is displayed, from which you can select an object to replace the object currently in the rule's **Source**.

**Edit** — Edit the object in the rule's **Source**.

The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Source**.

**Cut** — Delete the object currently in the rule's **Source** and put it on the clipboard.

**Copy** — Copy the object currently in the rule's **Source** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Source**.

## Original Packet — Destination

**Destination** can consist of only one object. The types of objects allowed for **Destination** under **Original Packet** depend on what is specified for **Destination** under **Translated Packet**, as listed in TABLE 14-6.

**TABLE 14-6** Original Packet - Destination

|                                                 | If Translated Packet - Destination is ...                  |                                                            |                                                 |
|-------------------------------------------------|------------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------|
|                                                 | Original                                                   | Hide                                                       | Static                                          |
| <b>Original Packet - Destination can be ...</b> | Machine, Network, Address Range or a group of one of these | Machine, Network, Address Range or a group of one of these | Machine, Network, Address Range but not a group |

**Add** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select a network object.

**Replace** — The **Object Manager** window ( on page 450) is displayed, from which you can select an object to replace the object currently in the rule's **Destination**.

**Edit** — Edit the object in the rule's **Destination**.

The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Destination**.

**Cut** — Delete the object currently in the rule's **Destination** and put it on the clipboard.

**Copy** — Copy the object currently in the rule's **Destination** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Destination**.

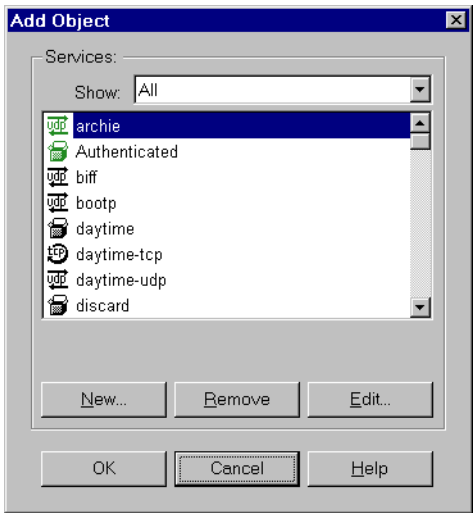
## Original Packet — Service

**Services** can consist of only one object. The types of objects allowed for **Services** under **Original Packet** depend on what is specified for **Services** under **Translated Packet**, as listed in TABLE 14-7.

**TABLE 14-7** Original Packet - Services

|                                              | If Translated Packet - Services is ...       |                                              |                                 |
|----------------------------------------------|----------------------------------------------|----------------------------------------------|---------------------------------|
|                                              | Original                                     | Hide                                         | Static                          |
| <b>Original Packet - Services can be ...</b> | TCP, UDP, Range or group of one of the above | TCP, UDP, Range or group of one of the above | TCP, UDP, Range but not a group |

**Add** — The **Services** window (FIGURE 14-25) is displayed, from which you can select a service.



**FIGURE 14-25** Services window

**Replace** — The **Services** window (FIGURE 14-25) is displayed, from which you can select an object to replace the object currently in the rule’s **Services**.

**Edit** — Edit the service.

The appropriate window is opened (depending on the type of the selected service), and you can change the service’s properties.

**Delete** — Delete the object currently in the rule’s **Services**.

**Cut** — Delete the object currently in the rule’s **Services** and put it on the clipboard.

**Copy** — Copy the object currently in the rule’s **Services** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule’s **Services**.

**Translated Packet — Source**

**Source** can consist of only one object. The types of objects allowed for **Source** depend on the type of Address Translation, as listed in .

**TABLE 14-8** Translated Packet - Source

|                                              | If the Address Translation is                                              |                                              |
|----------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------|
|                                              | Hide                                                                       | Static                                       |
| <b>Translated Packet - Source can be ...</b> | Machine, Network, or Range of same size as <b>Original Packet - Source</b> | Machine, Network, Router, or Range of size 1 |

**Add (Static)** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select a network object.

The **Source** object under **Original Packet** will be translated to **Source** under **Translated Packet**, in Source Static Mode.

**Replace (Static)** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select an object to replace the object currently in the rule's **Source**.

**Replace (Static)** is only available when the **Source** object was added by **Add (Static)**. If you wish to replace an **Add (Hide)** object by an **Add (Static)** object, first delete the **Add (Hide)** object, and then choose **Add (Static)** from the menu.

**Add (Hide)** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select a network object.

The **Source** object under **Original Packet** will be translated to **Source** under **Translated Packet**, in Hide mode.

**Replace (Hide)** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select an object to replace the object currently in the rule's **Source**.

**Replace (Hide)** is only available when the **Source** object was added by **Add (Hide)**. If you wish to replace an **Add (Static)** object by an **Add (Hide)** object, first delete the **Add (Static)** object, and then choose **Add (Hide)** from the menu.

**Edit** — Edit the **Source** object.

The appropriate window is opened (depending on the type of the **Source** object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Source**.

After you delete the object, **Source** is set to **Original**.

**Cut** — Delete the object currently in the rule's **Source** and put it on the clipboard.

After you cut the object, **Source** is set to **Original**.

**Copy** — Copy the object currently in the rule's **Source** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Source**.

Translated Packet — Destination

**Destination** can consist of only one object. The types of objects allowed for **Destination** depend on the type of Address Translation, as listed in TABLE 14-9.

TABLE 14-9 Translated Packet - Destination

|                                            | If the Address Translation is                                                   |                                              |
|--------------------------------------------|---------------------------------------------------------------------------------|----------------------------------------------|
|                                            | Hide                                                                            | Static                                       |
| Translated Packet - Destination can be ... | Machine, Network, or Range of same size as <b>Original Packet - Destination</b> | Machine, Network, Router, or Range of size 1 |

**Add (Static)** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select a network object.

The **Destination** object under **Original Packet** will be translated to **Destination** under **Translated Packet**, in Destination Static Mode.

**Replace (Static)** — The **Object Manager** window (FIGURE 14-24 on page 450) is displayed, from which you can select an object to replace the object currently in the rule's **Destination**.

**Replace (Static)** is only available when the **Destination** object was added by **Add (Static)**.

**Edit** — Edit the **Destination** object.

The appropriate window is opened (depending on the type of the **Destination** object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Destination**.

After you delete the object, **Destination** is set to **Original**.

**Cut** — Delete the object currently in the rule's **Destination** and put it on the clipboard.

After you cut the object, **Destination** is set to **Original**.

**Copy** — Copy the object currently in the rule's **Destination** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Destination**.

Translated Packet — Service

**Service** can consist of only one object. The types of objects allowed for **Service** are:

- TCP
- UDP
- Port Range

**Add (Static)** — The **Service** window (FIGURE 14-25 on page 452) is displayed, from which you can select a network object.

The **Service** object under **Original Packet** will be translated to **Service** under **Translated Packet**.

**Replace (Static)** — The **Service** window (FIGURE 14-25 on page 452) is displayed, from which you can select an object to replace the object currently in the rule's **Service**.

**Replace (Static)** is only available when the **Service** object was added by **Add (Static)**.

**Edit** — Edit the **Service** object.

The appropriate window is opened (depending on the type of the **Service** object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Service**.

After you delete the object, **Service** is set to **Original**.

**Cut** — Delete the object currently in the rule's **Service** and put it on the clipboard.

After you cut the object, **Service** is set to **Original**.

**Copy** — Copy the object currently in the rule's **Service** to the clipboard.




**Paste** — Paste the object on the clipboard in the rule's **Service**.

## Install On

The **Install On** field specifies which FireWalled objects will enforce the rule. You cannot change the **Install On** field for automatically generated rules, but you can change it for manual rules.

To modify the **Install On** field, right click on it. A menu is displayed, from which you can select one of the values listed in TABLE 14-10.

**TABLE 14-10** Install On Menu

| Install On                                                                          | Meaning                                                                                       |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|  | <b>Gateways</b> — Enforce on all network objects defined as gateways.                         |
|  | <b>Integrated FireWalls</b> — Enforce on all network objects defined as integrated FireWalls. |
|  | <b>Targets</b> — Enforce on the specified target object(s) only.                              |

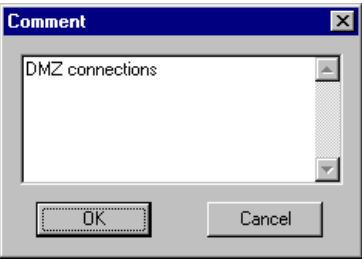
If you choose **Targets**, then the **Select Target** window is displayed, from which you can choose a FireWalled gateway or host (but not a router), on which to install the Address Translation rule.



**FIGURE 14-26** Select Target window

**Comment**

You can add comments to a rule. Double click on the **Comment** field to open the **Comment** window (FIGURE 14-27).






**FIGURE 14-27** Comment window

Type any text you wish in the text box and click on **OK**.

**Copying, Cutting and Pasting Rules**

To copy, cut or paste, select a rule or rules by selecting their numbers.

**TABLE 14-11** Copying, Cutting and Pasting Rules

| Action | Select from menu | Toolbar Button                                                                       |
|--------|------------------|--------------------------------------------------------------------------------------|
| Cut    | Edit>Cut         |  |
| Copy   | Edit>Copy        |  |
| Paste  | Edit>Paste       |  |



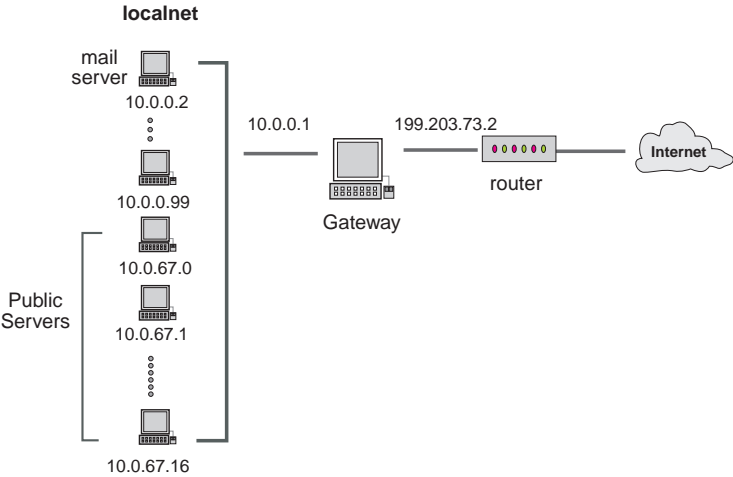
If you choose **Paste**, then the **Paste** menu will be opened. You must then select **Before**, **After**, **Top**, or **Bottom** to specify where in the Rule Base to paste the rule.

## Address Translation Examples

|                                      |                 |
|--------------------------------------|-----------------|
| <i>Gateway with Two Interfaces</i>   | <i>page 457</i> |
| <i>Gateway with Three Interfaces</i> | <i>page 460</i> |

### Gateway with Two Interfaces

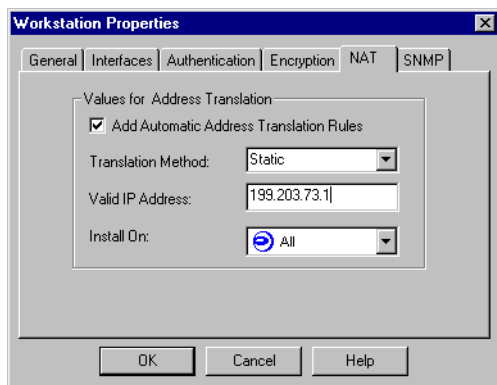
Consider the following network and Address Translation configuration:



**FIGURE 14-28** Gateway with Two Interfaces Example - Network

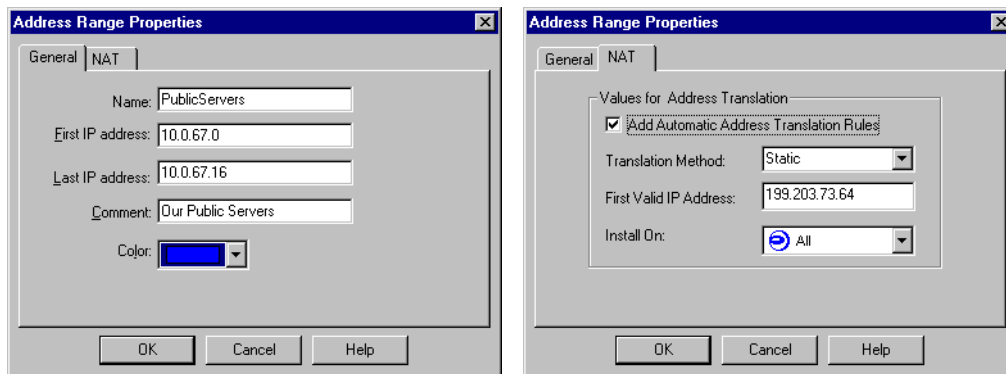
## Defining Address Translation

Since the mailserver accepts and initiates connections, it requires static translation, as shown in FIGURE 14-29.



**FIGURE 14-29** mailserver - static translation

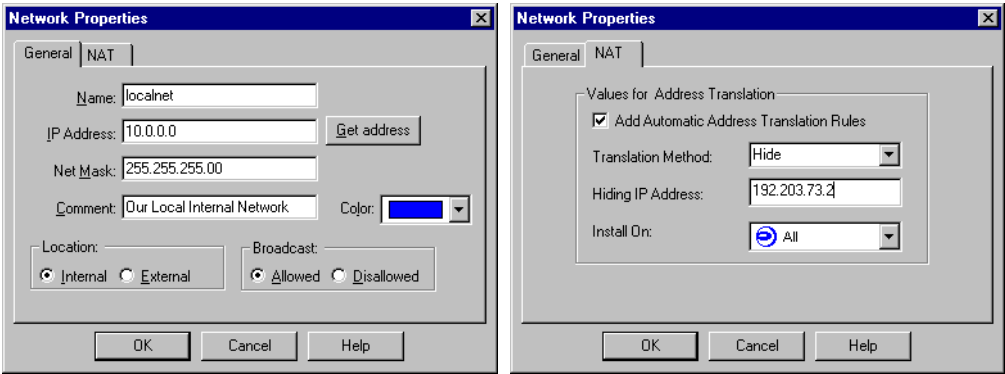
Similarly, the Address Range from 10.0.67.0 to 10.0.67.16 is meant to provide public services, such as HTTP or FTP, to the outside world, and so it too requires Static Translation.



**FIGURE 14-30** PublicServers Address Range

These addresses are mirrored as the seventeen (17) addresses from 199.203.73.64 to 199.203.73.80. So, for example, when an outside machine sends a packet to IP address 199.203.73.70, the packet will actually arrive at 10.0.67.6.

Finally, localnet addresses will be hidden behind the IP address of the gateway's external interface, 199.203.73.2 (FIGURE 14-31).



**FIGURE 14-31** localnet Network Properties and NAT tabs

The rules generated from these definitions are shown in FIGURE 14-32.

| No. | Original Packet |                                 |         | Translated Packet               |               |          |
|-----|-----------------|---------------------------------|---------|---------------------------------|---------------|----------|
|     | Source          | Destination                     | Service | Source                          | Destination   | Service  |
| 1   | mailserver      | Any                             | Any     | mailserver (Valid Address)      | Original      | Original |
| 2   | Any             | mailserver (Valid Address)      | Any     | Original                        | mailserver    | Original |
| 3   | PublicServers   | PublicServers                   | Any     | Original                        | Original      | Original |
| 4   | PublicServers   | Any                             | Any     | PublicServers (Valid Addresses) | Original      | Original |
| 5   | Any             | PublicServers (Valid Addresses) | Any     | Original                        | PublicServers | Original |
| 6   | localnet        | localnet                        | Any     | Original                        | Original      | Original |
| 7   | localnet        | Any                             | Any     | localnet (Hiding Address)       | Original      | Original |

**FIGURE 14-32** Address Translation Rule Base

### Routing

Assume that the Internet routes IP addresses in the network 199.203.73.0 to the router.

Then you should ensure that:

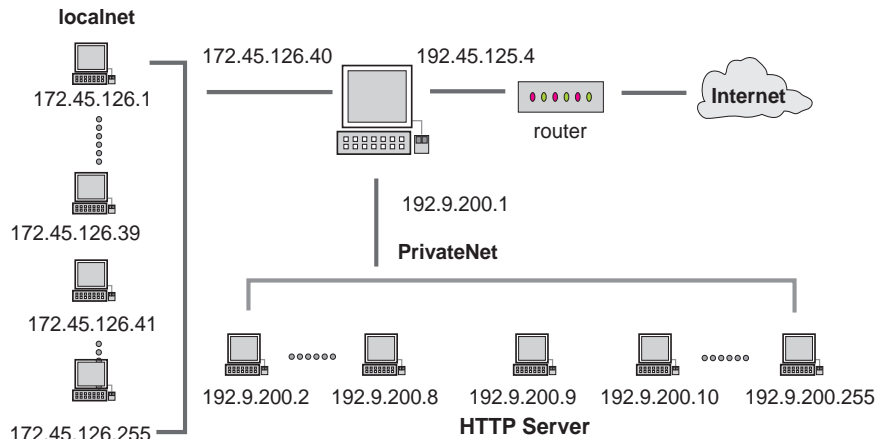
- 1 The router routes IP addresses in the network 199.203.73.0 to the gateway.
- 2 The gateway routes IP address 199.203.73.3 to the internal interface (10.0.0.1).

- 3** The gateway routes IP addresses 199.203.73.64 to 199.203.73.80 to the internal interface (10.0.0.1).

## Gateway with Three Interfaces

### Hide Mode and Static Mode

Consider the following network and Address Translation configuration:



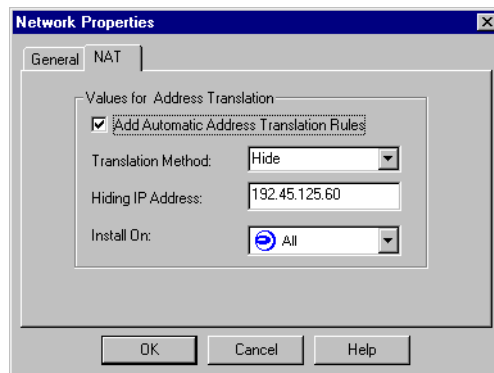
**FIGURE 14-33** Gateway with Three Interfaces Example - Network

Suppose we wish to hide all the localnet and DMZ hosts behind the gateway, except for host 192.9.200.9 (HTTPServer), which will be providing public services and so must be accessible from the Internet.

### Defining Address Translation

Hiding localnet

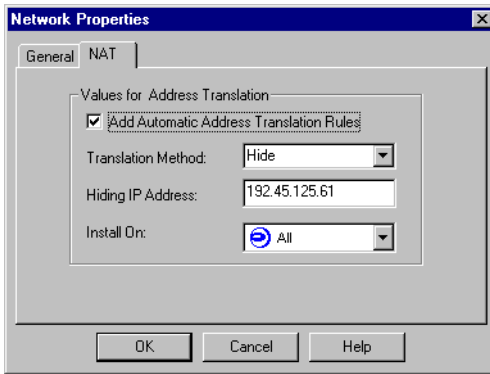
To hide localnet addresses, define Address Translation as follows for localnet:



**FIGURE 14-34** Hiding localnet

### Hiding PrivateNet

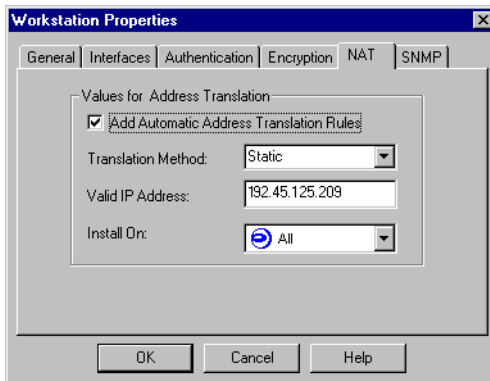
To hide PrivateNet addresses, define Address Translation as follows for PrivateNet:



**FIGURE 14-35** Hiding PrivateNet

### HTTPServer

To statically translate HTTPServer's address, define its Address Translation as follows:



**FIGURE 14-36** Translating HTTPServer

Rules

The rules generated from these definitions are shown in FIGURE 14-37.

| No. | Original Packet |                            |         | Translated Packet           |             |          | Install On |
|-----|-----------------|----------------------------|---------|-----------------------------|-------------|----------|------------|
|     | Source          | Destination                | Service | Source                      | Destination | Service  |            |
| 1   | HTTPServer      | Any                        | Any     | HTTPServer (Valid Address)  | Original    | Original | All        |
| 2   | Any             | HTTPServer (Valid Address) | Any     | Original                    | HTTPServer  | Original | All        |
| 3   | PrivateNet      | PrivateNet                 | Any     | Original                    | Original    | Original | All        |
| 4   | PrivateNet      | Any                        | Any     | PrivateNet (Hiding Address) | Original    | Original | All        |
| 5   | localnet        | localnet                   | Any     | Original                    | Original    | Original | All        |
| 6   | localnet        | Any                        | Any     | localnet (Hiding Address)   | Original    | Original | All        |

FIGURE 14-37 Automatically Generated Rules - Three Interfaces

Note that the Static Mode rules are positioned before the Hide Mode rules.

Communications Between Hosts in Different Internal Networks

The Address Translation Rule Base works much like the Security Policy Rule Base. The Address Translation rules are scanned sequentially, one after the other, until a match is found. The Address Translation indicated by the matching rule is performed, and then the packet is sent on its way.

Suppose host 172.45.126.47 (in localnet) tries to TELNET to host 192.45.125.209 (the valid address of HTTPServer ,whose invalid address is 192.9.200.9) in PrivateNet. The first rule that matches is rule 2, so the destination address 172.45.125.209 is translated to 192.9.200.9, and the packet arrives at its destination. The packet’s source address (172.45.126.47) remains untranslated, so the reply will be sent to 172.45.126.47 and arrive at its destination.

Routing

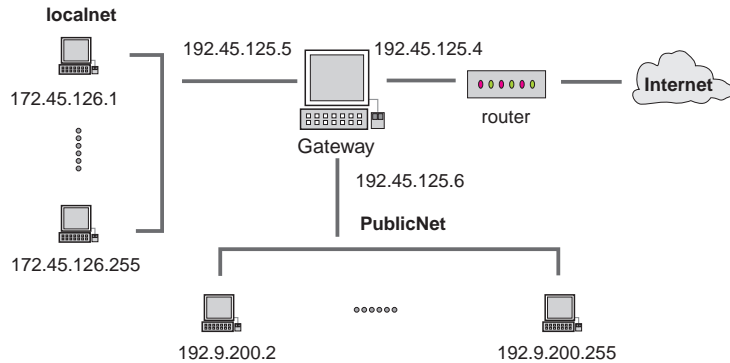
Assume that the Internet routes the IP addresses in the network 192.45.125.0 to the router.

You should ensure that:

- 1 The router routes the IP addresses in the network 192.45.125.0 to the gateway.
- 2 The gateway routes IP address 172.45.125.209 to the internal interface (192.9.200.1).

## Both Networks Statically Translated

Consider the following network and Address Translation configuration:



**FIGURE 14-38** Three Interfaces - Both Networks Statically Translated

Suppose we wish to statically translate the addresses in both networks (localnet and PublicNet). The automatically generated Address Translation Rule Base is shown in FIGURE 14-39.

| No. | Original Packet |                             |         | Translated Packet           |             |          | Install On |
|-----|-----------------|-----------------------------|---------|-----------------------------|-------------|----------|------------|
|     | Source          | Destination                 | Service | Source                      | Destination | Service  |            |
| 1   | PublicNet       | PublicNet                   | Any     | Original                    | Original    | Original | All        |
| 2   | PublicNet       | Any                         | Any     | PublicNet (Valid Addresses) | Original    | Original | All        |
| 3   | Any             | PublicNet (Valid Addresses) | Any     | Original                    | PublicNet   | Original | All        |
| 4   | localnet        | localnet                    | Any     | Original                    | Original    | Original | All        |
| 5   | localnet        | Any                         | Any     | localnet (Valid Addresses)  | Original    | Original | All        |
| 6   | Any             | localnet (Valid Addresses)  | Any     | Original                    | localnet    | Original | All        |

**FIGURE 14-39** Rule Base - Both Networks Statically Translated

## Communications Between Hosts Behind the Same Gateway

Suppose a host in localnet tries to TELNET to a host in PublicNet, using the PublicNet host's valid IP address as the destination IP address. The first rule that applies is rule 3, so the destination address is translated and the packet is correctly routed to the destination. The reply packets are correctly routed as well, since the source IP address is not translated.

On the other hand, suppose a host in PublicNet tries to TELNET to a host in localnet, using the localnet host's valid IP address as the destination IP address. The first rule that matches is rule 2, so the source address is translated, but the destination address is not translated, so the packet will *not* arrive at its destination.

Multiple Translation Rules

One solution is to add two rules before the automatically generated rules as follows:

Rules Added Manually

Automatically Generated Rules

| No. | Original Packet  |                             |         | Translated Packet           |                  |          |
|-----|------------------|-----------------------------|---------|-----------------------------|------------------|----------|
|     | Source           | Destination                 | Service | Source                      | Destination      | Service  |
| 1   | PublicNetInvalid | localNetValid               | Any     | PublicNetValid              | localNetInvalid  | Original |
| 2   | localNetInvalid  | PublicNetValid              | Any     | localNetValid               | PublicNetInvalid | Original |
| 3   | PublicNet        | PublicNet                   | Any     | Original                    | Original         | Original |
| 4   | PublicNet        | Any                         | Any     | PublicNet (Valid Addresses) | Original         | Original |
| 5   | Any              | PublicNet (Valid Addresses) | Any     | Original                    | PublicNet        | Original |
| 6   | localnet         | localnet                    | Any     | Original                    | Original         | Original |
| 7   | localnet         | Any                         | Any     | localnet (Valid Addresses)  | Original         | Original |
| 8   | Any              | localnet (Valid Addresses)  | Any     | Original                    | localnet         | Original |

FIGURE 14-40 Multiple Translation Rules Added to Automatically Generated Rules

Now, both source and destination IP addresses will be translated, so packets will be routed to their correct destinations.

Simple Rules

Another solution is to add the same two rules, but to set **Source** under **Translated Packet** to **Original**. This solution will work because there is really no need to translate the source IP address when both networks are connected to the same gateway, which knows how to route to the internal invalid IP addresses of both networks.

Communications Between Hosts Behind Different Gateways

Consider the case when the internal networks are connected to different gateways controlled from the same Management Station. In this case, both source and destination IP addresses must be translated, because each gateway knows how to route only to its own internal invalid IP addresses. Therefore, only the first of the above solutions (multiple translation rules) will work.

Managing PIX Address Translation

PIX Address Translation can be manually configured through the VPN-1/FireWall-1 Address Translation Rule Base editor (Windows GUI). This method of configuration simplifies the management of PIX Address Translation.



**Note** – PIX does not support automatically generated Address Translation rules. Properties defined in the **NAT** tab of a network object are not applied. Address Translation rules installed on a PIX blackbox must be manually configured. See “Defining Address Translation Rules” on page 445 for more information.



## Overview

PIX performs address translation for the networks on its inside interface only. These networks must be specified as the “**Inside Addresses**” in the **Setup A** tab of the **Blackbox Properties** window. Addresses of hosts on the PIX outside interface are not translated.

PIX maps addresses of the inside hosts to a range of valid IP addresses, known as the PIX “Global Pool.” PIX supports both the dynamic and static Address Translation modes, but manages these modes differently from VPN-1/FireWall-1.

### Dynamic

In PIX dynamic Address Translation, a range of internal, or “inside” addresses is mapped to the Global Pool. Valid addresses are dynamically assigned to internal hosts per connection. Valid addresses are assigned according to availability and are returned to the global pool when a connection closes or times out.

For example, the 15 hosts of an internal network share a global pool of 10 valid addresses. If 10 hosts have connections open, then each of the remaining 5 hosts must wait until a connection times out in order to receive a valid address and open a connection.

For more information on PIX dynamic Address Translation and global pools, consult the Cisco PIX documentation.

### Static

An invalid address from the inside private network is permanently mapped to a single valid address from the Global Pool. Static Address Translation is used for internal service hosts, such as an SMTP server. Static Mode ensures that a specific inside host can have unique, valid IP addresses.

## Using PIX in the Address Translation Rule Base

A subset of the VPN-1/FireWall-1 Address Translation Rule Base editor features are available for PIX. TABLE 14-12 compares the features supported by PIX and VPN-1/FireWall-1.

**TABLE 14-12** Comparison of PIX and VPN-1/FireWall-1 in the Address Translation Rule Base

|                                                         | PIX                                                                                                                                                                   | VPN-1/FireWall-1                                                                                                                                              |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dynamic Address Translation (Hide Mode)</b>          | A range of invalid addresses is dynamically mapped to a range of valid addresses (Global Pool).                                                                       | Many invalid addresses are translated to a single valid address. The invalid addresses are “hidden” behind a single address.<br>(see “Hide Mode” on page 429) |
| <b>Static Address Translation</b>                       | static source mode only                                                                                                                                               | both static source and static destination mode                                                                                                                |
| <b>compound conditions</b>                              | not available                                                                                                                                                         | available                                                                                                                                                     |
| <b>restrict rules to specific destination addresses</b> | not available                                                                                                                                                         | available                                                                                                                                                     |
| <b>multiple translation</b>                             | not available                                                                                                                                                         | available                                                                                                                                                     |
| <b>translate ports</b>                                  | not available                                                                                                                                                         | available                                                                                                                                                     |
| <b>restrict rules to specific services</b>              | not available<br>Rules restricting connections to translated hosts are specified in the Security Policy Rule Base. See “PIX Address Translation Example” on page 467. | available                                                                                                                                                     |

### Source

Dynamic and static Address Translation is performed only for the objects listed under **Source** in both **Original Packet** and **Translated Packet**.

**Source** can consist of only one object. The types of objects allowed for **Source** under **Original Packet** depend on what is specified for **Source** under **Translated Packet**, as listed in TABLE 14-13.

**TABLE 14-13** Original Packet - Source

|                                            | If Translated Packet - Source is ... |               |             |
|--------------------------------------------|--------------------------------------|---------------|-------------|
|                                            | Original                             | Hide          | Static      |
| <b>Original Packet - Source can be ...</b> | Workstation or Address Range         | Address Range | Workstation |

## Destination

The PIX blackbox does not allow you to specify rules to translate a packet's destination address in the Address Translation Rule Base. Connections from outside to inside hosts are enabled through the Security Policy Rule Base (see "PIX Address Translation Example" on page 467). When defining an Address Translation Rule Base, set **Destination** under **Original Packet** to **Any**. **Destination** under **Translated Packet** must be set to **Original**.

## Service

Rules which translate ports or restrict connections to specific services cannot be specified in the Address Translation Rule Base. Connections to inside hosts are restricted to specific services only through rules in the Security Policy Rule Base (see "PIX Address Translation Example" on page 467). When defining Address Translation rules, set **Service** under **Original Packet** to **Any**. **Service** under **Translated Packet** must be set to **Original**.

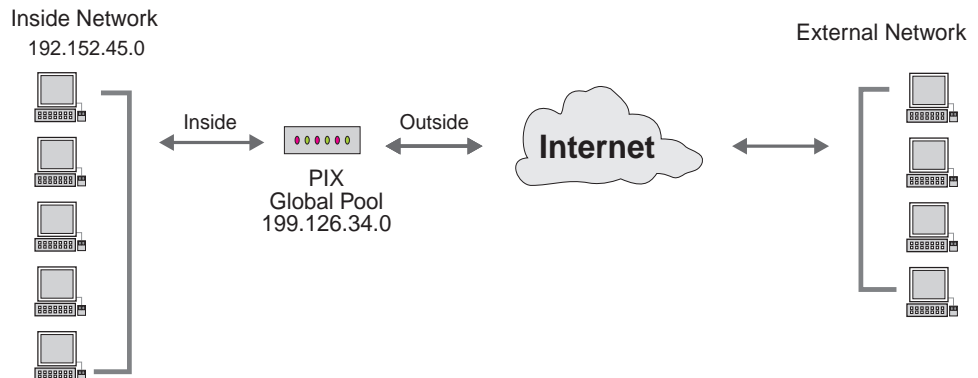
## Install On

Address Translation rules must be installed on the specific PIX blackbox that will enforce the rule. You must choose **Targets** from the **Install On** menu. The **Select Target** window (FIGURE 14-26 on page 456) is displayed, from which you can choose the PIX blackbox on which to install the Address Translation rule.

## PIX Address Translation Example

The following example describes how to define an Address Translation Rule Base for a single PIX blackbox with one network on the inside interface.

Consider the following configuration:



**FIGURE 14-41** Example Configuration

To implement Address Translation for this configuration, you must first define two Address Range objects: one for the inside network and one for the PIX Global Range of addresses.

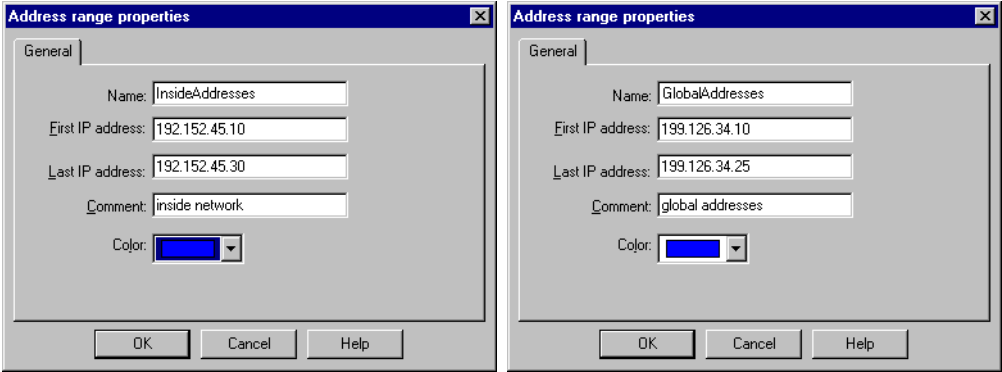


FIGURE 14-42 Address Range Properties — Inside Addresses and Global Addresses



**Note** – The Inside Network must already be specified as the PIX blackbox’s **Inside Addresses** in the **Setup A** tab of the **Blackbox Properties** window.

Next, define a Hide Mode rule that dynamically maps the inside network (**Inside Addresses**) to the range of **GlobalAddresses**. This rule must be located first in the Address Translation Rule Base, before any other rules.

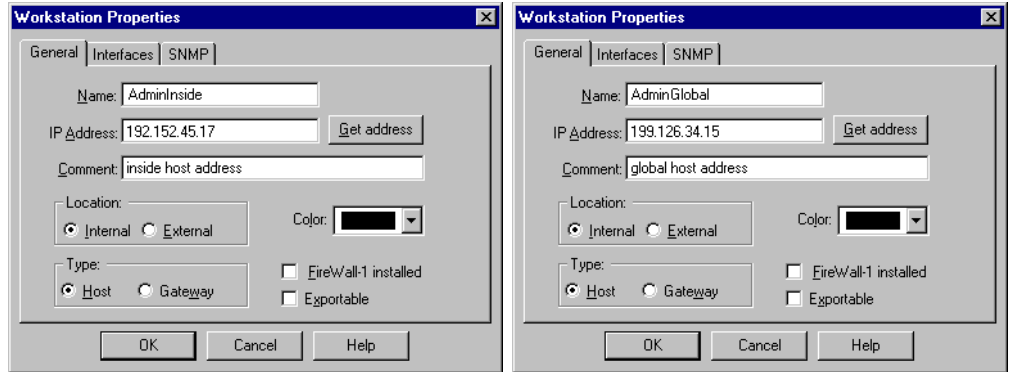
| No. | Original Packet |             |         | Translated Packet |             |          | Install On |
|-----|-----------------|-------------|---------|-------------------|-------------|----------|------------|
|     | Source          | Destination | Service | Source            | Destination | Service  |            |
| 1   | InsideAddresses | Any         | Any     | GlobalAddresses   | Original    | Original | PIX1       |

FIGURE 14-43 Hide Mode rule

Note that in the Address Translation Rule Base, Hide Mode rules are used to dynamically map the inside network to the PIX Global Pool.

The first rule only enables inside hosts to initiate connections to external hosts. In order to allow connections from the outside to a specific inside host, you must statically assign a Global Address to that host. This assures that this host has a unique, valid address and can always be reached from the outside.

To statically map a host, you must create two workstation objects: one specifying the host's internal address, and one with the host's Global Address (see FIGURE 14-44).



**FIGURE 14-44** Workstation Properties — Inside Host and Corresponding Global Address

Next, define an Address Translation rule that statically translates packets from the inside host to its Global Address. The Address Translation rules below provide static Global Addresses for two hosts: **AdminInside** and **InsideWeb**, a web server.

| Security Policy Address Translation |                 |             |         |                   |             |            |            |
|-------------------------------------|-----------------|-------------|---------|-------------------|-------------|------------|------------|
| No.                                 | Original Packet |             |         | Translated Packet |             |            | Install On |
|                                     | Source          | Destination | Service | Source            | Destination | Service    |            |
| 1                                   | InsideAddresses | Any         | Any     | GlobalAddresses   | = Original  | = Original | PIX1       |
| 2                                   | AdminInside     | Any         | Any     | AdminGlobal       | = Original  | = Original | PIX1       |
| 3                                   | InsideWeb       | Any         | Any     | WebGlobal         | = Original  | = Original | PIX1       |

**FIGURE 14-45** Address Translation Rule Base with Static Address Translation rules

You must then define rules in the Security Policy Rule Base that enable connections between the inside network and external hosts.

| Security Policy Address Translation |             |             |         |        |       |            |         |
|-------------------------------------|-------------|-------------|---------|--------|-------|------------|---------|
| No.                                 | Source      | Destination | Service | Action | Track | Install On | Comment |
| 1                                   | ExtNet      | Any         | Any     | accept | Long  | PIX1       |         |
| 2                                   | AdminInside | Any         | Any     | accept |       | PIX1       |         |
| 3                                   | Any         | WebGlobal   | http    | accept |       | PIX1       |         |
| 4                                   | Any         | ExtNet      | Any     | accept |       | PIX1       |         |

**FIGURE 14-46** Security Policy Rule Base

- Rule 1 enables connections from hosts in an external network (**Extnet**) to any inside host with a Global address.

- Rule 2 enables **AdminInside** to connect to any external host.
- Rule 3 enables any external host to access the web server.
- Rule 4 allows all hosts in the inside network to connect to a host on **Extnet**.

## Advanced Topics

### Address Translation and Anti-Spoofing

Anti-Spoofing examines the source IP address for incoming packets (entering a gateway), and the destination IP address for outgoing packets (leaving a gateway).

Anti-Spoofing is described in “Valid Addresses” on page 106.

Address Translation takes place as follows:

- for a packet going from the client (the initiator of the connection) to the server, just before the packet leaves the interface closest to the server
- for a packet going from the server to the client, just after the packet enters the interface closest to the server

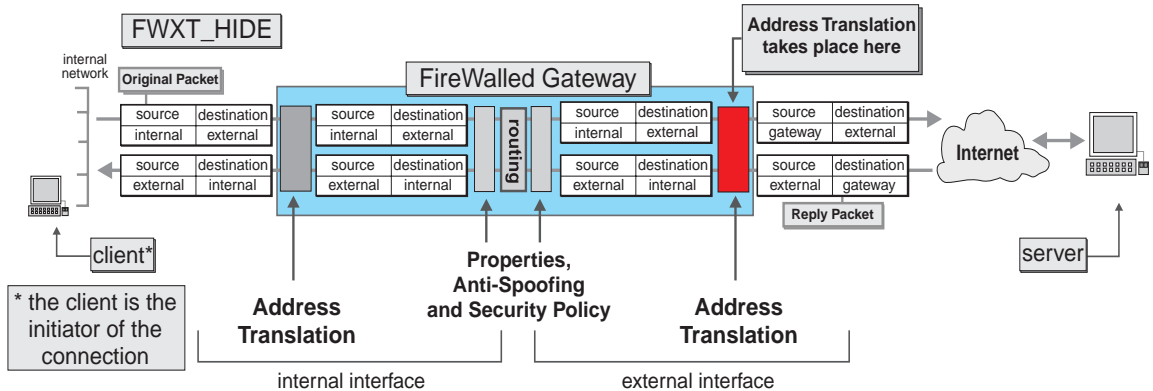
### Automatically Generated Rules

You do not have to do anything to ensure that anti-Spoofing is performed correctly for those objects for which you generate Address Translation rules automatically. There is one exception: for static destination mode translation, you must add the translated addresses to the internal interface’s **Valid Addresses**. See “Static Destination Mode” on page 473 for more information about this case.

This remainder of this section describes anomalies which must be considered when you define Address Translation manually. The examples illustrate the interaction between Address Translation and Anti-Spoofing for each of the Address Translation modes.

## Hide Mode

FIGURE 14-47 on page 471 shows a gateway performing both Address Translation (in Hide Mode) and Anti-Spoofing on a packet and its reply as they pass through the gateway.



**FIGURE 14-47** Address Translation and Anti-Spoofing (Hide Mode)

### Original Packet

On the internal interface, Anti-Spoofing sees an incoming packet with an internal source IP address, which is normal.

On the external interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is normal.

### Reply Packet

On the external interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is normal.

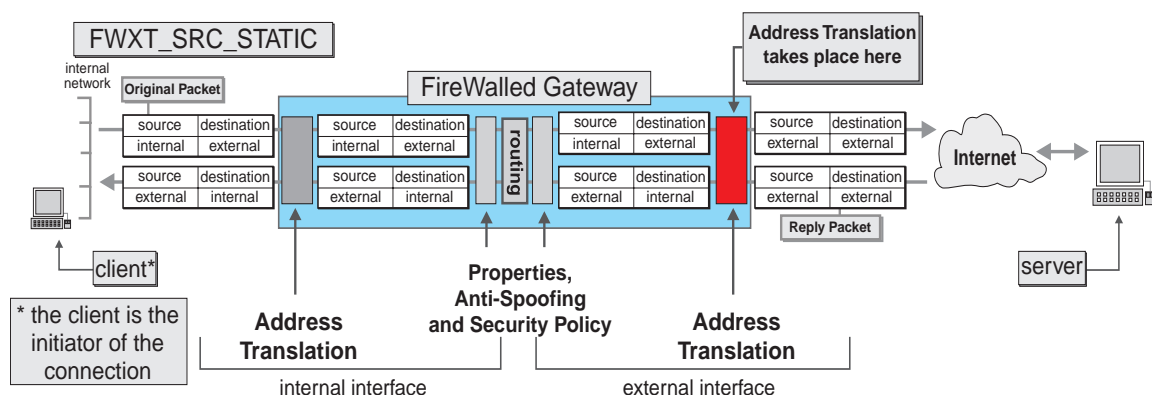
On the internal interface, Anti-Spoofing sees an outgoing packet with an internal destination IP address, which is normal.

### Conclusion

In Hide Mode, there is no conflict between Address Translation and Anti-Spoofing.

## Static Source Mode

FIGURE 14-48 shows a gateway performing both Address Translation (in Static Source Mode) and Anti-Spoofing on a packet and its reply as they pass through the gateway.



**FIGURE 14-48** Address translation and Anti-Spoofing (Static Source Mode)

### Original Packet

On the internal interface, Anti-Spoofing sees an incoming packet with an internal source IP address, which is normal.

On the external interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is normal.

### Reply Packet

On the external interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is normal.

On the internal interface, Anti-Spoofing sees an outgoing packet with an internal destination IP address, which is normal.

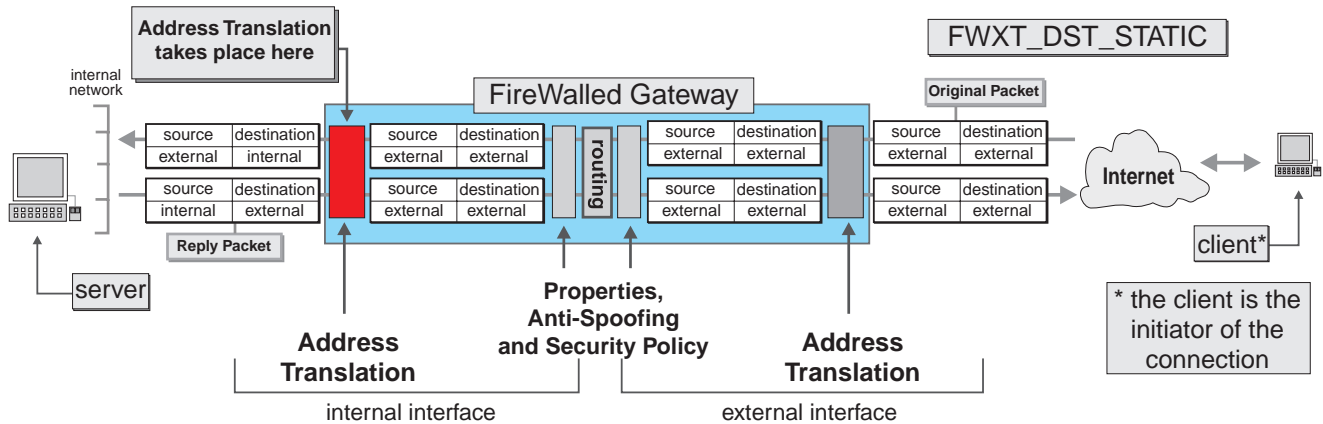
### Conclusion

In Static Source Mode, there is no conflict between Address Translation and Anti-Spoofing.



## Static Destination Mode

FIGURE 14-49 shows a gateway performing both Address Translation (in Static Destination Mode) and Anti-Spoofing on a packet and its reply as they pass through the gateway.



**FIGURE 14-49** Address translation and Anti-Spoofing (Static Destination Mode)

### Original Packet

On the external interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is normal.

On the internal interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is *not* normal.

To correct the problem, add the translated (external) IP addresses to the **Valid Addresses** on the internal interface.

### Reply Packet

On the internal interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is *not* normal.

To correct the problem, add the translated (external) IP addresses to the **Valid Addresses** on the internal interface.

On the external interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is normal.

Example

Consider the following network and Address Translation configuration:

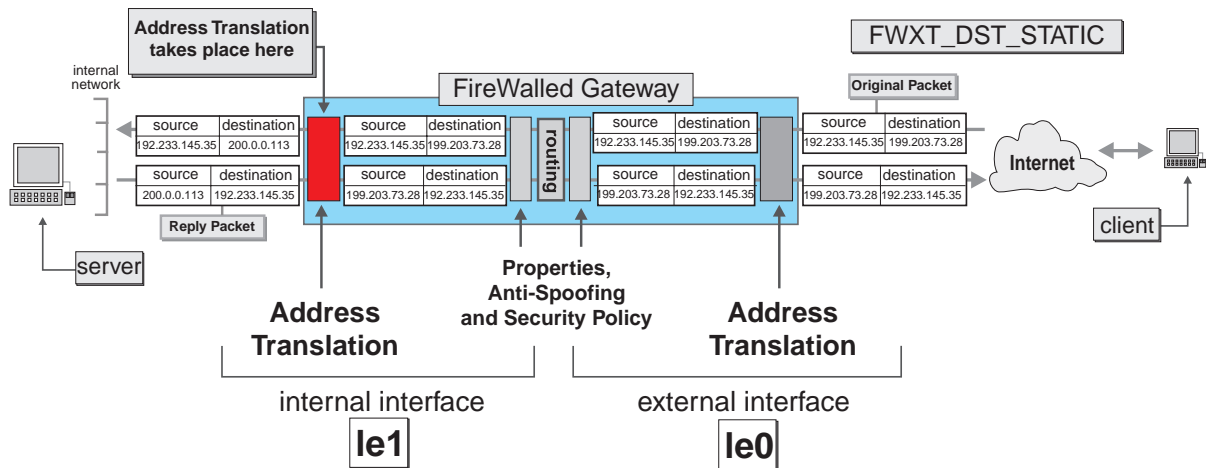


FIGURE 14-50 Address Translation and Anti-Spoofing (Example)

| No. | From Original Address (Port) | To Original Address (Port) | Method          | First Translated Address (Port) |
|-----|------------------------------|----------------------------|-----------------|---------------------------------|
| 0   | 199.203.73.15                | 199.203.73.115             | FWXT_DST_STATIC | 200.0.0.100                     |

On the internal interface (le1), Anti-Spoofing sees outgoing packets with external destination IP addresses (199.203.73.15 – 199.203.73.115) and incoming packets with external source IP addresses (199.203.73.15 – 199.203.73.115). To prevent these packets from being identified as spoofed packets, you must add the translated addresses to the internal interface’s **Valid Addresses**.

Defining Valid Addresses

- 1 Define a network object (for example, “localnet”) for the invalid internal network (200.0.0.0).
- 2 Define a network object (for example, “xlnet”) for the translated addresses (199.203.73.0).
- 3 Define a group (for example, “bothnets”) which consists of localnet and xlnet.
- 4 For le1 (the internal interface), define the **Valid Addresses** as **bothnets**.
- 5 For le0 (the external interface), define the **Valid Addresses** as **Others**.

# Rule Base



**Note** – This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

The Inspection Module sees the packet as the initiator of the connection sees it, and the Rule Base should be defined accordingly.

In the usual situation, this means that if the source (from the initiator’s point of view) is an internal host and the destination an external one, then the source object in the rule should be the internal invalid address.

If, from the initiator’s point of view, the source is an external host and the destination is an internal one, then the destination objects in the rule should be the external addresses of the FWXT\_DST\_STATIC translated hosts(s).

For example, consider the network configuration and Address Translation rules described in FIGURE 14-28 on page 457. A rule in the Rule Base that refers to incoming mail would specify the mail server (under **Destination**) as 199.203.73.3, because the initiator of the communication (the outside host) knows the mail server under that name (IP address).

On the other hand, a rule in the Rule Base that refers to outgoing mail would specify the mail server (under **Source**) as 10.0.0.2, because the initiator of the communication (the internal network) knows the mail server under that name (IP address).

## Frequently Asked Questions

Why do the translated addresses seem not to exist (I can’t even ping them) even though the Address Translation configuration is correct?

You must modify the gateway’s internal routing tables to enable this to happen.

Suppose the Address Translation is configured as follows:

| No. | From Original Address (Port) | To Original Address (Port) | Method          | First Translated Address (Port) |
|-----|------------------------------|----------------------------|-----------------|---------------------------------|
| 0   | 206.73.224.1                 | 206.73.224.1               | FWXT_SRC_STATIC | 192.168.145.11                  |
| 1   | 192.168.145.11               | 192.168.145.11             | FWXT_DST_STATIC | 206.73.224.1                    |
| 2   | 206.73.224.85                | 206.73.224.85              | FWXT_SRC_STATIC | 192.168.145.12                  |
| 3   | 192.168.145.12               | 192.168.145.12             | FWXT_DST_STATIC | 206.73.224.85                   |

If you ping 192.168.145.11 (whether from outside your network or from inside it), then the gateway routes the ping request to its external interface and it is never received by 192.168.145.11. This is because the internal routing takes place before the Address Translation (see “Address Translation and Anti-Spoofing” on page 470).

In order to be able to ping 192.168.145.11 and 192.168.145.12, you must add static routes in the gateway which tell it to forward packets destined for 192.168.145.11 and 192.168.145.12 to the internal interface.

For additional information, see “Configuring Routing on the Gateway” on page 435.

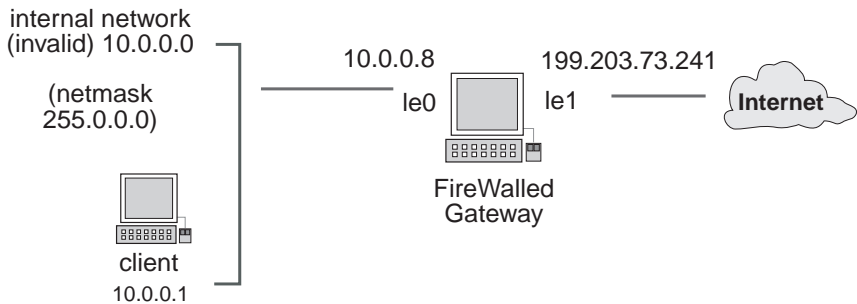
Can I translate the gateway’s internal address?



**Note** – This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

You should not translate the internal address (the address of the internal interface) of the translating gateway.

For example, consider the following network and Address Translation configuration:



**FIGURE 14-51** Hidden Internal Network

| No. | From Original Address (Port) | To Original Address (Port) | Method    | First Translated Address (Port) |
|-----|------------------------------|----------------------------|-----------|---------------------------------|
| 0   | 10.0.0.1                     | 10.255.255.255             | FWXT_HIDE | 199.203.73.200                  |

This example shows a simple translation scheme that hides the entire internal network, whose addresses are invalid, behind a valid address. The problem with this configuration is that the FireWalled gateway’s internal address (10.0.0.8) is also translated to the gateway’s external address, since 10.0.0.8 is in the range 10.0.0.0 – 10.255.255.255. An attempt to communicate from the gateway to an internal machine will not succeed.

For example, if you TELNET from the gateway to 10.0.0.1, the gateway’s internal address (10.0.0.8) will be translated to 199.203.73.200. The reply packet will not reach its destination, because 10.0.0.1 will not be able to route the reply to 199.203.73.200.

To solve this problem, use the following address translation scheme, which translates all the addresses except the gateway's address:

| No. | From Original Address (Port) | To Original Address (Port) | Method    | First Translated Address (Port) |
|-----|------------------------------|----------------------------|-----------|---------------------------------|
| 0   | 10.0.0.1                     | 10.0.0.7                   | FWXT_HIDE | 199.203.73.200                  |
| 1   | 10.0.0.9                     | 10.255.255.255             | FWXT_HIDE | 199.203.73.200                  |

How can I use Encryption and Address Translation together on the same system?



**Note** – You do not have to do anything to ensure that Encryption is performed correctly for those objects for which you generate Address Translation rules automatically. This section describes anomalies which must be considered when you define Address Translation manually.

For example, suppose you want to encrypt between Network-A and Network-B, where Network-A uses invalid addresses translated as follows:

| No. | From Original Address (Port) | To Original Address (Port) | Method          | First Translated Address (Port) |
|-----|------------------------------|----------------------------|-----------------|---------------------------------|
| 0   | 10.1.1.2                     | 10.1.1.2                   | FWXT_SRC_STATIC | 192.91.18.2                     |
| 1   | 192.91.18.2                  | 192.91.18.2                | FWXT_DST_STATIC | 10.1.1.2                        |
| 2   | 10.1.1.3                     | 10.1.1.255                 | FWXT_HIDE       | 192.91.18.3                     |

Network-B uses the valid addresses of network 195.8.5.0.

FireWall-A (Network-A's FireWall) should specify as its Encryption Domain both the invalid addresses (10.1.1.x) and the valid addresses (192.91.18.x).

FireWall-B (Network-B's FireWall) knows FireWall-A only by its valid address.

Encryption Rules

On FireWall-A, two Encryption rules are needed:

| Source    | Destination | Services | Action  | Track     | Install On |
|-----------|-------------|----------|---------|-----------|------------|
| 10.1.1.0  | 195.8.5.0   | Any      | Encrypt | Short Log | Gateways   |
| 195.8.5.0 | 192.91.18.0 | Any      | Encrypt | Short Log | Gateways   |

As with all Address Translation, the Inspection Module see the packets as the originator of the connection sees it, so the first rule applies to outgoing connections and the second rule applies to incoming connections.

Two Encryption rules are needed on FireWall-B as well:

| Source      | Destination | Services | Action  | Track     | Install On |
|-------------|-------------|----------|---------|-----------|------------|
| 192.91.18.0 | 195.8.5.0   | Any      | Encrypt | Short Log | Gateways   |
| 195.8.5.0   | 192.91.18.0 | Any      | Encrypt | Short Log | Gateways   |

Here too the first rule applies to outgoing connections and the second rule applies to incoming connections, but the same addresses are used in both rules, since FireWall-B doesn't know about Network-A's invalid addresses.



**Note** – When using an encryption scheme of type Tunnel Mode, it is usually not necessary to use NAT, because the packet's original IP header is replaced by an IP header in which the source IP address is that of the gateway's external interface and the destination IP address is that of the peer gateway's external interface.

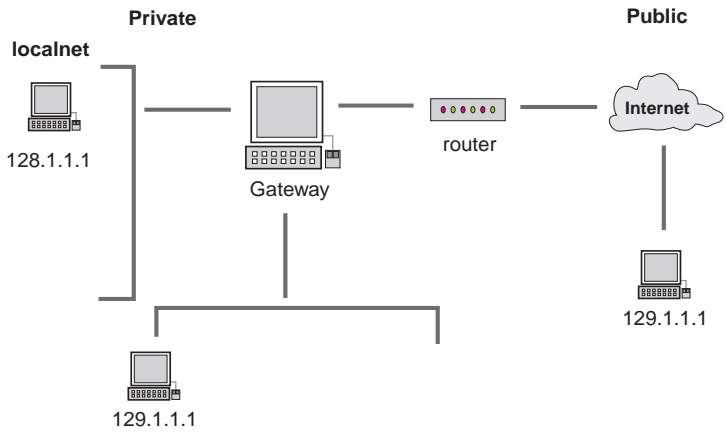
The sequence of actions between Network-A and Network-B is as follows (for a connection from Network-A to Network-B):

- 1** The packet's source IP address is translated by FireWall-A.
- 2** The packet is encrypted and encapsulated by FireWall-A.  
The outer IP header contains the gateways' IP addresses and the inner header contains the translated IP addresses.
- 3** The packet is decrypted by FireWall-B.
- 4** The return packet is encrypted by FireWall-B.
- 5** The return packet is decrypted by FireWall-A.
- 6** The return packet's destination IP address is translated by FireWall-A.

What happens when an internal host with an invalid internal IP address tries to communicate with an external host that has the same IP address?

In this case, the internal network does not conform to the IANA recommendations (see "Frequently Asked Questions" on page 475) but instead uses IP addresses that "belong" to another network.

Consider what happens when the internal host 129.1.1.1 in FIGURE 14-52 tries to talk to the external host 129.1.1.1.



**FIGURE 14-52** Invalid IP Addresses

The outbound packet will remain in the host, since it looks like this:

| Source IP Address | Destination IP address |
|-------------------|------------------------|
| 129.1.1.1         | 129.1.1.1              |

The host will route the packet right back to itself, and the packet will never reach the gateway.

If the internal host 128.1.1.1 tries to talk to the external host 129.1.1.1, the gateway will route the communication to the internal host 129.1.1.1 (connected to the gateway through another interface) rather than to the external host 129.1.1.1.

Using FWXT\_HIDE to hide the invalid IP addresses behind the gateway’s valid address will not help, because with FWXT\_HIDE the Address Translation takes place on the gateway’s external interface. The packet will not get that far because it will have been routed to the other internal interface (see “Address Translation and Anti-Spoofing” on page 470).





# Authentication

## In This Chapter

|                               |                 |
|-------------------------------|-----------------|
| <i>Overview</i>               | <i>page 481</i> |
| <i>User Authentication</i>    | <i>page 484</i> |
| <i>Session Authentication</i> | <i>page 515</i> |
| <i>Client Authentication</i>  | <i>page 526</i> |

## Overview

### VPN-1/FireWall-1 Authentication

VPN-1/FireWall-1’s Authentication feature enables you to control security by allowing some users access while disallowing others. Authentication is specified in a rule’s **Action** field, so you can be very flexible in the way you combine Authentication with the other fields in a rule. For example, you can allow a group of users at a host or group of hosts to use specific services on specific servers at a given time of day, but only after they successfully authenticate themselves.

| Source                                                                                                    | Destination                                                                                    | Service                                                                                 | Action                                                                                        | Track                                                                                    | Install On                                                                                     | Time                                                                                          |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|  Engineering@Local_Net |  FTP_Server |  ftp |  User Auth |  Long |  Gateways |  weekend |

**FIGURE 15-1** Authentication Rule

The rule shown in FIGURE 15-1 specifies that users in the group “Engineering” initiating an FTP connection from the local network to the FTP Server on weekends will be authenticated before the connection is allowed.

## Three Kinds of Authentication

There are three kinds of Authentication:

- User Authentication

User Authentication grants access on a per user basis. This method can only be used for TELNET, FTP, RLOGIN and HTTP, and requires a separate authentication for each connection. It is secure (because the authentication is valid only for one connection), but intrusive (because each connection requires another authentication).

- Session Authentication

Session Authentication is like User Authentication in that it requires an authentication procedure for each connection, but unlike User Authentication, it can be used with any service. It is secure but requires authentication for each connection. It also requires a Session Authentication agent running on the client or another machine in the network.

- Client Authentication

Client Authentication grants access on a per host basis. Client Authentication allows connections from a specific IP address after successful authentication. It can be used for any number of connections, for any service and the authentication is valid for the length of time defined by the administrator. It is less secure than User Authentication (because it allows any user access from the IP address or host) but is also less intrusive. It is best used when the client is a single-user machine, such as a PC.

## Transparent Authentication

Authentication is considered transparent when a user does not have to explicitly connect to the FireWalled gateway to perform the authentication before continuing to the destination. The connection attempt (for example, when the user issues the TELNET command) is intercepted by VPN-1/FireWall-1 on the gateway and the authentication procedure is activated. If the authentication is successful, and the connection is allowed by the rule, the connection proceeds to the destination.

## Comparison of Authentication Types

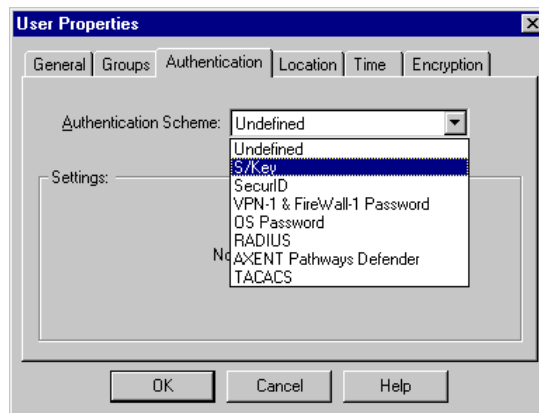
TABLE 15-1 compares the features of the three VPN-1/FireWall-1 Authentication types.

**TABLE 15-1** Comparison of Authentication Types

|                                         | User Authentication                                                 | Session Authentication                                                                                                                                          | Client Authentication                                                    |
|-----------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| which services                          | TELNET, FTP, RLOGIN, HTTP                                           | all services                                                                                                                                                    | all services                                                             |
| authentication is performed once per... | session                                                             | session                                                                                                                                                         | IP address                                                               |
| use when you want a user to...          | authenticate each time he or she uses one of the supported services | authenticate each time he or she uses <i>any</i> service (this requires a Session Authentication Agent running on the client or another machine in the network) | authenticate once, and then be able to use any service until logging off |

## How A User Authenticates

A user authenticates himself or herself by proving his or her identity according to the scheme specified under **Authentication Scheme** in the **Authentication** tab of his or her **User Properties** window (FIGURE 15-2).



**FIGURE 15-2** User Properties window — Authentication tab

## Authentication Schemes

VPN-1/FireWall-1 supports the following Authentication schemes:

- **Undefined** — No authentication is performed and access is always denied.
- **S/Key** — The user is challenged to enter the value of requested S/Key iteration.  
For an explanation of how to define S/Key authentication, see Chapter 5, “Managing Users.”
- **SecurID** — The user is challenged to enter the number displayed on the Security Dynamics SecurID card.
- **OS Password** — The user is challenged to enter his or her OS password.
- **VPN-1 & FireWall-1 Password** — The user is challenged to enter his or her VPN-1 & FireWall-1 password on the gateway.  
The advantage of a VPN-1 & FireWall-1 Password over the OS password is that a VPN-1 & FireWall-1 Password can be used even if the user does not have an OS account on the gateway.
- **RADIUS** — The user is challenged for the response, as defined by the RADIUS server.  
For information about defining RADIUS servers, see Chapter 10, “Server Objects”.
- **AXENT Pathways** — The user is challenged for the response, as defined by the AXENT Pathways server.  
For information about defining Axent Pathways servers, see Chapter 10, “Server Objects”.
- **TACACS** — The user is challenged for the response, as defined by the TACACS or TACACS+ server.  
For information about defining TACACS servers, see Chapter 10, “Server Objects”.

A user can have different passwords on different gateways (for example, if the Authentication Scheme is OS Password), but only one Authentication scheme for all gateways.

## User Authentication

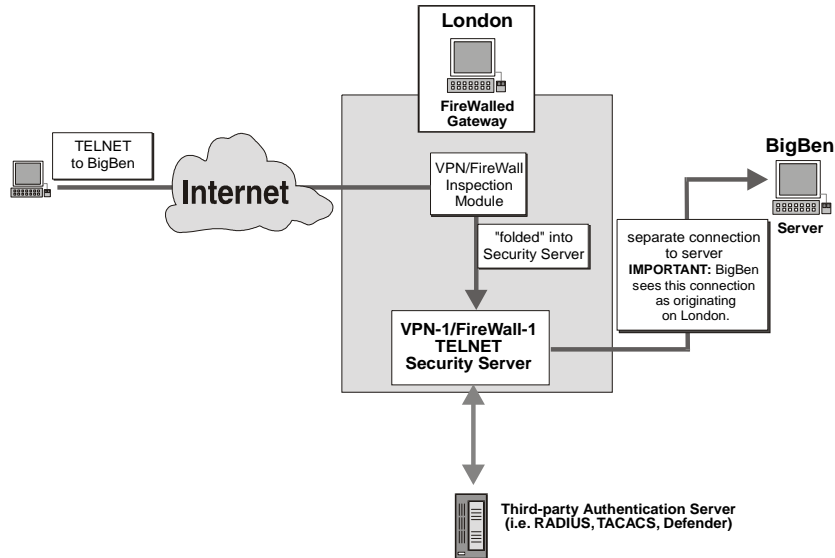
### In This Section

|                                                         |                 |
|---------------------------------------------------------|-----------------|
| <i>User Authentication — Overview</i>                   | <i>page 485</i> |
| <i>User Authentication — Deployment</i>                 | <i>page 486</i> |
| <i>Non-Transparent User Authentication</i>              | <i>page 495</i> |
| <i>User Authentication and the HTTP Security Server</i> | <i>page 497</i> |

## User Authentication — Overview

User Authentication is provided by the TELNET, FTP, HTTP and RLOGIN VPN-1/FireWall-1 Security Servers on the gateway. When a rule specifies User Authentication, the corresponding VPN-1/FireWall-1 Security Server is invoked in order to mediate the connection.

Consider the following configuration and rule:



**FIGURE 15-3** A connection mediated by the TELNET Security Server

| Source        | Destination | Services | Action   | Track    | Install On |
|---------------|-------------|----------|----------|----------|------------|
| All_Users@Any | BigBen      | telnet   | UserAuth | Long Log | Gateways   |

Under this rule, a user who TELNETs to BigBen is intercepted by the VPN/FireWall Module on the gateway London. The VPN/FireWall Module diverts the connection to the TELNET Security Server on the gateway, even though the user did not explicitly connect to the gateway.

The Security Server then authenticates the user, in accordance with the authentication scheme defined for the user in the **Authentication** tab of the **User Properties** window.

- If no authentication scheme is specified for a user, the user will be denied access.
- If an external authentication scheme is specified (that is, RADIUS, TACACS, or Axent Defender) the Security Server queries the appropriate third-party server regarding the user's permissions. The third-party server returns the appropriate data to the Security Server.

If authentication is successful, the TELNET Security Server opens a separate connection to the target server, in this case BigBen. Altogether, there are two connections, one to the Security Server on the gateway, and another from the Security Server to the final destination. The final destination server sees the connection as originating from the gateway, not the client. Authentication is transparent — the user TELNETs to BigBen, the target server, and not to the gateway.



**Note** – VPN-1/FireWall-1 also supports non-transparent authentication for TELNET, RLOGIN, HTTP and FTP. In non-transparent authentication, the user must first connect directly to the gateway and authenticate before being allowed to continue to the target host. For more information see “Non-Transparent User Authentication” on page 495.

User Authentication rules allow users if they authenticate successfully, but do not necessarily reject the connection if the user fails authentication. In addition, the fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. This is because the authenticating Security Server first checks if the connection can be allowed by a rule which does not require authentication. For more information, see “The ‘Insufficient Information’ Problem” on page 344.

## User Authentication — Deployment

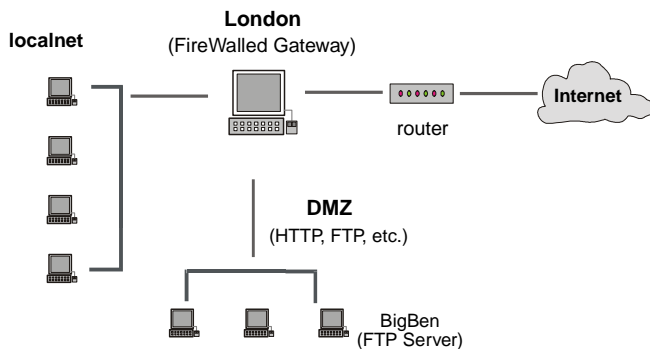
This section describes a deployment example for User Authentication. A deployment example consists of:

- an example network configuration
- what the Security Administrator must define in the VPN-1/FireWall-1 Rule Base
- what a user must do to authenticate

This example is not intended as a set of step by step instructions, but rather to illustrate how and where different components of User Authentication are configured in the VPN-1/FireWall-1 GUI.

## Example Configuration

FIGURE 15-4 depicts an example configuration in which London, the FireWalled gateway, protects a local network and a DMZ.



**FIGURE 15-4** Example configuration

The Security Administrator for this configuration may want to allow only localnet managers access to files on BigBen, the FTP server. The following rule allows a user group (**LocalManagers**) to access the FTP server after successful User Authentication.

| Source                                                                                              | Destination                                                                              | Service                                                                               | Action                                                                                      | Track                                                                                  | Install On                                                                                   |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|  LocalManagers@Any |  BigBen |  ftp |  User Auth |  Long |  Gateways |

**FIGURE 15-5** Example User Authentication Rule

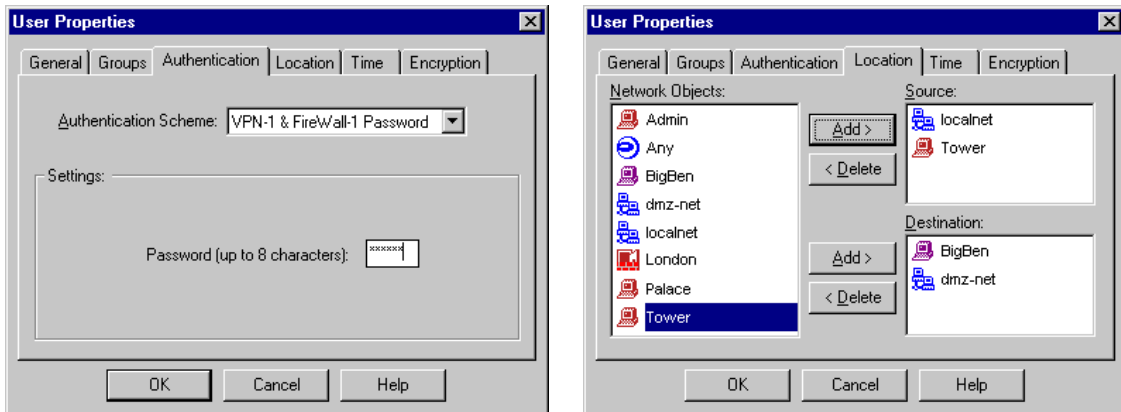
## Defining User Authentication

In order to implement User Authentication for this configuration and rule, you must define the following:

- the permitted user group
- authentication schemes supported by the gateway
- tracking and timeout parameters
- User Authentication rule properties

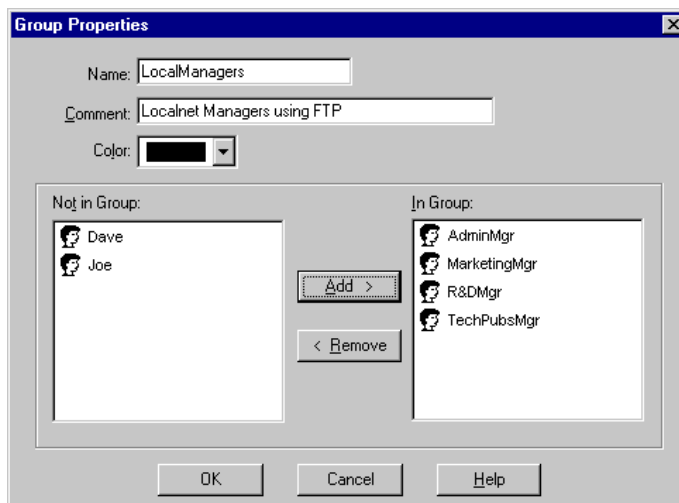
## Defining Permitted User Groups

In a User Authentication rule, the **Source** must be a user group (i.e., **allusers@localnet**). You must first define the permitted users, their authentication scheme or schemes and the network objects from which each user is allowed access. These properties are defined in the tabs of the **User Properties** window.



**FIGURE 15-6** User Properties window - Authentication tab and Location tab

You must next define a user group called “LocalManagers” consisting of the users who are allowed access.



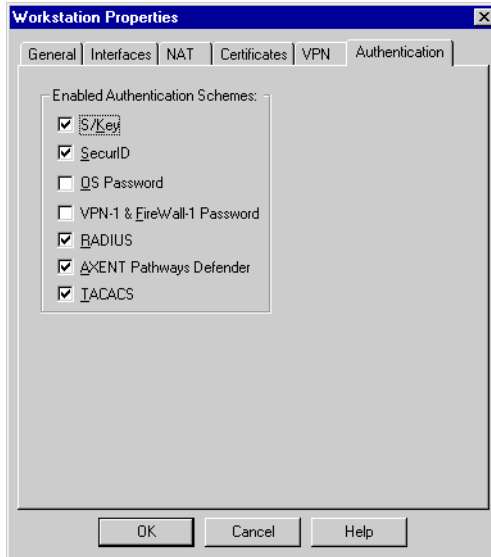
**FIGURE 15-7** Group Properties window - LocalManagers group

For more information on defining users and user groups, see Chapter 5, “Managing Users”.



## Defining the Gateway's Authentication Schemes

The gateway must support the same authentication schemes you defined for your users. For example, if some users in the group “LocalManagers” are using a VPN-1 & FireWall-1 Password, and others are using S/Key authentication, you must make sure the gateway supports both **VPN-1 & FireWall-1 Password** and **S/Key** authentication schemes. The gateway's authentication schemes are defined in the **Authentication** tab of the **Workstation Properties** window.



**FIGURE 15-8** Workstation Properties window — Authentication tab

Tracking and Timeout Parameters

You must specify tracking for failed authentication attempts and timeout parameters in the **Authentication** tab of the **Properties Setup** window. These parameters apply to all rules.

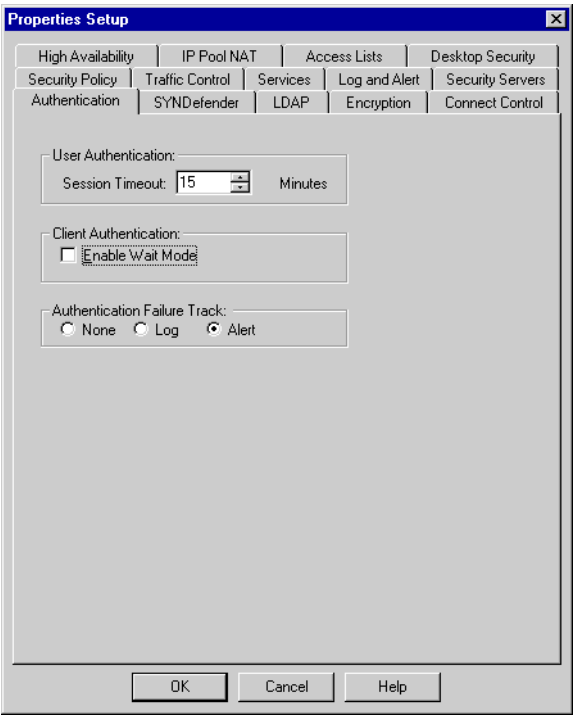


FIGURE 15-9 Properties Setup window — Authentication tab



**Note** – This window also specifies Client Authentication parameters. For more information, see “Client Authentication” on page 526.

**User Authentication: Session Timeout (minutes)** — the session will time out if there is no activity for this time period. See TABLE 15-2 for the meaning of the term “no activity.”

This applies to the FTP, TELNET, and RLOGIN Security Servers.

TABLE 15-2 Meaning of “No Activity”

| service | the term “no activity” means    |
|---------|---------------------------------|
| FTP     | no data transferred             |
| TELNET  | no keyboard (or mouse) activity |
| RLOGIN  | no keyboard (or mouse) activity |

**Session Timeout** has a different meaning for HTTP. Users of one-time passwords will not have to reauthenticate for each request during this time period. Each successful access resets the timer to zero.

Because each connection requires authentication, VPN-1/FireWall-1 extends the validity of one-time passwords for this period. In this way, users of HTTP do not have to generate a new password and reauthenticate for each connection.

**Authentication Failure Track** — the action to take if authentication fails (applies to all authentication rules)

- **None** — no tracking
- **Log** — Long Log
- **Alert** — the **User Authentication Alert Command** in the **Log and Alert** tab of the **Properties Setup** window.

The tracking for a successful authentication attempt is determined by the **Track** field of the enabling rule. If authentication is successful then:

- If access is allowed, the **Track** specified in the rule which allows the access is applied.
- If access is denied, the **Track** specified in the rule which denies the access is applied.

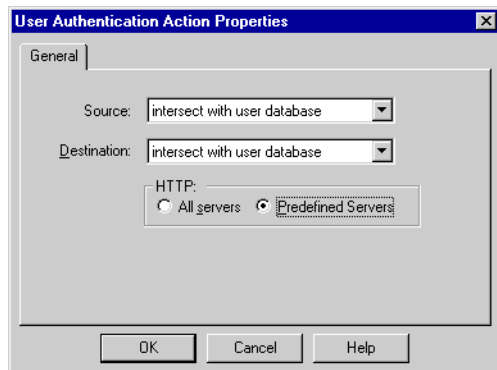
The fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. For more information, see “The ‘Insufficient Information’ Problem” on page 344.

For example, the rule depicted in FIGURE 15-5 on page 487 specifies logging in Long Log format. If authentication is successful, and access is allowed by this rule, the Long Log format is applied. A failed authentication attempt (for example, using an unauthorized password) is tracked according to the entry under **Authentication Failure Track** in the **Authentication** tab of the **Properties Setup** window.

## User Authentication Action Properties

You must also define the User Authentication properties of the enabling rule. The **User Authentication Action Properties** window specifies the parameters that apply to an individual rule. You can use this window to restrict user access to and from specific network objects.

To display the **User Authentication Action Properties** window, double-click on the rule's **Action**.



**FIGURE 15-10** User Authentication Action Properties window

**Source** — Reconcile **Source** in the rule with the allowed **Sources** in the **Location** tab of the **User Properties** window.

The allowed **Sources** in the **Location** tab of the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access from the source address, while the rule itself may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

**Destination** — Reconcile **Destination** in the rule with the allowed **Destinations** specified in the **Location** tab of the **User Properties** window.

The **Allowed Destinations** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access to the destination address, while the rule itself may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

**Ignore User Database** allows you to grant access privileges to a user without regard to the user's IP address. For example, if a user is temporarily away from the office and logging in from a different host, you may wish to allow that user access regardless of the network objects listed under the allowed **Source** specified in the **Location** tab of that user's **Properties** window (see FIGURE 15-6 on page 488). You can allow the user to work on the local network without extending access privileges to all users on that host.

**HTTP** — This option allows you to restrict access to specific HTTP servers. For more information, see “HTTP Servers List (Security Servers tab)” on page 499.

Example

Suppose the **Location** tab of a user’s **User Properties** window (FIGURE 15-6 on page 488) lists the network objects **Tower** and **localnet** under **Source**. This means that the user’s properties allow access from Tower and localnet. TABLE 15-3 summarizes various access possibilities.

**TABLE 15-3** Access Possibilities

| rule’s Source allows access from... | Source is “Intersect with User Database”                                                                                                                             | Source is “Ignore User Database”                                                                                 |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Tower</b>                        | The user is allowed access only from <b>Tower</b> , because only <b>Tower</b> is in both <b>Sources</b> in the <b>Location</b> tab and in the rule’s <b>Source</b> . | The user is allowed access only from <b>Tower</b> because <b>Tower</b> is in the rule’s <b>Source</b> .          |
| <b>Thames</b>                       | The user is denied access, because there is no network object that is in both <b>Sources</b> in the <b>Location</b> tab and the rule’s <b>Source</b> .               | The user is allowed access only from <b>Thames</b> , because only <b>Thames</b> is in the rule’s <b>Source</b> . |

## How the User Authenticates

When a user authenticates, he or she must provide the following information:

- user name on the gateway
- authentication data (password) on the gateway
- user name on the target host
- authentication data (password) on the target host

This user specifies this information using the syntax below.

**To enter user name:**

*dst\_user\_name* [*@auth\_user\_name*] @ *dst*

where:

- *dst\_user\_name* is the user name on the destination host
- *auth\_user\_name* is the user name on the gateway
- *dst* is the name of the destination host

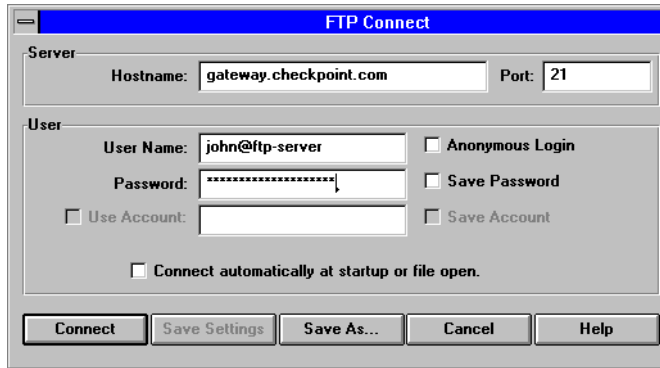
**To enter password:**

*dst\_password* [*@auth\_password*]

where:

- *dst\_password* is the password on the destination host
- *auth\_password* is the password on the gateway

This information is entered at the command line or, for FTP and TELNET, using a third-party GUI Client (such as the one in FIGURE 15-11).



**FIGURE 15-11** GUI FTP Authentication

**Parsing the Password String — FTP**

For FTP, VPN-1/FireWall-1 parses the password string as follows:

- Whatever is to the left of the last @ is interpreted as the password to the FTP server.
- Whatever is to the right of the last @ is interpreted as the User Authentication password.

For example, if the user types `jimb@BigBen.com@secret`, then `jimb@BigBen.com` is the FTP server password, and `secret` is the VPN-1/FireWall-1 User Authentication password.

This feature is important when using anonymous FTP and entering an email address as the password.

If the user wishes to postpone entering the VPN-1/FireWall-1 User Authentication password, then he or she should type the FTP server password and add @ at the end. The user will be prompted for the VPN-1/FireWall-1 Authentication password later.

Example - FTP Using O/S Password

In the example configuration depicted in FIGURE 15-4 on page 487, suppose a user in the **LocalManagers** group requests an FTP session on BigBen, the target server. The session might look something like this:

```
tower # ftp bigben
Connected to london.
220 london CheckPoint FireWall-1 secure ftp server running on London
Name (bigben:jim): jimb
331-aftpd: FireWall-1 password: you can use password@FW-1-password
Password: <Unix password on bigben>@<FireWall-1 password>
230-aftpd: User jimb authenticated by FireWall-1 authentication.
230-aftpd: Connected to bigben. Logging in...
230-aftpd: 220 bigben ftp server (UNIX(r) System V Release 4.0) ready.
230-aftpd: 331 Password required for jimb.
230-aftpd: 220 User jimb logged in.
```

The steps involved were as follows:

- 1 The user requested an FTP session on BigBen, the target server, by typing **ftp bigben**.  
The connection was intercepted by the FTP Security Server on London, the gateway. The Security Server prompted the user for his name on the gateway.
- 2 The user typed **jimb**, meaning that his user name on the target (BigBen) is jimb and his user name on the gateway is jimb.
- 3 The FTP Security Server challenged the user for his VPN-1/FireWall-1 password, in accordance with the authentication scheme specified for the user in the **Authentication** tab of the **User Properties** window.
- 4 The user correctly entered his VPN-1/FireWall-1 password and was connected to BigBen, the target server.  
The FTP Security Server on London supplied FTP on BigBen with the user's password, so the user did not have to enter it again.

Non-Transparent User Authentication

In This Section

|                                                      |                 |
|------------------------------------------------------|-----------------|
| <i>Non-Transparent User Authentication — Example</i> | <i>page 496</i> |
| <i>Enabling Non-Transparent User Authentication</i>  | <i>page 496</i> |

Non-transparent User Authentication can be implemented for user authenticated services (FTP, HTTP, RLOGIN, TELNET). Under non-transparent User Authentication, a user working with one of these services must first start a session for that service on

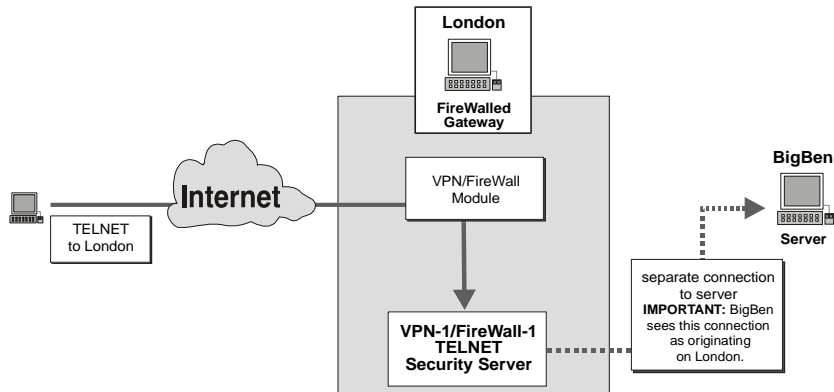
the gateway. After successful authentication, VPN-1/FireWall-1 opens a connection to the “true” destination. This method is known as non-transparent because the user does not directly request the target host, but must explicitly connect the gateway first.



**Note** – Transparent User Authentication is the default action for VPN-1/FireWall-1 version 3.0 and higher.

## Non-Transparent User Authentication — Example

Consider the following network configuration.



**FIGURE 15-12** Non-Transparent User Authentication.

In the above configuration, the user who wants to begin a TELNET session on Big Ben must first TELNET to London (the gateway) where the VPN-1/FireWall-1 TELNET Security Server is installed on the TELNET port in place of the standard TELNET daemon. The user must then specify BigBen as the ultimate destination. The VPN-1/FireWall-1 TELNET Security Server authenticates the user, and if the authentication is successful, opens a connection to BigBen, the “true” destination.

The user must provide the following information:

- user name on the gateway
- authentication data (password) on the gateway
- name of the target host — **this is the major difference between transparent and non-transparent authentication**
- user name on the target host
- authentication data (password) on the target host

## Enabling Non-Transparent User Authentication

Non-transparent user authentication is controlled by the `prompt_for_destination` parameter in the file `objects.C`.



The `prompt_for_destination` parameter determines what to do when the user connects directly to the FireWalled gateway. In this case, there are two possibilities:

- `prompt_for_destination` is false

This is the default value for VPN-1/FireWall-1 version 3.0 and higher. If `prompt_for_destination` is false, VPN-1/FireWall-1 implements transparent User Authentication. The VPN/FireWall Module assumes the user's "true" destination is the FireWalled machine, and does not prompt the user for the "true" destination.

- `prompt_for_destination` is true

If `prompt_for_destination` is true, VPN-1/FireWall-1 implements non-transparent User Authentication. If the user requests the gateway as the destination, the VPN/FireWall Module assumes the user's "true" destination is some other server, and prompts the user for the "true" destination.

Non-transparent User Authentication will be implemented only if the user first requests the gateway. If the user requests a host behind the gateway, VPN-1/FireWall-1 will implement non-transparent authentication, regardless of the setting for `prompt_for_destination`.



**Note** – After making changes to `objects.C`, you must download the database from the Management Station to the firewall in order for the changes to take effect. For more information, see, "fw dbload" on page 13 of *Check Point Reference Guide*.

## User Authentication and the HTTP Security Server

### In This Section

|                                                                |                 |
|----------------------------------------------------------------|-----------------|
| <i>HTTP Security Server — Overview</i>                         | <i>page 497</i> |
| <i>HTTP Security Server Configuration</i>                      | <i>page 498</i> |
| <i>Controlling Access to HTTP — User Authentication Rules</i>  | <i>page 501</i> |
| <i>The HTTP Security Server in Proxy Mode</i>                  | <i>page 502</i> |
| <i>HTTP Security Server — When the User Connects</i>           | <i>page 506</i> |
| <i>HTTP Security Server — Security Considerations</i>          | <i>page 508</i> |
| <i>HTTP Security Server and Non-Transparent Authentication</i> | <i>page 509</i> |

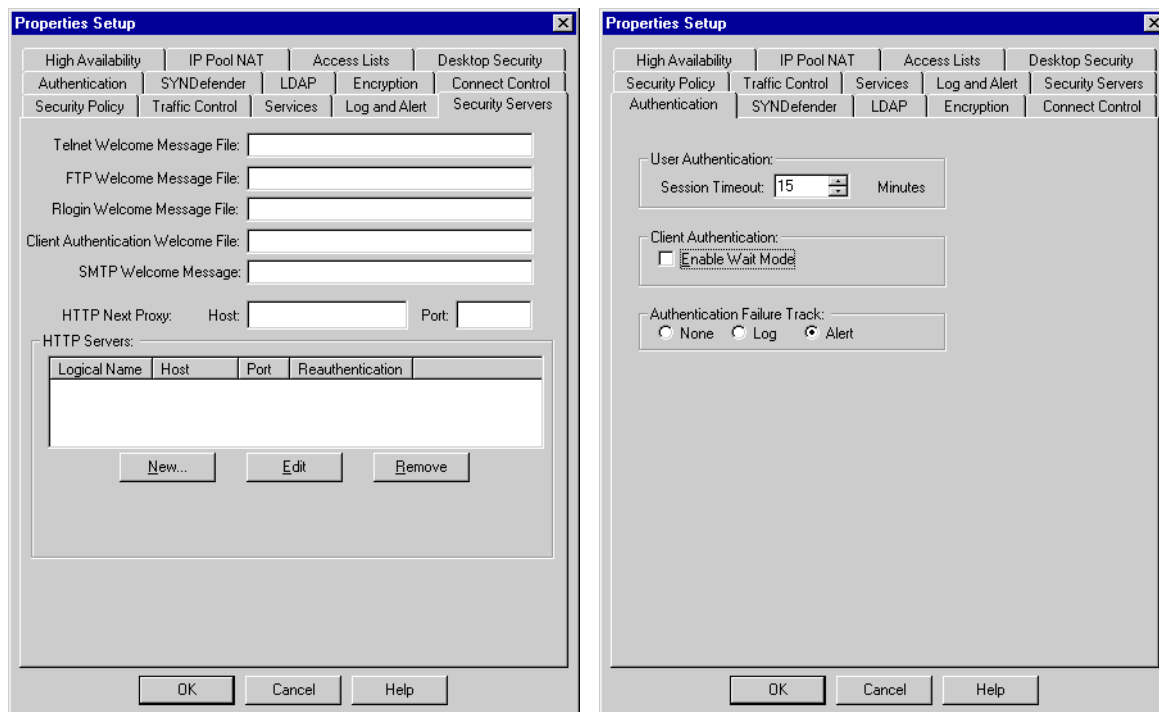
### HTTP Security Server — Overview

The VPN-1/FireWall-1 HTTP Security Server provides a mechanism for authenticating users of HTTP services. An HTTP Security Server on the gateway can protect any number of HTTP servers behind the gateway, and authenticate users accessing HTTP or HTTPS (HTTP encrypted by SSL).

The HTTP Security Server is invoked when a rule's action specifies **User Authentication**. The rule's **Service** can specify either the HTTP service or a Resource. This section describes the behavior of the HTTP Security Server for User Authentication rules. For more information on how the HTTP Security Server handles Resources, see Chapter 3 “Content Security” of this book.

## HTTP Security Server Configuration

HTTP Security Server parameters are defined in the **Security Servers** tab and the **Authentication** tabs of the **Properties Setup** window.



**FIGURE 15-13** Properties Setup window — Security Servers and Authentication tabs

The fields relating to the HTTP Security Server are explained below.

- **Session Timeout (Authentication tab)** — For HTTP, this applies to one-time passwords only. Users of one-time passwords do not have to reauthenticate during this time period. The HTTP Security Server extends the validity of a one-time password for this time period so the user does not have to generate a new password and reauthenticate for each connection. Each successful access resets the timer to zero. For more information, see “HTTP Security Server — Security Considerations” on page 508.
- **HTTP Next Proxy (Security Servers tab)** — This specifies the **Host** name and **Port** number of the HTTP proxy behind the HTTP Security Server (if there is one).

This option is useful if internal users have defined the HTTP Security Server as the proxy to their Web browsers (see “The HTTP Security Server as an HTTP Proxy” on page 503). The HTTP Security Server does not cache pages used by its client (the browser). If you wish to provide caching for HTTP users, you can put an HTTP proxy behind the HTTP Security Server.

Changing the **HTTP Next Proxy** fields takes effect after the VPN-1/FireWall-1 database is downloaded to the authenticating gateway, or after the Security Policy is re-installed.

## HTTP Servers List (Security Servers tab)

The **HTTP Servers** list in **Security Servers** tab of the **Properties Setup** specifies the host names and port numbers of HTTP servers.

Defining HTTP servers allows you to restrict incoming HTTP. You can control access to specific ports on specific hosts. You can also specify whether users must reauthenticate when accessing a specific server.

If you are implementing non-transparent authentication, then the **HTTP Servers** list provides a list of hosts and port numbers to which the HTTP Security Server can direct connections from the gateway. For more information, see “HTTP Security Server and Non-Transparent Authentication” on page 509.

If you change the location of an HTTP server (i.e., you install it on a new host or port), you must update the **HTTP Servers** list. For more information, see “Controlling Access to HTTP — User Authentication Rules” on page 501.

### Configuring HTTP Servers

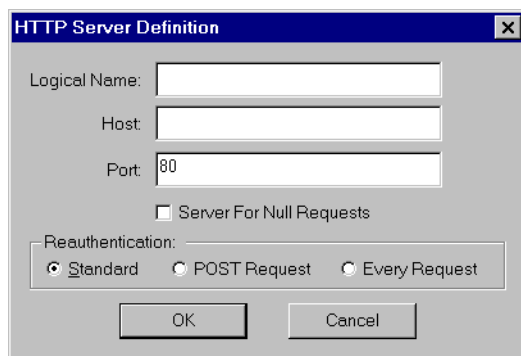
To add a new server, click on **New**. The **HTTP Server Definition** window (FIGURE 15-14) is then displayed.

To delete a server from the list, select it and click on **Remove**. More than one server can be selected at a time.

To modify a server’s host or port number, click on the server’s logical name in the **HTTP Servers** list and click on **Edit**. The server’s details are then displayed in the **HTTP Server Definition** window (FIGURE 15-14).

## HTTP Server Definition window

This window defines an HTTP server.



**FIGURE 15-14** HTTP Server Definition window

The fields in the **HTTP Server Definition** window are explained below:

**Logical Name** — the server’s logical name

**Host** — the host on which the server runs

**Port** — the port number on the host

**Server For Null Requests** — this option is relevant only if non-transparent authentication is enabled. For more information, see “Configuring a Server for Null Requests” on page 513.

## Reauthentication Options

Reauthentication options define whether a user must reauthenticate every time the HTTP server is accessed. Reauthentication options apply only when **Predefined Servers** is specified under **HTTP** in a rule’s **User Authentication Action Properties** window (FIGURE 15-10 on page 492).

Select one of the following options:

**Standard Authentication** — The user will not be required to enter a password again during the authorization period (as specified in the **Session Timeout** field in the **Authentication** tab of the **Properties Setup** window). Each successful access resets the timer to zero.

**Reauthentication for POST Requests** — Every request sent by the client which may change the server’s configuration or data requires the user to enter a new password.

If the password is not a one-time password, this option has no effect.

**Reauthentication for Every Request** — every request for a connection requires the user to enter a new password

If the password is not a one-time password, this option has no effect.

This option is useful when access to some pages must be severely restricted. It is recommended that pages such as these be handled by a separate server.

The Reauthentication status of each HTTP Server is displayed under **Reauthentication** in the **HTTP Servers** list.

## Controlling Access to HTTP — User Authentication Rules

### Restricting Incoming HTTP

If you wish to restrict access to internal HTTP services by external users, proceed as follows:

- 1 Define a rule similar to the following:

| Source        | Destination | Services | Action   | Track    | Install On |
|---------------|-------------|----------|----------|----------|------------|
| All_Users@Any | localnet    | http     | UserAuth | Long Log | Gateways   |

The above rule requires external users to authenticate before accessing HTTP services in the local network. Incoming HTTP is intercepted by the HTTP Security Server on the gateway.

- 2 In the rule's **User Authentication Action Properties** window (FIGURE 15-10 on page 492), choose **Predefined Servers** under **HTTP**.

This restricts external access to the HTTP servers listed in the **Security Servers** tab of the **Properties Setup** window. This will also activate the **Reauthentication** options specified for the HTTP servers. For more information, see “HTTP Servers List (Security Servers tab)” on page 499.

### Restricting Internal Users' Access to External HTTP

To restrict internal users' access to external HTTP, proceed as follows.

- 1 Define a rule similar to the following:

| Source             | Destination | Services | Action   | Track    | Install On |
|--------------------|-------------|----------|----------|----------|------------|
| All_Users@localnet | any         | http     | UserAuth | Long Log | Gateways   |

This rule allows internal users to use external HTTP if they first authenticate themselves on the gateway.

- 2 In the rule's **User Authentication Action Properties** window (FIGURE 15-10 on page 492), choose **All Servers** from the HTTP options. This allows the connection to continue on to any port.

If **All Servers** is chosen, then the options defined in the HTTP Server window for predefined servers are ignored.

### 3 Define another rule as follows:

| Source | Destination | Services | Action | Track    | Install On |
|--------|-------------|----------|--------|----------|------------|
| any    | any         | any      | Reject | Long Log | Gateways   |

This rule prevents the use of HTTP without User Authentication on the gateway.

## Restricting Incoming and Outgoing HTTP

Assume the following Rule Base:

| Source            | Destination | Services | Action   | Track    | Install On |
|-------------------|-------------|----------|----------|----------|------------|
| AllUsers@any      | localnet    | http     | UserAuth | Long Log | Gateways   |
| AllUsers@localnet | any         | http     | UserAuth | Long Log | Gateways   |
| any               | any         | any      | Reject   | Long Log | Gateways   |

The first rule requires users of incoming HTTP to authenticate before accessing internal HTTP servers defined in the HTTP servers window (FIGURE 15-14 on page 500).

The second rule applies to internal users accessing external HTTP. According to the second rule, internal users must be authenticated before accessing external HTTP.

## The HTTP Security Server in Proxy Mode

For internal users, the behavior of the HTTP Security Server also depends on whether it is defined as the proxy to the users' Web browser (in the browser's proxy settings). There are two different proxy settings. Each setting has specific advantages and implications for local users.

### ■ HTTP proxy

The HTTP Security Server can be defined as the HTTP proxy to the user's Web browser. This provides several advantages regarding entering user passwords and managing authentication. For more information, see "The HTTP Security Server as an HTTP Proxy" on page 503.

### ■ Security proxy

The HTTP Security Server can be defined as the Security Proxy to the user's Web browser. The HTTP Security Server proxies HTTPS (HTTP encrypted by SSL) connections. Although it does not inspect content of HTTPS connections, the

administrator can provide security by specifying User Authentication for outgoing HTTPS. For more information, see “HTTP Security Server as a Security Proxy — Authenticating Outgoing HTTPS” on page 504.



**Note** – Proxy settings are not mutually exclusive and can be used together.

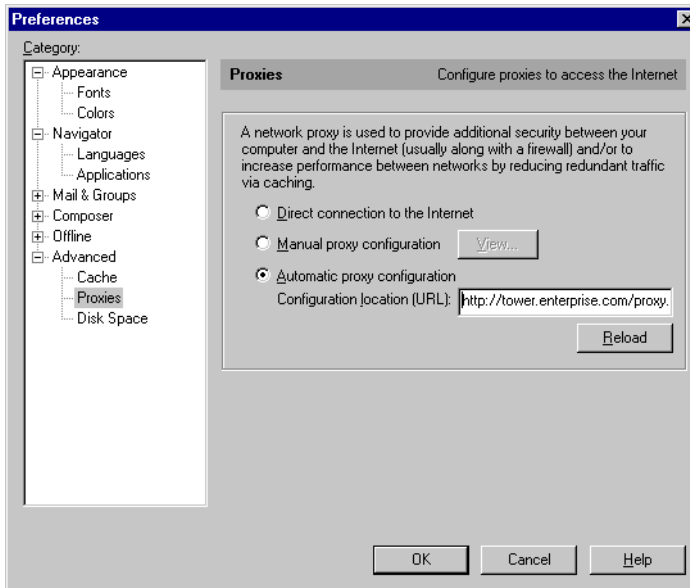
## The HTTP Security Server as an HTTP Proxy

Internal users can define the HTTP Security Server as the HTTP proxy to their Web browsers. The HTTP Security Server is defined as an HTTP proxy in the proxy settings of the user’s Web browser.



**Note** – The VPN-1/FireWall-1 HTTP Security Server will only handle proxy requests for authenticated HTTP connections and resources. If you do not use authentication or resources, you cannot use the VPN-1/FireWall-1 HTTP Security Server as an HTTP proxy.

FIGURE 15-15 shows the proxy settings window for Netscape 4.0.



**FIGURE 15-15** Defining the gateway as the HTTP proxy — Netscape 4.0

Defining the HTTP Security Server as a proxy offers several advantages:

- You can centralize Authentication information to one location, the VPN-1/FireWall-1 machine.
- When defined as the HTTP proxy, the HTTP Security Server can handle FTP requests through a Web browser. For more information, see “HTTP Security Server” on page 350.

- When a local user requests a URL in the Web browser, the browser sends the entire URL path to the HTTP Security Server.

When the HTTP Security Server is not defined as a proxy, it only receives the name of the requested server from the Web browser. This means HTTP Security Server must retrieve the entire URL.

- All outgoing HTTP connections are mediated by the HTTP Security Server.

In addition, the HTTP Security Server offers several advantages over other Authentication Servers.

- VPN-1/FireWall-1 supports S/Key, SecurID, RADIUS, TACACS and AXENT Defender authentication.
- VPN-1/FireWall-1 supports restriction by day of week and/or time of day.
- VPN-1/FireWall-1 can automatically expire a user according to the **Expiration Date** specified in the **General** tab of the **User Properties** window.



**Note** – Although it is defined as the HTTP proxy to the Web browser, the HTTP Security Server is not an official HTTP proxy, that is, it does not relay HTTP traffic in the way that, for example, the CERN HTTP proxy does. It is not an independent daemon that runs outside of FireWall.

Caching — Using an HTTP Proxy behind the HTTP Security Server

A disadvantage to using the HTTP Security Server as a proxy is that it does not cache pages used by its client (the browser). If you wish to provide caching for HTTP users, you can put an HTTP proxy behind the VPN-1/FireWall-1 HTTP Security Server. To do this, you must specify the host and port of the proxy in the **HTTP Next Proxy** field in the **Security Servers** tab of the **Properties Setup** window.

### **HTTP Security Server as a Security Proxy — Authenticating Outgoing HTTPS**

HTTPS (HTTP encrypted by SSL) connections can be handled by the HTTP Security Server when it is defined as the Security Proxy to the local user's Web browser. The HTTP Security Server proxies outgoing HTTPS connections, but does not inspect content. This option is used to authenticate internal users accessing external HTTPS.

The user can configure a Security Proxy for the following Web browsers:

- Internet Explorer version 3.0x and higher
- Netscape version 4.0x and higher

For details, see “Security Proxy Mode” on page 352 of Chapter 11, “Security Servers and Content Security.”



Authenticating Internal Users Accessing External HTTPS (Security Proxy Mode)

To authenticate users of outgoing HTTPS, proceed as follows:

- 1 Internal users must define the HTTP Security Server as the Security Proxy on port 443. This is done in the proxy settings of the user’s Web browser. For more information, see “Security Proxy Mode” on page 352 of Chapter 11, “Security Servers and Content Security.”
- 2 Add the following line to the file `$FWDIR/conf/fwauthd.conf`:

```
443 bin/in.ahttpd wait 0
```

This enables the HTTP Security Server to run on the port specified for the Security Proxy.

- 3 In the HTTPS service properties, set the **Protocol Type** to **URI** (FIGURE 15-16). This assures that the HTTPS service (using port 443) will be mediated by the HTTP Security Server.

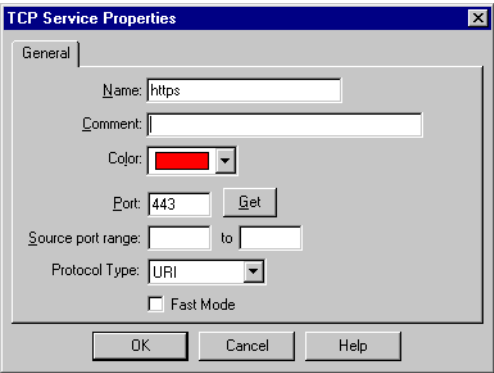


FIGURE 15-16 HTTPS Service Definition

- 4 Define a rule similar to the following

| Source                 | Destination | Services | Action   | Track    | Install On |
|------------------------|-------------|----------|----------|----------|------------|
| All_Users<br>@localnet | any         | https    | UserAuth | Long Log | Gateways   |

According to this rule, internal users must authenticate before accessing external HTTPS.

- 5** In the rule's **User Authentication Action Properties** window, check **All Servers** under **HTTP**.

This assures that the outgoing connections will be allowed to continue from the HTTP Security Server to any external host or port.

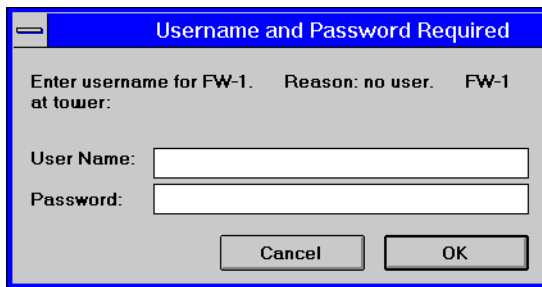


**Tip** – You can also configure the HTTP Security Server to encrypt and decrypt HTTPS connections on the gateway. For more information, see “Support For HTTPS — Controlling External Access to Internal HTTPS” on page 509.

## HTTP Security Server — When the User Connects

### Password Prompt

When a user is intercepted by the HTTP Security Server, a password prompt window is displayed in which the user is asked to enter a user id and a password. The format of the window depends on the HTTP browser in use, since it is the browser that displays the window, not VPN-1/FireWall-1. However, some of the data displayed in the window is supplied to the browser by the HTTP Security Server.



**FIGURE 15-17** A Typical User ID and Password Window

The information given in the password prompt window usually includes:

- the Authentication scheme required by VPN-1/FireWall-1
- whether Authentication is required for the HTTP server, and if so, the server's realm name
- a “reason” message giving the reason for the last Authentication failure

### Multiple Users and Passwords

This applies only when the HTTP Security Server is not being used as a user's Web proxy. This is relevant for external users accessing internal HTTP, and internal users who have not defined the HTTP Security Server as a proxy.

In HTTP, the Web browser automatically supplies the user's password to the server once the user authenticates. If the user requests another server, the browser cannot send the password to the new server, and the user must reauthenticate.

The user can specify different user names (and passwords) at the password prompt for the HTTP server and VPN-1/FireWall-1, as follows:

```
server_username@VPN-1/FireWall-1_username
```

In the same way, the user can enter two passwords, as follows:

```
server_password@VPN-1/FireWall-1_password
```

If there is no password for the server, only the VPN-1/FireWall-1 password should be entered.

If the user enters one user name and two passwords, the same user name is used for both the HTTP server and VPN-1/FireWall-1, but the different passwords are used as indicated.

If @ is part of the password, the user should type it twice (for example if the password is mary@home, type mary@@home).

### **“Reason” Messages**

Authentication attempts may be denied for any of the following reasons. The browser displays these messages in the password prompt.

**TABLE 15-4** HTTP Security Server “Reason” messages

| <b>error</b>     | <b>meaning</b>                                                                                                                             |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| no user          | No user id was entered.                                                                                                                    |
| no password      | No password was entered.                                                                                                                   |
| wrong password   | The OS or VPN-1/FireWall-1 password was incorrect.                                                                                         |
| S/Key            | S/Key authentication failed.                                                                                                               |
| SecurID          | SecurID authentication failed.                                                                                                             |
| WWW server       | The VPN-1/FireWall-1 password was correct, but the server did not authorize the user (probably because the server password was incorrect). |
| user limitations | The user is not authorized for the given day of week, time of day, source or destination, or the user has expired.                         |
| FW-1 rule        | The VPN-1/FireWall-1 password was correct, but the user was not authorized because there was no matching rule in the Rule Base.            |

In addition to “Reason” messages, additional messages may be displayed by the browser.

**TABLE 15-5** Browser Messages

| message                                              | meaning and/or corrective action                                                                                                                                         |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failed to connect to the WWW server                  | Notify your system manager.                                                                                                                                              |
| Unknown WWW server                                   | VPN-1/FireWall-1 could not determine to which server the URL should be sent. This can happen for two reasons:<br>The URL is incorrect, or there is a resolution problem. |
| Authentication Services are unavailable              | Notify your system manager.                                                                                                                                              |
| VPN-1/FireWall-1 is currently busy - try again later | Wait and try again. If the problem persists, notify your system manager.                                                                                                 |
| Simple requests (HTTP 0.9) are not supported         | HTTP 0.9 clients are not supported by the VPN-1/FireWall-1 HTTP Security Server. Note that HTTP 0.9 servers are supported.                                               |

Additional messages may be displayed if VPN-1/FireWall-1 encounters an error, such as no OS password defined for a user who is required to supply a OS password, or problems with SecurID server etc. In the event one of these messages is encountered, the user should notify the system administrator.

## Differences Between Clients

Some clients do not display authorization information in the password prompt window, or display only some of the information.

When using such a client, the user can sometimes view the missing information by clicking on **Cancel** (to view the information) and then **Reload** (to display the password prompt window again), or by performing the equivalent functions.

If the password prompt window does not display what kind of password must be entered (this can happen if the user name is unknown), the user should enter the user name without the password and click on **OK**. If the client requires a non-empty password, the user should type a single space. The window will be displayed again, including the password type.

## HTTP Security Server — Security Considerations

In HTTP, the Web browser automatically supplies the password to the server for each connection. This creates special security considerations when using the HTTP Security Server with one-time passwords.

To avoid forcing users of one-time passwords to generate a new password for each connection, the HTTP Security Server extends the validity of the password for the time period defined in **Authorization Timeout** in the **Authentication** tab of the **Properties Setup** window. Users of one-time passwords do not have to reauthenticate for each request during this time period.

Each successful access resets the timer to zero. Because the authorization period is renewable, and the Web browser keeps supplying the password, the time period during which a one-time password can be used can be unlimited.

This problem can be solved by using the Reauthentication options in the HTTP Server definition (“HTTP Servers List (Security Servers tab)” on page 499). For example, you can specify that every request to a specific HTTP server requires a new password, or that requests that change a server’s configuration require a new password. For more information, see “HTTP Servers List (Security Servers tab)” on page 499.

## HTTP Security Server and Non-Transparent Authentication

This section describes how the HTTP Security Server is configured when implementing Non-transparent Authentication. In Non-transparent Authentication, the user must explicitly connect to the FireWalled gateway in order to authenticate before continuing to the target host. For an overview see “Non-Transparent User Authentication” on page 495.

If you are implementing Non-transparent Authentication, the HTTP Security Server can be configured to encrypt and decrypt HTTPS connections. This option enables the HTTP Security Server to inspect the contents of HTTPS connections.

The connection can be encrypted between the client and the HTTP Security Server, and then possibly again from the HTTP Security Server to the target server. For example, you can specify that connections between the client and HTTP Security Server are encrypted. The HTTP Security Server on the gateway decrypts and inspects the connection. The connection can then be encrypted again from the HTTP Security Server to the target host. The authentication session is encrypted as well.

Because the HTTP Security Server is not defined as a Security Proxy to the user’s Web browser, Non-transparent Mode is best used to authenticate external users accessing internal servers. For information on putting an existing HTTP server behind the HTTP Security Server, see “Putting Existing HTTP Servers Behind the HTTP Security Server” on page 514.

## Support For HTTPS — Controlling External Access to Internal HTTPS

To configure support for HTTPS, proceed as follows:

- 1** In the `objects.C` file, set the `prompt_for_destination` parameter to `true`.

This value indicates that if the user requests the gateway as the destination, the VPN/FireWall Module assumes the user’s “true” destination is some other server, and prompts the user for the “true” destination.

## Generating CA Keys

Next, generate the CA Key pair to be used by the Management Station and the FireWalled gateway.

- 2** Generate the CA Key for the Management Station using the `fw ca genkey` command. This command is entered on the Management Station as follows:

```
fw ca genkey DN
```

DN is the distinguished name of the Certificate Authority. The following shows the `fw ca genkey` command with the DN of an example Certificate Authority:

```
fw ca genkey ou=research,o=widgetcorp,c=us
```

where `ou` is the organizational unit, `o` is the organization, and `c` is the country of the Certificate Authority.

- 3** Distribute the CA Key to the FireWalled gateway using the `fw ca putkey` command. This command is entered on the Management Station as follows:

```
fw ca putkey [-p password] target
```

The parameter `target` is the IP address or resolvable name of the machine on which you are installing the CA key (the FireWalled gateway).

`-p password` is a password that will be used to authenticate future communication between the Management Station and the gateway. The password can be entered on the command line (using the `-p` argument). If you do not enter a password on the command line, you will be prompted for one.

- 4** On the FireWalled gateway, generate a Certificate. You must enter the following command on the FireWalled gateway:

```
fw certify ssl management target
```

`management` is the IP address or resolvable name of the FireWalled gateway's Management Station. `target` is the IP address or resolvable name of the machine on which you are installing the CA key.

You will be prompted for a password. You must enter the same password you used when you issued the `fw ca putkey` command on the Management Station in step 3.

## Modifying the Security Server Configuration File

- 5** Next modify the file `$FWDIR/conf/fwauthd.conf` by adding a line which enables the HTTP Security Server to run on an additional service port dedicated to HTTPS. According to the example below, HTTPS connections will connect to the gateway on port 443.

For example:

```
443 bin/in.ahhttpd wait 0 ec
```

The last field specifies what to do with HTTPS (SSL) connections. TABLE 15-6 lists the available options:

**TABLE 15-6** HTTPS options

| option | meaning                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------|
| ec     | encrypt connections between the client and the gateway                                                              |
| es     | encrypt connections between the gateway and the server                                                              |
| eb     | encrypt both — encrypt connections between the client and the gateway, and then between the gateway and the server. |
| ns     | no SSL (no encryption)                                                                                              |

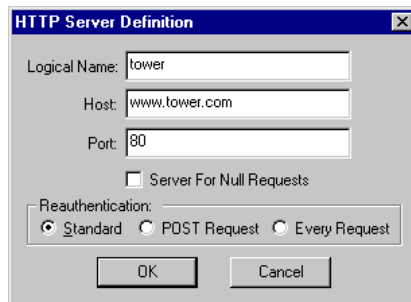
Leaving this field empty is the same as specifying `ns`.

For more information about the file `$FWDIR/conf/fwauthd.conf`, see “Security Server Configuration” on page 357.

## HTTP Servers

- 6** Define the HTTP servers to which HTTPS connections are allowed.

HTTP servers are defined in the **HTTP Server Definition** window (FIGURE 15-18). For information on defining HTTP servers, see “HTTP Servers List (Security Servers tab)” on page 499 in this chapter.



**FIGURE 15-18** Example HTTP Server definition

You must specify the **Logical Name**, **Host** and **Port** number on which you installed the servers which will handle HTTPS connections.

#### HTTPS Service Properties

- 7** Modify HTTPS properties to assure that the service will be mediated by the HTTP Security Server. In the HTTPS service definition, set the **Protocol Type** to **URI** (see FIGURE 15-16 on page 505).

#### User Authentication Rule

- 8** Next, define a rule similar to the following:

| Source        | Destination | Services | Action   | Track    | Install On |
|---------------|-------------|----------|----------|----------|------------|
| All_Users@any | localnet    | https    | UserAuth | Long Log | Gateways   |

In the rule's **User Authentication Action Properties** window, specify **Predefined Servers** under **HTTP**. This restricts incoming HTTPS to the servers listed in the **Security Servers** tab of the **Properties Setup** window (the HTTP Servers you defined in step 6 on page 511).

### How the User Connects

An external user of HTTP must specify the name of the FireWalled gateway and the logical name of the target server in the requested URL. This assures that the request will be intercepted by the HTTP Security Server on the gateway. The URL is set up as follows:

```
https://<gateway_name>/<logical_server_name>/...
```

For example, if the gateway name is London, and the target server (behind London) is Tower, then the user specifies the following URL:

```
https://www.london.com/tower/...
```

For information on how to set up URLs for Non-transparent Authentication, see "Configuring URLs" below.

### Configuring URLs

Suppose that in the configuration depicted in FIGURE 15-19 on page 513, there are HTTP servers on all the hosts (Tower, Palace, and BigBen) which are protected by an HTTP Security Server on the gateway London.

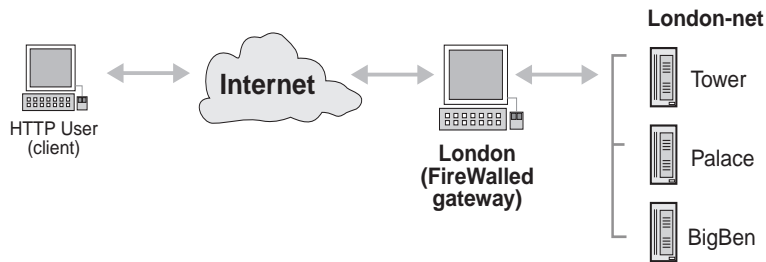
The URLs should be set up as follows:

```
http://gateway/logical server name/...
```



where the ellipsis (...) indicates the part of the URL that the server receives and parses. This is usually a file name.

For example, assume HTTP servers running on London-net, as listed in FIGURE 15-19.



**FIGURE 15-19** HTTP Servers behind a FireWalled gateway

**TABLE 15-7** Servers and URLs

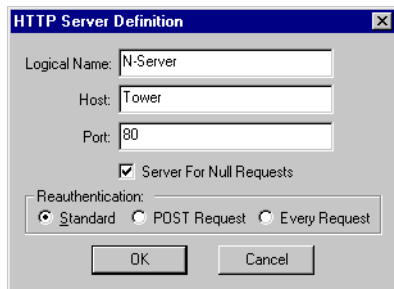
| server name | URL                                         | host   | port |
|-------------|---------------------------------------------|--------|------|
| info        | http://www.London.com/info/info.html        | BigBen | 80   |
| tickets     | http://www.London.com/tickets/ordrtick.html | Palace | 80   |
| actors      | http://www.London.com/actors/bios.html      | Tower  | 8000 |
| reviews     | http://www.London.com/reviews/clips.html    | Tower  | 8080 |

In this case, the gateway is `www.London.com` and the server names are those specified under **HTTP Servers** in the **Security Servers** tab of the **Properties Setup** window (see FIGURE 15-13 on page 498), where the connection between the server name and the host and port is defined. The only externally known name is `www.London.com`.

A user who wishes to access the HTTP server “actors” on the host Tower, must specify a URL of `http://www.London.com/actors/bios.html` (where `bios.html` is a specific page maintained by the server). The connection is intercepted by the HTTP Security Server on the gateway London.

### Configuring a Server for Null Requests

A Server for Null Requests is used when the URL is of the form `http://gateway/` or `http://gateway`. In this case, the URL passed to the server is “/”. In Non-transparent Authentication, this allows a user to connect to the gateway without having to specify the name of a target server behind the gateway. The Server for Null Requests is defined using the **HTTP Server Definition** window (FIGURE 15-20).



**FIGURE 15-20** HTTP Server Definition — Server for Null Requests

For example, a user connects to London, the FireWalled gateway, as follows:

`http://www.london.com`

If you have specified an HTTP server as a **Server for Null Requests** and checked **Predefined Servers** in the **User Authentication Action Properties** window of the relevant rule, the HTTP Security Server on the gateway directs the connection to the Server for Null Requests.

You can configure this server to display a Web page with links to internal servers. This server then provides an “entry point” to other internal servers. In this way, the user does not have to know the names of the target servers behind the gateway. All the user needs to know is the name of the FireWalled gateway.

### Putting Existing HTTP Servers Behind the HTTP Security Server

This section applies to users who wish to implement Non-transparent authentication.

To put an existing HTTP server behind the HTTP Security Server, proceed as follows:

#### ▼ If you have only one HTTP server, and it is on your gateway

- 1** Replace the HTTP server with the HTTP Security Server.
- 2** Put the HTTP server elsewhere.
- 3** For security reasons, it is recommended that you put the HTTP server on a different computer. However, you can also put it on a different port on the same computer.
- 4** Update the **HTTP Servers** list in the **Security Servers** tab of the **Properties Setup** window in accordance with where you put the HTTP server (see previous step).

#### ▼ If you have only one HTTP server, and it is **NOT** on your gateway

- 1** Arrange for the server address to be directed to the HTTP Security Server (host name) on the gateway.

This is done outside of VPN-1/FireWall-1, either by publicizing the new address for the existing host name, or by creating a new host name and notifying your authorized users.

- 2 Add the server to the list of HTTP servers in the **Control Properties/Security Servers** window.

Even if there is only one server behind VPN-1/FireWall-1, you should still give it a name and add it to the HTTP server table in the **Control Properties/Security Servers** window (see “HTTP Servers List (Security Servers tab)” on page 499). However, the server name may be omitted from the URLs that refer to it (if there is only one server), so there is no need to change URLs when putting a single server behind VPN-1/FireWall-1 if the host name for the FireWall and the server are the same.

### ▼ If you have more than one HTTP server

- 1 Arrange for the server address to be directed to the HTTP Security Server (host name) on the gateway.
- 2 This is done outside of VPN-1/FireWall-1, either by publicizing the new addresses for the existing host name, or by creating a new host name and notifying your authorized users.
- 3 Add the servers to the list of HTTP servers in the **Control Properties/Security Servers** window.
- 4 Modify all the HTML source code so that absolute references point to the appropriate servers.

This step is necessary for non-transparent authentication only.

The first field of an absolute URL should be replaced by “*gateway/logical server name/*”.

It is not necessary to modify relative references.

## Session Authentication

### In This Section

|                                            |                 |
|--------------------------------------------|-----------------|
| <i>Session Authentication — Overview</i>   | <i>page 515</i> |
| <i>Session Authentication — Deployment</i> | <i>page 517</i> |

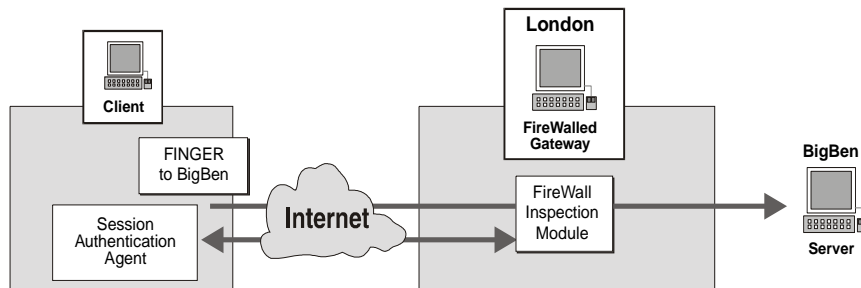
### Session Authentication — Overview

Session Authentication can be used to authenticate users of any service. FIGURE 15-21 shows what happens when a rule’s Action specifies Session Authentication.

The Session Authentication process is as follows:

- 1 The user initiates a connection directly to the server.

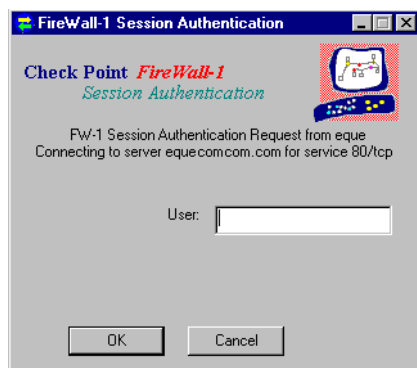
- 2 The VPN-1/FireWall-1 Inspection Module intercepts the connection. The Inspection Module connects to a Session Authentication Agent on the client. In the above configuration, the Session Authentication Agent is running on the client, but it can run on another machine (on any of the supported platforms).



**FIGURE 15-21** Session Authentication

- 3 The Session Authentication Agent prompts the user for authentication data and returns this information to the Inspection Module.
- 4 If the authentication is successful, then the VPN/FireWall module allows the connection to pass through the gateway and continue on to the target server.

In contrast to User Authentication, Session Authentication does not result in an additional connection to the server. The advantage of Session Authentication is that it can be used for every service. It requires a Session Authentication Agent which prompts the user through a series of pop-up screens.



**FIGURE 15-22** VPN-1/FireWall-1 Session Authentication Agent Prompt

The Session Authentication Agent is an application that communicates with the VPN/FireWall Module using the VPN-1/FireWall-1 Session Authentication Agent Protocol. The Session Authentication Agent can be running on the following network objects:

- the source of the connection (i.e., the client that initiated the connection)
- the destination of the connection
- a specific host

## Session Authentication — Deployment

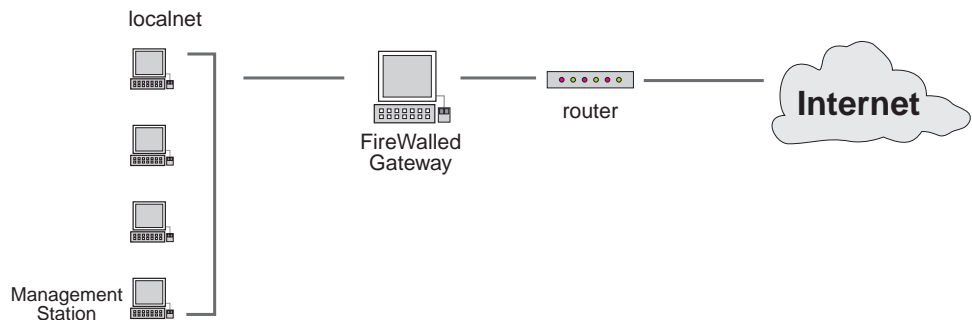
This section describes a deployment example for Session Authentication. This example consists of the following:

- an example network configuration
- what the Security Administrator must define in the VPN-1/FireWall-1 Rule Base
- what the user must do to authenticate

This example is not intended as a set of step by step instructions, but rather to illustrate how and where different components of Session Authentication are configured in the VPN-1/FireWall-1 GUI.

### Example Configuration

In the configuration depicted in (FIGURE 15-23), all localnet users must be authenticated before accessing the Internet.



**FIGURE 15-23** Example configuration

The following rule allows users of any service external access after successful Session Authentication.

| Source              | Destination | Service | Action       | Track | Install On |
|---------------------|-------------|---------|--------------|-------|------------|
| All Users@Local_Net | Any         | Any     | Session Auth | Short | Gateways   |

**FIGURE 15-24** Example Session Authentication Rule

### Defining Session Authentication

To enable Session Authentication for this configuration, you must do the following:

- install and configure the Session Authentication Agent
- pre-configure the Session Authentication Agent for distribution to multiple users, if desired
- configure Session Authentication for encryption, if desired
- define Session Authentication action properties
- define logging and tracking

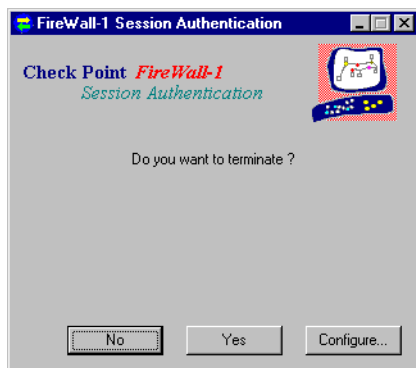
## Installing and Configuring the Session Authentication Agent

### Windows

To install the Session Authentication agent for Windows, run the `SETUP` program in the `DESKTOP PRODUCTS\SESSIONAGENT` directory on the CD-ROM.

### Opening the Session Authentication Agent

To open the Session Authentication agent, double-click on its icon in the system tray. The **FireWall-1 Session Authentication** window (FIGURE 15-25) is displayed.



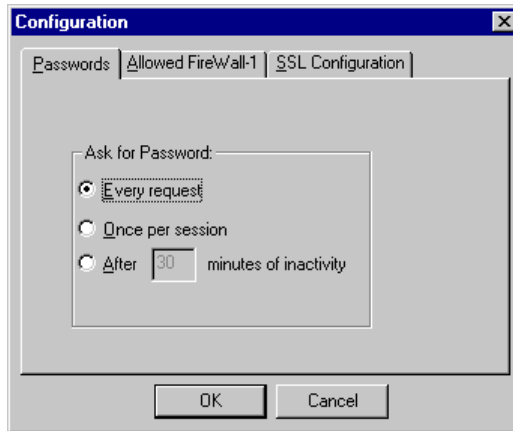
**FIGURE 15-25** FireWall-1 Session Authentication window

Perform one of the following:

- To terminate the Session Authentication agent, click on **Yes**.
- To configure the Session Authentication agent, click on **Configure**.
- To close the **FireWall-1 Session Authentication** window, click on **No**.

## Configuration

When you click on **Configure** in the **Session Authentication** window, the **Configuration** window (FIGURE 15-26) is displayed.



**FIGURE 15-26** Configuration window — Passwords tab

The **Configuration** window has three tabs, explained below.

### Passwords Tab

The **Passwords** tab of the **Configuration** window enables you to specify how frequently the user is asked to supply a password (that is, to authenticate himself or herself). One-time passwords (such as SecurID) cannot be cached.

Check one of the available choices:

**Every request** — The user will be prompted for the password each time the VPN/FireWall Module requests authentication.

Each time the user initiates a session to which a Session Authentication rule applies, the user will be prompted for a password. In this case, no password caching occurs.

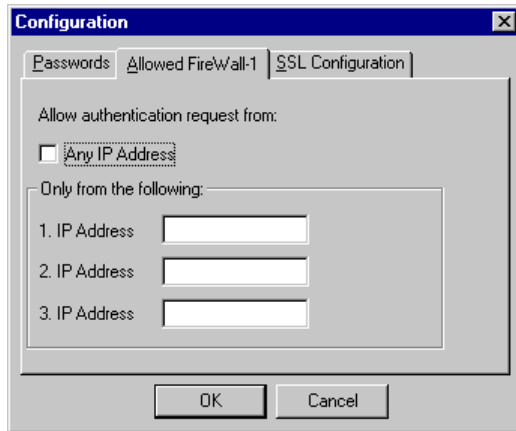
**Once per session** — The user will be prompted for a password once per Session Authentication agent session.

In this case, the user supplies the password once and the Session Authentication agent caches the password indefinitely. This option cannot be used with one-time passwords.

If the Session Authentication agent is terminated and then re-started, the user will have to supply the password again.

**After ... minutes of inactivity** — This option is the same as **Once per session**, except that the user will be prompted again for a password if there has been no authentication request for the specified time interval.

### Allowed FireWall-1 Tab



**FIGURE 15-27** Configuration window — Allowed FireWall-1 tab

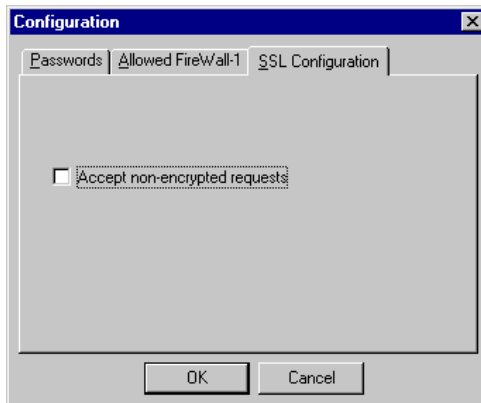
The **Allowed FireWall-1** tab of the **Configuration** window enables you to specify the VPN/FireWall Modules for which this Session Authentication agent may provide authentication services.

**Any IP Address** — This Session Authentication agent may provide authentication services for any VPN/FireWall Module.

**IP Address** — This Session Authentication agent may provide authentication services only for a VPN/FireWall Module running on the specified IP address.

You can specify up to three IP addresses.

### SSL Configuration Tab



**FIGURE 15-28** Configuration window — SSL Configuration tab



The **SSL Configuration** tab of the **Configuration** window (FIGURE 15-28) enables you to specify whether to accept Session Authentication requests from VPN/FireWall Modules that do not support SSL encryption.

Communication between the Session Authentication Agent and the VPN/FireWall Module can be encrypted using SSL. In this way, a user's name and password are not sent over the network unencrypted. For more information, see "Configuring Session Authentication with SSL" on page 521.

## Pre-configuration

The `SETUP.INI` file in the `DESKTOP PRODUCTS\SESSIONAGENT` directory enables you to pre-configure the Session Authentication agent. This feature is useful if you plan to distribute the Session Authentication agent to many users and you do not want them to configure the agent themselves.

The file is in the standard `.INI` format. It is divided into sections, each of which consists of a list of parameters and their values (FIGURE 15-29FIGURE 15-29).

```
[FireWall]
IPAddress=
Any=FALSE
[Cache]
Method=Every time
Timeout=30
```

**FIGURE 15-29** `SETUP.INI` file

The Session Authentication agent for Windows included with VPN-1/FireWall-1 provides for password caching and for restricting authentication to specific FireWalls.

When you start the Session Authentication agent, it is minimized and its icon appears in the system tray. From this point on, one of two things can happen:

- The user can open the Session Authentication agent and configure it.
- The Session Authentication agent can receive an authentication request from a VPN/FireWall Module.

## Configuring Session Authentication with SSL

By default the user's name and password are sent over the network unencrypted. To ensure security with fixed passwords, such as O/S passwords or VPN-1/FireWall-1 Passwords, Session Authentication communications can be encrypted using SSL.

To use Session Authentication with SSL, you must modify the following:

- VPN-1/FireWall-1 `objects.C` configuration file
- Session Authentication Agent configuration

Modifying the VPN-1/FireWall-1 Configuration

- 1 On the Management Station, issue the `fwstop` command.
- 2 Modify the file `$FWDIR/conf/objects.C` as follows:  
under the line that includes the token `:props (`  
add one of the following lines:

```
:snauth_protocol ("none")
```

```
:snauth_protocol ("ssl")
```

```
:snauth_protocol ("ssl + none")
```

The `ssl` option in the `:snauth_protocol` line specifies how to encrypt communications with the Session Authentication agent. TABLE 15-8 explains each option.

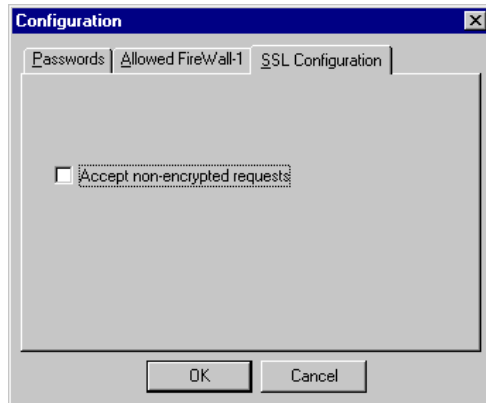
TABLE 15-8 SSL options

| option   | explanation                                                                                                                                             |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| none     | communication with the Session Authentication agent is not encrypted                                                                                    |
| ssl      | activate SSL on all Session Authentication agents. Previous versions of the Session Authentication agent will <i>not</i> be able to authenticate users. |
| ssl+none | activate SSL on all Session Authentication agents. Previous versions of the Session Authentication agent will be able to authentication users.          |

- 3 On the Management Station, issue the `fwstart` command.
- 4 Reinstall the Security Policy.

## Modifying the Session Authentication Agent Configuration

The **SSL Configuration** tab of the **Configuration** window (FIGURE 15-28) enables you to specify whether to accept Session Authentication requests from VPN/FireWall Modules that do not support SSL encryption (For example, version 3.0 modules).



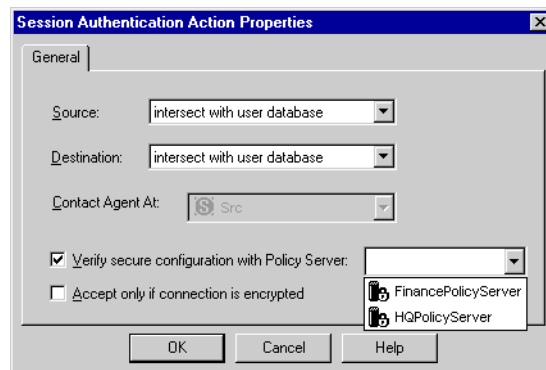
**FIGURE 15-30** SSL Configuration Tab — Session Authentication Agent

When an agent is configured to support SSL, a lock icon appears on the screen after the SSL encryption channel is set to indicate that user parameters are sent encrypted

## Defining Session Authentication Action Properties

To display the **Session Authentication Action Properties** window (FIGURE 15-31) for a Session Authentication rule, double-click on the rule's **Action**.

In the **Session Authentication Action Properties** window, specify parameters that define Session Authentication for the rule.



**FIGURE 15-31** Session Authentication Action Authentication Properties window

**Source** — Reconcile **Source** in the rule with **Allowed Sources** in the **User Properties** window.

The **Allowed Sources** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access from the source address, while the rule may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

See “Example” on page 493 for more information.

**Destination** — Reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

The **Allowed Destinations** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access to the destination address, while the rule may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

See “Example” on page 493 for more information.

**Contact Agent At** — Select the computer on which the Session Authentication Agent for this rule is running.

- Choose **Src** to specify that the Session Authentication Agent on the session’s **Source** object will authenticate the session.

This is the most commonly used option.

- Choose **Dst** to specify that the Session Authentication Agent on the session’s **Destination** object will authenticate the session.

This option would normally be used for the X protocol.

- Choose one of the computers in the list to specify that the Session Authentication Agent that will authenticate this session is running on that computer. The computers displayed in the list are the network objects defined as machines (both internal and external).

This option enables an administrator to manually authorize connections.

**Verify secure configuration with Policy Server** — Apply the rule only if the SecureClient is properly configured.

Select a Policy Server from the drop-down list. A misconfigured SecureClient is denied access under the rule. The configuration components verified are the components checked in the **Desktop Security** tab of the **Properties Setup** window.

**Accept only if connection is encrypted** — Apply the rule only if the connection is encrypted, in other words, only if the source is a SecureClient machine.

## Defining Logging and Tracking

Logging and tracking is specified in two places for Session Authentication:

- **Authentication Failure Track** in the **Authentication** tab of the **Properties Setup** window (FIGURE 15-9 on page 490)

The options under **Authentication Failure Track** specify the action to take for failed authentication. These options apply to all rules.

- **Rule Base Track**

The tracking for a successful Authentication attempt is determined by the **Track** field of the applied Session Authentication rule.

## How the User Authenticates

When a local user in the rule depicted in FIGURE 15-24 on page 517 initiates a connection to the Internet, the VPN/FireWall Module on the gateway intercepts the connection and requests that the Session Authentication agent authenticate a user. The Session Authentication agent displays the **Session Authentication** window (FIGURE 15-32).



**FIGURE 15-32** Session Authentication window — user prompt

The user enters his or her user name, and is then prompted to enter a password (FIGURE 15-33).



**FIGURE 15-33** Session Authentication window — password prompt

The form of the password prompt depends on the user’s Authentication method.

# Client Authentication

## In This Section

|                                                        |                 |
|--------------------------------------------------------|-----------------|
| <i>Client Authentication — Overview</i>                | <i>page 526</i> |
| <i>Client Authentication — Deployment</i>              | <i>page 531</i> |
| <i>Client Authentication — Examples</i>                | <i>page 545</i> |
| <i>Encrypted Client Authentication</i>                 | <i>page 553</i> |
| <i>Client Authentication — Security Considerations</i> | <i>page 553</i> |
| <i>Client Authentication — Additional Features</i>     | <i>page 554</i> |

## Client Authentication — Overview

Client Authentication allows connections from a specific IP address after successful authentication. In contrast to User Authentication, which allows access per user, Client Authentication allows access per IP address. The user working on a client performs the authentication by providing a name and password, but it is the client that is granted access.

Client Authentication is less secure than User Authentication because it allows multiple users and connections from the authorized IP address or host. The authorization is per machine, because the supported services do not have an initial login procedure. For example, if FINGER is authorized for a client machine, then all users on the client are authorized to use FINGER, and will not be asked to supply a password during the authorization period. For this reason, Client Authentication is best enabled for single user machines.

The advantage of Client Authentication is that it can be used for any number of connections, for any service and the authentication is valid for any length of time.

Consider the following rules:

| Security Policy   Address Translation |             |             |         |             |       |            |
|---------------------------------------|-------------|-------------|---------|-------------|-------|------------|
| No.                                   | Source      | Destination | Service | Action      | Track | Install On |
| 1                                     | Sales@Tower | DbaseHost   | Lotus   | Client Auth | Long  | Gateways   |
| 2                                     | Any         | DbaseHost   | Lotus   | reject      | Alert | Gateways   |
| 3                                     | Any         | Any         | Any     | reject      | Long  | Gateways   |

**FIGURE 15-34** Example Client Authentication Rule Base

In the example rules shown in FIGURE 15-34, the first rule specifies Client Authentication for lotus service connections whose destination is a database server. The **Source** of a Client Authentication rule indicates the group of users that can authenticate, and the host or hosts from which they can authenticate. A user is authenticated according to the scheme defined in the **Authentication** tab of his or her **User Properties** window.

Unauthorized attempts to use the lotus service on the database host will be detected by the second rule, and an alert will be issued.

Administrators can also define authorization periods and the number of permitted sessions. For example, a user working on Tower can sign on and authenticate at the start of the day and remotely access the database host throughout the day. At the end of the day, the user signs off and closes the connection with the database host.

## Sign On Methods

Sign On methods specify how a user begins a Client Authentication session. Sign On methods are specified in the **Client Authentication Action Properties** window of a rule. There are four Sign On methods:

### ■ Manual Sign On

The Manual Sign On method requires a user to initiate the Client Authentication session on the gateway. Manual Sign On is not transparent, because the user must first connect to the gateway. The user may initiate the Client Authentication session in one of the following ways:

- **TELNET session** — the user starts a TELNET session on port 259 of the gateway
- **Web Browser** — the user requests an HTTP connection to port 900 on the gateway using a Web browser.

VPN-1/FireWall-1 also supports encrypted Client Authentication through a Web browser. This feature is available for HTTPS (HTTP encrypted by SSL) only. The user can request an HTTPS connection to a specific port on the gateway. For more information on configuring the gateway to support HTTPS, see “Encrypted Client Authentication” on page 553.

For examples using Manual Sign On, see “Manual Sign On Method” on page 545.

#### ■ **Partially Automatic Sign On**

Partially Automatic Sign On provides transparent Client Authentication for authenticated services (HTTP, TELNET, RLOGIN, and FTP). A user working with one of these services can directly request the target host. The user is then prompted and signed on through the User Authentication mechanism. If authentication is successful, access is granted from the IP address from which the user initiated the connection. The disadvantage of using this method is that it is available only for authenticated services.

For an example using Partially Automatic Sign On, see “Partially Automatic Sign On Method” on page 549.

Also see “HTTP Requests — Redirection According to Host Header” on page 554.



## ■ Fully Automatic Sign On

Fully Automatic Sign On provides transparent Client Authentication for all services. A user working with any service directly requests the target server. Users of authenticated services are signed on through the User Authentication mechanism, while users working with all other services are signed-on using the VPN-1/FireWall-1 Session Authentication Agent. If authentication is successful, access is granted from the IP address that initiated the connection.

Fully Automatic Sign On is available for all services, but requires a VPN-1/FireWall-1 Session Authentication Agent on the client in order to handle non-authenticated services.

It is recommended to use Fully Automatic Sign On only if you know users have the Session Authentication Agent installed on their machines. If users do not have the Session Authentication Agent, it is recommended to use the Partially Automatic sign on method. This at least allows users of authenticated services to open a Client Authentication session on the target host without having to connect to the gateway first.

For an example using Fully Automatic Sign On, see “Fully Automatic Sign On Method” on page 550.

For more information on the VPN-1/FireWall-1 Session Authentication Agent, see “Session Authentication” on page 515.

Also see “HTTP Requests — Redirection According to Host Header” on page 554.

## ■ Agent Automatic Sign On

Agent Automatic Sign On provides transparent Client Authentication for all services. Users are signed on through the VPN-1/FireWall-1 Session Authentication Agent. If authentication is successful, access is granted from the IP address that initiated the connection.

Agent Automatic Sign On requires that a VPN-1/FireWall-1 Session Authentication Agent be installed on each client.

If users do not have the Session Authentication Agent, it is recommended to use the Partially Automatic sign on method. This at least allows users of authenticated services to open a Client Authentication session on the target host without having to connect to the gateway first.

For an example using Agent Automatic Sign On, see “Agent Automatic Sign On Method” on page 551.

For more information on the VPN-1/FireWall-1 Session Authentication Agent, see “Session Authentication” on page 515.

■ **Single Sign On**

Single Sign On is enabled through integration with Meta IP. This is Check Point's address management feature which provides transparent network access. In this method, the VPN-1/FireWall-1 consults the user IP address records to determine which user is logged on at a given IP address. For more information see "Integration with Meta IP" on page 543.

For more information, see "Single Sign On — Additional Features" on page 542.

For an example using Single Sign On, see "Single Sign On Method" on page 552.

Partially and Fully Automatic Client Authentication rules allow users if they authenticate successfully, but do not necessarily reject the connection if the user fails authentication. In addition, the fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. This is because if the service is an authenticated service, the appropriate Security Server is invoked. The authenticating Security Server first checks if the connection can be allowed by a rule which does not require authentication. For more information, see "The 'Insufficient Information' Problem" on page 344.

**How Services are Authorized**

After successful authentication, the user can work with the services and hosts permitted by the rule, depending on the rule's authorization parameters. The **General** tab of the rule's **Client Authentication Action Properties** window specifies how the user works with the services permitted by the rule, as follows:

■ **Standard Sign On**

Standard Sign On enables the user on the client machine to use all the services permitted by the rule for the authorization period without having to perform authentication for each service.

■ **Specific Sign On**

With Specific Sign On, only connections that match the original connection are allowed without additional authentication. If a rule specifies more than one service or host, the user on the client must reauthenticate for each service or host. Specific Sign On enables you to limit access to services and target hosts.

For example, consider the following Partially Automatic Sign On rule:

| Source      | Destination | Services      | Action      | Track    | Install On |
|-------------|-------------|---------------|-------------|----------|------------|
| Sales@Tower | BigBen      | ftp<br>rlogin | Client Auth | Long Log | Gateways   |

Suppose a user on Tower initiates an FTP session on BigBen and is successfully authenticated. The user can now work with FTP on BigBen for the specified authorization period without having to reauthenticate for each FTP connection. If the

user on Tower closes the initial FTP session, and decides to initiate a new FTP session (within the authorized time period) to download additional files, he or she does not have to reauthenticate.

If the same user initiates an RLOGIN session to BigBen, he or she will have to reauthenticate if **Specific Sign On** is required. If **Standard Sign On** is required, then the user will not have to reauthenticate in order to use RLOGIN.

For more information, see “Defining Client Authentication Action Properties” on page 534.

## Client Authentication — Deployment

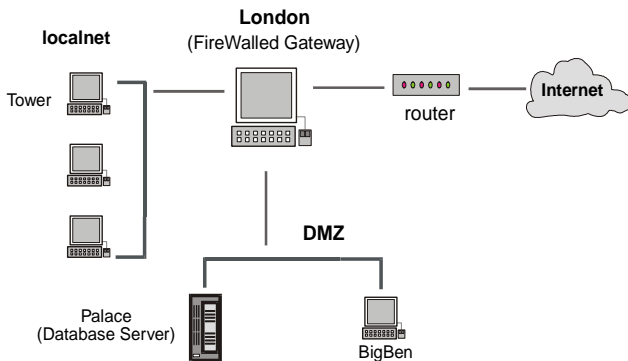
This section describes a deployment example for Client Authentication. This example consists of the following:

- an example network configuration
- what the Security Administrator must define in the VPN-1/FireWall-1 Rule Base

This example is not intended as a set of step by step instructions, but rather to illustrate how and where different components of Client Authentication are configured in the VPN-1/FireWall-1 GUI.

### Example Configuration

FIGURE 15-35 depicts a configuration in which a FireWalled gateway (London) protects a PC network (localnet) and a DMZ network, which includes a database server on the host Palace.



**FIGURE 15-35** Example configuration — Client Authentication

A group of users in the QA department requires frequent access to the database on Palace. Access to Palace is allowed from localnet hosts. Each user can sign on at the beginning of the day and can use the service for a specified time period and number of sessions. If a user forgets to sign off, the connection to Palace is timed out at end of authorization period.

Access to the database server from QA users on Tower is enabled by the following rule:

| No. | Source       | Destination | Service | Action      | Track | Install On |
|-----|--------------|-------------|---------|-------------|-------|------------|
| 1   | QA@Local_Net | Palace      | Lotus   | Client Auth | Long  | Gateways   |

FIGURE 15-36 Example Client Authentication rule

Defining Client Authentication

To enable Client Authentication for this configuration, you must define the following:

- the users who must authenticate before accessing the target server
- the gateway’s supported authentication schemes
- Client Authentication rule properties
- Client Authentication properties that apply to all rules (i.e., tracking for unsuccessful authentication)
- logging and tracking

Defining User Properties

In a Client Authentication rule, the **Source** must be a user group. You must first define the properties of the permitted users, such as their authentication schemes and the network objects from which they are allowed access. These properties are defined in the tabs of the **User Properties** window.

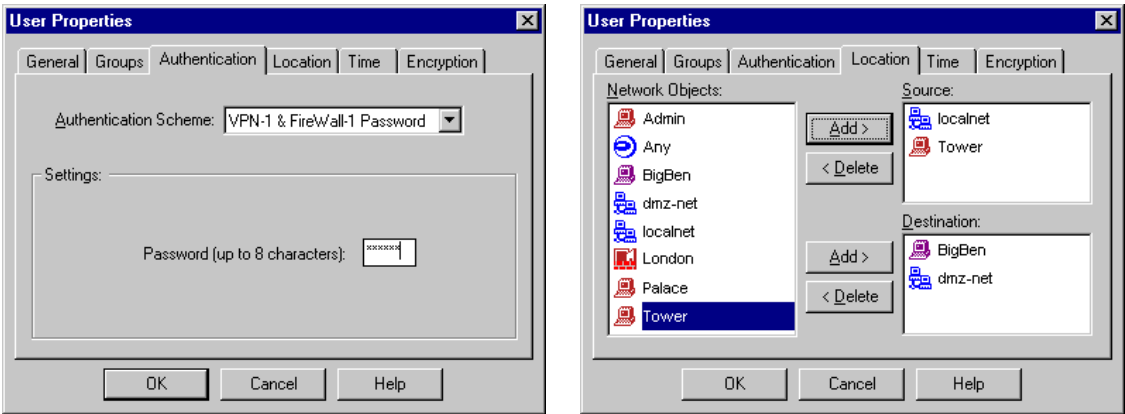
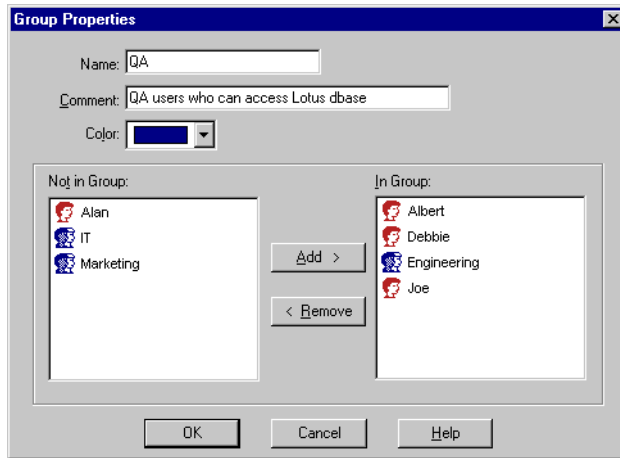


FIGURE 15-37 User Properties window - Authentication tab and Location tab

You must then define a group which includes the users who must authenticate before they access the database server.



**FIGURE 15-38** Group Properties window — Defining Permitted Users

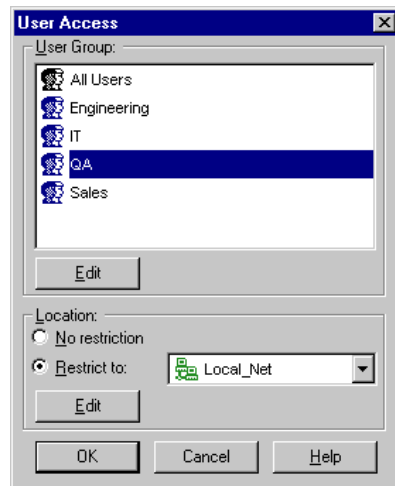
For more information on defining users, see Chapter 5, “Managing Users.”

## Defining User Access

The **Source** field also specifies the host or network object from which the user group is allowed access.

You can add a user group to a rule using the **User Access** window, as follows:

- 1** To display the **User Access** window, right-click on the rule’s **Source**, and choose **Add User Access** from the drop-down menu.



**FIGURE 15-39** User Access window

- 2 Click on the user group you want to add.
- 3 Using the options under **Location**, specify the objects from which the users in the selected group are allowed access.

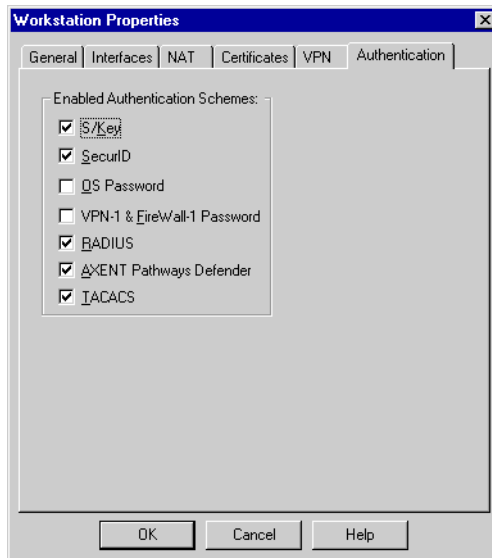
If you choose **No Restriction**, then the users will be allowed access from any source.

If you choose **Restrict To**, you must then select the network object from which the users will be allowed access.

In the example depicted in FIGURE 15-39, users in the QA group will be allowed access only from the Local\_Net hosts.

## Defining the Gateway's Authentication Schemes

The gateway must support the same authentication schemes you defined for your users. Gateway authentication schemes are defined in the **Authentication** tab of the gateway object's **Workstation Properties** window.



**FIGURE 15-40** Workstation Properties window — Authentication tab

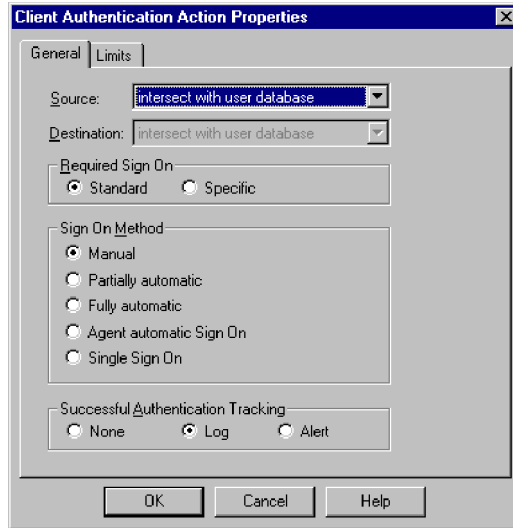
## Defining Client Authentication Action Properties

You must define the Client Authentication properties of the enabling rule. These properties are defined in the tabs of the **Client Authentication Action Properties** window, and include the following:

- how allowed sources and destinations should be reconciled
- how services are authorized
- how authentication is initiated
- tracking for successful authentication

- authorization timeout periods
- the number of sessions allowed

To display the **Client Authentication Action Properties** window, double-click on the rule's **Action**.



**FIGURE 15-41** Client Authentication Action Properties window — General tab

#### Reconciling Allowed Sources and Destinations

**Source** — Reconcile **Source** in the rule with **Allowed Sources** in **User Properties** window (**Location** tab).

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

For the configuration depicted in FIGURE 15-35 on page 531, if the **Location** tab of a QA user allowed access only from Thames on localnet, you would choose **Ignore User Database** to allow that user access from Tower, the allowed **Source** in the rule.

See “Example” on page 493 for more information.

**Destination** — Reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.

- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

See “Example” on page 493 for more information.



**Note** – If **Standard Sign On** is specified in **Rule Requires** then this option is automatically set to **Ignore User Database** because, under Standard Sign On, the user can access all the destinations allowed by the rule. You can change this setting only if you specify **Specific Sign On** (see FIGURE 15-41 on page 535).

How services are authorized

**Required Sign On** — Specify how the services permitted by the rule are authorized by selecting one of the following values:

- **Standard Sign On** — All the services allowed for the user are authorized together. For an example of how Standard Sign On is used, see “Example — Standard Sign On” on page 547.
- **Specific Sign On** — The user must request each service and destination individually. For example, if a rule specifies more than one service, then each service must be authorized separately. For an example of how Specific Sign On is used, see “Example — Specific Sign On” on page 548.

How Client Authentication is initiated

**Sign On Method** — Specify the sign on method by selecting one of the following values:

- **Manual** — The user must initiate Client Authentication on the gateway through either a TELNET session on port 259 or an HTTP session on port 900.

For an example using Manual Sign On with TELNET, see “Example—Manual Sign On Using TELNET” on page 545.

For an example using Manual Sign On through a Web browser (HTTP), see “Example—Manual Sign On Using HTTP” on page 549.

- **Partially Automatic** — If a connection matches the rule, and the service is an authenticated service (RLOGIN, TELNET, HTTP, FTP), the user is signed on through User Authentication.

For an example using Partially Automatic Sign On, see “Partially Automatic Sign On Method” on page 549.

- **Fully Automatic** — If a connection using a non-authenticated service matches the rule, and the VPN-1/FireWall-1 Session Authentication Agent is installed on the client, the user is signed on by the Session Authentication Agent. If a connection using an authenticated service matches the rule, then the user is signed on through User Authentication.

For an example using Fully Automatic Sign On, see “Fully Automatic Sign On Method” on page 550.



- **Agent automatic Sign On** — If a connection matches the rule, and the VPN-1/FireWall-1 Session Authentication Agent is installed on the client, the user is signed on by the Session Authentication Agent.

For an example using Agent Automatic Sign On, see “Agent Automatic Sign On Method” on page 551.

- **Single Sign On** — If a connection matches the rule, then VPN-1/FireWall-1 sends a query to the UAM server with the source IP. In return, the UAM Server sends VPN-1/FireWall-1 the user name that is registered to the source IP. If the user name is authenticated by VPN-1/FireWall-1, then the user connection is allowed to continue.

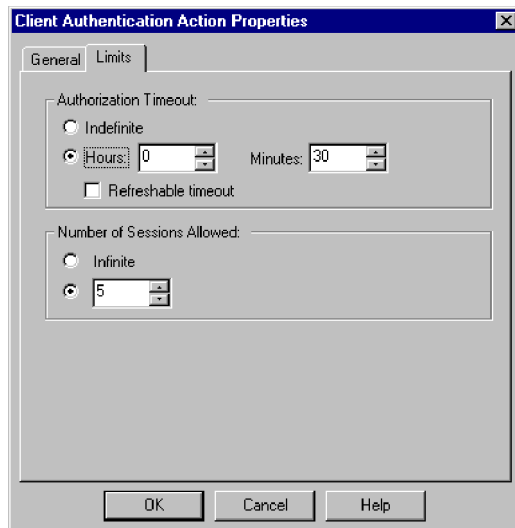
### Tracking

**Successful Authentication Tracking** — logging option for the sign on session. Choose one of the following:

- **None** — no tracking
- **Log** — Long Log
- **Alert** — the **Authentication Alert Command** in the **Log and Alert** tab of the **Properties Setup** window

These settings specify logging and tracking for the sign on session only. For information on additional logging and tracking parameters for Client Authentication, see “Defining Logging and Tracking” on page 540.

The **Limits** tab of the **Client Authentication Action Properties** window specifies the period during which the user is authorized to work with permitted services, and how many sessions are allowed.



**FIGURE 15-42** Client Authentication Action Properties window — Limits tab

## Authorization Timeout Periods

**Authorization Timeout** — Specifies the length of time after the client is authenticated during which the user (at the source IP address specified under **Source** in the relevant rule in the Rule Base) may start the specified service.

Once the service is started, there is no restriction on how long it can remain open.

If you do not wish to restrict the authorization timeout period, check **Indefinite**.

**Refreshable Timeout** — the **Authorization Timeout** period is reset with every new connection authorized by the rule.

This option is useful if the user remains at the authorized client after successful authentication. For example, suppose that the **Authorization Timeout** is set to 15 minutes, **Refreshable Timeout** is checked, and the service allowed by the rule is FINGER. Then, a user who initiates a FINGER connection after 10 minutes resets the authorization period to 15 minutes.

If **Refreshable Timeout** is not checked, and the user does not start a FINGER connection during the 15-minute authorization timeout period, the session times out and the user must reauthenticate.

See also “Timeouts” on page 553.

## Number of Sessions Allowed

**Sessions Allowed** — the number of sessions (connections) allowed after the authentication

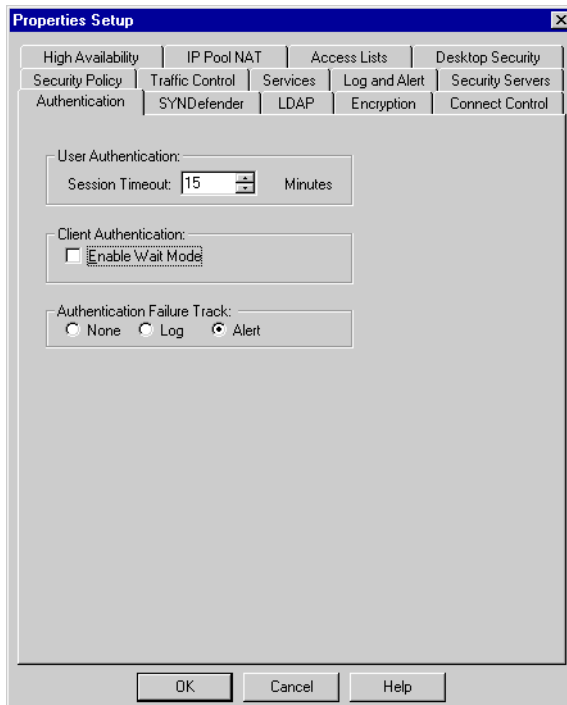
If you do not wish to restrict the number of sessions, check **Infinite**.

If the rule specifies a service group, and **Sessions Allowed** is not set to **Infinite**, then the number of sessions allowed for the services in the group depends on what is specified under **Required Sign On** in the **General** tab of the **Client Authentication Action Properties** window:

- If **Specific Sign On** is used, then each service in the group will be allowed the number of sessions specified. For example, if **Sessions Allowed** is set to **2**, and the service group consists of FINGER and RSTAT, then each service will be allowed two sessions.
- If **Standard Sign On** is used, then the number of sessions applies to all the services in the group together.

## Defining Client Authentication Properties for all Rules

The **Authentication** tab of the **Properties Setup** window specifies Client Authentication parameters that apply to all rules. To display this window, choose **Properties** from the **Policy** menu.



**FIGURE 15-43** Properties Setup window — Authentication tab

**Enable Wait Mode** — This option applies only when the user initiates Client Authentication through a TELNET session to port 259 on the gateway. For information on using TELNET to initiate Client Authentication, see “Example—Manual Sign On Using TELNET” on page 545.

If **Enable Wait Mode** is checked, the initial TELNET session remains open. The Client Authentication session is closed when the TELNET session is closed or timed out. VPN-1/FireWall-1 regularly pings the client during the authorization period. If for some reason the client machine has suddenly stopped running (for example, because of a power failure), VPN-1/FireWall-1 closes the TELNET session and Client Authentication privileges from this IP address are withdrawn.



**Note – Enable Wait Mode** works only with Client Authentication rules which specify **Standard Sign On**. If you select **Enable Wait Mode**, Client Authentication rules which require **Specific Sign On** are not applied.

If **Enable Wait Mode** is not checked, the initial TELNET session is automatically closed when the user chooses **Standard Sign On** or **Specific Sign On**. The user must initiate another TELNET session to the gateway in order to sign off the Client Authentication session..



**Note** – The VPN/FireWall Module monitors the connection by pinging the user's host. You should define rules to allow the ping as follows:

- Allow the echo-request service from the VPN/FireWall Module to the user's host.
- Allow the echo-reply service from the user's host to the VPN/FireWall Module.

**Authentication Failure Track** — these options specify tracking for unsuccessful authentication attempts. These tracking options apply to all rules.

## Defining Logging and Tracking

There are three places in which logging and tracking for Client Authentication is specified:

### 1 Rule Base Editor — **Track**

The tracking in this window applies to the initial communication attempt to the gateway for the authentication, and to the authenticated session.

### 2 **Authentication** tab of the **Properties Setup** window — **Authentication Failure Track** (FIGURE 15-43 on page 539)

The tracking in this window applies to all authentication failures.

### 3 The **General** tab of the **Client Authentication Action Properties** window — **Successful Authentication Track** (FIGURE 15-41 on page 535)

The tracking in this window applies to successful authentications.

#### Example 1

Suppose that a Manual Sign On rule specifies **Client Authentication** for the user group **QA@Tower**. Next suppose that a QA user logs in to the gateway and attempts to initiate a TELNET session under the rule.

- The tracking for the login attempt to the gateway is determined by the entry in the Rule Base **Track** for that rule.
- If the user is successfully authenticated, then the tracking for the successful authentication attempt is determined by the entry in the rule's **Client Authentication Action Properties** window.
- If the user fails the authentication, the tracking is determined by the entry in the **Authentication** tab of the **Properties Setup** window.

Example 2

Consider the following rule:

| Source                                                                                         | Destination                                                                              | Service                                                                                  | Action                                                                                        | Track                                                                                   | Install On                                                                                   |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|  QA@Local_Net |  Palace |  finger |  Client Auth |  Short |  Gateways |

Suppose a user wishes to start a Client Authentication session for the FINGER service on the host Palace. The target host is behind the London FireWalled gateway. The **Manual Sign On** method is specified in the **General** tab of the rule's **Client Authentication Action Properties** window.

First, the user attempts to TELNET to the gateway (London) by typing:

```
telnet london 259
```

The logging in effect for this step is defined in the **Track** column of the rule in the Rule Base that controls this user's ability to access TCP port 259 on London.

Next, the user is asked to specify the user name, password, and optionally host name and service.

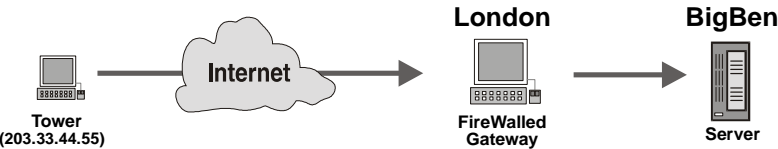
If the user is successfully authenticated, then the tracking for the successful authentication attempt is determined by the entry in the **General** tab of the rule's **Client Authentication Action Properties** window. The user then starts a FINGER session on the target server. The tracking for the FINGER session is determined by the **Track** column of the above rule.

If the user fails the authentication, the tracking is determined by the entry in the **Authentication** tab of the **Properties Setup** window.

## Single Sign On — Additional Features

### Single Sign On on Behalf of Multiple Users

The **Single Sign On** method for Client Authentication enables a privileged user to sign on and sign off on behalf of other users. The privileged user does not necessarily have to be a person, but can also be an application that enables special access privileges to users based on data in its own database. Consider the following configuration and Rule Base.



**FIGURE 15-44** Single Sign On Extension.

| Source        | Destination | Services    | Action      | Track    | Install On |
|---------------|-------------|-------------|-------------|----------|------------|
| All_Users@Any | BigBen      | telnet, ftp | Client Auth | Long Log | Gateways   |

A user on Tower would, in the usual case, TELNET to port 259 on London and authenticate himself or herself, and then request access to BigBen. With the Single Sign On System Extension, another user can open the connection to BigBen in advance on behalf of a user on Tower.

The system administrator must define a user named `sso-root`. `sso-root` must be given Client Authenticated TELNET access to London. `sso-root` can then open and close connections on behalf of other users as follows:

- 1 `sso-root` TELNETs to port 259 on London and authenticates himself (or herself).  
It makes no difference from which machine `sso-root` TELNETs to London.
- 2 After the authentication is successful, the following prompt appears:

```
[real-name@]real source:
```

This prompt only appears for `sso-root`.

- 3** sso-root now enters the name and client of another user for whom access is to be allowed, for example:

```
[real-name@]real source:lisa@tower
```

or

```
[real-name@]real source:lisa@203.33.44.55
```

- 4** Next, sso-root must choose (on behalf of lisa):

```
Choose:
(1) Standard Sign On
(2) Sign Off
(3) Specific Sign On
```

- 5** From this point on, lisa on the host tower (IP address 203.33.44.55) can TELNET or FTP to BigBen (under the rule shown above) without having to first authenticate herself on London.

If sso-root had entered only the client name (in step 3 above), then all users on tower with open Client Authenticated sessions would have been immediately signed off.

## Integration with Meta IP

Integration with Meta IP Check Point's address management feature enables transparent single sign on for network access. The UAM service of Meta IP captures Windows NT login information and dynamically assigns an IP address and a user-IP address record is created.

The SSO feature is enabled through Client Authentication rules. Instead of the user needing to authenticate to the VPN-1/FireWall-1 Client Authentication daemon, VPN-1/FireWall-1 can consult user-IP address records to determine which user is logged on at a given IP address.



**Warning** – All user names must be defined in VPN-1/FireWall-1 in capital letters, unless the following line `clauth_tolower_users (true)` is added to Objects.C in the FireWall directory.

## How it Works

Step A: Client Machine Boots

- 1** The client machine uses DHCP to obtain an IP address.

- 2 The MetaIP DHCP Server, after leasing an IP address for the client, sends a UAT record to the UAM server reporting the lease information.

Step B: The User Logs On

- 1 The user logs in to the Windows NT Domain Controller.
- 2 The MetaIP UAT module at the Domain Controller intercepts the logon event and sends a UAT record to the UAM server reporting the logon information.
- 3 The UAM server matches that logon record with the previously recorded lease record, creating a valid user-IP record.

Step C: The User Connects to the Internet

- 1 The user tries to access the Internet through VPN-1/FireWall-1.
- 2 VPN-1/FireWall-1 intercepts the packet and based on the Security Policy matches the packet with a UAM-enabled rule.
- 3 VPN-1/FireWall-1 contacts the UAM server to get the user name that is logged on at the source IP address of the connection. The user is then matched to the Rule Base, and the packet is released if it is allowed.

## Platform Limitations

This feature is available for VPN/FireWall Modules running on Windows NT only. If you try to use the feature on a Unix VPN/FireWall Module, you will receive error messages on your console.

## Activating the Feature

Installing MetaIP (refer to the MetaIP Installation instructions)

- 1 Install the Check Point MetaIP Product, including MetaIP DNS and MetaIP DHCP Server.
- 2 Install the MetaIP UAT Module on the VPN/FireWall Module machine.
- 3 Install the MetaIP UAT Module on all the Windows NT Domain Controllers.

On the VPN/FireWall Module

- 1 Stop VPN-1/FireWall-1.
- 2 Install the file fwuam.dll under C:\WINNT\System32.
- 3 Start VPN-1/FireWall-1.

On the Management Station

- 1 Stop VPN-1/FireWall-1.
- 2 In %FWDIR%\lib\fwui\_head.def (C:\WINNT\FW\lib\fwui\_head.def in Windows NT), uncomment line number 67 - “#define HAS\_SSO 1”



- 3 In `$FWDIR\lib\setup.C`, add the line “`:has_sso (true)`” as the second line in the file.
- 4 Start VPN-1/FireWall-1.
- 5 Define a rule with action Client Authentication.
- 6 In the **Client Authentication Rule Properties** window of the rule, specify **Single Sign On** as the sign on method.
- 7 Install the Security Policy.

## Client Authentication — Examples

This section contains examples of the different Sign On methods:

- Manual Sign On
- Partially Automatic Sign On
- Fully Automatic Sign On
- Agent Automatic Sign On
- Single Sign On

For a general overview, see “Sign On Methods” on page 527.

### Manual Sign On Method

The Manual Sign On method requires a user to initiate the Client Authentication on the gateway. The user may initiate Client Authentication by requesting a TELNET connection or an HTTP connection to the gateway.

#### Example—Manual Sign On Using TELNET

The rule depicted in FIGURE 15-45 allows Engineering users on a single host, Tower, access to the hosts Palace or Thames after successful Client Authentication. Palace is protected by London, a FireWalled gateway.

| Source                                                                                                | Destination                                                                                                                                                                              | Service                                                                                                                                                                                 | Action                                                                                          | Track                                                                                    | Install On                                                                                    |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|  Engineering@Tower |  Palace<br> Thames |  rstat<br> finger |  Client Auth |  Long |  Gateway |

**FIGURE 15-45** Client Authentication Rule

An Engineering user wishing to access the destination hosts must first TELNET to London, the gateway:

```
telnet london 259
```

The user is then prompted for the following data:

- user name

- password

Next, the user is asked to choose:

Choose:

- (1) Standard Sign On
- (2) Sign Off
- (3) Specific Sign On

If there is at least one matching rule that specifies **Standard Sign On** in the **Rule Requires** field of the **Rule Client Authentication Properties** window (FIGURE 15-41 on page 535), then the user can choose **Standard Sign On** from this menu. Otherwise, the user may choose only **Specific Sign On** or **Sign Off**.

If the user chooses **Standard Sign On**, then the authentication is for all services on all destination hosts, as allowed by the relevant rule or rules. The number of relevant rules is displayed by the Security Server if the authentication is successful (see FIGURE 15-46 on page 547).

If the user chooses **Specific Sign On**, then the user is prompted for the service name and host name (FIGURE 15-47 on page 548).

If the user chooses **Sign Off**, then all permissions accorded to this IP address (the host from which the user initiated the session) are withdrawn and the session is terminated (see FIGURE 15-48 on page 549).



**Note** – When Client Authentication is defined, VPN-1/FireWall-1 adds an implicit rule allowing TELNET connections to the authorization port (default 259) on the gateway. It is not necessary for the system administrator to explicitly add such a rule to the Rule Base. At the same time, the system administrator should not block access by another rule.

Once this data has been entered, the user receives either an “authorized” or “unauthorized” message, and the TELNET session is automatically closed (if **Enable Wait Mode** is not checked in the **Authentication** tab of the **Properties Setup** window).

If **Enable Wait Mode** is checked in the **Authentication** tab of the **Properties Setup** window, the TELNET session remains open. Client Authentication privileges are withdrawn from this IP address only when the TELNET session is closed or timed out.

Timeout periods and sessions allowed depend on what is specified in the **Limits** tab of the rule’s **Client Authentication Action Properties** window:

- If the user is authorized, the client machine is allowed to use the service on the specified host for the period specified in **Authorization Timeout**, unless the user signs off earlier.
- The number of connections (sessions) allowed in the given time frame is determined by the **Sessions Allowed** parameter.

## Example — Standard Sign On

```
tower 1% telnet london 259
Trying 191.23.45.67 ...
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on london
Login: jim
FireWall-1 Password: *****
User authenticated by FireWall-1 auth.

Choose:
 (1) Standard Sign On
 (2) Sign Off
 (3) Specific Sign On

Enter your choice: 1

User authorized for standard services (1 rules)
Connection closed by foreign host.
```

**FIGURE 15-46** Client Authentication - Standard Sign On for all Services and Destinations Allowed Under Rule

## Example — Specific Sign On

```
tower 3% telnet london 259
Trying 191.23.45.67 ...
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on london
Login: jim
FireWall-1 Password: *****
User authenticated by Internal auth.

Choose:
 (1) Standard Sign On
 (2) Sign Off
 (3) Specific Sign On

Enter your choice: 3
Service: rstat
Host: palace
Client Authorized for service
Another one (Y/N): Y
Service: finger
Host: thames
Client Authorized for service
Another one (Y/N): n
Connection closed by foreign host.
```

**FIGURE 15-47** Client Authentication - Specific Sign On for two Services (Each One on a Different Host)

## Example — Sign Off

```

tower 2% telnet london 259
Trying 191.23.45.67 ...
Connected to London.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on London
Login: jim
FireWall-1 Password: *****
User authenticated by Internal auth.

Choose:
 (1) Standard Sign On
 (2) Sign Off
 (3) Specific Sign On

Enter your choice: 2

User was signed off from all services
Connection closed by foreign host.

```

**FIGURE 15-48** Client Authentication - Signing Off**Example—Manual Sign On Using HTTP**

A user can also initiate a Client Authenticated session by beginning an HTTP session on port 900 on the gateway. The requested URL must specify the gateway name and port as follows:

**FIGURE 15-49** HTTP session on port 900

The browser prompts the user for a name and password. The browser then presents HTML pages listing the Client Authentication options described in “Example—Manual Sign On Using TELNET” on page 545.



**Note** – When Client Authentication is defined, VPN-1/FireWall-1 adds an implicit rule allowing HTTP connections to the authorization port (default 900) on the gateway. It is not necessary for the system administrator to explicitly add such a rule to the Rule Base. At the same time, the system administrator should not block access by another rule.

**Partially Automatic Sign On Method**

Partially Automatic Sign On provides transparent Client Authentication for authenticated services including HTTP, TELNET, RLOGIN, and FTP. A user working with one of these services directly requests the target host. If a connection using one of these services matches a partially automatic Client Authentication rule, the user is

prompted and signed on through the User Authentication mechanism. If authentication is successful, access is granted from the IP address from which the user initiated the connection.

Suppose the following rule specifies **Partially Automatic Sign On** in the rule's **Client Authentication Action Properties** window (FIGURE 15-41 on page 535).

| Source      | Destination | Services | Action      | Track    | Install On |
|-------------|-------------|----------|-------------|----------|------------|
| Sales@Tower | BigBen      | ftp      | Client Auth | Long Log | Gateways   |

According to the above rule Jim, a Sales user at the host Tower can FTP directly to BigBen. The user on Tower is authenticated by the FTP Security Server on the London, the gateway.

```
tower # ftp bigben
Connected to london.
220 london CheckPoint FireWall-1 secure ftp server running on London
Name (bigben:jim): jimb
331-aftpd: FireWall-1 password: you can use password@FW-1-password
Password: <Unix password on bigben>@<FireWall-1 password>
230-aftpd: User jimb authenticated by FireWall-1 authentication.
230-aftpd: Connected to bigben. Logging in...
230-aftpd: 220 bigben ftp server (UNIX(r) System V Release 4.0)
ready.
230-aftpd: 331 Password required for jimb.
230 User jimb logged in.
```



**Note** – Although the user is authenticated by the Security Server, the connection is entered as a Client Authentication connection in the VPN-1/FireWall-1 connections table, and access is authorized from the IP address from which the user initiated the connection.

## Fully Automatic Sign On Method

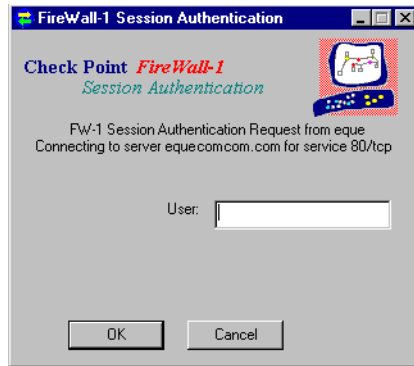
Suppose the following rule specifies **Fully Automatic Sign On** in the rule's **Client Authentication Action Properties** window (FIGURE 15-41 on page 535).

| Source      | Destination | Services | Action      | Track    | Install On |
|-------------|-------------|----------|-------------|----------|------------|
| Sales@Tower | BigBen      | any      | Client Auth | Long Log | Gateways   |

A user on Tower who initiates a connection to BigBen using any authenticated service is signed on through User Authentication. A user on Tower working with any other service, such as FINGER, is signed on through the VPN-1/FireWall-1 Session Authentication Agent (FIGURE 15-50).



**Note** – To enable Fully Automatic Sign On for non-authenticated services, the VPN-1/FireWall-1 Session Authentication Agent must be installed on the client.



**FIGURE 15-50** VPN-1/FireWall-1 Session Authentication Agent prompt

The user can work with services and destinations in the rule according to what is specified under **Required Sign On** in the **General** tab of the rule's **Client Authentication Action Properties** window (FIGURE 15-41 on page 535).

If **Standard Sign On** is specified, then the user can work with the all the services and destinations permitted by the rule without having to reauthenticate.

If **Specific Sign On** is specified, only connections which match the connection which opened the rule do not have to be reauthenticated.

The authorization period and the number of connections (sessions) allowed are specified in the **Limits** tab of the rule's **Client Authentication Action Properties** window.

## Agent Automatic Sign On Method

Suppose the following rule specifies **Agent automatic Sign On** in the rule's **Client Authentication Action Properties** window (FIGURE 15-41 on page 535).

| Source      | Destination | Services | Action      | Track    | Install On |
|-------------|-------------|----------|-------------|----------|------------|
| Sales@Tower | BigBen      | any      | Client Auth | Long Log | Gateways   |

Then, for any service, a user on Tower who initiates a connection to BigBen is signed on through the VPN-1/FireWall-1 Session Authentication Agent (FIGURE 15-50 on page 551).



**Note** – To enable Agent Automatic Sign On for non-authenticated services, the VPN-1/FireWall-1 Session Authentication Agent must be installed on the client.

## Single Sign On Method

Suppose an ISP wishes to make a special service available only to dial-up customers who have paid an additional fee. One way to accomplish this is as follows:

- 1** Define a rule allowing access to the service only after Client Authentication.

| Source        | Destination           | Services               | Action      | Track    | Install On |
|---------------|-----------------------|------------------------|-------------|----------|------------|
| All_Users@Any | <i>special server</i> | <i>special service</i> | Client Auth | Long Log | Gateways   |

- 2** After a customer dials in, gains access to the ISP and is assigned an IP address (presumably after some authentication procedure), a user-written application determines whether the customer is authorized to use the special service.
- 3** If the customer is authorized to use the special service, a user-written application TELNETs to port 259 on the FireWall and authenticates itself as follows:

| parameter                | value                                    |
|--------------------------|------------------------------------------|
| user                     | sso-root                                 |
| password                 | sso-root's password                      |
| [real-name@]real source: | customer@dynamically-assigned IP address |

From this point on, the customer can access the special service without undergoing any additional authentication procedures.

- 4** When the customer logs off from the ISP (or if the dial-up connection drops), the user-written application signs the client off.

The user-written application TELNETs to port 259 on the FireWall and authenticates itself as follows:

| parameter                | value                           |
|--------------------------|---------------------------------|
| user                     | sso-root                        |
| password                 | sso-root's password             |
| [real-name@]real source: | dynamically-assigned IP address |



See also “Single Sign On — Additional Features” on page 542”.

## Encrypted Client Authentication

### HTTPS Connections

VPN-1/FireWall-1 Client Authentication also supports HTTPS (HTTP encrypted by SSL) connections. This feature is supported only for Client Authentication sessions initiated through a Web browser. To enable encrypted Client Authentication, you must modify the gateway and Security Server configuration file, as follows:

Generating CA Keys

- 1 Generate the CA Key pair to be used by the Management Station and the gateway. For more information on generating CA Keys, see “Generating CA Keys” on page 510.

Modifying the Security Server Configuration File

- 2 Modify the file `$FWDIR/conf/fwauthd.conf` by specifying SSL encryption for the HTTP Client Authentication daemon on an additional service port:

```
950 bin/in.ahclientd wait 950 ssl
```

How the User Connects

In the Web browser, the user initiates an HTTPS session on the gateway. The user must specify the gateway name and the port to which to connect, for example:



**FIGURE 15-51** Beginning an encrypted Client Authentication Session

The above example uses port 950, but any unused port number can be specified.

## Client Authentication — Security Considerations

### Timeouts

The Client Authentication authorization period is specified in the **Limits** tab of the **Client Authentication Action Properties** window. When the authorization period for the rule times out, the user must sign on and reauthenticate.

When using HTTP (for example, in a Partially Automatic Sign on rule), the **User Authentication Timeout** period in the **Properties Setup** window also affects the period of time during which the user may work without having to reauthenticate. For HTTP, a

one-time password is considered valid for this time period. A user working with HTTP does not have to generate a new password and reauthenticate for each connection. Each successful access resets the User Authentication timeout to zero.

If the User Authentication Timeout period is longer than the Client Authentication timeout, an authorized user with a one-time password can continue working without having to reenter the password, even after the Client Authentication timeout has expired. This is because the browser automatically re-sends the password for each connection. If the user initiates an HTTP connection after the Client Authentication authorization times out, the browser automatically sends the previously used password. If the User Authentication period has not timed out, then the password is still valid.

## Client Authentication — Additional Features

### HTTP Requests — Redirection According to Host Header

As in all types of transparent authentication, when the user attempts to connect to a certain host, the connection is redirected through VPN-1/FireWall-1. Once the user is authenticated, VPN-1/FireWall-1 completes the connection to the requested destination. By default, this is done using the destination's IP address. However, for HTTP requests authenticated by Fully or Partially Automatic Client Authentication, it is possible to configure VPN-1/FireWall-1 so that the connection is completed according to the destination specified in the HTTP host header. This handles the case where several HTTP hosts share the same virtual IP address.

To enable redirection according to the HTTP host header, follow these steps:

- 1** On the Management Station, issue the `fwstop` command.
- 2** In the file `$FWDIR/conf/objects.C`, under the line that includes the token `:props (`  
add the following line:

```
: http_use_host_h_as_dst (true)
```

- 3** On the Management Station, issue the `fwstart` command.

### Authorizing All Standard Sign On Rules

By default, the automatic sign on methods (Partially or Fully Automatic) open one rule after successful authentication — the rule for which the sign on was initiated. For example, if a user successfully authenticates according an automatic sign on rule, that user is allowed to work with the services and destinations permitted only by that rule.

You can configure VPN-1/FireWall-1 to automatically open all Standard Sign On rules after successful authentication through Partially or Fully Automatic Sign On. If a user successfully authenticates according to an automatic sign on rule, then all Standard Sign On rules which specify that user and source are opened. The user is then

permitted to work with all the services and destinations permitted by the relevant rules. In other words, VPN-1/FireWall-1 knows which user is on the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On Rules after successful Partially or Fully Automatic authentication, set the `automatically_open_ca_rules` property in the file `objects.C` to `true`. The new value will take effect after you install the Security Policy.

## Changing the Client Authentication Port Number

To change the port number used for the Client authentication feature, proceed as follows:

- 1 Stop VPN-1/FireWall-1 (`fwstop`).
- 2 Modify the port number in the **TCP Services Property** window for the following services:
  - If you want to modify the port number for TELNET sign on, then modify the port number of the `FW1_clntauth_telnet` service.
  - If you want to modify the port number for HTTP sign on, then modify the port number of the `FW1_clntauth_http` service.

These services are special VPN-1/FireWall-1 services provided as part of the Client Authentication feature.

- 3 In the file `$FWDIR/conf/fwauthd.conf`, change the port number for the Client Authentication daemon to the same port number as in the previous step.
  - For TELNET Sign On, modify the first column in the `in.aclientd` line.
  - For HTTP Sign On, modify the first column in the `in.ahclientd` line.

|       |                  |      |     |
|-------|------------------|------|-----|
| 21    | bin/in.aftpd     | wait | 0   |
| 80    | bin/in.ahttpd    | wait | 0   |
| 513   | bin/in.arlogind  | wait | 0   |
| 25    | bin/in.asmtpd    | wait | 0   |
| 23    | bin/in.atelnetd  | wait | 0   |
| 259   | bin/in.aclientd  | wait | 259 |
| 900   | bin/in.ahclientd | wait | 900 |
| 10081 | bin/in.lhttpd    | wait | 0   |

**FIGURE 15-52** `$FWDIR/conf/fwauthd.conf` file



**Warning** – Do not change anything else in the line.

For a description of the fields in this file, see “Security Server Configuration” on page 357.

- 4** Make sure that there is no rule that blocks the connection to the new port.
- 5** Restart VPN-1/FireWall-1 (`fwstart`).

Not all of the parameters shown in the sample file above will necessarily be present in your file.

# Active Network Management

---

## In This Chapter

|                                               |                 |
|-----------------------------------------------|-----------------|
| <i>VPN-1/FireWall-1 State Synchronization</i> | <i>page 557</i> |
| <i>High Availability</i>                      | <i>page 563</i> |
| <i>Server Load Balancing</i>                  | <i>page 581</i> |
| <i>Connection Accounting</i>                  | <i>page 587</i> |
| <i>Active Connections</i>                     | <i>page 587</i> |

## VPN-1/FireWall-1 State Synchronization

VPN-1/FireWall-1 provides Stateful Inspection even for stateless protocols such as UDP and RPC. To do this, the VPN/FireWall Module creates a virtual state for such connections, and updates this state according to the data transferred. In addition, VPN-1/FireWall-1 maintains state information for Address Translation and Encryption.

Different VPN/FireWall Modules running on different machines can synchronize their states, that is, they can share this information and can mutually update each other with the different states of the connections.

The VPN-1/FireWall-1 state synchronization provides two benefits:

### 1 High Availability

When one of the FireWalled gateways stops functioning and another one takes its place, the second FireWalled gateway has the updated state of the first FireWalled gateway's connections, so the connections can be maintained.



**Note** – The VPN-1/FireWall-1 state synchronization feature provides the mechanism for synchronizing the states of the VPN/FireWall Modules. The VPN-1/FireWall-1 High Availability feature provides the mechanism for detecting failures and changing routing accordingly. The VPN-1/FireWall-1 High Availability feature is described in “High Availability” on page 563. High Availability for encrypted connections is described in Chapter 12, “High Availability for Encrypted Connections” of *Check Point Virtual Private Networks*.

### 2 Different Routes for Connections (Asymmetric Routing)

The IP protocol supports a network configuration in which packets sent from host A to host B may be routed through gateway C, while all packets sent from host B to host A may be routed through gateway D.

## Implementation

This section describes how to implement state synchronization between VPN/FireWall Modules.

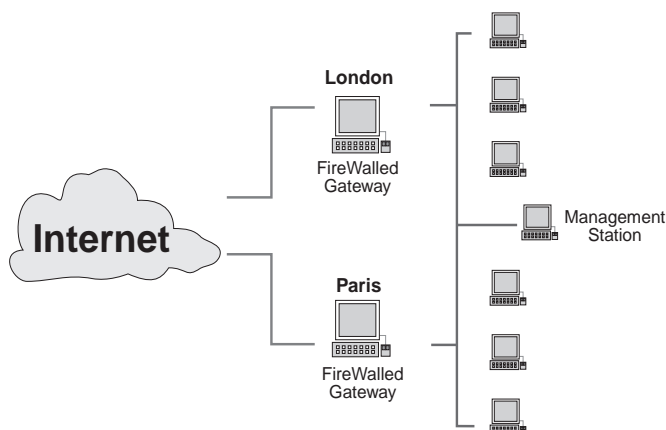
On each VPN/FireWall Module, the `$FWDIR/conf/sync.conf` file lists the other VPN/FireWall Modules (in the form of IP addresses or resolvable names) to which this VPN/FireWall Module sends its state information.

A control path must be established between all the VPN/FireWall Modules (using the `fw putkey` command), if one does not already exist.

When one VPN/FireWall Module goes down, the other VPN/FireWall Modules take over after the routing is re-configured.

## Example

FIGURE 16-1 shows a configuration in which two VPN/FireWall Modules (London and Paris) protect a network.



**FIGURE 16-1** Two VPN/FireWall Modules in Synchronized Configuration

### ▼ To configure London and Paris as synchronized VPN/FireWall Modules

On London

- 1** Create a `$FWDIR/conf/sync.conf` file containing one line:

```
Paris
```

- 2** Stop VPN-1/FireWall-1 with the `fwstop` command.
- 3** Establish a control path from London to Paris using the `fw putkey` command.  
You must do this only if there is not already a control path between London and Paris.

For information on how to use the `fw putkey` command, see “fw putkey” on page 12 of *Check Point Reference Guide*.

- 4** Start VPN-1/FireWall-1 with the `fwstart` command.

On Paris

- 1** Create a `$FWDIR/conf/sync.conf` file containing one line:

```
London
```

- 2** Stop VPN-1/FireWall-1 with the `fwstop` command.
- 3** Establish a control path from Paris to London using the `fw putkey` command.  
You must do this only if there is not already a control path between London and Paris, as follows:  
On London, enter the following command:

```
fw putkey Paris <the authentication password (key)>
```

On Paris, enter the following command:

```
fw putkey London <the authentication password (key)>
```

For information on how to use the `fw putkey` command, see “`fw putkey`” on page 12 of *Check Point Reference Guide*. For a detailed example of establishing control paths between computers, see “Synchronizing Authentication Passwords” on page 76.

- 4** Start VPN-1/FireWall-1 with the `fwstart` command.

London and Paris will now begin to exchange the necessary state information to enable each of them to take the other’s place if one of them goes down.

On the Management Station

Since the Management Station is not a VPN/FireWall Module, you do not have to do anything on the Management Station. Specifically, do not create a `$FWDIR/conf/sync.conf` file.

## Timing Issues

Synchronized VPN/FireWall Modules update each other with their state information approximately every 100 milliseconds.

The time on the synchronized VPN/FireWall Modules must be within seconds of each other. You should install some software that keeps the time synchronized between the two machines. Under Solaris2, you can use `xntpd`.

If one of the VPN/FireWall Modules goes down, the other VPN/FireWall Module may be unaware of connections initiated by the first VPN/FireWall Module in the 50 milliseconds before it went down. These connections will probably be lost.

If the VPN-1/FireWall-1 Synchronization feature is being used to implement different routes in and out of a network (see “Different Routes for Connections (Asymmetric Routing)” on page 558), the following situation may arise (refer to FIGURE 16-1 on page 559):



One of the local network's computers initiates a connection to the Internet through London. The reply comes back through Paris. If the reply had come through London, it would have been allowed because the connection is in London's connection table. However, if the reply arrives before London and Paris synchronize their state information, then Paris will be unaware of connection, and will not allow the reply to pass.

The solution to this problem is for the Rule Base to drop these packets instead of rejecting them. When a TCP packet is dropped, no reset is sent to the packet's sender, so the sender will simply resend the packet after a delay. During this delay, London and Paris will have synchronized their states, so the packet will be allowed to pass on the second try.

These packets will be logged if the **Log Established TCP Packets** property is checked.

This solution is effective only for TCP.

## Restrictions

The following restrictions apply to synchronizing VPN/FireWall Modules:

### General

- 1** Only VPN/FireWall Modules running on the same platform can be synchronized.  
For example, it is not possible to synchronize a Windows NT VPN/FireWall Module with a Solaris2 VPN/FireWall Module.
- 2** The VPN/FireWall Modules must be the same software version.  
For example, it is not possible to synchronize a Version 4.0 VPN/FireWall Module with a Version 4.1 VPN/FireWall Module.
- 3** The VPN/FireWall Modules must be managed by the same Management Module.
- 4** The VPN/FireWall Modules must have the same Security Policy installed.  
For example, suppose one VPN/FireWall Module accepts FTP and the other rejects FTP. If an FTP connection is opened through the first VPN/FireWall Module, the reply packets returning through the second VPN/FireWall Module will be accepted because the FTP connection is in the connections table. This behavior is inconsistent with the Security Policy on the second VPN/FireWall Module.

### Encryption

- 5** For information about state synchronization of encrypted connections, see Chapter 12, "High Availability for Encrypted Connections" of *Check Point Virtual Private Networks*.
- 6** The SKIP key management protocol cannot be used on a synchronized VPN/FireWall Module.

## Address Translation

- 7** If you are performing Network Address Translation with synchronized VPN/FireWall Modules, you must give very careful consideration to the subject of routing. If the routing through the VPN/FireWall Modules is asymmetric (that is, if packets go out through one VPN/FireWall Module and replies return through the other), then you must make sure that routers on either side of the VPN/FireWall Module take into account the statically translated addresses.

Similarly, with the hidden IP addresses, you must think about which VPN/FireWall Module should be answering the ARP requests for those IP addresses.

## Authentication

- 8** An authenticated connection through a VPN/FireWall Module will be lost if the VPN/FireWall Module goes down. Other synchronized VPN/FireWall Modules will be unable to resume the connection.
- 9** Authenticated connections will not work in the case where the synchronized feature is being used to implement different routes in and out of a network (see “Different Routes for Connections (Asymmetric Routing)” on page 558).

The reason for these restrictions is that VPN-1/FireWall-1 authentication is implemented by Security Servers, which are processes, and thus cannot be synchronized on different machines in the way that data can be synchronized.

## Resources

The state of connections using resources is maintained in a Security Server, so these connections cannot be synchronized for the same reason that authenticated connections cannot be synchronized.

## Accounting

- 10** If two VPN/FireWall Modules act as backups for each other, then accounting data cannot be accurately maintained by both VPN/FireWall Modules.

## Troubleshooting

Snoop ports 256 to see the communication activity between the two VPN/FireWall Modules. If the machines are synchronizing properly you will see:

- A message about them being connected on `fwstart`.
- An exchange of information every 50 milliseconds.

If you disconnect one VPN/FireWall Module from the network, the other VPN/FireWall Module should notice this.

# High Availability

## Overview

VPN-1/FireWall-1 enables two or more VPN/FireWall Module machines to be configured so that each one acts as a backup for the others. If one of the VPN/FireWall Module machines fails for any reason, another VPN/FireWall Module takes its place in a manner that minimizes the number of lost connections.



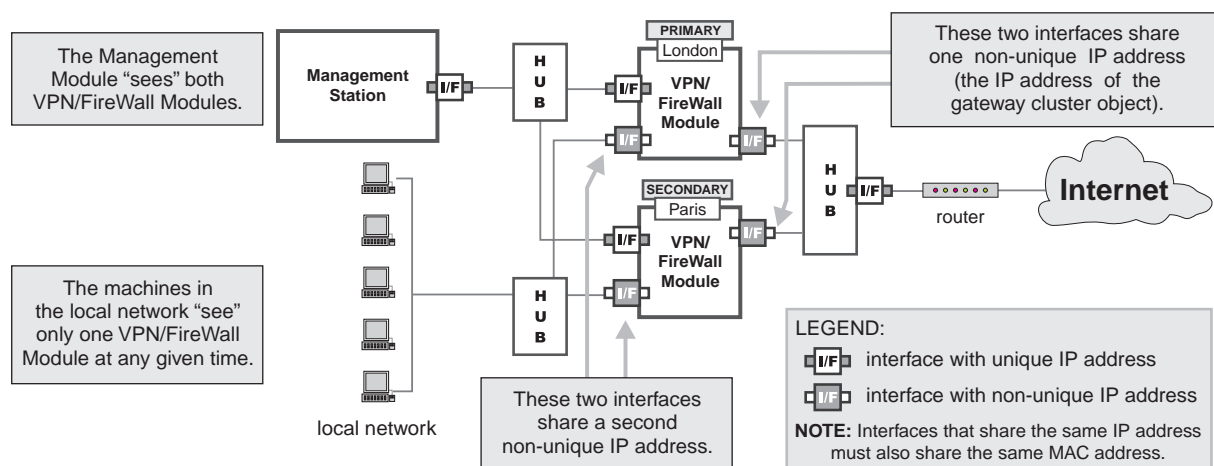
**Note** – The VPN-1/FireWall-1 High Availability feature provides the mechanism for detecting failures and changing routing accordingly. The VPN-1/FireWall-1 synchronization feature provides the mechanism for synchronizing the states of the VPN/FireWall Modules. High Availability is described in this section. High Availability for encrypted connections is described in Chapter 12, “High Availability for Encrypted Connections” of *Check Point Virtual Private Networks*.

One of the machines is designated as the primary machine, and this machine serves as the gateway in normal circumstances. If the primary machine fails, control is passed to the first secondary machine. If that machine fails, control is passed to the next secondary machine, and so on.



**Note** – The High Availability feature is currently available for Windows NT and Solaris.

FIGURE 16-2 shows one possible network configuration for implementing the High Availability feature.



**FIGURE 16-2** High Availability configuration

In this configuration, there are two VPN/FireWall Modules: London (the primary) and Paris (the secondary) each with three interfaces, as follows:

- an interface with a unique IP address, facing the Management Station

These are the interfaces the Management Station sees. Because the Management Station must be able to download a Security Policy to both VPN/FireWall Modules, each VPN/FireWall Module must have its own unique IP address so that the Management Station can “see” them both at any given time. The machines also require unique IP addresses for system maintenance purposes.

The network configuration in FIGURE 16-2 shows the Management Station connected to the same hub as the VPN/FireWall Modules, but this is one of many possible configurations. The only requirement is that there be a route from the Management Station to the unique IP addresses of each of the VPN/FireWall Modules, so that the Management Station can “see” all the VPN/FireWall Modules at any given time. The advantage of connecting through a hub is that the connection between the Management Station and the VPN/FireWall Module is then secured (see “Secured Interfaces” on page 566).

- a second interface with a non-unique IP address, facing the Internet through a hub

This is the interface that the outside world sees. Because there are two interfaces (one on each VPN/FireWall Module) with the same IP (and MAC) address, only one of them can be active (that is, the outside world can see only one of them) at any given time. This is also the IP address defined for the gateway cluster object (see “Network Configuration” on page 234 of *Check Point Virtual Private Networks*) that includes these gateways.

- a third interface with a different non-unique IP address, facing the local network through a hub

This is the interface that the local network sees. Because there are two interfaces (one on each VPN/FireWall Module) with the same IP address, only one of them can be active (that is, the local network can see only one of them) at any given time.

There can be any number of local networks, each of which is connected to both VPN/FireWall Modules on interfaces that share the same non-unique IP address (but each local network shares a different non-unique IP address).

**Note –**



- You will need at least three machines to implement High Availability: a Management Station and two VPN/FireWall Modules.
- Interfaces that share the same IP address must also share the same MAC address. For information on how to configure MAC addresses, see “Configure Shared Interfaces Window” on page 569 for Windows platforms or “MAC Addresses” on page 572 for Solaris platforms.
- Both the unique and non-unique IP addresses may be illegal.
- If the High Availability machines are synchronized, there must be a control channel between all the machines. For more information, see “Synchronization” on page 573.

## When Does a VPN/FireWall Module Become Active?

A VPN/FireWall Module becomes active in place of another VPN/FireWall Module if the active VPN/FireWall Module fails, that is, if one of the following occurs on the active VPN/FireWall Module:

- The FireWall daemon (`fw`) or any other process specified with the `cphaprob` command (see “`cphaprob`” on page 575) terminates.
- The `cphaprob` command reports a problem in the FireWall daemon (`fw`) or any other specified process.

By default, a VPN/FireWall Module reports a problem (using the `cphaprob` command — see “`cphaprob`” on page 575) when the Security Policy is uninstalled.

- An interface or cable fails.
- The machine crashes.
- The Security Policy is uninstalled.

When a VPN/FireWall Module goes down, another VPN/FireWall Module becomes active and (if the VPN/FireWall Modules are synchronized) also “takes over” the connections of the failed VPN/FireWall Module (see “Synchronization” on page 573 for more information on synchronization).

## Before Configuring High Availability

Before you configure the High Availability feature, define the same IP address for each machine participating in the High Availability configuration.

To avoid network conflicts, proceed as follows:

- 1** Disconnect the machines participating in the High Availability configuration from the hub.

**2** Define the IP addresses.

You must define the IP addresses before configuring the High Availability feature, because the export and import of shared MAC addresses requires that the shared IP addresses be already configured.

**3** Install VPN-1/FireWall-1.

At the end of the installation you are prompted to reboot the computer.

**4** Reconnect the machines participating in the High Availability configuration from the hub before or during the reboot.

## Secured Interfaces

An interface is considered secured if a connection through that interface can be trusted (for example, if the interfaces that share the same IP and MAC addresses are connected with a cross cable or dedicated hub). If a Management Station and a VPN/FireWall Module are connected through secured interfaces, then the connection between the machines can be trusted because there is no way for an intruder to send packets on that connection. In addition, a secured interface can be safely used to transmit synchronization and High Availability information.

In a High Availability configuration, each machine should have at least one secured interface. Additional secured interfaces are recommended for backup purposes.

If there secured interfaces are configured, a VPN/FireWall Module will accept state change commands only on those interfaces. If there are no secured interfaces, a VPN/FireWall Module will accept state change commands on any interface.

## Sharing IP and MAC Addresses

The recommended procedure is as follows:

**1** On the primary machine, define the MAC addresses and other parameters for each interface.

In most cases, you can use the default definitions.

**2** Export the default MAC addresses from the primary machine to a file.**3** On each of the other (secondary) machines, import the file.

### Note –



- MAC addresses can be freely exported and imported between Windows NT and Solaris machines.
- If you uninstall VPN-1/FireWall-1, then the original MAC addresses will be restored on Solaris machines but will not be restored on Windows NT machines.

## Installation

The High Availability feature is part of the standard VPN-1/FireWall-1 installation. It should be installed only in a distributed configuration, that is, only when the Management Station and the VPN/FireWall Modules are installed on different machines.



**Warning** – Make sure the same version of VPN-1/FireWall-1 (including the build number) is installed on the Management Station and each VPN/FireWall Module.

When installing VPN-1/FireWall-1 for the first time, the Check Point configuration application is run automatically and you can configure the High Availability parameters at that time. Otherwise, you should reboot the machine after upgrading VPN-1/FireWall-1 and then configure the High Availability parameters.

You must configure the High Availability parameters separately on each VPN/FireWall Module machine. It is recommended that you configure the primary machine first and then configure each of the secondary machines in turn.

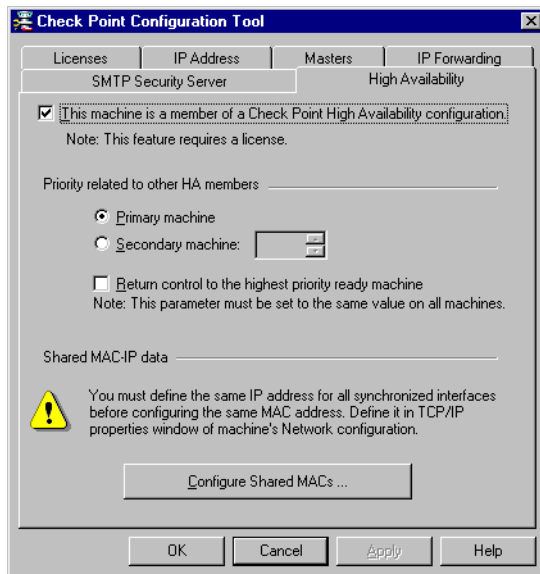


**Note** – Make sure you have obtained a license to use the High Availability feature.

## Windows NT

### Configuration

High Availability parameters are specified in the **High Availability** tab (FIGURE 16-3).



**FIGURE 16-3** VPN-1/FireWall-1 Configuration - High Availability tab

**This machine is a member of a Check Point High Availability configuration** — Check this box to indicate that this machine participates in a High Availability configuration.

**Priority related to other HA members** — Select one of:

**Primary machine** — Check this box if this machine is the primary machine in the HA hierarchy.

**Secondary machine** — If this machine is one of the secondary machines in the HA hierarchy, specify its priority sequence number.

The primary machine's priority sequence number is 1, and control is passed to the secondary machines according to their priority sequence numbers. In other words, if the primary machine fails, control is passed to the secondary machine with sequence number 2. If that machine fails, control is passed to the secondary machine with sequence number 3, and so on.

If secondary machine 3 has control and secondary machine 2 is restored, then control will be returned to secondary machine 2 if **Return control to a higher priority machine when it is restored** is checked (see below).



**Warning** – This property must be set consistently on all the machines that participate in the High Availability configuration. Only one machine should be specified as the primary machine, and no two machines should have the same priority numbers.



**Return control to a higher priority machine when it is restored** — This option is useful when a secondary VPN/FireWall Module machine is less powerful than the primary VPN/FireWall Module machine. If this machine has control because all the machines with higher priorities have failed, control returns to the higher priority machine when it is restored.

If this option is not checked, then control will be returned to the higher priority standby machine only when the machine that has control fails (or is rebooted).



**Warning** – This property must be set to the same value on all the machines that participate in the High Availability configuration.

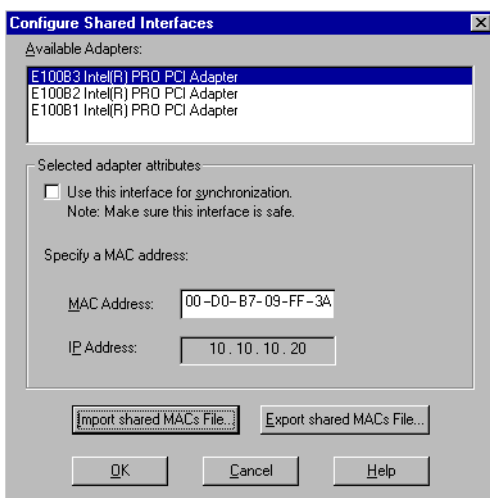
**Configure Shared MACs** — Click on this button to display the **Configure Shared Interfaces** window (FIGURE 16-4).

See FIGURE 16-2 on page 563 and the accompanying text for an explanation of shared IP and MAC addresses.

## Sharing IP and MAC Addresses

The shared MAC addresses of interfaces on the High Availability machines are defined in the **Configure Shared Interfaces** window (FIGURE 16-4).

Configure Shared Interfaces Window



**FIGURE 16-4** Configure Shared Interfaces window

**Available Adapters** — Select the adapter from the list.



**Note** – You should carefully scroll through all the adapters to confirm that the correct information is exported and imported.

**Use this interface for synchronization** — Check this box if this interface is secure (for example, if the interfaces that share the same IP and MAC addresses are connected with a cross cable) and can be safely used to transmit synchronization and High Availability information.

- See “Secured Interfaces” on page 566 for more information on secured interfaces.
- See “Synchronization” on page 573 for more information on synchronization.

**MAC Address** — This is the MAC address.

There is usually no reason to edit this field directly. Use the original MAC addresses from the primary machine.

**IP Address** — This is the IP address, and cannot be edited.

**Import shared MACs file** — Import the information about this machine’s interfaces from a file.

A window will be displayed in which you will be asked to specify the file’s location. It is recommended that you export on the primary machine and then import on the secondary machines.

**Export shared MACs file** — Export the information about this machine’s interfaces to a file.

A window will be displayed in which you will be asked to specify the file’s location. It is recommended that you export on the primary machine and then import on the secondary machines.

## Solaris

### Configuration

To configure the High Availability parameters, run the `cpconfig` program and select the Enable High Availability option (see “`cpconfig`” on page 4 of *Check Point Reference Guide*).

```
Configuration Options:

(1) Licenses
(2) Masters
(3) SMTP Server
(4) SNMP Extension
(5) Groups
(6) IP Forwarding
(7) Default Filter
(8) Enable High Availability

(9) Exit
```

You will be asked to configure:

- secured interfaces
- MAC Addresses
- High Availability parameters

## Secured Interfaces

See “Secured Interfaces” on page 566 for more information on secured interfaces.

See “Synchronization” on page 573 for more information on synchronization.

```
Configuring High Availability Secured Interfaces...
=====
The following interfaces are configured on your machine
hme0 hme1 hme2
Secured interfaces are interfaces on which sensitive High Availability
information can be exchanged securely with other members of this
cluster.

Do you want to add secured interfaces (y/n) [y] ? y
Please enter the list of interfaces that will be secured interfaces.
Enter one interface per line, terminating with CTRL-D or your EOF
character.
hme0
Is this correct (y/n) [y] ? y
```

## MAC Addresses



**Note** – It is highly recommended that you use the original MAC addresses from the primary machine by importing the file.

```
Configuring High Availability MAC Addresses...
=====

Do you wish to import MAC addresses configurations file (y/n) [n] ? y
Please enter the file name [/tmp/cphamacs] ? /tmp/cpha1
Following are the MAC addresses in the cphamacs file:
hme0: 8:0:20:b5:7c:12

NOTE: You can export this configuration to any other High Availability
machine
by launching cpha_export.
Would you like to modify the above configuration (y/n) [y] ? n
```

You will be asked to specify the location of the file to import. This file is created by the `cpha_export` command (see “`cpha_export` (Solaris only)” on page 579).

## High Availability Parameters

Configure the High Availability parameters.

```
Configuring High Availability Priorities...
=====

You must configure the priority and the mode:
 Priority = 1 for the primary machine; 2,3,4... for the standby
 machines.
 Mode = active-up or primary-up.
Following is the current configuration:
Priority: 1
mode: active-up
Would you like to modify the above configuration (y/n) [y] ? y
Priority (1..n) [1]:2
mode (active-up/primary-up) [active-up]:primary-up

Is this correct (y/n) [y] ? y

You have changed the High Availability configuration.
Would you like to restart VPN-1/FireWall-1 now
so that your changes will take effect? (y/n) [y] ? y
```

priority is 1 for the primary machine and greater than 1 for secondary machines.

primary-up corresponds to checking **Return control to a higher priority machine when it is restored** in the **High Availability** tab (FIGURE 16-3 on page 568).

## Synchronization

It is not necessary for the High Availability machines to be synchronized. The advantage of synchronization is that connections will not be lost when a machine takes control from a machine that has gone down (but there are exceptions — see “Restrictions” on page 561 of *VPN-1/FireWall-1 Administration Guide* for more information). The disadvantage is the cost of synchronizing internal tables on all machines.

If you do not require synchronization, you must still configure the High Availability machines with synchronization set to `no sync` in the `$FWDIR/conf/sync.conf` file (see TABLE 16-1 on page 573).

If the High Availability machines are synchronized, there must be a control channel between all the machines (see “fw putkey” on page 12 of *Check Point Reference Guide* for more information). Synchronization information is transmitted on TCP port 256 on the unique IP addresses.

There are three possible synchronization modes:

- 1** no synchronization
- 2** “old style” synchronization (compatible with previous versions of VPN-1/FireWall-1)
- 3** “new style” synchronization on UDP port 8116 (compatible with the High Availability feature described in this section) — this option should be used with caution.

Synchronization is defined in the `$FWDIR/conf/sync.conf` file (see “VPN-1/FireWall-1 State Synchronization” on page 557 of *VPN-1/FireWall-1 Administration Guide*).

The type of synchronization is specified by the `SyncMode` parameter, as follows:

```
SyncMode=mode
```

where *mode* is one of the following values:

**TABLE 16-1** SyncMode values

| value                 | meaning                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <code>no sync</code>  | There is no synchronization. This is the default setting, so there is no need to change existing configurations.                |
| <code>CPHAP</code>    | “new style” synchronization on UDP port 8116. All other lines in the file are ignored. This option should be used with caution. |
| <code>TCP sync</code> | “old style” synchronization (default value). Other lines in the file specify VPN/FireWall Modules with which to synchronize.    |

If any other value is specified for *mode*, then there is no synchronization and control will not pass to this machine.



**Warning** – Synchronization must be configured in the same way on all the machines that participate in the High Availability configuration.

If you do not wish to use synchronization, define `no sync` in the `$FWDIR/conf/sync.conf` file and restart VPN-1/FireWall-1.

## Using High Availability in Virtual Private Networks

When implementing High Availability, the VPN/FireWall Modules should be defined as members of a gateway cluster in order to:

- synchronize connections and other important information required for VPN Single Entry Point implementation between the VPN/FireWall Modules, and
- ensure that the same Security Policy is installed on all the VPN/FireWall Modules.

For information about configuring the VPN/FireWall Modules as members of a cluster, see “VPN-1/FireWall-1 Configuration (SEP)” on page 235 of *Check Point Virtual Private Networks*.

In a Check Point High Availability configuration, the gateway cluster’s IP address (defined in the **General** tab of the **Gateway Cluster Properties** window) should be the non-unique IP address facing the Internet that the gateways share (see FIGURE 16-2 on page 563). The IP address of each of the gateways in the cluster should be defined as the unique address facing the Management Station.

## Log Viewer

Every change of a VPN-1/FireWall-1 Module status is recorded as an entry of the Log File and can be viewed with the Log Viewer. See “Log Viewer” on page 389 of *VPN-1/FireWall-1 Administration Guide* for more information

## System Status

The status of High Availability modules can be viewed with the System Status Viewer. See “System Status Viewer” on page 369 of *VPN-1/FireWall-1 Administration Guide* for more information.

## Commands

The following commands can be used with the High Availability feature:

- `cphastart`
- `cphastop`
- `cphaprob`
- `cpha_export`

- cpha\_import
- fw hastat

## cphastart

cphastart enables the High Availability feature on the machine. In NT, this is done when the VPN/FireWall Module is started. In Solaris, the cphastart command is part of the fwstart script.

### Syntax

```
cphastart
```

## cphastop

cphastop disables the High Availability feature on the machine.

### Syntax

```
cphastop
```

## cphaprob

cphaprob defines “critical” processes. When a critical process fails, the machine is considered to have failed.

### Syntax

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> register
cphaprob -f <file> register
cphaprob -d <device> unregister
cphaprob -a unregister
cphaprob -d <device> -s <ok|init|problem> report
cphaprob [-i[a]] [-e] list
cphaprob state
cphaprob [-a] if
```

Options

| parameter             | meaning                                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d <device>           | Add <device> to the list of devices that must be running for the VPN/FireWall Module to be considered active (in other words, if <device> fails, then the VPN/FireWall Module is considered to have failed)                                  |
| -s                    | The status to be reported — one of: <ul style="list-style-type: none"><li>■ “ok” — &lt;device&gt; is alive</li><li>■ “init” — &lt;device&gt; is initializing (the machine is down)</li><li>■ “problem” — &lt;device&gt; has failed</li></ul> |
| -t <timeout>          | If <device> fails to contact the VPN/FireWall Module in <timeout> seconds, <device> will be considered to have failed. To disable this parameter, enter <0> as the timeout value.                                                            |
| -f <file><br>register |                                                                                                                                                                                                                                              |
| register              | Register <device> as a critical process.                                                                                                                                                                                                     |
| unregister            | Unregister <device> as a critical process.                                                                                                                                                                                                   |
| state                 | Display the state of this VPN/FireWall Module and all the other VPN/FireWall Modules in the High Availability configuration.                                                                                                                 |
| -i[a] -e list         | Display the state of devices.                                                                                                                                                                                                                |
| report                | Report the status of High Availability VPN/FireWall Modules and their status.                                                                                                                                                                |
| if                    | Display the state of interfaces.                                                                                                                                                                                                             |

A process specified by <device> should run `cphaprob` with the “-s ok” parameter to notify the High Availability module that the process is alive. If this notification is not received in <timeout> seconds, the process (and the machine) will be considered to have failed.

Example

This example illustrates how to manually cause a machine to fail and another machine to take over.

**1** Verify that the primary machine is currently active with the following command:

```
#cphaprob state
```

Information similar to the following should be displayed:

```
1 (local) <IP-address> active
2 <IP-address> stand-by
```



- 2** Register a device that initializes with a problem report:

```
#cphaprob -d failDevice -s problem report
```

The machine will immediately fail, and the secondary machine will take over. `failDevice` is the name of a non-existent device in this case.

- 3** To reactivate the machine, enter the following command:

```
#cphaprob -d failDevice -s ok report
```

The machine will become active if **Return control to a higher priority machine when it is restored** in the **High Availability** tab (FIGURE 16-3 on page 568) (or the Solaris equivalent) is checked.

### Example

These examples illustrate various uses of the `chaprob` command.

```
[root@tutil]/opt/CPfw1-41/bin>cphaprob if

hme0 UP
hme1 UP
hme2 UP
```

```
[root@tutil]/opt/CPfw1-41/bin>cphaprob -a if

Required interfaces: 3
Required secured interfaces: 2

hme0 UP
hme1 UP (secured)
hme2 UP (secured)
```

```
[root@tutil]/opt/CPfw1-41/bin>cphaprob -i list
```

Built-in Devices:

Device Name: Interface Active Check  
Current state: OK

Device Name: HA Initialization  
Current state: OK

Registered Devices:

Device Name: sync & filter  
Registration number: 0  
Timeout: none  
Current state: problem  
Time since last report: 383.5 sec

Device Name: fwd  
Registration number: 1  
Timeout: 2 sec  
Current state: OK  
Time since last report: 0.2 sec

```
[root@tutil]/opt/CPfw1-41/bin>cphaprob -i -e list
```

Registered Devices:

Device Name: sync & filter  
Registration number: 0  
Timeout: none  
Current state: problem  
Time since last report: 569.9 sec

Device Name: fwd  
Registration number: 1  
Timeout: 2 sec  
Current state: OK  
Time since last report: 0.6 sec

**cpha\_export (Solaris only)**

cpha\_export (usually run on the primary machine) writes MAC address information to stdout. If the output is redirected to a file, it can be input (stdin) to cpha\_import on another machine.

Syntax

```
cpha_export
```

**cpha\_import (Solaris only)**

cpha\_import (usually run on the secondary machines) imports MAC address information from stdin and updates the machine’s MAC addresses accordingly. The normal procedure is to redirect stdin to read a file created by cpha\_export on the primary machine.

Syntax

```
cpha_import
```

**fw hastat**

The fw hastat command displays information about High Availability machines and their states.

Syntax

```
fw hastat [<target>]
```

Options

| parameter | meaning                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------|
| <target>  | A list of machines whose status will be displayed. If target is not specified, the status of the local machine will be displayed. |

**Additional Configuration Parameters**

**Cluster ID**

If multiple High Availability clusters are defined, and machines from different clusters are connected to the same hub, then you must define, on each machine, the cluster to which it belongs.

To configure this parameter, proceed as follows:

## Setting the Cluster ID (NT)

- 1** Run `regedt32`.
- 2** Select the **HKEY\_LOCAL\_MACHINE** window.
- 3** Browse to the following path:  
HKEY\_LOCAL\_MACHINE/System/CurrentControlSet/Services/CPHA  
This path exists only when the High Availability feature is installed.
- 4** Make sure “CPHA” key is selected.
- 5** From the menu, choose **Edit>Add value**.
- 6** In the **Add Value** window, enter “ClusterID”.
- 7** Under **Data Type**, select “REG\_DWORD”.
- 8** Click on **OK**.
- 9** When asked to enter the value (of the new registry value), enter an integer (default should be 0) that is unique to all the members of that cluster (High Availability configuration).
- 10** Stop the High Availability Module with the `cphastop` command.
- 11** Restart the High Availability Module with the `cphastart` command.

## Setting the Cluster ID (Solaris)

- 1** Edit the file `$FWDIR/conf/cpha.conf`.
- 2** Insert a line:

ClusterID X

- 3** Replace `x` with an integer value for this cluster, usually one digit.
- 4** Save the file.
- 5** Stop the High Availability Module with the `$FWDIR/bin/cphastop` command.
- 6** Restart the High Availability Module with the `$FWDIR/bin/cphastart` command.

## Setting the Number of Required Interfaces

You can optionally specify the number of interfaces that must be active in order for a machine to be considered available. There is usually no need to do this, because the High Availability feature configures this automatically.

To configure this parameter, proceed as follows:

**Setting the Number of Required Interfaces (NT)**

Add a “RequiredInterfaces” value to the registry. The procedure is identical to the one given in “Setting the Cluster ID (NT)” on page 580, except that the value is “RequiredInterfaces” instead of “ClusterID”.

**Setting the Number of Required Interfaces (Solaris)**

Add a `RequiredInterfaces` line to `$FWDIR/conf/cpha.conf`. The procedure is identical to the one given in “Setting the Cluster ID (Solaris)” on page 580, except that the value is “RequiredInterfaces” instead of “ClusterID”.

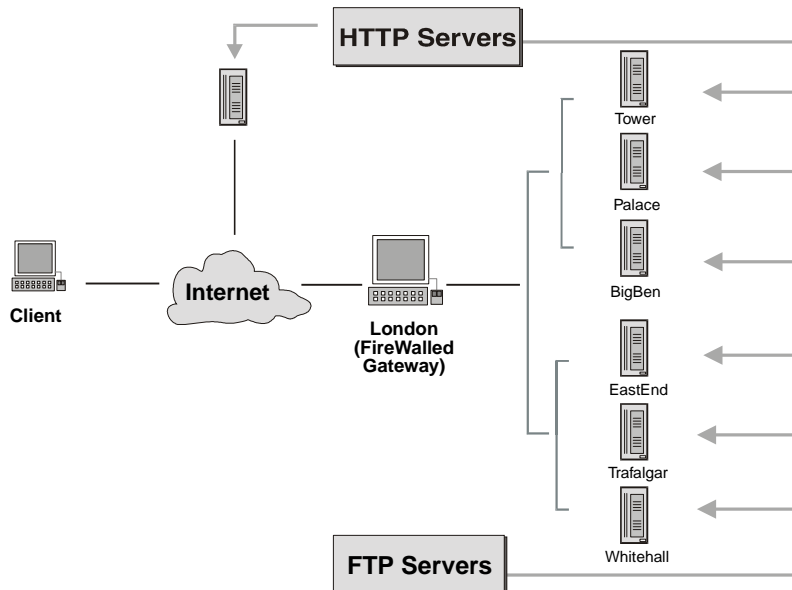
## **Server Load Balancing**

### **The Need for Server Load Balancing**

The VPN-1/FireWall-1 Load Balancing feature enables several servers providing the same service to share the load among themselves.

Consider the configuration depicted in FIGURE 16-5 on page 582. All the HTTP servers can provide the HTTP client with the same services (but note that not all of the HTTP servers are behind the FireWalled gateway). In the same way, all the FTP servers can provide the FTP client with the same services.

The system administrator wishes to ensure that the service load is balanced among the servers. The client will be unaware of the different servers. From the client's point of view, there is only one HTTP server and only one FTP server. When the service request reaches the gateway, VPN-1/FireWall-1 determines which of the servers will fulfill the request, based on the load balancing algorithm specified by the system administrator.



**FIGURE 16-5** Load Balancing among several servers



**Note** – The IP address returned by the DNS should be the IP address of the Logical Server, to allow the VPN/FireWall Module to perform the load balancing between the physical servers.

## How Server Load Balancing Works

### HTTP

When **HTTP** is chosen under **Servers Type** in the **Logical Server Properties** window, Load Balancing is performed as follows:

- 1** VPN-1/FireWall-1 detects a service request for a Logical Server (see “Logical Servers” on page 584).

For example, the client starts an HTTP session on the Logical Server **HTTP\_servers** (whose **Server** is defined as **HTTP\_Group**, consisting of the servers Tower, Palace and BigBen, as shown in FIGURE 16-5 on page 582).

- 2** VPN-1/FireWall-1 determines that the session is to be redirected to a particular server.

For example, VPN-1/FireWall-1 determines, on the basis of the load balancing algorithm defined for the Logical Server **HTTP\_Servers**, that BigBen will be the server for this session.

- 3** VPN-1/FireWall-1 redirects the connection to the Load Balancing daemon (lhttpd).

This is done using the translate port feature of the Address Translation mechanism.

- 4** VPN-1/FireWall-1 notifies the client that the URL is being redirected to the chosen server.

This is done using the URL Redirection feature of HTTP to redirect the client to a specific IP address rather than the IP address of the Logical Server.

- 5** The rest of the session is conducted between the client and the chosen server, without the intervention of VPN-1/FireWall-1.

When **Other** is chosen under **Servers Type** in the **Logical Server Properties** window, Load Balancing for HTTP is performed using the Address Translation mechanism (as described in “Non-HTTP” on page 583). Each HTTP connection is then handled separately, and connections may be redirected to different servers. This may cause problems in some cases, for example, in an application where a user fills in a number of HTTP forms and a single server is expected to process all the data.

## Non-HTTP

- 1** VPN-1/FireWall-1 detects a service request for a Logical Server (see “Logical Servers” on page 584).

For example, the client starts an FTP session on the Logical Server **FTP\_servers** (whose **Server** is defined as **FTP\_Group**, consisting of the servers EastEnd, Trafalgar and Whitehall, as shown in FIGURE 16-5 on page 582).

- 2** VPN-1/FireWall-1 determines that the session is to be redirected to a particular server.

For example, VPN-1/FireWall-1 determines, on the basis of the load balancing algorithm defined for the Logical Server **FTP\_Servers**, that Trafalgar will be the server for this session.

- 3** Using the Address Translation mechanism, VPN-1/FireWall-1 modifies the destination IP address of incoming packets.

If a back connection is opened (for example, in FTP), the connection is correctly established between the server and the client automatically. The source IP address of reply packets is changed back to the Logical Server’s IP address.

## Load Balancing Algorithms

The available load balancing algorithms are:

**1** server load

VPN-1/FireWall-1 queries the servers to determine which is best able to handle the new connection. There must be a load measuring agent on the server.

**2** round trip

VPN-1/FireWall-1 uses PING to determine the round-trip times between the VPN/FireWall Module and each of the servers, and chooses the server with the shortest round trip time.

This method will not give optimum results for HTTP if some of the HTTP servers are not behind the VPN/FireWall Module, because it measures the round-trip time between the VPN/FireWall Module and the servers, and not between the client and the servers.

**3** round robin

VPN-1/FireWall-1 simply assigns the next server in the list.

**4** random

VPN-1/FireWall-1 assigns a server at random.

**5** domain

VPN-1/FireWall-1 assigns the “closest” server, based on domain names.

## Logical Servers

To implement the VPN-1/FireWall-1 Load Balancing feature, proceed as follows (the example is based on the configuration depicted in FIGURE 16-5 on page 582):

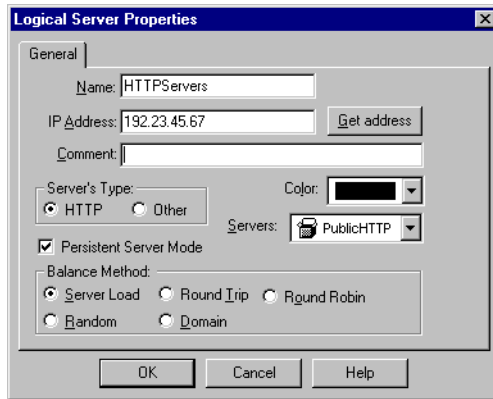
**1** Define a group network object consisting of all the servers that will be providing the given service.

For example, define a group network object **HTTP\_Group** that consists of Tower, Palace, BigBen and Louvre. There should be no other servers in the group.

**2** Define a network object of type Logical Server, and define its properties.



### 3 Define a Logical Server as in FIGURE 16-6.



**FIGURE 16-6** Logical Server Properties window

**IP Address** must be an address for which communications are routed to or through the VPN/FireWall Module. This should be either the VPN/FireWall Module's address, or the address of a non-existing computer in the network behind the VPN/FireWall Module. This is the address that clients use to communicate with the Logical Server.

**Persistent Server Mode** — If this is checked, then once a client is connected to a physical server, the client will continue to connect to that server for the duration of the session.

**Servers** is **HTTP\_Group**.

None of the network objects that belong to **Servers** may have the IP address listed under **IP Address**.

**Balance Method** is one of the algorithms described under "Load Balancing Algorithms" on page 584.

**Servers Type** is **HTTP**.

This parameter determines how the redirection is performed. For further information, see "How Server Load Balancing Works" on page 582. Note that even for a Logical Server consisting of HTTP servers, **Servers Type** can be **Others**.

4 Add the appropriate rules to the Rule Base, for example, the one in FIGURE 16-7.



















| No. | Source                                                                                          | Destination                                                                                    | Service                                                                                | Action                                                                                      | Track                                                                                   | Install On                                                                                   |
|-----|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 1   |  Any           |  HTTP_Servers |  http |  accept    |  Short |  Gateways |
| 2   |  All Users@Any |  HTTP_Group   |  http |  User Auth |  Long  |  Gateways |
| 3   |  Any           |  Any          |  Any  |  reject    |  Long  |  Gateways |

FIGURE 16-7 Using Logical Servers in a Rule

TABLE 16-2 Explanation of Rule Base

| Rule No. | Explanation                                                                                               |
|----------|-----------------------------------------------------------------------------------------------------------|
| 1        | balances the load for connections to the Logical Server <b>HTTP_Servers</b>                               |
| 2        | specifies that HTTP connections to <b>HTTP_Group</b> be User Authenticated (could also be <b>Accept</b> ) |
| 3        | rejects and logs all other communications                                                                 |

Rule Base

Using HTTP Logical Servers in a Rule

When an HTTP Logical Server is the **Destination** in a rule, the rule’s **Action** refers to the connection between the VPN/FireWall Module and the client (the connection that serves to redirect the client to the proper server), and must be either **Accept** or **Encrypt**. There must be a different rule that allows the connection between the client and the server. That rule can specify another action, for example, **User Authentication**.

The rule specifying the Logical Server as **Destination** must come before the rule specifying the physical servers as **Destination**.

In the configuration depicted in FIGURE 16-5 on page 582, HTTP connections to the HTTP servers behind the VPN/FireWall Module will be User Authenticated (in accordance with the second rule in FIGURE 16-7 on page 586), but HTTP connections to Louvre will not be User Authenticated, because they do not pass through the VPN/FireWall Module, even though they were enabled by the VPN/FireWall Module.

Using non-HTTP Logical Servers in a Rule

There are no special considerations for using non-HTTP Logical Servers in a rule. One rule, with the Logical Server as **Destination**, is sufficient.

Load Measuring

CheckPoint provides a sample load measuring agent application for installation on servers on which VPN-1/FireWall-1 is not installed, as well as an protocol for users who wish to write their own agents.

The load measuring agent is a service running on the port number specified in the **Load Agents Port** property (in the **Connect Control** tab of the **Properties Setup** window) and returns information about the server's load to VPN-1/FireWall-1. All the load measuring agents in a configuration must use the same port number.

The load measuring agent measures the load at the interval specified by the **Load Measurement Interval** property, also defined in the **Connect Control** tab of the **Properties Setup** window.

For example, in the configuration depicted in FIGURE 16-5 on page 582, the server Louvre is not FireWalled, so the only way for VPN-1/FireWall-1 on London to know what Louvre's load is (and to what extent Louvre is able to handle additional clients), is for Louvre's system administrator to install a VPN-1/FireWall-1 compatible load measuring agent on Louvre.



**Note** – The VPN/FireWall Module determines the availability of a Logical Server by pinging it. You should define rules to allow the ping as follows:

- allow the echo-request service from the VPN/FireWall Module to the Logical Servers
- allow the echo-reply service from the Logical Servers to the VPN/FireWall Module

## Connection Accounting

You can generate accounting log entries by choosing **Accounting** in a rule's **Track** field. The accounting log entries show the start and end times of each connection, and the number of bytes transferred.

For additional information, see Chapter 13, “Log Viewer.”

## Active Connections

You can view the Active connections at any moment from the Log Viewer.

For additional information, see Chapter 13, “Log Viewer.”



# Routers and Embedded Systems

---

## In This Chapter

|                                        |                 |
|----------------------------------------|-----------------|
| <i>Overview</i>                        | <i>page 589</i> |
| <i>Routers and Blackboxes</i>          | <i>page 590</i> |
| <i>Embedded Systems and Appliances</i> | <i>page 591</i> |

## Overview

A VPN-1/FireWall-1 enforcement point is a machine or device that enforces at least some part of the Security Policy. An enforcement point can be a workstation, router, switch or any machine that can be managed by a Management Module by installing a Security Policy or Access List.

VPN-1/FireWall-1 includes the following types of enforcement points:

- Routers and Security Devices
- Embedded systems and Appliances

# Routers and Blackboxes

## Open Security Extension

The Open Security Extension features enables VPN-1/FireWall-1 to manage third-party routing and security devices. The number of managed routers or devices depends on your license. Routers include hardware and software packet filters. VPN-1/FireWall-1 also supports hardware security devices which provide routing and additional security features, such as Network Address Translation and Authentication. Security devices are managed in the Security Policy as Integrated Firewall objects. The Management Module generates Access Lists from the Security Policy and downloads them to selected routers and devices.

For more information on defining routers or integrated firewalls, see the following sections in Chapter 4, “Network Objects”:

- “Router Properties” on page 118
- “Integrated FireWall Properties” on page 141

TABLE 17-1 summarizes the VPN-1/FireWall-1 features supported by managed routers and blackboxes.

**TABLE 17-1** Routers and Blackboxes - supported VPN-1/FireWall-1 features

| Platform and Version         | Accept/Reject Rules | Anti-Spoofing | Properties     | Logs and Alerts <sup>3</sup> | Implied Last “Reject All” Rule | FTP Data Connections <sup>4</sup> | Access List Import |
|------------------------------|---------------------|---------------|----------------|------------------------------|--------------------------------|-----------------------------------|--------------------|
| Bay Networks Router          | Y                   | Y             | Y              | Y                            | N                              |                                   |                    |
| 3Com Router                  | Y                   | Y             | Y              | Y                            | Y                              | Y                                 | Y                  |
| Cisco Router 9               | Y                   | N             | Y              | Y                            | Y                              |                                   |                    |
| Cisco Router 10.x and higher | Y                   | Y             | Y              | Y                            | Y                              |                                   | Y                  |
| Cisco PIX Firewall 3.0, 4.x  | Y                   | N             | N              | Y                            | Y                              |                                   | Y <sup>7</sup>     |
| Microsoft Steelhead          | Y <sup>1</sup>      | N             | Y <sup>2</sup> | N                            | Y <sup>3</sup>                 | N                                 | Y                  |

1. Action is defined per Policy. You cannot have Accept and Reject rules in the same Policy.

2. Relevant only for a Policy with Accept rules.

3. This is done using the router’s syslog service.

4. This column indicates whether an FTP rule apply to the data connection as well as to the control connection. If the FTP rule does not apply, some other mechanism must be found for allowing the data connection (perhaps by opening all the high ports).

6. Microsoft Steelhead is supported by the Windows GUI only.

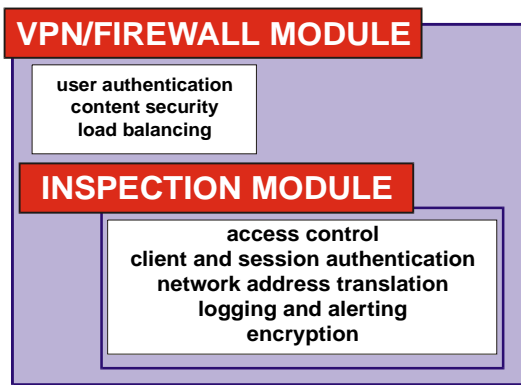
7. PIX version 4.x and higher.

A Bay Networks router can function in either of two modes: as a packet filter (in which case VPN-1/FireWall-1 installs Access Lists on the router), or as an embedded system, (in which case VPN-1/FireWall-1 installs a Security Policy on the router). For more information, see TABLE 17-2 on page 592.

## Embedded Systems and Appliances

Embedded systems and appliances include machines or hardware devices on which a VPN/FireWall Module or an Inspection Module is installed. Inspection Code is generated from the Security Policy and downloaded to targeted devices. Embedded systems implement different VPN-1/FireWall-1 features, depending on whether a VPN/FireWall Module or an Inspection Module is installed.

FIGURE 17-1 depicts the relationship between VPN/FireWall Module and Inspection Module features.



**FIGURE 17-1** FireWall and Inspection Modules

The VPN/FireWall Module includes the Inspection Module, the VPN-1/FireWall-1 Security Servers (which implement Content Security and User Authentication), and the FireWall Synchronization feature. The Inspection Module implements the Security Policy, logs events, and communicates with the Management Module using the daemons.

TABLE 17-2 summarizes the VPN-1/FireWall-1 features supported by embedded systems.

**TABLE 17-2** Embedded Systems - supported FireWall-1 feature

| Platform and Version | Insepection Module (i)/<br>FireWall Module (F) | Anti-Spoofing  | Logs and Alerts | Session and Client<br>Authentication | Network Address<br>Translation (NAT) | Encryption | Accounting | Content Security | Time Objects |
|----------------------|------------------------------------------------|----------------|-----------------|--------------------------------------|--------------------------------------|------------|------------|------------------|--------------|
| <b>Bay RS</b>        | I                                              | Y <sup>1</sup> | Y               | N                                    | N                                    | N          | N          | N                | Y            |
| <b>Bay CES</b>       | I                                              | Y <sup>1</sup> | Y               | N                                    | Y                                    | N          | N          | N                | Y            |
| <b>Xylan Switch</b>  | I                                              | Y              | Y               | N                                    | N                                    | N          | N          | N                | Y            |
| <b>Nokia</b>         | F                                              | Y              | Y               | Y <sup>2</sup>                       | Y                                    | Y          | Y          | Y <sup>3</sup>   | Y            |

1. Interface names on Bay routers are incorrectly retrieved by **Get**, and must be modified manually.

2. Supports SecurID.

3. Content Security includes the following FireWall-1 features:

- Resources (FTP, URI, SMTP)
- User Authentication
- CVP and UPF Server Objects

The following is true for all embedded systems, regardless of the settings in **Control Properties (Properties Setup)** window.

- **Apply Gateway Rules to Interface Direction** is always Eitherbound.
- Fast Mode is always enabled.



**Note** – The above restrictions do not apply to Nokia IP Routing.



# SNMP and Network Management Tools

---

## In This Chapter

|                                         |                 |
|-----------------------------------------|-----------------|
| <i>Overview</i>                         | <i>page 593</i> |
| <i>FireWall-1 HP OpenView Extension</i> | <i>page 595</i> |
| <i>VPN-1/FireWall-1 MIB Source</i>      | <i>page 600</i> |

## Overview

### VPN-1/FireWall-1 SNMP Agent (daemon)

VPN-1/FireWall-1 includes a full SNMP V2 agent with both V1 (r/w community) and V2 security features. Furthermore, VPN-1/FireWall-1 pre-defines the SNMP and SNMP-read services so you can further protect your SNMP agent by restricting read and write access to it.

The VPN-1/FireWall-1 SNMP daemon (`snmpd`) is compatible with network management software such as HP OpenView. In addition, the VPN-1/FireWall-1 SNMP daemon is compatible with RFCs 1155, 1156, and 1157. The Management Information Base (MIB) in `$FWDIR/lib/snmp/mib.txt` supports RFCs 1155 -1213. The SNMP daemon also provides FireWall-1 specific variables.

Installing the VPN-1/FireWall-1 SNMP daemon is optional. VPN-1/FireWall-1 does not require that any SNMP daemon be installed.

### Ports to Which the VPN-1/FireWall-1 SNMP daemon binds

VPN-1/FireWall-1's SNMP daemon is started when VPN-1/FireWall-1 is started (`fwstart`) and is stopped when VPN-1/FireWall-1 is stopped (`fwstop`).

The VPN-1/FireWall-1 SNMP daemon tries to bind to the standard SNMP port (161) and also to port 260. If it fails to bind to port 161 (presumably because another SNMP daemon is already bound to that port), then it binds only to port 260 and passes on all non-VPN-1/FireWall-1 specific SNMP queries to the SNMP daemon on port 161.

If there is no daemon bound to port 161, FireWall-1's daemon binds to both ports (161 and 260). This allows all clients to use VPN-1/FireWall-1's daemon. If another SNMP daemon attempts to bind to port 161 after FireWall-1's SNMP daemon is started, the other daemon will fail to bind to the port. In the event that it is important for you to use an SNMP daemon other than FireWall-1's, start it before you start FireWall-1.

Trap alert as well as status reports can be sent to SNMP-based management software.

Under Windows NT, the VPN-1/FireWall-1 SNMP agent is an extension of the NT SNMP agent. If you have not installed the standard NT SNMP agent, you will not be able to use the VPN-1/FireWall-1 SNMP agent.

## Initial Communities ("Keys")

The initial SNMP communities ("keys") are public and private for read and write, respectively. To change these keys, edit `$FWDIR/conf/snmp.C`, and set the values for the read and write attributes for `:snmp_community`.

## VPN-1/FireWall-1 MIB

The variable definitions for VPN-1/FireWall-1's SNMP daemon are located in the files `$FWDIR/lib/snmp/chkpnt.mib`. This file can be used to incorporate the Check Point MIB into any MIB browser or network management system. All of VPN-1/FireWall-1's SNMP variables are located in the subtree `1.3.6.1.4.1.2620.1.1` (also known as `enterprises.checkpoint.products.fw`).



**Note** – Previous versions of VPN-1/FireWall-1 used enterprise ID 1919 for Check Point private MIB. VPN-1/FireWall-1 version 4.0 uses 2620 — the official Check Point enterprise ID (1.3.6.1.4.1.2620). as the prefix for all Check Point specific MIB variables. SNMP traps also use the updated enterprise ID.

TABLE 18-1 lists the variables that are unique to VPN-1/FireWall-1, and unless otherwise noted, are strings of up to 256 bytes.

**TABLE 18-1** VPN-1/FireWall-1 MIB Variables

| Variable      | Meaning                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| fwModuleState | the state of the Inspection Module                                                                                 |
| fwFilterName  | the name of the currently loaded Security Policy                                                                   |
| fwFilterDate  | the date the Security Policy was installed                                                                         |
| fwAccepted    | the number of packets accepted by the Inspection Module since the last Security Policy was installed (an integer)  |
| fwRejected    | the number of packets rejected by the Inspection Module since the last Security Policy install (an integer)        |
| fwDropped     | the number of packets dropped by the Inspection Module since the last Security Policy install (an integer)         |
| fwLogged      | the number of packets logged by the Inspection Module since the last Security Policy was installed (an integer)    |
| fwMajor       | the VPN-1/FireWall-1 major release number (for example, for VPN-1/FireWall-1 Version 4.0 this is 4) — an integer   |
| fwMinor       | the VPN-1/FireWall-1 minor release number (for example, for VPN-1/FireWall-1 Version 4.0 this is “0”) — an integer |
| fwProduct     | the VPN-1/FireWall-1 product                                                                                       |
| fwEvent       | the last SNMP trap sent by VPN-1/FireWall-1                                                                        |

The source of the VPN-1/FireWall-1 MIB is listed in “VPN-1/FireWall-1 MIB Source” on page 600.

## FireWall-1 HP OpenView Extension

HP OpenView Network Node Manager displays hierarchical maps of the network topology. The VPN-1/FireWall-1 extension provides information on FireWalled objects in the network. The extension enables administrators to:

- display FireWalled objects within the context of the entire network
- specify network objects and devices as FireWalled objects
- open the FireWall-1 Log, Security Policy and System Status views

To enable this feature, the machine running the OpenView Network Node Manager session must have a FireWall-1 GUI client installed. The GUI client must be permitted by the FireWall-1 Management Server, and you must be one of the allowed administrators.

- display connection statistics and SNMP alert information for FireWalls
- access Check Point MIB data

## Installing the FireWall-1 HP OpenView Extension

TABLE 18-2 lists the minimum hardware, operating system, and software requirements for installing the FireWall-1 Extension for HP OpenView Network Node Manager.

**TABLE 18-2** Minimum Requirements

|                         |                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------|
| <b>Platforms</b>        | HP PA-RISC 700/800, Sun SPARC-based systems                                          |
| <b>Operating System</b> | HP-UX 10.x, Solaris 2.3 and higher                                                   |
| <b>Software</b>         | VPN-1/FireWall-1 X/Motif GUI Client<br>HP OpenView Network Node Manager version 4.1x |

For hardware and software requirements of HP OpenView Network Node Manager, consult the HP documentation.

You can install the VPN-1/FireWall-1 HP OpenView Extension either directly from the CD-ROM, or you can recursively copy the installation files from the CD-ROM to a directory on your disk and install from there.

### ▼ To install the VPN-1/FireWall-1 HP OpenView Extension (Solaris2)

- 1** Become superuser.
- 2** Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).
- 3** Enter the following command to install the VPN-1/FireWall-1 HP OpenView Extension:

```
hostname# pkgadd -d .
```

- 4** pkgadd presents a list of packages, and asks you to choose one to install.  
Specify the VPN-1/FireWall-1 HP OpenView Extension by entering either its name or its number in the list.

### ▼ To install the VPN-1/FireWall-1 HP OpenView Extension (HP-UX)

If you encounter a problem with the depth of the CD-ROM directories, use the files in `hpux/TarFiles`.

- 1** Become superuser.
- 2** Copy the installation files to the `/tmp` directory.

- 3** If the `/tmp` directory has not been registered as an installation directory, enter the following command to register it.

```
hostname# swreg -l depot -x select_local=true /tmp
```

For information about the `swreg` command, refer to the HP-UX documentation.

- 4** Enter the following command to install the VPN-1/FireWall-1 HP OpenView Extension:

```
hostname# swinstall &
```

- 5** The **SD Install - Software Selection** window is displayed, and then the **Specify Source** window is displayed on top of it.  
For information about the `swinstall` command, refer to the HP-UX documentation.
- 6** Click on **Source Depot Path**.
- 7** In the **Depot Path** window, select the directory in which the installation files are located.
- 8** Click on **OK** to close the **Depot Path** window.
- 9** Click on **OK** to close the **Specify Source** window.
- 10** In the **SD Install - Software Selection** window, select **FireWall-1 HP OpenView Extension**.
- 11** From the **Actions** menu, select **Install (analysis)**.
- 12** When the analysis phase completes, click on **OK**.
- 13** When the installation phase completes, click on **Done**.
- 14** From the **File** menu, select **Exit**.

## Uninstalling the VPN-1/FireWall-1 HP OpenView Extension

### ▼ To uninstall the VPN-1/FireWall-1 HP OpenView Extension (Solaris2)

Use the `pkgrm` application to uninstall the VPN-1/FireWall-1 HP OpenView Extension.

## ▼ To uninstall the VPN-1/FireWall-1 HP OpenView Extension (HP-UX)

- 1 Become superuser.
- 2 Type the following command:

```
hostname# swremove FWMap
```

## Viewing FireWalled Objects

### Network Submap

HP OpenView Windows displays a hierarchical map of all the devices, systems and FireWalls in the network. FireWalled objects are represented in a network submap by a FireWall icon.

### FireWalls Window

The FireWalls window displays only the FireWalled objects in the network. To open the FireWalls window, double-click on the **FireWalls** icon in the root submap. To access the root submap, click on the **Root Submap** icon on the Open View toolbar.

HP OpenView identifies as FireWalled objects only those objects running the VPN-1/FireWall-1 SNMP daemon.

The FireWall discovery takes place when HP OpenView Windows (ovw) is started and whenever a new device is added to the network. If you start VPN-1/FireWall-1 after the FireWall discovery, the object will not be identified as FireWalled unless specifically queried (see “Query Selected” below).

If HP OpenView discovers a FireWalled object with the VPN-1/FireWall-1 SNMP daemon on port 260, it changes its default SNMP port for that object to 260.

## FireWall Menu

The FireWall menu appears in the menu bar of the submap window.

**TABLE 18-3** FireWall Menu Commands

| Menu Entry        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-------------|----------|--------------------|-----------------|---------------------------|---------------|------------------------------|------------|--------------------------------------------------------------------------------------------------------------------|
| Query Selected    | Performs discovery on the selected objects.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| Set as FireWall   | Sets a network object as a FireWall. This option is enabled only if a VPN/FireWall Module was not detected on the selected object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| Unset as FireWall | Clears FireWall settings from the selected object. This option is enabled only if the object was manually set as a FireWall.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| FireWall-1        | <p>This entry displays a sub-menu with the following options:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td>Log View</td><td>Opens the Log View</td></tr> <tr> <td>Security Policy</td><td>Opens the Security Policy</td></tr> <tr> <td>System Status</td><td>Opens the System Status View</td></tr> <tr> <td>Statistics</td><td>Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall.</td></tr> </table> <p>You can also access the above options by right-clicking on a FireWalled object.</p> <p><b>Note:</b> In order to open the Check Point GUI, the machine running the current OpenView Windows session must have a Check Point GUI client installed. In addition, the GUI client must be permitted by the VPN-1/FireWall-1 Management Server and you must be one of the allowed administrators.</p> | Option | Description | Log View | Opens the Log View | Security Policy | Opens the Security Policy | System Status | Opens the System Status View | Statistics | Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall. |
| Option            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| Log View          | Opens the Log View                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| Security Policy   | Opens the Security Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| System Status     | Opens the System Status View                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |
| Statistics        | Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |        |             |          |                    |                 |                           |               |                              |            |                                                                                                                    |

## VPN-1/FireWall-1 Management Servers

When you start one of the VPN-1/FireWall-1 GUI applications (Security Policy, Log Viewer or System Status), the applications runs against the FireWalled object's Management Server, which is not necessarily the same machine as the FireWalled object. If the VPN/FireWall Module and the Management Server are on different machines, then you must configure the FireWalled object as follows:

- 1 Select the FireWalled object.
- 2 From the **Edit** menu, choose **Describe/Modify Object**.
- 3 In the **Object Description** dialog box, choose **FireWall-1 Management**. The **FireWall-1 Management** dialog box displays the host name of the Management Server.

- 4 Enter the name of the Management Server and click on **OK**.  
Specify the correct host name or IP address.

## VPN-1/FireWall-1 SNMP Traps

The **Application Alert Events** browser displays a log of SNMP traps. All VPN-1/FireWall-1 SNMP traps appear in the **Application Alert Events** browser.



**Note** – You must first direct VPN-1/FireWall-1 SNMP traps to the host running OpenView using the `snmp_trap` command. For more information see “`snmp_trap`” on page 31.

## Check Point MIB Data

The Check Point MIB is accessible through the Network Node Manager SNMP MIB browser.

To access the Check Point MIB, proceed as follows:

- 1 Choose **SNMP MIB Browser** from the **Misc** menu. The **Browse MIB** dialog box is displayed.
- 2 Navigate to the Check Point MIB, which is located under the **Enterprises** subtree.

## VPN-1/FireWall-1 MIB Source

This section presents the source code for the VPN-1/FireWall-1 MIB (in `$FWDIR/lib/snmp/chkpnt.mib`).

```
CHECKPOINT-MIB DEFINITIONS ::= BEGIN

-- SUBTREE: 1.3.6.1.4.1.2620.1.1
-- iso.org.dod.internet.private.enterprises.checkpoint.products.fw

IMPORTS

 enterprises
 FROM RFC1155-SMI
 TRAP-TYPE
 FROM RFC-1215
 OBJECT-TYPE
 FROM RFC-1212;

-- textual conventions

DisplayString ::=
 OCTET STRING
```



```

-- This data type is used to model textual information taken
-- from the NVT ASCII character set. By convention, objects
-- with this syntax are declared as having
--
-- SIZE (0..255)

 checkpoint OBJECT IDENTIFIER ::= { enterprises 2620 }
 products OBJECT IDENTIFIER ::= { checkpoint 1 }
 fw OBJECT IDENTIFIER ::= { products 1 }

 -- the FW group
 -- Overall statistics and state
 -- To be added a table of statistics by interfaces.

fwModuleState OBJECT-TYPE
 SYNTAX DisplayString (SIZE (0..255))
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "The state of the fw module."
 ::= { fw 1 }
fwFilterName OBJECT-TYPE
 SYNTAX DisplayString (SIZE (0..255))
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "The name of the loaded filter."
 ::= { fw 2 }
fwFilterDate OBJECT-TYPE
 SYNTAX DisplayString (SIZE (0..255))
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "When was the filter installed (STRING!)"
 ::= { fw 3 }
fwAccepted OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "The number of accepted packets."
 ::= { fw 4 }

fwRejected OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "The number of rejected packets."

```

```

 ::= { fw 5 }

fwDropped OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "The number of dropped packets."
 ::= { fw 6 }

fwLogged OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "The number of logged packets."
 ::= { fw 7 }

fwMajor OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "FireWall-1 Major Version."
 ::= { fw 8 }

fwMinor OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "FireWall-1 Minor Version."
 ::= { fw 9 }

fwProduct OBJECT-TYPE
 SYNTAX INTEGER
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "FireWall-1 Product."
 ::= { fw 10 }

fwEvent OBJECT-TYPE
 SYNTAX DisplayString (SIZE (0..255))
 ACCESS read-only
 STATUS mandatory
 DESCRIPTION
 "A string containing the last snmp trap sent via fw"

```

```
::= { fw 11 }
```



**Note** – The following comment lines are a description of the MIB used by the SNMP traps generated by VPN-1/FireWall-1.

```
-- fwTrap TRAP-TYPE
-- ENTERPRISE fw
-- VARIABLES { fwEvent }
-- DESCRIPTION
-- "FireWall-1 SNMP trap"
-- ::= 0

END
```



# FAQ (Frequently Asked Questions)

---

## In This Chapter

|                                           |                 |
|-------------------------------------------|-----------------|
| <i>Defining Objects and Services</i>      | <i>page 605</i> |
| <i>Daemons</i>                            | <i>page 609</i> |
| <i>Security Servers</i>                   | <i>page 609</i> |
| <i>Logging</i>                            | <i>page 614</i> |
| <i>Security</i>                           | <i>page 616</i> |
| <i>VPN-1/FireWall-1/n Issues</i>          | <i>page 622</i> |
| <i>Supported Protocols and Interfaces</i> | <i>page 623</i> |
| <i>Inspecting</i>                         | <i>page 625</i> |
| <i>Administrative Issues</i>              | <i>page 627</i> |
| <i>Performance</i>                        | <i>page 628</i> |

## Defining Objects and Services

### Which Network Objects Are on My Network?

Refer to the files `/etc/hosts` and `/etc/networks`. For Unix systems, see the manual pages for `hosts` and `networks`.

If NIS/YP (Network Information Service, formerly Sun Yellow Pages) is running on your system, use the commands `ypcat hosts` and `ypcat networks` to access network information. For Unix systems, see the manual pages for `ypcat`.

## How Do I Define the “Internet” or “Others”?

You might wish to define rules that apply to the “Internet” or to “all other hosts and networks but mine”. To do that, you should first define a group network object that includes all network objects that are “mine”: all your hosts, networks, domains, groups, etc.

Add the “mine” network object to the source or the destination of the rule you are defining and select it. Then use the menu options **Negate**. This will put a cross over the “mine” network object, which indicates: any network object that **Negate** mine (that is, not in “mine” group).

## What’s the difference between hosts, gateways and interfaces?

In defining network objects, it is important to keep in mind the distinction between hosts, gateways, and interfaces.

A gateway is a host whose **Type** is defined in the **Workstation Properties** window as **Gateway**.

A gateway will have more than one interface, but the gateway itself is a single object and should be defined as such. Each of the interfaces is defined as a separate item in the **Network Interfaces** section of the **Workstation Properties** window.

A host’s name is the string returned by the `hostname` command. The IP address is the one corresponding to the host’s name, as given in `/etc/hosts`, NIS/YP (Yellow Pages) or DNS.

## Which Services and Protocols Are on My Network?

Refer to the files `/etc/services`, `/etc/rpc`, and `/etc/protocols`. For Unix systems, see the manual pages for `services`, `rpcinfo`, and `protocols`.

If NIS/YP (Network Information Service, formerly Sun Yellow Pages) is running on your system, use the commands `ypcat services` and `ypcat protocols` to access network information. For Unix systems, see the manual pages for `ypcat`.

## Which Services Have More Than One Type?

Some services are available under more than one protocol; that is, they have more than one type. For instance, `time` and `domain` are available under both UDP and TCP; `nfs` is a UDP service and an RPC program. Some services are available under more than one protocol; that is, they have more than one type. For instance, `time` and `domain` are available under both UDP and TCP; `nfs` is a UDP service and an RPC program.

**TABLE 19-1** Services available under both TCP and UDP

| service name | port number | service name | port number |
|--------------|-------------|--------------|-------------|
| chargen      | 19          | echo         | 7           |
| daytime      | 13          | sunrpc       | 111         |
| discard      | 9           | time         | 37          |
| domain       | 53          |              |             |

**TABLE 19-2** Services available both as RPC and TCP or UDP

| RPC name   | RPC program number | TCP/UDP name | TCP/UDP number   |
|------------|--------------------|--------------|------------------|
| portmapper | 100000             | sunrpc       | UDP/TCP port 111 |
| nfs        | 100003             | nfs          | UDP port 2049    |

### Which Services Are Dependent on Other Services?

Common services that require other services to function correctly are listed in TABLE 19-3 on page 607. Some services are available in several types (for instance, `nfs` could be UDP or RPC). Each type may have different dependencies..



**Note** – VPN-1/FireWall-1 is supplied with predefined service groups that ensure that access is allowed to all other services required for a service to function properly.

**TABLE 19-3** Services Dependent on Other Services

| Service                      | Type     | Number | Required                                  | Recommended |
|------------------------------|----------|--------|-------------------------------------------|-------------|
| ypserv                       | RPC      | 100004 | ypbind<br>yppasswd<br>ypupdated<br>ypxfrd |             |
| nfs                          | RPC      | 100003 | mountd<br>nlockmgr                        | ypserv      |
| nfsd                         | UDP      | 2049   | mountd                                    |             |
| r* (rcp, rsh but not rlogin) | commands |        | shell (TCP)                               |             |

### Dual DNS (Internal and External)

In a configuration that includes two Domain Name Servers (DNS) — an internal DNS for resolving internal names and an external DNS for resolving external names — the internal names can be hidden from external users by the following strategy:

- the external DNS has primary entries to a limited number of internal hosts
- the external DNS cannot issue inquiries to the internal DNS
- the internal DNS can issue inquiries to the external DNS

In this way, the internal DNS is restricted to resolving internal names for internal users while external users can gain no knowledge of internal names.

VPN-1/FireWall-1 can be used to enforce this strategy. The external DNS can reside on the FireWalled gateway.

## How Many Rules Are Supported?

Theoretically, the Policy Editor can support a large number of rules, and Rule Bases of more than 150 rules are not uncommon. In practice, even very complex policies are normally defined in about 15 rules. Since the rules can contain group objects, a small number of rules is usually sufficient to define the Security Policy.

Is it necessary to define each of a gateway's interfaces as a separate network object? If yes, are they all gateways, or should the other interfaces be defined as hosts? Why doesn't VPN-1/FireWall-1 treat a gateway and all its interfaces as a single object?

The interface is not a separate network object, but rather part of another network object (gateway, router, etc.). You should *not* define interfaces as network objects. Instead, define interfaces as part of the workstation definition in the **Interfaces** tab of the **Workstation Properties** window.

Is there a way to allow only specific ports to communicate with a system?

To limit source port number from 2000 to 3000, proceed as follows:

- 1** In the Services Manager, create a new service of type TCP or UDP.
- 2** In **Source Port Range**, enter the range 2000 - 3000.
- 3** Then use the newly created service in your Rule Base.

How can I control FTP from HTTP?

There is no difference, from VPN-1/FireWall-1's point of view, between an FTP session that originated as such (for example, a user typing `ftp elvis.com`) and an FTP session created when a user downloads a file by clicking on its name in a Web page. A rule that applies to one applies to the other.

If you wish to enable your users to use FTP from their Web browsers, you must define a rule allowing them to use FTP in general, without reference to HTTP. In addition, you must also:

- *not* define an FTP proxy to the browser
- set the **Enable PASV FTP Connections** property (required by some HTTP servers)

How can I restrict ping information to allow a set of machines to ping freely without restrictions, while preventing other hosts from pinging through the firewall?

Create two rules, one to allow the set of machines to send echo-requests and another to allow that same set of machines to receive echo-replies.

You can combine the two rules, either by putting both services in the same rule or by specifying "echo" (a pre-defined group which includes echo-request and echo-reply) as the service.

Because ping is an ICMP service and therefore has no port numbers, it is treated differently from other services, such as FTP and TELNET, which are automatically allowed to return information. The ping information is checked when it leaves and



when it comes back, preventing a single rule from allowing a set of machines unrestricted pings, as the returns from the remote machines are dropped by VPN-1/FireWall-1.

## Daemons

`inetd.conf` and the VPN-1/FireWall-1 TELNET Daemon

*Question:* If I am running VPN-1/FireWall-1 with User Authentication, can I still allow a standard TELNET to the FireWalled host itself? In other words, will making a rule that allows TELNET (without User Authentication) re-install the standard `in.telnetd` in `inetd.conf`?

*Answer:* The answer to the second question is no. Once you install the VPN-1/FireWall-1 Security Servers, VPN-1/FireWall-1 modifies `inetd.conf` and comments out the standard TELNET and FTP daemons.

## Security Servers

How can I hide that the fact that VPN-1/FireWall-1 is running from users of authenticated TELNET and FTP services?

If you want users to see only the user defined message file, and not the “VPN-1/FireWall-1 authenticated telnet gw...” message, then add the following line to `objects.C`, under “:props”:

```
:undo_msg (true)
```

How is VPN-1/FireWall-1 configured in relation to the SecurID ACE software?

The VPN-1/FireWall-1 software uses the standard client library of the ACE/Server. In order to use SecurID, proceed as follows:

- 1 Install and configure the ACE Server.

You will need an ACE Server somewhere in your network. The ACE Server does not have to reside on the VPN-1/FireWall-1 machine. For information about how to install and configure your ACE server, refer to the SecurID documentation.

- 2 In VPN-1/FireWall-1, create a user whose authentication scheme is SecurID.

- 3 Configure your VPN-1/FireWall-1 machine as an ACE Client.

The VPN-1/FireWall-1 software uses the standard client library of the ACE/Server. This means that you don't have to do anything special in order to integrate the software. All you have to do is to prepare the FireWalled machine as an ACE Client.

For information about how to install and configure an ACE Client, refer to the SecurID documentation.

VPN-1/FireWall-1 reads the `sdconf.rec` file to determine the ACE Server and other parameters involving ACE Client-Server communications. So, copy `sdconf.rec` from the ACE Server to the ACE Client.

**TABLE 19-4** `sdconf.rec` directory

| sdconf.rec directory |                |
|----------------------|----------------|
| Unix                 | /var/ace       |
| Windows NT           | WINNT/SYSTEM32 |

How can I define an Authentication rule for individual users rather than for groups?

The short answer is that it's not possible, but you can achieve the effect by defining a group for every user. Then you might have a user Alice and a group GrpAlice (with only Alice as a member), a user Bob and a group GrpBob (with only Bob as a member), and so on for each of your users.

The long answer is that it's not clear what the benefit of this would be, since you can define restrictions at the user level that are enforced for each user in a group. For example, suppose you have a rule like this:

| Source            | Destination | Services | Action   | Track     | Install On |
|-------------------|-------------|----------|----------|-----------|------------|
| DayUsers@localnet | Any         | Any      | UserAuth | Short Log | Gateways   |

The rule does not apply equally to all the users in the group **DayUsers**. It allows each user access only in accordance with his or her access privileges, as defined in each user's **User Properties** window. (This is true if you have chosen the default value, **Intersect with User Database**, in the rule's **User Authentication Action Properties** window.)

Suppose you want to allow Alice access only in the morning, and Bob access only in the afternoon. Just set their access privileges accordingly in their **User Properties** windows. Then, no matter which groups they belong to, they will be allowed access during those times only.

You can also set each user's **Allowed Sources** to his or her own PC. Then Alice and Bob will each be allowed access only during their defined times and only from their own PCs.

On the other hand, suppose you want to restrict Alice to using only FTP and Bob to using only TELNET. Then you really do have to define separate groups, for example, GrpFTP and GrpTELNET, and define Alice as a member (perhaps the only member) of the first group and Bob as a member (perhaps the only member) of the second group, and write two rules:

| Source             | Destination | Services | Action   | Track     | Install On |
|--------------------|-------------|----------|----------|-----------|------------|
| GrpFTP@localnet    | Any         | ftp      | UserAuth | Short Log | Gateways   |
| GrpTELNET@localnet | Any         | telnet   | UserAuth | Short Log | Gateways   |

If these are the only rules in the Rule Base which apply to the members of these groups, then they will be restricted to using the given services, because the default rule will deny them access to all other services.

The interplay between the group's access privileges (as defined in the rule) and the users' access privileges (as defined in the **User Properties** window) gives you considerable flexibility.

Is it possible to authenticate FTP through a Web browser? For example, when the user tries to download a file through the Web browser, he or she should have to enter a name and password. But, when we try this, we get an error message from the browser.

When using a browser without defining a proxy in the browser, all HTTP requests use the HTTP protocol and all FTP requests use the FTP protocol. Only part of the FTP protocol is supported in this mode; only anonymous ftp requests can be performed.

When using a browser with a proxy defined for FTP (this is defined in the browser), the defined proxy should be an HTTP proxy and not an FTP proxy. There is no way of using an FTP proxy for FTP connections when the client is a Web browser — this is a limitation of the Web browser and not of VPN-1/FireWall-1.

When using this configuration, the connection between the browser and the proxy uses the HTTP protocol. It is up to the proxy to convert the request from the HTTP protocol of the FTP protocol:



**FIGURE 19-1** Accessing FTP through an HTTP proxy

The VPN-1/FireWall-1 HTTP Security Server does not support this kind of protocol conversion. So, if you wish to use the VPN-1/FireWall-1 to authenticate FTP requests from a Web browser, a second proxy which does support this kind of protocol conversion should be installed, and defined to VPN-1/FireWall-1 as the next HTTP proxy. This configuration is shown in FIGURE 19-2.



**FIGURE 19-2** Authenticating FTP through the HTTP Security Server

If you do not define a next proxy to VPN-1/FireWall-1, then you will get an error message “scheme ftp not supported” when you attempt to authenticate an FTP request.

For additional information, see “The HTTP Security Server in Proxy Mode” on page 502.

How can I go across two or more FireWalls for authenticated services?

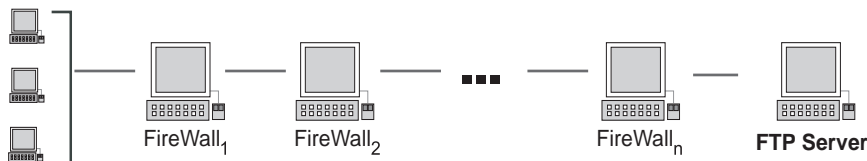
TELNET

This is easy enough to do with TELNET — just TELNET to one FireWall after the other in sequence, authenticating yourself each time, until you get to your final destination.

FTP

For FTP, it’s a little more complicated. Suppose you have  $n$  FireWalls, as in FIGURE 19-3:

localnet



**FIGURE 19-3**  $n$  FTP authenticating FireWalls

- 1** FTP to the first FireWall.
- 2** Then, as your user name, enter:
  - the user name on the FTP server and the FTP server IP address (or name), followed by
  - the user name and the IP address (or name) of the next authenticating FireWall, one after the other, separated by @ characters, *in reverse order*:

```

FtpUser@FtpServerIP@FW_nUser@FW_nIP@FW_{n-1}User@FW_{n-1}IP ...
@FW_2User@FW_2IP

```

- 3** As your password, enter each password one after the other, separated by @ characters, *in reverse order*:

```
FtpPass@FWnPass@FWn-1Pass ... @FW1Pass
```

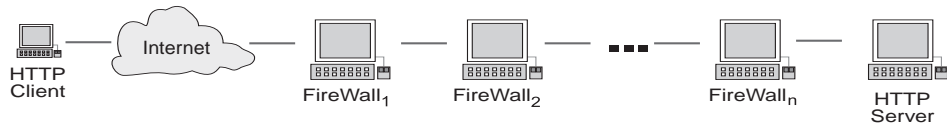
## HTTP

For HTTP outbound connections, just define the VPN-1/FireWall-1 HTTP Authenticating Server as your proxy in the browser and you will get the authentication prompts, one after the other.

If you are using a Netscape browser or Internet Explorer 3.0, then the authentication for outbound HTTP (when VPN-1/FireWall-1 is defined as a proxy to the browser) and inbound HTTP is done separately, that is, the user is prompted for each authentication separately, as he or she moves outward from the client.

For HTTP inbound connections, enter the list of passwords and users *in reverse order*. Since a password or user name can include a @ character, the passwords in the list are separated in an unusual way:

Suppose you have  $n$  FireWalls, as in FIGURE 19-4:



**FIGURE 19-4**  $n$  HTTP Authenticating FireWalls

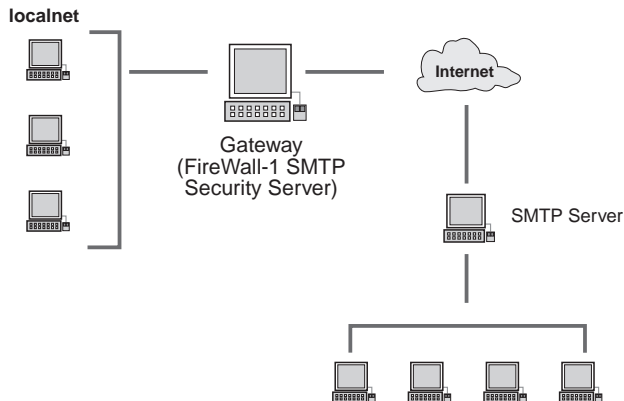
After the  $n^{\text{th}}$  user enter  $2^{n-2}$  @ characters, followed by the  $(n-1)^{\text{th}}$  user and  $2^{n-3}$  @ characters, etc.

```
HttpUser(2n-1@)HttpServerIP@FWnUser(2n-2@)FWnIP@FWn-1User(2n-3@)FWn-1IP ... @FW2User@FW2IP
```

## SMTP

When the VPN-1/FireWall-1 SMTP Security Server detects an error, I expect that it will notify the sender of the mail message (assuming the **Notify Sender on Error** field is checked in the SMTP Resource definition). Instead, I get a “connection to original-MTA failed” error message in the log.

This situation arises when there is no SMTP server between the sender and the VPN/FireWall Module. To understand what is happening, consider the networks in FIGURE 19-5.



**FIGURE 19-5** “connection to original-MTA failed”

Suppose a message sent from localnet is rejected by the VPN-1/FireWall-1 SMTP Security Server. If **Notify Sender on Error** is checked, then the Security Server will attempt to send a mail message to the original source. If that workstation is running Windows, there will usually not be a mail server listening on port 25, and the result will be the “connection to original-MTA failed” message in the log. Unix workstations usually do have mail servers installed on port 25.

On the other hand, if the original mail message arrives at the VPN-1/FireWall-1 SMTP Security Server from the Internet, then there will be a mail server on the return path and the notification will be successful.

In practice, this is rarely a problem, since nearly all mail messages will have passed through a mail server before arriving at the VPN-1/FireWall-1 SMTP Security Server.

## Logging

### How Can I Do a Statistical Analysis of My Log File?

Use the command `fw log` and redirect its output to a file. You can then parse the file with standard Unix tools like `perl`, `sort`, `awk`, or `sed`. Alternatively, the file can be used as input to database or spreadsheet programs.

You can also export the Log File by choosing **Export** in the **File** menu, or with the `fw logexport` command (see “fw expdate” on page 46 of *Check Point Reference Guide*).

Some Log entries refer to rule zero (or to rules with negative numbers!), but there are no such rules in the Rule Base.

#### Rule Zero

Rule zero is the rule VPN-1/FireWall-1 adds before the rules in Rule Base to implement Anti-Spoofing, dropping of packets with IP options, and some aspects of authentication. Anti-spoofing is implemented before any rules are applied, so anti-spoof track logging shows rule zero as the relevant rule.

For example, if a user fails to log in to an authentication server, then the log shows rule zero because at the time of the failure, the relevant rule (that is, the rule under which the user would have been granted or denied access had the login been successful) is unknown, since the requested service is unknown.

#### Rules with Negative Numbers

These are rules added by VPN-1/FireWall-1 to implement certain features. For example, a log entry generated as a result of an `fw sam` command (see “fw sam” on page 17 of *Check Point Reference Guide*) carries a negative rule number.

Is there any way I can choose to not log certain services? My Log File is filling up with recurring traffic through certain ports, and I don't know what these services are.

If you do not want these services to be logged, then define a rule (early in the Rule Base) that accepts them without logging them. However, from a security point of view, you should not be allowing communications unless you know what they are, so your first priority should be to identify the nature of the unknown traffic.

In my Log Viewer, I see some entries where my internal router is the Source and the protocol is ICMP. I have no idea what these entries are, or whether I should be concerned about them.

Some routers send ICMP packets from time to time, and you need not be concerned about it. You can remove the Log entries by adding a rule to the Rule Base that accepts ICMP packets from the internal router but does not log them.

How can I switch my Log File on a periodic basis?

You can do this in NT with the following command:

```
at <time> c:\winnt\fw\bin\fw logswitch
```

## Security

### Does Packet Reassembly Pose a Security Risk?

VPN-1/FireWall-1 performs virtual packet reassembly, and does not send a packet until all its fragments have been collected and inspected. The algorithm used is stricter than the standard packet reassembly algorithm, and does not permit overlays.



**Note** – Since IP specifications forbid a router from reassembling IP fragments, VPN-1/FireWall-1 does not send the reassembled packet but rather the fragments as VPN-1/FireWall-1 received them. This is the origin of the term “Virtual Defragmentation.”

### Do Aliased (or Virtual) Interfaces Pose a Security Risk?

VPN-1/FireWall-1 ignores virtual interfaces, so that inspection and anti-spoofing is performed on the physical interface.

If you want to use virtual interfaces with anti-spoofing, you must define two network objects, one for each subnet, and then create a network group which consists of the two network objects. Then you can put the group in the physical interface’s anti-spoofing entry, just as you would if there were another physical network connected to the interface.

### How does VPN-1/FireWall-1 prevent session hijacking?

VPN-1/FireWall-1’s Encryption feature is the best solution, if you are concerned about this problem. Encryption would prevent hijacking by anyone who does not have the key.

### How does VPN-1/FireWall-1 prevent attacks based on TCP sequence number prediction?

Here too, VPN-1/FireWall-1’s Encryption feature is the best solution. Even if the attacker knows the sequence number, he or she would be unable to interfere with the encrypted connection.

### How does VPN-1/FireWall-1 Deal with IP Options?

VPN-1/FireWall-1 drops packets with IP options, because they are considered to pose a serious security risk.

### Is a FireWalled Host Not Secured When It Re-boots?

If IP Forwarding is disabled, then there is no time during the re-boot process during which a protected network is not secured. For further information, see “IP Forwarding” on page 22.

For information about protecting the FireWalled host during the re-boot process, see “Default Security Policy” on page 305.



## Can VPN-1/FireWall-1 secure modem connections?

VPN-1/FireWall-1 can secure modem connections provided that:

- the modem is “in front” of the FireWalled gateway, and
- the dial-up lines provide PPP or SLIP connections

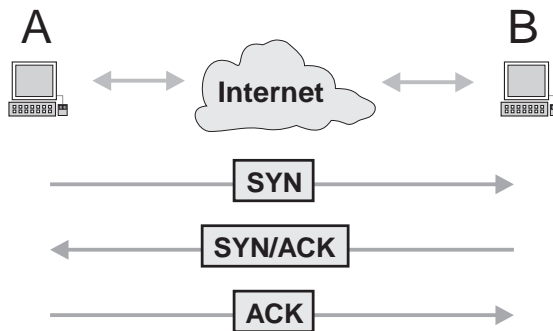
If both these conditions are true, then VPN-1/FireWall-1 treats connections via the modems the same ways it treats connections via Ethernet, token ring, etc.

## What is the TCP SYN Flooding Attack?

### The TCP SYN Handshake

TCP (Transport Control Protocol) is a connection-oriented, reliable transport protocol. Two participating hosts must first establish a connection by a three-way handshake between them. TCP assigns sequence numbers to every byte in every segment and acknowledges all data bytes received from the other end.

For example, if host A wants to establish a connection with host B, A begins by sending a SYN packet (a TCP packet with the SYN bit set) to B. B replies with a SYN/ACK packet (a TCP packet with the SYN and ACK bits set). A completes the three-way hand-shake with a TCP ACK packet.



**FIGURE 19-6** TCP SYN handshake

When B receives the SYN packet, it allocates substantial memory for the new connection. If there were no limit to the number of connections, a busy host would quickly exhaust all of its memory trying to process TCP connections. However, there is usually a small upper limit to the number of concurrent TCP connection requests (“backlog queue”) a given application can have running on the host.

Typically, the upper limit for each server program (for example, a Web server) running on the host is ten outstanding unacknowledged (un-ACK’d) connection requests. When the backlog queue limit is reached, an attempt to establish another connection will fail until one of the backlogged connection either becomes established (SYN/ACK packet is ACK’d), is reset (a RST packet is received) or times out (usually after 75 seconds).

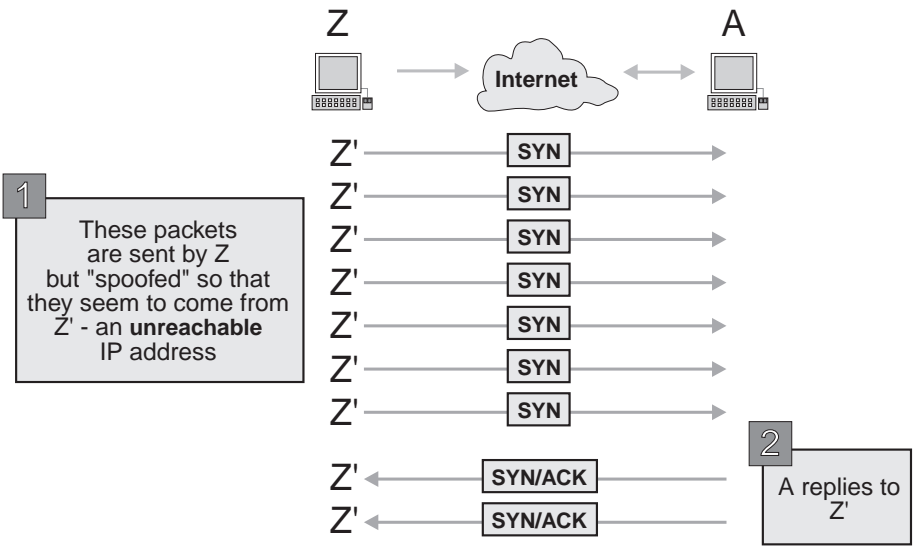
## How the Attack Works

The following description of a SYN flooding attack is based on an in-depth description published online in Phrack Magazine (<http://www.fc.net/phrack/files/p48/p48-13.html>).

A client initiates a TCP connection by a request with the SYN flag set in the TCP header. Normally the server replies with a SYN/ACK identified by the source IP address in the IP header. The client then sends an ACK to the server (FIGURE 19-6 on page 617) and data exchange begins.

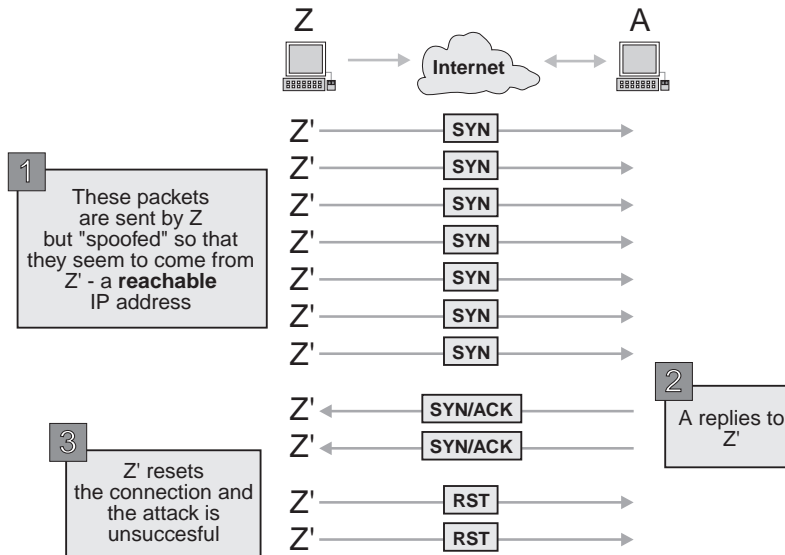
When the client IP address is spoofed (changed) to that of an unreachable host, the targeted TCP cannot complete the three-way hand-shake and will keep trying until it times out. This is the basis for the SYN flood attack.

The attacking host (Z) sends a small number (less than 10 is sufficient) of SYN requests to the target TCP port (for example, the Web server). The attacking host also spoofs the source IP address as that of another (Z'), currently unreachable host. The process is depicted in FIGURE 19-7.



**FIGURE 19-7** SYN Attack

The source IP address (Z') must be unreachable because the attacker does not want any host to receive the SYN/ACKs from the target TCP, which would elicit a RST from that host (an RST packet is issued when the receiving host does not know what to do with a packet) and thus foil the attack (FIGURE 19-8).



**FIGURE 19-8** The SYN Attack unsuccessful, because Z' is reachable

Instead, until the SYN requests time out, A will not accept any connection requests. If the attacks were, for example, against A's Web server, then that Web server will be inaccessible for some 75 seconds as a result of an attack that lasted less than one second.

### VPN-1/FireWall-1 SYNDefender

Check Point's SYNDefender provides two different approaches for defending against a SYN flooding attack:

- SYNDefender Gateway
- SYNDefender Passive Gateway

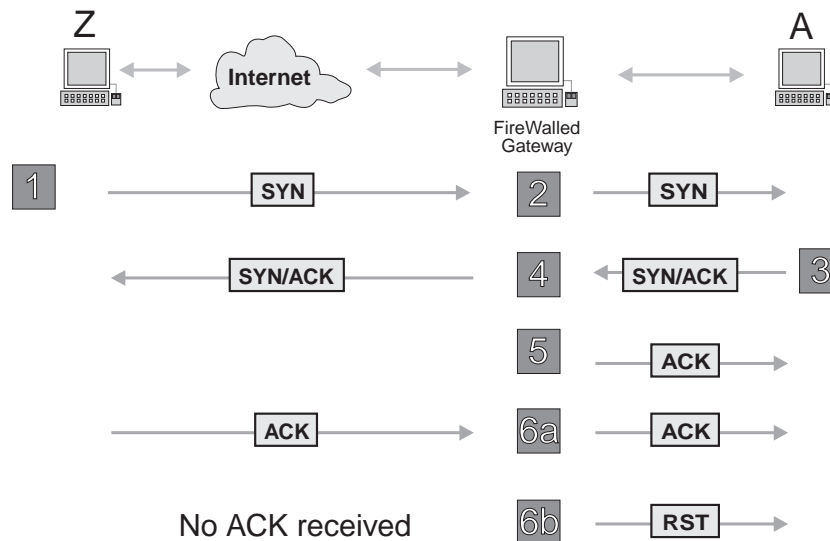
Both of these solutions are integrated into the VPN-1/FireWall-1 Inspection Module, a high-performance kernel-level process that intercepts all packets before they are observed by the operating system and performs Stateful Inspection on these packets. The system administrator can choose which of the solutions is best suited to a particular environment.

#### SYNDefender Gateway

In order for the resetting of SYN connection attempts to be effective against the SYN flooding attack, the reset timer must be short enough to keep A's backlog queue from filling up, while at the same time long enough to enable users coming over slow links to connect. The SYNDefender Gateway solution surmounts this problem by ensuring that an ACK packet is sent in immediate response to A's SYN/ACK packet.

When A receives the ACK packet, the connection is moved out of the backlog queue and becomes an open connection on A. Internet servers can typically handle hundreds or thousands of open connections, so the SYN flooding attack is no more effective in creating a denial of service condition than a hacker trying to establish an excessive number of valid connections to the server. The backlog queue is effectively kept clear and it is possible to wait longer before resetting connections which have not been completed.

SYNDefender Gateway is depicted in FIGURE 19-9.



**FIGURE 19-9** SYNDefender Gateway

- 1** VPN-1/FireWall-1 intercepts a SYN packet going to host A and records the event in an INPSPECT state table.
- 2** VPN-1/FireWall-1 lets the SYN packet continue on to A.
- 3** VPN-1/FireWall-1 intercept A's SYN/ACK reply to Z and correlates with the corresponding SYN packet sent by Z.
- 4** VPN-1/FireWall-1 lets the SYN/ACK continue on its way to Z.
- 5** VPN-1/FireWall-1 sends an ACK packet to A, which moves the connection out of A's backlog queue.
- 6** At this point, one of two things will happen, depending on whether the connection attempt is valid.
  - a** If Z's connection attempt is valid, then VPN-1/FireWall-1 will receive an ACK from Z which it will pass on to A.  
A ignores this second redundant ACK since the three-way handshake has already been completed.

- b** If Z's IP address does not exist, then no ACK packet will return from Z to A and the reset timer will expire. At this point, VPN-1/FireWall-1 resets the connection.

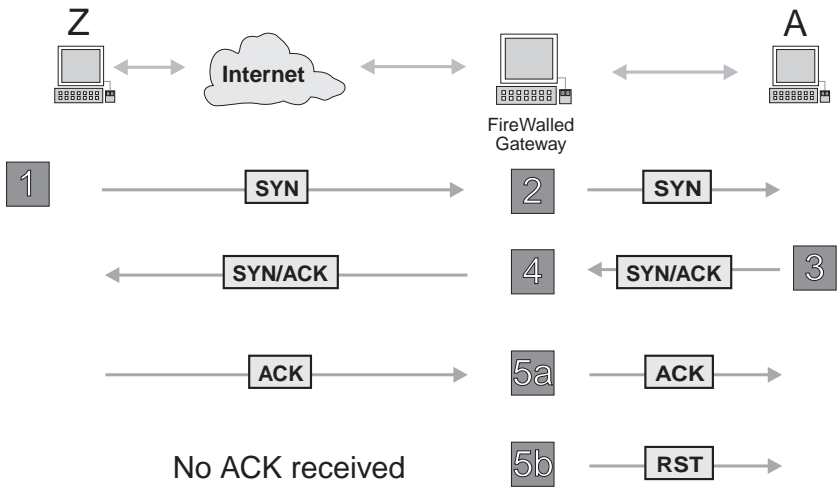
The effectiveness of the SYNDefender Gateway solution is based on quickly moving connection attempts out of the backlog queue. SYN flood connection attempts then fail to fill up the backlog queue and remain as harmless as one of the host's open connections, until the VPN-1/FireWall-1 timer expires and the connection is reset or canceled.

#### SYNDefender Passive Gateway

SYNDefender Passive Gateway is similar to SYNDefender Gateway, except that VPN-1/FireWall-1 does not simulate Z's ACK packet to A, and instead waits for Z's ACK before passing it on to A.

The unacknowledged connection remains in A's backlog table, but times out after FireWall's timeout period, which is much shorter than the backlog queue's timeout period.

FIGURE 19-10 depicts SYNDefender Passive Gateway.



**FIGURE 19-10** SYNDefender Passive Gateway

## Guidelines for Deploying SYNDefender

While there are no strict rules for when to use each of the SYNDefender solutions, some basic guidelines will help establish the appropriate policy for a given situation.

### SYNDefender Gateway

SYNDefender Gateway has two primary advantages:

- Users establishing valid connections with the protected server will not incur any delay in connection setup time.

- There is very little overhead on VPN-1/FireWall-1.

However, since connections are established on the server, that is, moved from the backlog queue, it is important to consider how many established connections the protected server can support relative to the normal load handled by the server.

## Choosing an Appropriate SYNDefender Method

As a first step, you should consider whether you need SYNDefender at all. Since the SYN flooding attack is a “denial of service” attack rather than a security breach, it may be more effective to deploy SYNDefender only after a SYN attack actually occurs.

## VPN-1/FireWall-1/n Issues

How are these products restricted?

VPN-1/FireWall-1 products enforce restrictions based on the number of protected hosts. If these restrictions are exceeded, VPN-1/FireWall-1 will issue an error message. These restrictions are:

### 1 number of internal hosts

Up to  $n$  nodes behind the gateway are allowed, where  $n$  is the number in the product name. For example, FireWall-1/50 is restricted to 50 nodes, VPN/FireWall-1/250 is restricted to 250 nodes, *etc.*

A node is defined as a computing device with an IP address. A multi-user computer with one IP address is counted as one node.

This restriction relates to the number of protected hosts. Every host behind VPN-1/FireWall-1 is protected by VPN-1/FireWall-1, even if no connections to the outside are initiated from that host.

Every node protected by VPN-1/FireWall-1 is counted against the limit, even if its IP address is hidden from VPN-1/FireWall-1 by a proxy or by other means.

### 2 number of external interfaces

For all VPN-1/FireWall-1/ $n$  products, only one external interface may be connected to the FireWalled machine.

There is *no* restriction on the number of internal interfaces on the FireWalled machine.

**3** no external VPN/FireWall Modules

An additional restriction for these products is that they cannot manage external VPN/FireWall Modules, that is, the Management Module and the VPN/FireWall Module must both be on the same machine. However, the Management Module can be deployed in a Client/Server configuration.



**Warning** – If you exceed the restriction on the number of protected hosts, VPN-1/FireWall-1 will display warning messages on the system console notifying you that you have violated the terms of the VPN-1/FireWall-1 license. You should immediately upgrade to the appropriate product in order to be in compliance with the terms of the VPN-1/FireWall-1 license. In the meantime, your security is not compromised and VPN-1/FireWall-1 will continue to protect your network.

## Supported Protocols and Interfaces

Can VPN-1/FireWall-1 inspect IPX packets?

VPN-1/FireWall-1 completely ignores other IP level protocols, such as IPX and DecNET, which are processed by a different protocol stack. This means that if these protocol stacks are installed on the gateway they will be passed without being inspected.

Installing protocol stacks on the gateway which are not inspected by VPN-1/FireWall-1 is considered a security risk.

Does VPN-1/FireWall-1 Support the Talk protocol?

VPN-1/FireWall-1 does not currently support the Talk protocol.

Can I Use DES With ACE (SecurId)?

VPN-1/FireWall-1 supports the DES option of the SecurID ACE server.

Does VPN-1/FireWall-1 support PPP, SLIP and X.25?

VPN-1/FireWall-1 supports PPP, SLIP and X.25, but these interfaces must be installed before VPN-1/FireWall-1 starts.

Does VPN-1/FireWall-1 support Kerberos?

VPN-1/FireWall-1 supports the Kerberos service, but the Kerberos authentication scheme is not supported.

Does VPN-1/FireWall-1 support AXENT Pathways' SecureNet Keys?

Starting with VPN-1/FireWall-1 Version 3.0, The VPN-1/FireWall-1 Security Servers support the SecureNet Keys (SNK) authentication scheme. For further information, see Chapter 15, "Authentication."

Are there any special considerations for ISDN interfaces?

If you are implementing a default Security Policy (see “Default Security Policy” on page 305) on a gateway with ISDN interfaces, VPN-1/FireWall-1 will not recognize the ISDN interfaces. The reason is that during the boot process, the ISDN interfaces are loaded just after the default Security Policy. When the real Security Policy is loaded, VPN-1/FireWall-1 “knows” that it has been loaded before, so it does not scan for new interfaces. There are several possible solutions to this problem:

- Disable the default Security Policy, at the cost of leaving the gateway exposed during the boot process.
- Deploy the default Security Policy only after the ISDN interfaces have been configured, exposing the gateway until that point.

Since the gateway is only connected to the Internet after the ISDN interfaces are configured, this solution entails a relatively short period of vulnerability.

- Leave the default Security Policy in its normal place and configure the ISDN interfaces after the real Security Policy is loaded.

In Unix systems, you will get an error message when you add the ISDN interfaces, and you must then uninstall the VPN-1/FireWall-1 kernel and install it, as follows:

```
fw ctl uninstall
fw ctl install
fw fetch localhost
```

For information on the `fw ctl` command, see “fw ctl” on page 21 of *Check Point Reference Guide*.

How does VPN-1/FireWall-1 deal with Secure Socket Layer (SSL) and HTTPS connections?

Since all SSL negotiation, authentication and encryption take place outside the VPN-1/FireWall-1 software (for example, between an HTTP client and an HTTP server), VPN-1/FireWall-1 does not deal with SSL directly.

HTTPS is an HTTP protocol on top of SSL. The default HTTPS port number is 443, as assigned by the Internet Assigned Numbers Authority (IANA). To allow HTTPS connections, create a new service of type TCP and port number 443. Then use HTTPS in your Rule Base. For example:

| Source   | Destination | Services | Action | Track     | Install On |
|----------|-------------|----------|--------|-----------|------------|
| localnet | Any         | https    | Accept | Short Log | Gateways   |

Note that HTTPS is not HTTP, so the VPN-1/FireWall-1 HTTP Authenticating Server doesn’t work with HTTPS.



## How Can I Handle Multicast?

Firewall-1 does not treat multicast as a special case, so for VPN-1/FireWall-1, a multicast packet is simply an IP packet with a class D (224.0.0.0 — 239.255.255.255) destination address.

If you wish to specify a rule which will apply to all multicast packets, define a network object (of type network) whose IP address is 224.0.0.0 and whose netmask is 240.0.0.0. This network will encompass all legal multicast destination addresses.

To use multicast with Anti-Spoofing, add the multicast network to all the interfaces to which multicast packets might be sent. You must do this because Anti-Spoofing checks both the destination and source IP addresses.

## Inspecting

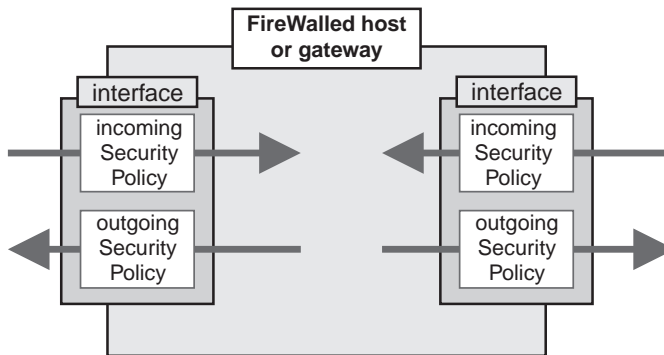
### How is a Security Policy enforced on a host's different interfaces?

A Security Policy is enforced on all the interfaces of a FireWalled host or gateway. The only way to restrict the enforcement of a rule to specific interface is by using INSPECT.

On each interface, the Security Policy is enforced differently for incoming and outgoing packets, depending on the rule's **Install On** field.



**Note** – The terms “outgoing” and “incoming” relate to the machine, not to the networks to which the machine is connected. “Incoming” means entering the machine and “outgoing” means leaving the machine, regardless of the packet’s source or destination (see FIGURE 19-11)



**FIGURE 19-11** Incoming and Outgoing Communications

TABLE 19-5 describes the Security Policy enforced for FireWalled gateways. The information applies to the machines defined as **Gateways** in the **Workstation Properties** window when a rule’s **Install On** field is **Gateways**.

**TABLE 19-5** Gateways - Direction of Enforcement

| Apply Gateway Rules to Interface Direction property | what is enforced for incoming packets | what is enforced for outgoing packets                          |
|-----------------------------------------------------|---------------------------------------|----------------------------------------------------------------|
| Inbound                                             | Rule Base and Properties              | Properties (most importantly, <b>Enable Outgoing Packets</b> ) |
| Outbound                                            | Properties                            | Rule Base and Properties                                       |
| Eitherbound                                         | Rule Base and Properties              | Rule Base and Properties                                       |

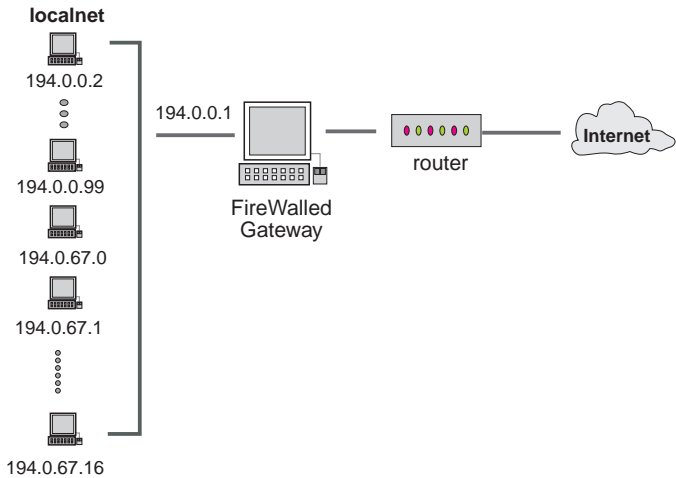
TABLE 19-6 describes the Security Policy enforced for FireWalled hosts. The information applies to machines defined as **Host** in the **Workstation Properties** window when a rule’s **Install On** field is not **Gateways**.

**TABLE 19-6** Hosts - Direction of Enforcement

| Install On                             | what is enforced for incoming packets | what is enforced for outgoing packets |
|----------------------------------------|---------------------------------------|---------------------------------------|
| Source                                 | Properties                            | Rule Base and Properties              |
| Destination                            | Rule Base and Properties              | Properties                            |
| Targets (host is explicitly specified) | Rule Base and Properties              | Rule Base and Properties              |

How can I protect my internal hosts from each other?

Consider the following configuration:



**FIGURE 19-12** Protecting Internal Hosts

Assume that the Security Policy installed on the gateway does not allow TELNETs to the hosts in localnet. What happens when 194.O.O.2 TELNETs to 194.O.67.14?

The answer is that this TELNET is allowed, because the connection does not pass through the FireWall. 194.O.67.14 responds to 194.O.O.2's ARP request, and 194.O.O.2 routes the connection directly to 194.O.67.14. VPN-1/FireWall-1 on the gateway does not see the connection and does not inspect it.

#### When is a Modified Security Policy Implemented?

Changes are implemented when the Security Policy is installed. The only time it is necessary to stop VPN-1/FireWall-1 and restart it is after a FireWalled host's physical interfaces have changed.

#### How should VPN-1/FireWall-1 be stopped?

The correct way to stop VPN-1/FireWall-1 is with the `fwstop` command. If you kill the VPN-1/FireWall-1 daemon, the VPN/FireWall Module continues to operate, but there is no logging or authorization, and no new encryption sessions can be started.

Note that when you stop VPN-1/FireWall-1, your network is completely exposed. Disabling IP forwarding will protect the networks behind the gateway, but the gateway itself will still be exposed. The only way to protect the gateway in this case is to physically disconnect the network cables.

## Administrative Issues

#### Are there any security hazards the administrator should be aware of when using VPN-1/FireWall-1?

VPN-1/FireWall-1 provides *transparent* connectivity to *all* Internet resources.

Some client-server implementations may pose security hazards, e.g., older versions of sendmail. The administrator should ensure that any application is safe to use before authorizing its use through a firewall. Since VPN-1/FireWall-1 enables the administrator to authorize any application, he or she has to carefully examine each one and assess the risk of allowing the use of that particular application (client or server).

#### Unregistered IP Addresses

VPN-1/FireWall-1 enables using a large number of unregistered or concealed internal IP addresses by presenting on external traffic only a small number of registered IP addresses.

VPN-1/FireWall-1's Address Translation feature enables a network to use unregistered Internet addresses or to hide the internal IP addresses. For additional information, see Chapter 14, "Network Address Translation."

#### How Does VPN-1/FireWall-1 Address Vulnerable Applications?

To address vulnerable applications, VPN-1/FireWall-1 can be set up to allow inbound connections of a particular service only to a specific server that has been enhanced to handle possible failures. For example, all inbound SMTP traffic can be directed to a

server running an enhanced version of sendmail. By providing such an open solution, the administrator can always acquire the latest and best application for any desired platform.

## Performance

### Does VPN-1/FireWall-1 Introduce Performance Degradation?

The VPN-1/FireWall-1 Kernel Module itself introduces practically no performance degradation, but encryption, Accounting and Live Connection features do have a measureable impact on performance.

### What are the Guidelines for Improving VPN-1/FireWall-1 Performance?

#### Management Module

Installing a Security Policy on a remote VPN/FireWall Module can often be speeded up by listing both machines in the `hosts` (Unix) or `lhosts` (Windows) files.

#### VPN/FireWall Module

VPN-1/FireWall-1 performance depends on the hardware, the Security Policy, and the characteristics of the network traffic. While the Firewall is inspecting packets, the time of handling a packet spends in the kernel increases. The conclusion is that VPN-1/FireWall-1 has a greater impact on latency (connection latency or transaction latency) and less on the bandwidth.

Benchmarks have shown that, while there is usually little throughput degradation, the latency may well be significantly degraded in some cases. This degradation can as a rule, be successfully addressed. Acquiring faster hardware is always helpful. In addition, the following suggestions should improve performance as well:

Keep the Rule Base simple.

Performance degrades when there is a very large number of rules, or when the rules are complex.

Position the most frequently applied rules first in the Rule Base.

For example, if most connections are HTTP packets, the rule which accepts HTTP should be the first rule in the Rule Base. Be sure to keep this rule as simple as possible.

#### Properties

- Enable the **Fast Mode** property for selected TCP services in the **TCP Service Properties** window (FIGURE 6-3 on page 194).

If you are not using Encryption, Authentication, Live Connections or Accounting, you can enable the **Fast Mode** property to increase the connections-per-second rate. See “TCP Service Properties” on page 194 for more information.

- Decrypt on accept

This property should be disabled if you are not using Encryption or SecuRemote.

## Overhead

Logging, Accounting, Encryption, Network Address Translation and Security Servers all degrade performance to some extent.

Logging, Accounting and Security Servers add I/O overhead and context switches. The degradation in performance might be significant if they are used in frequently applied rules.

## Memory

If the VPN-1/FireWall-1 Kernel Module's memory pool is exhausted, more memory should be allocated when VPN-1/FireWall-1 is installed. You can find out how much memory is available by using the following command:

```
fw ctl pstat
```

## Example

To allocate more memory (for example, 6 Mbytes), proceed as follows:

### ■ Solaris

- 1** Add the following line to `/etc/system`.

```
set fw:fwhmem = 0x600000
```

- 2** Reboot.

### ■ IBM/AIX

- 1** Enter the following command:

```
echo "fwhmem?W600000" | adb -w /etc/drivers/fw.ext
```

- 2** You must also increase the size of the pinned heap memory dedicated to the VPN-1/FireWall-1 kernel driver by changing the value of `fw_heap_size`.

To view the current value of `fw_heap_size`, enter the following command:

```
echo "fw_heap_size?X" | adb /etc/drivers/fw.ext
```

To modify `fw_heap_size`, enter the following command:

```
echo "fw_heap_size?Wxxxxx" | adb -w /etc/drivers/fw.ext
```

where xxxxx is the new value (in hexadecimal).

- 3** Stop VPN-1/FireWall-1 with the following command:

```
fwstop
```

- 4** Restart VPN-1/FireWall-1 with the following command:

```
fwstart
```

#### ■ HP-UX

- 1** Enter the following command:

```
echo "fwhmem?W600000" | adb -w stand/vmunix
```

- 2** Reboot.

#### ■ Windows NT

- 1** Set the `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\FWL\Parameters\Memory` parameter in the Registry to the desired value (a DWORD).



**Warning** – Setting the above parameter to too high a value may hang the machine during the boot process.

- 2** Reboot.

How can I estimate VPN-1/FireWall-1's memory usage?

For the VPN/FireWall Module, you can use the following general guidelines:

- Each session requires about 120 bytes of memory, more if the session is authenticated or if Network Address Translation is applied.
- In addition, there is some static overhead as well.
- The VPN/FireWall Module does not release the memory used by a session until about 50 seconds after the session ends, so if there are many sessions significantly shorter than a minute, the VPN/FireWall Module needs more memory than the number of active sessions would indicate.
- For HTTP, each URL access is a separate session.

The general formula is:

```
MemoryUsage =
((ConcurrentConnections)/(AverageLifetime))*(AverageLifetime
+ 50 seconds)*120
```

### To What Extent is VPN-1/FireWall-1 Fault Tolerant?

The VPN/FireWall Modules will continue inspecting and reporting logs, alerts, and status even if the Master is not active for any reason (host went down, application exited, etc.). Users can define multiple default Masters to which the VPN/FireWall Modules will report logs, alerts, and status in the event that the first Master is unavailable. The status and statistics of VPN/FireWall Modules can be monitored constantly by a number of Management Stations or SNMP platforms. If the VPN/FireWall Module host is rebooted, the VPN/FireWall Module can be loaded automatically and brought up with the latest Security Policy installed. The VPN/FireWall Module can also be configured to fetch its Security Policy from various Management Stations every time it boots.

The SNMP daemon is used to report status and even if it dies, the only thing that would happen is that in Firewall/VPN's Status Window or on the SNMP platform, the user would see that it is no longer possible to communicate with the daemon.

The Firewall/VPN daemon (`fwd`) is used to control the VPN/FireWall Module. If it dies, the user would not be able to control it, but the VPN/FireWall Module would continue to enforce the Security Policy that was last loaded.

As long as a gateway is up and routing, all packets are subject to VPN/FireWall Module inspection. If the gateway reboots, the VPN/FireWall Module is immediately loaded into the kernel and the latest Security Policy is loaded into it and enforced. VPN-1/FireWall-1 can be configured so that IP Forwarding is enabled only when the Security Policy is being enforced (see "IP Forwarding" on page 22 of *Check Point Reference Guide* for additional information).

The VPN/FireWall Module keeps a local copy of the latest Security Policy, so that even if the Management Station is down when the gateway reboots, the VPN/FireWall Module will still load the latest Security Policy.

With respect to logging, the VPN/FireWall Module can be configured to send logs and alerts to a certain host (the Master). If the Master is not available, the VPN/FireWall Module can be configured to attempt logging to another host, and another and another. Even if logging fails, the VPN/FireWall Module will still continue to function.





# Index

---

## SYMBOLS

\$FWDIR/conf/smtp.conf  
description, 350  
@ symbol  
central alerts machine, 80

## NUMERICS

2000  
specifying year 2000 or later, 157  
32-bit version  
OS support, 44  
3Com routers  
managing in the rule base, 136  
setup, 131  
64-bit version  
OS support, 44

## A

abandon parameter  
smtp.conf, 350  
Accept FireWall-1 Control  
Connections property, 68  
Accept ICMP, 241  
Accept Outgoing Packets  
property, 238, 282  
Accept VPN-1 & FireWall-1 Control  
Connections  
new meaning of, 240  
access  
limiting to specific ports, 608  
Access Control  
logging, 62  
Access Lists  
Properties, 245  
router, installing, 305  
Account Management, 174, 318

defining users in both LDAP and  
VPN-1/FireWall-1, 181, 190  
Account Management Client, 170  
Account Management for Enterprise  
Console, 9  
Account Unit  
managing users on, 170  
step by step instructions on how to  
use in Security Policy, 178  
Account Unit tab  
availability, 104  
accounting, 392, 587  
and synchronized FireWalls, 562  
incompatible with  
FASTPATH, 196  
ACE  
configuring FireWall-1 to work with  
ACE software, 609  
sdconf.rec file, 610  
using DES option with FireWall-  
1, 623  
Action Selection window, 411  
active connections, 393, 587  
ActiveX, 215  
adb, 629  
Additional Information Selection  
window, 414  
add-on products, 8  
address range, 150  
defining, 446  
menu choice, 101  
Address Translation  
and auxiliary connections, 307  
and FTP PASV, 307  
communications between hosts in  
different internal

networks, 462, 463  
compound conditions, 444  
FTP port command, 440  
gateway with three  
interfaces, 460  
gateway with two interfaces, 457  
Hide mode, 428, 429  
hiding the gateway's internal  
address, 476  
interaction with anti-  
Spoofing, 470  
internal host with illegal IP  
address tries to communicate  
with external host with same IP  
address, 478  
multiple translation, 445  
need for, 425  
PIX, 464  
reply packets, 435  
restrictions on rshell service, 440  
restrictions on sqlnet2  
service, 440  
restrictions on Xing service, 440  
routing considerations, 435  
Rule Base, 475  
Static Destination mode, 434  
Static Source mode, 432  
translation both source and  
destination, 445  
using with Encryption on the same  
system, 477  
Address Translation Rules  
generating automatically, 440  
Address Translation tab  
Network Properties window, 116  
Workstation Properties

- window, 113
- administrators
  - adding or deleting, 15
  - authenticating, 68
- AIX, see IBM AIX
- alert command
  - anti spoof, 244
  - anti-spoof, 244
  - mail, 244
  - popup, 243
  - SNMP, 244
  - SNMP Trap, 244
  - User Authentication, 244
  - user authentication, 244
  - user defined, 244
- alerts
  - received by, 385
  - sent to, 385
- aliased interfaces, 616
- America OnLine, 224
- anti-spoof Alert Command, 244
- anti-spoofing, 106, 136
  - compatibility with Address Translation, 470
  - example, 107, 123
  - interaction with Address Translation, 470
- AOL, 224
- appliances, 591
- application
  - silently dropping, 278
- Apply Gateway Rules to Interface
  - Direction property, 626
- Apply Selection Criteria option, 418
- archie, 231
- ARP, 562
- asymmetric routing, 558
- authenticated services
  - going across two or more FireWalls, 612
- authentication
  - and synchronized FireWalls, 562
  - authentication methods, 482
  - authentication schemes, 484
  - comparison of different types, 483
  - re-authenticating an FWZ
    - SecuRemote connection, 250
  - transparent authentication, 482
  - when to use each type, 483
- Authentication methods, 75, 482
- Authentication Passwords

- synchronizing, 76
- Authentication tab
  - availability, 104
- auxiliary connections, 307
- AXENT Pathways Defender, 484, 504
  - defining as server, 333
- AXENT Pathways SecureNet, 623
- B**
- back connection
  - requested port, 307
- back connections, 196
- backup
  - backing up a Security Policy, 84
- backward compatibility
  - Version 4.0 and earlier versions, 21
- BackWeb, 231, 307
- Bay CES, 592
- Bay Networks router, 2, 5, 274, 302
  - defining network object as, 104, 130
  - installing Encryption Module on, 5
  - installing VPN-1/FireWall-1 on, 119
  - setup, 130
- Bay RS, 592
- before installing VPN-1/FireWall-1, 23
- Blackbox Properties, 137, 142
- Block Intruder window, 394
- Block Request window, 395
- boot process
  - protecting networks during, 305
  - protecting the gateway during, 305
- bootp, 231

- C**
- cable failure, 565
- central alerts collection, 80
- central logging
  - Customer Log Module, 78
- certificate, 250
- Certificate Authority, 339
- certreq access operation, 74
- chargen, 224, 231
- checksum errors, 244
- Cisco PIX firewall
  - setup, 143, 145
- Cisco router

- setup, 128
- Client Authentication
  - authorizing services, 530, 536
  - configuring, 531
  - configuring support for HTTPS, 553
  - defining on a per-user rather than a per-group basis, 610
  - logging, example of, 540, 541
  - overview, 526
  - sign on methods, 527
  - signing on through a Web browser, 549
  - Single Sign On System Extension, 542
  - timeouts, 537
  - tracking, 537
- Client Authentication Sign On Methods
  - agent automatic sign on, 529
  - fully automatic sign on, 529
  - manual sign on, 527
  - manual sign on through a Web browser, 549
  - manual sign on using TELNET, 545
  - partially automatic sign on, 528
  - single sign on, 530
  - using agent automatic sign on, 551
  - using fully automatic sign on, 550
  - using partially automatic sign on, 549
- CLIENT keyword
  - \$FWDIR/lib/control.map file, 75
- Client/Server deployment of Management Module, 14
- ClusterID
  - parameter in conf/cpha.conf, 580
  - registry value, 580
- clusters
  - High Availability, 574
- color, 194, 197, 198, 200, 203, 447, 448
- Column menu, 398
- comment, 194, 197, 198, 199, 200, 203, 447
  - adding to a rule, 276
- communication
  - between VPN-1/FireWall-1 components on different machines, 69

- compatibility
  - Version 4.0 and earlier
  - versions, 21
- compression
  - availability, 258
  - dictionary, 258
- conf/loggers, 70, 71, 72, 80, 420
  - Customer Log Module, 79
- conf/masters, 70, 72, 420
- conf/sync.conf file, 558
- configuration
  - Security Servers, 357
- configurations
  - managing distributed FireWall-1
  - configurations, 69
- Conn. ID, 393, 396
- Connected OnLine Backup, 224
- connection to original-MTA failed
  - error message, 614
- connections
  - blocking, 394
  - different routes for, 558
  - lost when Security Policy re-installed, 85
  - terminating, 394
- connections table, 196, 308
- Content Vectoring Server, see CVP Server
- control connection
  - accepting, 239, 240
  - authentication and encryption, 240
  - encrypting, 71
- control connections
  - encrypting without encryption license, 76
- Control Properties
  - displaying windows, 91
- control.map, 71
  - access operations, list of, 74
  - description of, 73
  - example, 75
- control.map file
  - modified during VPN-1/FireWall-1 reconfiguration, 84
- CoolTalk, 307
  - enabling back connections, 225
- cp.license file
  - modified during reconfiguration, 84
- cpha\_export command, 579
- cpha\_import command, 579

- cphaprob command, 565, 575
- cphasopt command, 575
- cphastart command, 575
- creating groups, 20
- CRL, 335
- cross cable, 566
- CU-SeeMe, 231
- Customer Log Module, 78
  - description, 79
- CVP Inspection
  - step by step procedure, 366
- CVP inspection
  - FTP resource, 222
  - SMTP resource, 219
  - URI resource, 215
- CVP Manager
  - configuration syntax errors, 325
- CVP Server, 322
  - how it is invoked, 362
  - step by step procedure for using, 366
- CVP Server Properties window, 322
- cvpm.conf file, 325
- cvpm\_putkey command, 328

## D

- daytime, 225, 231
- DB Download, 154
- db\_download access operation, 74
- DCE-RPC, 227, 234
  - required by MS Exchange, 307
- debugging
  - TCP/IP, 233
- DecNET
  - inspecting, 623
- decrypt on accept, 239
- dedicated hub, 566
- default directory
  - VPN-1/FireWall-1, 30
- default route, 435
- Default Security Policy
  - fstop while active, 305
- default Security Policy, 56, 305
  - restrictions under IBM AIX, 48
  - verifying that it is loaded, 306
- default\_server, 216
- default\_server parameter
  - smtp.conf, 350
- DES
  - using ACE (SecurID) DES with FireWall-1, 623

- Destination Selection window, 407, 409
- dest-unreach, 235
- DHCP, 543
- Different Routes for
  - Connections, 558
- direction of enforcement, 625
- direction of gateway rules, 238
- directory
  - installing VPN-1/FireWall-1 in a directory other than the default directory, 30
- discard, 225, 231
- displaying
  - System Status Viewer Window, 370
- distributed configuration
  - diagram, 23
- distributed management
  - VPN-1/FireWall-1 configuration, 69
- DN
  - logging in using, 251
- DNS, 225
- dns, 231
- DNS, dual, 607
- domain
  - load balancing algorithm, 584
  - menu choice, 101
  - using a domain object in a rule, 117
- Domain Controller, 544
- Domain Name Download, 240, 246
- domain name download,
  - enabling, 240, 246
- Domain Name Queries, 240, 245
- domain name queries,
  - enabling, 240, 245
- downtime
  - minimizing while upgrading, 22
- Drop
  - differences from Reject, 272
- dropping an application, 278

## E

- echo, 225, 231
- echo-reply, 235, 608
  - Logical Servers, 587
  - Wait Mode, 540
- echo-request, 235, 608
  - Logical Servers, 587
  - Wait Mode, 540

- egp, 236
- ELA proxy server
  - Solaris start, 61
  - Windows NT stop, 61
  - Windows NTstart, 61
- Elapsed column
  - method of calculation, 392, 393
- embedded systems
  - where to install license, 59
- Enable Domain Name
  - Download, 240, 246
- Enable Domain Name Queries, 240, 245
- Enable ICMP, 240, 246
- Enable Outgoing Packets, 241
- Enable Outgoing Packets
  - property, 626
- Enable Response of FTP Data
  - Connections, 242
- Enable RIP, 240, 245
- Enable UDP Replies, 239
- encryption
  - and synchronized FireWalls, 561
  - incompatible with
    - FASTPATH, 196
  - using with Address Translation on the same system, 477
- encryption license
  - encrypting control connections without, 76
- Encryption Module, 8
  - installing on Bay Networks and Xylan, 5
- encryption scheme mismatch, 244
- Enforcement Point
  - definition of, 1
- enforcing and installing, difference between, 278
- enterprise ID, 594
- error message
  - "connection to original-MTA failed", 614
  - No Response from Server, 89
- error\_server parameter
  - smtp.conf, 350
- established TCP, 137
- established TCP connections, 308
- established TCP packets, 244
- established TCP sessions, 308
- excessive log grace period, 243
- exec, 225
- explicitly defined rules

- interaction with implicit rules, 281
- external FireWall Module
  - not managed by FireWall-1/n, 7, 623
- external FireWalled object, 103, 116, 119, 138, 143
- external group, 179
  - creating, 170
  - deleting, 173
  - modifying, 173
  - when changes take effect, 166, 170
- external interface
  - hiding IP address, 429
  - of gateway, specifying for IKE, 19
- external interfaces
  - restricted in FireWall-1/n, 7, 622
- external users
  - managing, 170
- external.if file
  - modified during VPN-1/FireWall-1 reconfiguration, 84

## F

- Fast mode, 196
- Fastpath, 196
- fault tolerance, 631
- fetch access operation, 74
- Fetch command (Named Masks window), 287
- Find Date, 401
- Find in all Fields window, 402
- Find menu, 401
- Find window, 401
- finger, 225
- FireWall Module, 8
  - description of, 13
- FireWall synchronization
  - example, 559
  - implementation, 558
  - overview, 557
- FireWall-1 HP OpenView Extension
  - installing, 596
- FireWalled gateway
  - definition of, 1
- FireWalled host
  - definition of, 1
- first IP address, 446
- first port, 447
- format file
  - name displayed in status bar, 391
- FreeTel, 232, 307

- FTP, 196, 307, 483
  - authenticating through the HTTP Security Server, 611
  - back connection, 85
  - data connection, 85
  - data connection, enabling
    - response of, 242
  - file names logged for
    - authenticated sessions, 343, 396
  - from HTTP, 608
  - get and put logged for User
    - Authenticated FTP, 343
  - PORT command, 85
  - User Authentication, 483
- ftp, 225
- FTP daemon, 609
- FTP data connections, 225, 242, 307
- FTP PASV, 307
  - enabling FTP Passive
    - Connections, 242
- FTP proxy
  - defining to browser, 608, 611
- FTP resource
  - CVP inspection, 222
  - matching, 347
- FTP resources
  - command matching, 347
  - file name matching, 347
  - matching, 347
- fw hastat command, 579
- fw putkey, 77
- fw\_heap\_size, 629
- FW1\_clntauth, 555
- fw1\_service, 239
- fw1allowed-dst, 187
- fw1allowed-src, 187
- fw1allowed-vlan, 187
- fw1authmethod, 185
- fw1auth-server, 185
- fw1day, 186
- fw1enc-fwz-expiration, 187
- fw1expiration-date, 186
- fw1groupTemplate, 187
- fw1hour-range-from, 186
- fw1hour-range-to, 186
- fw1pwdLastMod, 186, 250
- fw1Skey-mdm, 186
- fw1Skey-passwd, 186
- fw1Skey-seed, 186
- fw1sr-auth-track, 187
- fw1SR-datam, 187

- fw1SR-keym, 187
- fw1SR-mdm, 187
- fwa1
  - definition of, 75
- fwa1 authentication, 75
- fwauth.keys file
  - modified during VPN-1/FireWall-1 reconfiguration, 84
- fwauthd.conf, 555
- fwauthd.conf file
  - modified during VPN-1/FireWall-1 reconfiguration, 84
- FWDIR
  - importance of setting correctly, 30
- FWDIR/conf/masters file, 75
- FWDIR/lib/control.map file, 75
- fwhmem, 629, 630
- fwinfo debugging tool
  - incorrect functioning, 30
- fwstart, 48, 562
- fwstop, 48
  - and killing the FireWall-1 daemon, difference between, 627

## G

- gateway
  - defining network object as, 104
  - hiding IP address of external interface, 429
  - protecting, 305
  - renaming when encryption properties are defined, 103
  - specifying communication direction of rules on, 238
- gateway cluster
  - menu choice, 101
- gateways
  - defining interfaces as separate objects, 608
  - direction of enforcement on, 626
- generic services
  - service properties, 200
- get\_logdom access operation, 74
- get\_tab\_name access operation, 74
- getkey access operation, 74
- gettopo access operation, 74
- gettopossl access operation, 74
- gpp, 236
- Global Pool, 466
- gopher, 225
- grace period
  - logging, 243

- group
  - menu choice, 101
- GUI Client
  - minimum requirements, 24
- GUI Clients
  - adding or deleting, 14
- GUI windows
  - closing, 91
  - displaying, 91
- guidelines
  - performance, 628

## H

- H.323, 196, 226, 307
  - enabling back connections, 226
- heap memory, 629
- heuristic check of Rule Base, 277
- hidden rules, 283
  - displaying, 283
  - unhiding, 284
- Hide mode, 429
- Hide/Unhide menu, 398
- hiding IP addresses, 627
- hiding rules, 283
- High Availability, 55, 558
  - clusters, 574
  - different Management Modules, 561
  - different Security Policies, 561
  - encrypting connections between synchronized FireWalls, 561
  - fw putkey, 565, 573
  - installation, 28
  - minimum number of machines needed, 565
  - secured interfaces, 566
  - SKIP, 561
  - synchronizing different version VPN/FireWall Modules, 561
  - synchronizing VPN/FireWall Modules on different platforms, 561
  - using illegal IP addresses, 565
- hijacking sessions, 616
- HKEY\_LOCAL\_MACHINE\Software\checkPointPolicy Editor4.1, 90
- hostname command, 606
- hosts
  - defining network objects as, 104
  - direction of enforcement on, 626
- hosts file, 19, 103, 119, 628
- Hosts, Gateways and Interfaces

- distinction between, 606
- HP
  - FireWall-1 HP OpenView extension, 595
- HP OpenView Extension
  - installing, 596, 597
  - specifying the Management Server for FireWalled objects, 599
- HP OpenView, see FireWall-1 HP OpenView extension
- HP-UX
  - disabling IP Forwarding, 18
  - supported versions, 5
- HP-UX 10
  - transitional links option, 46
- HP-UX 11
  - X/Motif GUI support, 47
- HTML Weeding, 215
- HTTP
  - allowing FTP sessions from, 608
  - restricting inbound, 501
  - restricting outbound, 501
  - User Authentication, 483
  - using a Server for Null Requests, 513
  - using reauthentication options, 500
- http, 225
- HTTP Security Server
  - as proxy, 350
  - configuring multiple ports, 507
  - defining as a Security Proxy, 504
  - defining as an HTTP proxy, 503
  - error messages, 507
  - overview, 497
  - putting a proxy behind, 498
  - support for FTP, 350
  - support for HTTPS, 352, 354
- HTTP Servers
  - defining, 499
- HTTPS, 624
  - authenticating outbound, 504
  - using URI Resource rules with, 353
  - with non-transparent authentication, 509
- https, 225

## I

- IANA, 439, 624
- IBM AIX

- IP Forwarding, 48
  - overwriting previous
    - installation, 49
  - supported versions, 5
  - X/Motif library version, 49
- ICMP, 240, 241
  - enabling, 240, 246
  - match string, 199, 200
- ICMP Redirect
  - enabling, 241, 246
- Icons View, 376
- ident, 226
- ied, 93
- igrp, 236
- IKE, 103
  - specifying the encrypting
    - gateway's IP address, 19
- imap, 226
- implicit rules
  - see implied rules
- implied rules, 241
  - interaction with explicitly defined
    - rules, 281
  - toggling display of, 93
- Implied Rules option on View
  - menu, 282
- in.telnetd, 609
- incoming communications
  - Security Policy enforced on, 625
- inetd.conf, 609
- Info field
  - get and put logged for
    - authenticated FTP, 396
- info-reply, 235
- info-req, 235
- Inspection Code
  - compiling from Inspection
    - Script, 278
- Inspection Code Loading, 301
- Inspection Module and FireWall
  - Module, differences
    - between, 4, 591
- Inspection Script
  - compiling Inspection Code
    - from, 278
  - manually editing, 278
  - viewing, 299
- Install On field
  - NAT tab, 441
- installing
  - router access list, 305
  - Security Policy, 298

- what to do before, 18
- installing a VPN-1/FireWall-1
  - license, 59
- installing and enforcing, difference
  - between, 278
- installing VPN-1/FireWall-1, 18
- Insufficient Information problem, 344
- integrated firewall
  - menu choice, 101
- Integrated FireWalls
  - general properties, 142
  - PIX setup, 143
- Integrated Firewalls, 141
- interface
  - sharing, 569
- interface data
  - fetching automatically, 105
- interface failure, 565
- Interface names
  - Bay routers, 592
- Interface Selection Criteria
  - window, 406
- Interface Selection dialog box, 406
- interfaces
  - aliased, 616
  - defining a gateway's interfaces as
    - separate objects, 608
  - defining as an object, 608
  - how Security Policy is enforced on
    - different, 625
  - network, properties of, 105
  - required for High Availability, 580
  - result of failing to define, 105
  - virtual, 616
- interfaces, external
  - restricted in FireWall-1/50 and
    - FireWall-1/250, 7, 622, 623
- internal FireWalled object, 103, 116,
  - 119, 138, 143
- internal hosts
  - number restricted in FireWall-1/
    - n, 6, 622
- internal interfaces
  - not restricted in VPN-1/FireWall-1/
    - n, 7, 622
- internal network objects, 154
- Internet
  - defining to FireWall-1, 606
- InternetPhone, 232
- intruders
  - blocking connections from or to
    - suspected, 394

- ioctl access operation, 75
- IP Address, 115, 138
- IP address
  - sharing, 569
  - unique and non-unique, 564
- IP addresses
  - hiding, 627
  - unregistered, 627
  - when does changing take
    - effect, 85
  - which to use when directing
    - logging to, 72, 80
- IP Forwarding, 21
  - disabling in the Solaris2 and HP-
    - UX kernels, 18
  - IBM AIX, 48
- IP Options, 616
- IP options, 244
- IP Tunnels, 132
- IPX packets
  - inspecting, 623
- irc, 226
- ISAKMP see IKE
- ISDN interfaces, 624

**J**

- JAVA, 215
  - blocking JAVA applets, 215
- JAVA applets
  - already in cache, 215
- JAVA Script, 215

**K**

- Kerberos, 623
- kerberos, 226, 232
- kernel, 629

**L**

- last IP address, 446
- last port, 447
- LDAP, 169
  - Account Unit, 177, 179
  - default user template, 338, 339
  - defining users in both LDAP and
    - FireWall-1, 181
  - defining users in both LDAP and
    - VPN-1/FireWall-1, 190
  - exporting users from the VPN-1/
    - FireWall-1 User
      - Database, 188
  - FireWall-1-specific attributes, 338

- port number for SSL
    - connection, 340
  - schema checking, 189
  - security issues, 189
  - users maintained by third-party
    - clients, 338, 339
  - version with which VPN-1/
    - FireWall-1 is compliant, 189
  - LDAP Account Unit
    - step by step instructions on how to
      - use in Security Policy, 178
  - LDAP Client
    - third-party, 338, 339
  - LDAP server, see also Account Unit
  - LDAP servers
    - indexing, 189
    - optimizing, 189
  - ldap service, 226
  - LDAP Version 2.0, 189
  - LDAP Version 3.0, 189
  - LDAPservers
    - defining, 334
  - ldap-ssl, 226
  - license
    - confirming that you are using
      - correct licenses, 61
    - installing, 59
    - obtaining, 58
    - reconfiguring with cpconfig, 51
    - removing old licenses, 59
    - where to install, 58
    - where to install for embedded
      - systems, 59
  - Linux
    - supported versions, 5
  - live connections, 587
  - LiveLan, 226
  - lmhosts file, 19, 103, 119, 628
  - load access operation, 74
  - Load Agents
    - defining parameters, 254
  - Load Agents Port property, 587
  - Load Balancing
    - step by step instructions, 584
  - load balancing
    - servers, 581
  - load balancing algorithms, 584
  - Load Measurement Interval
    - property, 587
  - Load Measuring, 586
  - local.arp file, 437
  - locking mechanism
    - used to prevent simultaneous
      - updates, 62
  - lockmanager, 234
  - Log
    - rule number zero, 615
    - rule with negative number, 615
  - log
    - established TCP packets, 309
    - printing, 420
    - saving, 420
    - scrolling, 400
    - viewing, 389
  - log access operation, 75
  - Log entries, selecting by
    - additional information, 414
    - address translation
      - parameters, 408
    - destination, 407, 408, 411, 412, 413
    - DstKeyID, 414
    - Info., SrcKeyID, DstKeyID, 414
    - interface, 405
    - number, port, rule, date, time, 405
    - origin, source, destination, user or
      - service, 407, 408, 411, 413
    - port, 405
    - product, 412
    - protocol, 413
    - rule, 405
    - service, 407, 408, 411, 412, 413
    - source, 407, 408, 411, 412, 413
    - SrcKeyID, 414
    - type, 409
    - user, 407, 411, 412
  - Log File
    - deleting, 420
    - exporting, 420
    - miscellaneous functions, 420
    - name displayed in title bar, 391
    - opening another, 419
    - printing, 420
    - reload, 421
    - saving, 420
    - starting a new, 419
    - stop updating, 421
  - log file
    - analysis of, 614
    - managing, 419
    - navigating and searching in, 400
    - periodically switching, 615
    - saving, 420
    - searching for a text string in, 402
    - statistical analysis of, 614
  - log grace period, 243
  - Log Server
    - definition of, 390
  - Log Station
    - which IP address to use when
      - directing logging to, 80
  - Log Viewer, 389
    - displaying, 91
    - selection criteria, 404
  - loggers
    - multiple, 80
  - loggers file
    - description of, 79
  - logging
    - Access Control, 62
    - packets as dropped though
      - connection continues, 309
  - Logging and Alerting
    - Security Policy, 243
  - Logical Server
    - echo-request, echo-reply, 587
  - logical server
    - menu choice, 101
  - Logical Servers, 584
    - step by step instructions on
      - using, 584
    - using HTTP Logical Servers in
      - rule, 586
  - logical servers, 149
    - persistent server mode, 585
  - login, 226
    - with DN or user name, 251
  - logswitch access operation, 75
  - Lotus Notes, 226
- ## M
- MAC address, 565
    - format, 437
  - High Availability, 564
  - importing and exporting, 566
  - in local.arp file, 437
  - NAT, 435
  - sharing, 569
  - Mail Alert Command, 244
  - manage.lock file, 62
  - Management Module
    - definition of, 2
    - description of, 13
    - minimum requirements
      - (Windows), 25
  - Management Point

- definition of, 2
- Management Server
  - Customer Log Module, 79
  - definition of, 2
  - description of, 14
  - name displayed in status bar, 391
  - name of executable, 14
  - problems in connecting to, 89
  - timeout in connecting to, 89
- Management Station
  - definition of, 2
  - protecting, 68
- Managing 3Com Filters
  - routers, 136
- mangling
  - packets of an established TCP connection, 309, 310
- masking rules, 283
- mask-reply, 235
- mask-request, 235
- masks
  - applying, 287
- Master, 71
  - redirect logging to another Master, 420
  - which IP address to use when directing logging to, 72
- master separate from central logger, 79
- MASTERS
  - parameter in control.map file, 73
- masters file
  - description of, 72
  - modified during VPN-1/FireWall-1 reconfiguration, 84
- MASTERS keyword
  - \$FWDIR/conf/masters file, 74
  - \$FWDIR/lib/control.map file, 75
- match, 199, 200
- memory usage guidelines, 629
- MIB, 594
  - chkpnt.mib file, 594
  - chkpnt.mib file source code, 600
  - RFC support, 593
- Microsoft Conferencing, 227
- Microsoft Exchange, 227
- Microsoft NetMeeting, 227
- Microsoft NetShow, 227
- Microsoft RRAS, 133
- Microsoft SQL Server, 227
- MIME attachments
  - definable in an SMTP

- Resource, 218
- definition syntax in SMTP
  - Resource, 218
  - stripping specified types from message, 218
- minimum requirements
  - GUI Client, 24
  - Management Server, 25
  - Unix platforms, 44
- modem connections
  - securing, 617
- Monitoring System Status, 369
- monitoring system status, 369
- Mosaic, 227
- mountd, 234
- moving VPN-1/FireWall-1 to another machine, 83
- MS Exchange, 307
- multicast, 625

## N

- name, 194, 197, 198, 199, 200, 202, 232, 446, 447
- named, 240, 245
- NAT
  - and Tunnel mode, 478
- nbdatagram, 232
- nbname, 232
- nbssession, 137, 227
- NBT, 227
- negate rules, 136
- net mask, 115
- NetBEUI
  - disabling on the gateway, 18
- NetBEUI, see NBT
- NetShow, 307
- netstat, 228
- network
  - menu choice, 101
- network interface properties, 105
- network object
  - creating, 100
  - creating groups of network objects, 148
  - defining, 97
  - deleting, 101
  - editing existing, 101, 320
  - group, 148, 315, 331
  - group, adding service to, 203
  - group, defining properties of, 158
  - group, deleting service from, 203
  - internal, 154

- modifying, 101
- on network, 605
- properties, 97, 317, 318
- network object group
  - deleting from, 149
- network objects
  - which are on my network?, 605
- Network Objects Manager
  - displaying, 91
- NFS, 234
- nfsd, 232
- nfsprog, 234
- NIS, 234
- nisplus, 234
- nntp, 228
- node
  - definition of, 2
- nodes
  - number restricted in VPN-1/FireWall-1/n, 6, 622
- non IP protocols
  - NetBEUI, 18
- Non-Transparent Authentication and HTTP, 509
- Non-transparent Authentication
  - prompt\_for\_destination parameter, 497
- non-unique IP address, 564
- Notify Sender on Error field, 614
- ntp, 228, 232
- Number Selection Criteria
  - window, 405

## O

- objects.C file, 496
- OnTime, 232
- Open Platform for Secure Enterprise Connectivity, see OPSEC
- Open Security Extension, 9
- Open Windows, 228
- OpenView, see FireWall-1 HP OpenView extension
- OPSEC, 361, 366
- opsec access operation, 74
- OPSEC PKI, 335
- opsec\_putkey command, 240
- OPSEC-certified products
  - obtaining evaluation copies, 366
- Options window, 418
- ospf, 236
- outgoing communications
  - Security Policy enforced on, 625



- outgoing packets
  - accepting, 241
- overwriting previous AIX installation, 49

## P

- packet filter
  - installing Security Policy on, 302
- packet reassembly, 616
  - security risks associated with, 616
- param-prblm, 235
- password
  - limitation on length in Windows, 34
  - verifying, 184
- password expiration, 250
- PASV
  - enable FTP PASV, 242
  - enabling FTP Passive Connections, 242
- pcnfsd, 234
- performance
  - improving, 628
- performance guidelines, 628
- period of vulnerability, 624
  - description of, 305
- physical address, 435
- ping, 235
  - allowing unrestricted, 608
- PIX Address Translation
  - managing, 464
- PIX blackbox
  - authentication properties, 144
  - encryption properties, 145
  - location of management server, 147
  - management guidelines, 147
- PointCast, 228
- pop2, 228
- pop3, 228
- PopUp Alert Command, 243
- port 161
  - failure to bind to, 593
- port 256, 562, 573
- port number, 194
  - assigning in Address Translation Hide mode, 429
- ports
  - limiting access to specific ports, 608
- Ports Range
  - defining, 447
- postmaster parameter
  - smtp.conf, 350
- PPP, 623
- pre-shared secret, 250
- previous version FireWall Modules
  - managing from current version Management Station, 21
- printing
  - log entries, 420
- privilege level, 62
- prog number, 198
- program number, 198
- prologue, 201
- prologue, adding to rules, 201
- prompt\_for\_destination
  - User Authentication, 496
- properties
  - interaction with Rule Base, 281
  - network object, 97, 317, 318
  - of defined object, displaying, 192
  - of network interface, 105
  - of service object, defining, 192
  - time object, 311
- protocol, 448
  - which available on network?, 606
- Protocol Selection Criteria
  - window, 413
- Protocol Selection window, 413
- protocol type, 195
- proxy
  - putting behind VPN-1/FireWall-1 HTTP Authenticating Server, 498
- proxy ARP method, 437

## R

- RADIUS, 232, 484
  - defining server, 329
  - enabling connections from FireWall Module to server, 239
- RADIUS Servers
  - Server Groups, 340
- radius\_versions, 330
- random
  - load balancing algorithm, 584
- range of addresses, 150
- RAS, 228, 232
- RDP, 232
- RealAudio, 228, 307
  - enabling back connections, 228

- re-configuration
  - files modified during, 84
- Red Hat Linux, 5
- redirect, 236
- refresh access operation, 74
- Reject
  - differences from Drop, 272
- Reply Timeout, 239
- RequiredInterfaces
  - parameter in conf/cpha.conf, 581
  - registry value, 581
- resend\_period parameter
  - smtp.conf, 350
- resolve name timeout
  - Log Viewer, 243
- resource
  - group, defining properties of, 223
- resources
  - and synchronized FireWalls, 562
- reverse DNS, 210
- rexec, 228
- RFC 1155, 593
- RFC 1155 - 1213, 593
- RFC 1156, 593
- RFC 1157, 593
- RFC 1521, 219
- RFC 1631, 440
- RFC 1631 compliant Address Translation feature, 426
- RFC 1858, 132
- RFC 1918, 439
- RIP, 240
- rip, 232
- RIP, enabling, 240, 245
- RLOGIN
  - User Authentication, 483
- login, 228
- round robin
  - load balancing algorithm, 584
- round trip
  - load balancing algorithm, 584
- Route Recording, 132
- router
  - anti-spoofing on, 122
  - menu choice, 101
- Router Access Lists
  - importing, 302
  - managing imported access lists, 303
  - verifying and viewing, 304
- router interface
  - specifying name of, 121

- routers
    - anti-spoofing capabilities, 122
    - definition of, 2
    - installing access lists on, 305
    - installing Security Policy on, 275, 299
  - Routing and Remote Access Service, see Microsoft RRAS
  - Routing Information Protocol, enabling, 240, 245
  - RPC
    - enable FireWall-1 to control, 243
    - service properties, 197
  - RPC Control, 307
  - rsh, 229
  - RSH/REXEC, 307
  - rshell
    - and Address Translation, 440
  - rstat, 234
  - Rule Base
    - adding a new rule, 265, 449
    - deleting rule from, 277, 456
    - interaction with Properties, 281
    - masking rules, 283
    - number of rules supported, 608
    - sequential application of rules, exception to, 344
    - using ping in, 608
    - verifying, 277
  - rule zero
    - in Log Viewer, meaning of, 397, 615
  - rules
    - adding and inserting, 265, 266
    - adding to Rule Base, 265, 449
    - consistency and redundancy check of, 277
    - copying to clipboard, 266
    - cutting to clipboard, 266
    - deleting, 266
    - deleting from Rule Base, 277, 456
    - disabling, 298
    - hiding, 283
    - how executed, 261
    - masking, 283
    - modifying, 267
    - pasting from clipboard, 266
  - rules, see also Security Policy
  - rundir parameter
    - smtp.conf, 350
  - rwall, 234
- S**
- S/Key, 484
    - authentication specified in control.map file, 74
    - Secret Key minimum length, 159, 160
  - saving
    - log entries, 420
    - log file, 420
  - scan\_period parameter
    - smtp.conf, 350
  - Secure Socket Layer, 624
  - SecureClient, 30, 53
  - secured interfaces
    - High Availability, 566
  - SecuRemote connection
    - reauthenticating, 250
  - SecureServer, 53
  - SecurID, 229, 232, 233, 484
  - securidprop, 229
  - Security Policy
    - and ISDN interfaces, 624
    - backing up, 84
    - creating new, 264
    - default, 56, 305
    - installing, 298
    - modified, when implemented, 627
    - opening, 264
    - retrieving, 264
    - viewing, 264
  - Security Servers
    - configuration file, 357
    - FTP resource matching, 347
    - incoming connections, 346
    - interaction with OPSEC products, 354
    - outgoing connections, 346
    - using to authenticate other services, 360
  - Selection, 418
  - selection criteria for Log Viewer, 404
  - Selection Criteria Manager, 404
  - Selection Criteria window, 403
  - server
    - logical, 149
  - server load
    - load balancing algorithm, 584
  - server load balancing, 581
    - defining parameters, 254
    - how it works, 582
  - server object
    - adding a server to a group, 331
    - creating, 319
    - creating groups of server objects, 331
    - defining, 317, 318
    - deleting, 320
    - deleting a server from a group, 332
    - modifying, 320
  - SERVER\_TIMEOUT, 90
  - ServerTimeout, 90
  - service object
    - creating new, 193
    - defining, 192
    - deleting, 193
    - modifying, 193
  - Service Properties window, 202
  - Service Selection Criteria window, 416
  - services
    - dependence on other services, 607
    - which available on network?, 606
    - which have more than one type, 606
  - Services Manager, 192
    - displaying, 91
  - Session Authentication
    - configuring, 517
    - overview, 515
  - Session Authentication Agent
    - required for Session Authentication, 483
  - Session Authentication agent
    - configuring, 519
    - pre-configuring, 521
  - session hijacking, 616
    - preventing, 616
  - session timeout
    - UDP, 239
  - setup.C file, 330
  - shared interfaces, 569
  - shared MAC addresses, 569
  - shared-secrets
    - third party LDAP Servers, 338
  - Show, 419
  - shutdown command, 58
  - Single Sign On System
    - Extension, 542
  - SKIP
    - rekey policy mismatch, 244
    - restrictions on using with High Availability, 561

- specifying the encrypting gateway's IP address, 103
  - SLIP, 623
  - SMTP
    - badly formed header, 215
    - pipe, 215
    - source routing, 216
  - SMTP resource
    - CVP inspection, 219
    - restricting message size, 219
  - SMTP Security Server, 348, 614
    - configuration file, 350
    - supported protocols, 349
  - smtp service, 229
  - smtp.conf file, 216
  - smtp\_rfc822 property, 215
  - SNMP, 134, 233
  - snmp, 233
  - SNMP daemon
    - initial keys, 594
    - initial communities, 594
    - optional, 593
    - read and write communities (keys), 594
    - VPN-1/FireWall-1, 593
  - snmp service, 233
  - SNMP Trap Alert Command, 244
  - SNMP Trap Alert command, 244
  - SNMP traps, 594
  - snmp.C file, 594
  - snmp-trap, 233
  - Solaris
    - supported versions, 5
  - Solaris 2.7, 5
  - Solaris Operating Environment 7, 5
  - Solaris2
    - disabling IP Forwarding, 18
  - Source Object Selection Criteria window, 407
  - source port range, 195, 197
  - source-quench, 235
  - Specific Sign-on, 536
  - spoofing, 106
  - SQLNet, 229
  - sqlnet2, 307
    - and Address Translation, 440
  - Src Routing, 132
  - SrcSpoofing (3Com), 132
  - SSL, 624
    - port number for LDAP connection, 340
  - SSL connections, 339
  - Standard Sign-on, 536
  - stat access operation, 74
  - state synchronization
    - implementation, 558
    - overview, 557
  - state tables
    - cleared when Security Policy re-installed, 85
  - Static Destination mode, 434
  - Static Source mode, 432
  - status display
    - updating, 383
  - stderr
    - rsh/rexec reverse stderr connections, 228, 229, 242
  - Steelhead, see Microsoft RRAS
  - StreamWorks, 233
  - suspected intruders
    - blocking connections to and from, 394
  - switch
    - definition of, 2
    - menu choice, 101
    - setup, 138
    - Xylan, 138
  - Sybase SQL, 229
  - synchronization
    - "new style", 573
    - "old style", 573
    - timing issues, 560
  - synchronized FireWall Modules
    - restrictions on implementation, 561
  - synchronized FireWalls
    - resources, 562
    - restrictions, 561
  - synchronizing VPN/FireWall Modules on different platforms, 561
  - SYNDefender
    - guidelines for choosing between methods, 621
    - when changes to Maximum Sessions take effect, 248
  - SYNDefender Gateway
    - description of, 619
  - SYNDefender Passive Gateway
    - description of, 621
  - syslog, 233
  - System Status
    - displaying, 91
  - system status
    - changing and updating display of, 383
  - System Status window, 376
- ## T
- tab\_stat access operation, 74
  - TACACS, 233, 484
  - TACACS Server
    - enabling connections from VPN/FireWall Module to, 239
  - TACACS servers
    - defining, 332
  - TACACS+, 229
  - Talk protocol, 623
  - TCP
    - service properties, 194
  - TCP connections
    - established, 308
  - TCP sequence number
    - prediction, 616
  - TCP Session Timeout, 239
  - TCP sessions
    - established, 308
  - TELNET
    - User Authentication, 483
    - VPN-1/FireWall-1 daemon, 609
  - telnet, 229
  - TELNET daemon, 609
  - tftp, 233
  - time object
    - creating, 312
    - creating groups of time objects, 315
    - defining, 311
    - deleting, 312
    - editing existing, 312
    - groups, 315
    - modifying, 312
    - properties, 311
  - time object group
    - deleting from, 316
  - time service, 230, 233
  - Time Stamping, 132
  - time-exceeded, 236
  - timeout
    - changing default, 89
    - connection to Management Server, 89
    - Log Viewer resolve name, 243
  - timeout parameter
    - smtp.conf, 350
  - timestamp, 236
  - timestamp reply, 236

- timestamp request, 236
- timing issues
  - synchronization, 560
- Tiny Fragments, 132
- traceroute, 233
- transitional links option, 46
- Transparent Authentication, 482
- trusted interfaces
  - High Availability, 566
- Tunnel Mode
  - and NAT, 478
- two or more FireWalls
  - going across for authenticated services, 612
- Type Selection Criteria window, 409

## U

- UDP
  - accept replies, 239
  - enabling replies, 239
  - service properties, 196
  - virtual session timeout, 239
- UDP response, 134
- UFP Server
  - step by step procedure for using, 363
- UFP Servers, 320
- UFP servers
  - defining, 320
- unique IP address, 564
- Unix platforms
  - minimum requirements, 44
- Unknown Network Objects, 304
- unload access operation, 74
- upgrading
  - from version prior to 4.0, 21
  - from versions before 4.0, 21
  - minimizing downtime during, 22
  - reinstalling Security Policy
    - after, 84
  - to the current version from earlier versions, 21
  - VPN-1/FireWall-1 loses its state after, 23
  - what objects are carried over from previous version, 84
- URI Specification File
  - format, 213
- URL Filtering, 363
- URL filtering
  - step by step procedure, 363
- user

- generic, 167
- group, defining properties of, 165
- restricting internal user's access to
  - JAVA applets, 215
- User Authentication
  - authentication rule, 279
  - defining on a per-user rather than a per-group basis, 610
  - deployment, 486
  - entering user name and password, 493
  - overview, 485
  - tracking and timeout parameters, 490
- User Authentication Alert Command, 244
- User Database
  - downloading, 154, 167
  - installing, see User Database, downloading
  - when changes take effect, 166
- User Defined Alert Command, 244
- user group
  - adding to source of rule, 268
  - in rule, 268
  - restricting access based on, 268
- user properties, 156
- User-Defined Service Properties
  - Example, 201
- users
  - defining in both LDAP and FireWall-1, 181
  - defining in both LDAP and VPN-1/FireWall-1, 190
  - exporting from VPN-1/FireWall-1 database to LDAP
    - directory, 188
  - restricting internal user's access to
    - JAVA applets, 215
- Users Manager
  - displaying, 91
- Uses H.323, 227
- uucp, 230

## V

- Valid Addresses, 106
- VDO-Live, 230
  - enabling back connections, 230
- VDOLive, 196, 307
- Version 3.0
  - upgrading from, 21
- version 3.0 and earlier

- compatibility with Version 4.0, 21
- Version 4.0
  - upgrading from version prior to, 21
- version 4.0
  - compatibility with earlier versions, 21
- View menu, 282
- viewing
  - Inspection Script, 299
  - log, 389
- virtual interfaces, 616
- virtual packet reassembly, 616
- virtual session timeout
  - UDP, 239
- Vosaic, 230
- VPN, 4
- VPN/FireWall Module
  - minimum requirements (Windows), 25
- VPN/FireWall Module and Inspection Module, differences between, 4
- VPN/FireWall Modules
  - restrictions on
    - synchronization, 561
- VPN-1 Module, 8
- VPN-1 SecuRemote/n, 9
- VPN-1/FireWall-1
  - uninstalling, 57
- VPN-1/FireWall-1
  - administrative issues, 627
  - before installing, 18
  - disabling (NT), 44
  - installing in a directory other than the default directory, 30
  - killing the daemon and fw stop, difference between, 627
  - loss of state after upgrading, 23
  - moving to another machine, 83
  - objects carried over from previous version, 21
  - previous version not overwritten during installation, 21
  - reconfiguring, 57
  - reconfiguring (NT), 44
  - stopping, 627
  - stopping (NT), 43
  - stopping inspection (NT), 43
  - uninstalling (NT), 43
  - uninstalling (Unix), 57
  - upgrading, 57

- upgrading to a new version of, 21
- VPN-1/FireWall-1 components on
  - different machines
  - communication between, 69
- VPN-1/FireWall-1 HP OpenView
  - Extension
  - installing, 598
- VPN-1/FireWall-1 HP OpenView
  - extension
  - default SNMP port for FireWalled
    - objects, 598
  - FireWall discovery, 598
- VPN-1/FireWall-1 password
  - advantage over OS
  - password, 484
- VPN-1/FireWall-1 SNMP
  - daemon, 593
- VPN-1/FireWall-1 software
  - installation problems, 57
- VPN-1/FireWall-1 license
  - installing, 59

## W

- wais, 230
- Wait Mode
  - echo-request,echo-reply, 540
- WebTheatre, 230, 307
- Wellfleet, see Bay Networks
- who service, 233
- Width window, 399
- Windows NT
  - supported versions, 5
- Windows Registry, 630
- WinFrame, 230
- workstation
  - menu choice, 101
- workstation objects
  - listing in hosts and lmhosts
    - files, 103, 119
- www.opsec.com, 354

## X

- X.25, 623
- X/Motif
  - obtaining a license for, 59
  - starting the GUI, 88
  - starting the Log Viewer, 370, 390
  - where to install license, 59
- X/Motif GUI
  - HP-UX 11 support, 47
- X/Motif libraries
  - version used by VPN-1/

- FireWall-1, 49, 58
- X11, 230
- Xing, 233
  - and Address Translation, 440
- Xlated Destination Port Selection
  - Criteria window, 409
- Xlated Dst Selection Criteria
  - window, 408
- Xlated Source Port Selection Criteria
  - window, 409
- Xlated Src Selection Criteria
  - window, 408
- Xylan, 2, 5
  - installing Encryption Module on, 5
- Xylan switch, 592
  - setup, 138

## Y

- year
  - format, 157
  - specifying year 2000 or later, 157
- ypbind, 234
- yppasswd, 234
- ypserv, 235
- ypupdated, 235
- ypxfrd, 235

