Essential Check Point FireWall-1™

An Installation, Configuration, and Troubleshooting Guide

Dameon D. Welch-Abernathy

Addison-Wesley
Boston • San Francisco • New York • Toronto • Montreal
London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

©2000 Check Point Software Technologies Ltd. All rights reserved. Check Point, the Check Point logo, FireWall-1, FireWall-1 SecureServer, FloodGate-1, INSPECT, IQ Engine, Meta IP, MultiGate, Open Security Extension, OPSEC, Provider-1, SVN, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Appliance, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 SecuRemote, VPN-1 SecureServer, and ConnectControl are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and Addison-Wesley was aware of a trademark claim, the designations have been printed in initial capital letters or in all capitals.

Although we have made every effort to ensure the correctness and completeness of the material contained in this book, we cannot provide any warranties. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility if a person or an entity suffers a loss or damage from correctly or incorrectly applying the information contained in this book.

The publisher offers discounts on this book when ordered in quantity for special sales. For more information, please contact:

Pearson Education Corporate Sales Division
One Lake Street
Upper Saddle River, NJ 07458
(800) 382-3419
corpsales@pearsontechgroup.com

Visit AW on the Web: www.aw.com/cseng/

Library of Congress Cataloging-in-Publication Data

Welch-Abernathy, Dameon D.
Essential Check Point FireWall-1 : an installation, configuration, and troubleshooting guide / Dameon D. Welch-Abernathy.
p. cm.
Includes bibliographical references and index.
ISBN 0-201-69950-8 (alk. paper)
1. Computer networks—Security measures—Computer programs. 2. Computer security—Computer programs. 3. Fire Wall-1. I. Title.

TK 5105.59.W45 2001
005.8—dc21 2001041246

Copyright © 2002 by Pearson Education, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior consent of the publisher. Printed in the United States of America. Published simultaneously in Canada.

ISBN 0-201-69950-8
Text printed on recycled paper
1 2 3 4 5 6 7 8 9 10—CRS—0504030201
First printing, October 2001

Contents

Foreword **xvii**
Preface **xix**

Chapter 1 **Introduction to Firewalls** **1**
What Is a Firewall? 1
What a Firewall Cannot Do 2
Overview of Firewall Security Technologies 2
Packet Filters 3
Application Proxies 3
Stateful Inspection 4
Technology Comparison: Passive FTP 5
Technology Comparison: Traceroute 6
What Kind of Firewall Is FireWall-1? 8
Do You Really Need FireWall-1? 8
More Information 9

Chapter 2 **Planning Your Firewall Installation** **11**
Network Topology 11
A Word about Subnetting 12
Developing a Sitewide Security Policy 13
The What, Who, and How 14
Implementing Firewalls without a Written Security Policy 15
An Example of a Security Policy 16
Fun with Check Point Licensing 17
Node-Limited Firewall Licenses 18
Single-Gateway Product 19
Inspection Module 19
FireWall-1 Host 19
Management Console 19

Motif GUI Licenses 19
Small-Office Products 20
Getting Licenses 20
Summary 21

Chapter 3 **Installing FireWall-1** **23**

Selecting an Operating System 23
Windows NT/2000 24
Sparc Solaris 25
x86 Solaris 25
AIX and HP/UX 26
Nokia Security Platform (IPSO) 27
Linux 28
Installing the Operating System 29
Preparing for the OS Installation 29
Guidelines for the OS Installation 31
Securing the Operating System 32
Installing FireWall-1 34
UNIX-Based Systems 35
Windows NT/2000 41
Summary 50

Chapter 4 **Building Your Rulebase** **51**

The Management GUIs 51
Configuring a Management User 52
Configuring Which Hosts Can Use Management GUIs 55
Files Modified by the GUIs 56
Security Policy Editor Restrictions 57
GUI Demonstration Mode 57
Rulebase Components 58
Objects 58
Anti-Spoofing 68
Policy Properties 69
Rules 74
Sample Rules 75
Order of Operations 76
Making Your First Rulebase 78
Knowing Your Network 79

Defining Objects 80
Defining the Rules 83
Tweaking the Policy Properties 84
Rules That Should Be in Every Rulebase 86
Installing the Policy 88
Frequently Asked Questions 90
4.1: Which Files Make up My Security Policy? 90
4.2: How Do I Edit `objects.C` and `rulebases.fws` Manually? 90
4.3: Does Any Service Really Mean Any Service? 91
4.4: When Should I Reinstall My Security Policy? 91
4.5: Which Characters or Words Cannot Be Used When Naming Objects? 91
4.6: Are the Rulebase Properties per Firewall or Global? 93
4.7: How Do I Enable DNS Verification When I Use the Rulebase Property to Allow DNS Queries? 93
4.8: Why Are Some Services Slow in Connecting? 93
Troubleshooting 93
4.9: Client Is a Non-VPN, Whereas Management Server Is a VPN Version 93
4.10: My Rulebases Have Disappeared! 94
4.11: Log Viewer Does Not Show All Fields 94
4.12: Using the GUI over Slow Links 95
4.13: I Cannot Fetch a Host's Interfaces 96
Summary 96

Chapter 5 **Logging and Alerts** **97**
The System Status Viewer 97
System Status Information from the Command Line 102
The Log Viewer 103
Viewing Logs from the Command Line 106
Active Mode and Blocking Connections 107
Alerts 111
Messages in the Log 113
Rule 0 113
len xx 116
The Service ident 116

lvfile_open: failed to open logfile c:\winnt\fw\log\fw.log log ptrs problem 116
Log Maintenance 117
Automating fw logswitch on UNIX and IPSO 117
Automating fw logswitch on Windows NT 117
Rotate and Download Logs from Firewall to Management Console 117
Summary 118

Chapter 6 **Remote Management** **119**
The Components 119
The Management Console to Firewall Module Connection 121
The control.map File 122
Commands and Authentication Types Supported in control.map 123
The Workings of Different Authentication Schemes 124
The fw putkey Command 125
Establishing an Authenticated Control Connection 126
Special Remote Management Conditions 128
What You Can Do with Remote Management 132
Control Policy on a Firewall Module 132
View State Tables of Firewall Modules 133
Updating Licenses 134
Moving Management Consoles 136
Moving a Firewall Module off the Management Console 136
Moving the Management Console off the Firewall Module 137
Troubleshooting Remote Management Issues 138
6.1: General Tips 138
6.2: Peer Asked for Deny Authentication or Authentication for Command X Failed 138
6.3: IP Address a.b.c.d Tries to Exchange a Control Security Key, but Has One (or Doesn't Have Any) 139
6.4: WARNING: Using S/Key Authentication Instead of FWA1: No Encryption License 139
6.5: Failed to Install xxxx Control Key: Bad Signature 139
6.6: Operation Would Block 139

6.7: If You Have Recently Changed IP Addresses for One of Your Modules 140
6.8: If All Else Fails 140
Large-Scale Management Issues 141
Security Policies 142
Number of Firewalls 143
Having a Large Amount of Logs 143
Summary 143
Sample Configurations 143
Adding a New Firewall Module to Manage 144
Changing the Default Authentication Scheme to SSL 145
Moving the Firewall off the Management Console 147
Moving the Management Console off the Firewall 149

Chapter 7 **Authentication** **153**
Passwords 153
FireWall-1 Password 154
OS Password 154
S/Key 154
SecurID 156
Axent Pathways Defender 156
Remote Access Dial-In User Service (RADIUS) 157
Terminal Access Controller Access Control System (TACACS/TACACS+) 157
Lightweight Directory Access Protocol (LDAP) 158
How Users Authenticate 158
User Authentication 158
Session Authentication 161
Client Authentication 162
Which Authentication Type Should You Use? 166
Setting Up Authentication 166
Creating Users 167
Creating Groups 173
Setting Supported Authentication Schemes 173
User Authentication 174
The Importance of Rule Order in User Authentication 178
Session Authentication 179

Client Authentication 180

Integrating External Authentication Servers 183

SecurID 184

Axent Pathways Defender 184

RADIUS 185

TACACS/TACACS+ 187

LDAP 188

Frequently Asked Questions 194

7.1: How Do I Use All the Users in My External Authentication Server without Entering Them into FireWall-1? 194

7.2: How Do I Integrate FireWall-1 into a Windows NT Domain? 194

7.3: How Do I Allow People Access Based on What They Are Logged in As on Their Windows Workstation? 195

7.4: How Do I Import or Export Users from a FireWall-1 User Database? 195

7.5: How Do I Add My Own Custom Message for Authentication? 196

7.6: How Do I Forward Authenticated HTTP Requests to an HTTP Proxy? 196

7.7: Can I Use FireWall-1 As a "Reverse HTTP Proxy"? 196

7.8: How Do I Remove the Check Point Banner from Authentication? 199

7.9: Can I Use FireWall-1 As a Proxy? 199

7.10: Can I Use FireWall-1 As an FTP Proxy for My Web Browser? 199

7.11: How Do I Authenticate HTTP over Different Ports? 200

7.12: How Do I Authenticate Outbound HTTPS Traffic? 200

7.13: Can I Authenticate Access to Internal HTTPS Servers? 201

7.14: How Can I Authenticate with HTTP to a Site Requiring Its Own Authentication? 203

7.15: How Can Users Change Their Own Passwords? 203

7.16: Can a User Reset His Own S/Key Chain? 203

7.17: Can I Customize the HTTP Client Authentication Pages? 204

Troubleshooting Authentication Problems 204

7.18: This Gateway Does Not Suppoort X 205

7.19: The Connection Is Closed by a Session Authentication Agent 205

7.20: Authenticated FTP Connections Stop If a Download Takes Longer Than 15 Minutes 205

7.21: Authentication Services Are Unavailable. Connection Refused. 206

7.22: Session Authentication Is Not Secure 206

7.23: Using Session Authentication with Content Security 206

7.24: Authenticating on Each URL 207

7.25: No Client Auth Rules Available 207

7.26: Policy Install Logs out Client Auth Users 207

7.27: Partially Automatic Client Authentication Redirects Site to an IP Address 207

7.28: Using @ in a Username or Password with Client Auth via HTTP 207

7.29: FW-1 Form Has Expired 208

7.30: Users Are Not Being Prompted for Authentication 208

7.31: Request to Proxy Other Than Next Proxy Resource http://proxy.foo.com 208

7.32: Cannot Telnet to the Firewall 208

7.33: My User's Group Association Is Being Ignored 209

7.34: When Accessing Certain Sites, the Connections Are Dropped with the Following in the Logs: Content-Encoding Type Not Allowed 209

Summary 210

Sample Configurations 210

A User Authentication Example 210

A Session Authentication Example 213

A Client Authentication Example 215

Chapter 8 **Content Security** **219**

The Security Servers 219

A Word about Licensing and Third-Party Products 219

CVP and UFP 220

Resources and Wildcards 221

HTTP Security Server 221
    Filtering HTTP without a UFP or CVP Server 222
    UFP with the HTTP Security Server 226
    CVP with the HTTP Security Server 229
Frequently Asked Questions about the HTTP Security Server 231
    Performance Tuning the HTTP Security Server 234
    Troubleshooting Issues with the HTTP Security Server 240
FTP Security Server 242
Frequently Asked Questions about the FTP Security Server 244
SMTP Security Server 246
    $FWDIR/conf/smtp.conf 246
    SMTP Resources 248
Frequently Asked Questions about the SMTP Security Server 251
    Troubleshooting the SMTP Security Server 253
TCP Security Server 256
General Questions about the Security Servers 257
    8:25: Why Do All the Connections I Make through the Security Servers Appear to Originate from the Firewall Instead of the Client? 257
    8.26: Why Is the Security Server Used Even If the Rule Matched Does Not Use a Resource? 257
    8.27: Can I Mix User Authentication and Content Security? 258
    8.28: Can I Mix Session Authentication and Content Security? 258
Debugging the Security Servers 258
Summary 258
Sample Configurations 259
    SMTP Content Security 259
    FTP Content Security 263
    HTTP Content Security 266

Chapter 9 **Network Address Translation** **271**

Introduction 271
RFC-1918 and Link Local Addresses 274
How NAT Works in FireWall-1 275
    The Order of Operations 276

Implementing NAT: A Step-by-Step Example 278
Determine Which IP Addresses Will Be Used 279
Proxy-ARPs 280
Static Host Routes 283
Network Objects 284
Anti-Spoofing 284
Security Policy Rules 284
Address Translation Rules 284
Install the Security Policy and Test 284
Limitations of NAT 284
Dual NAT (Translating Both Source and Destination) 288
Binding the NAT IP Address to the Loopback Interface 290
Troubleshooting NAT 290
ARPs 291
SYN Packets with No Response 292
SYN Followed by RST 294
Useful `tcpdump` Flags 296
Useful `snoop` Flags 297
Summary 299
Sample Configurations 299
A Simple Network with NAT 299
Migrating to a Larger Net with NAT 302
Double-Blind Network Configuration 307

Chapter 10 **Site-to-Site VPNs** **313**

Introduction to a VPN 313
Concepts 314
Encryption 314
Encryption Key 314
Symmetric Encryption 314
Asymmetric Encryption 314
Hash Function 315
Certificate Authority (CA) 315
Diffie-Hellman (DH) Keys 315
Encryption Domain 315
A Word about Licensing 316

Supported Key-Management and Encryption Schemes 317
FWZ 317
IPSec 318
How to Configure Encryption 320
Planning Your Deployment 320
Using IKE 322
Using Manual IPSec 327
SKIP and FWZ 330
Gateway Clusters for High-Availability VPNs 335
Frequently Asked Questions about VPNs in FireWall-1 338
10.1: Does FireWall-1 Interoperate with Third-Party VPN Products? 338
10.2: Does the Gateway Clusters Feature Interoperate with Third-Party VPN Products? 338
10.3: Can I Run Microsoft Networking Protocols through a VPN? 339
10.4: Can I Set up a VPN with a Site without Giving It Access to All My Machines? 339
10.5: Can I Set up More Than One VPN with Different Sites Each Using Different Encryption Schemes? 339
10.6: Can I Set up More Than One VPN with Different Sites and Use a Different Source IP Address for Each Site? 339
10.7: Does FireWall-1 Support a "Hub and Spoke" Model Like Some VPN Hardware Devices Support? 339
10.8: How Does NAT Interact with Encryption? 340
10.9: Can I Require User Authentication in Addition to Encryption? 340
Troubleshooting VPN Problems 340
10.10: General Troubleshooting Guidelines for VPN Problems 340
10.11: Crypt Rule X Not Found 341
10.12: Encryption Failed: Gateway Connected to Both Endpoints 341
10.13: Encryption Failure: One of the Keys Is Not Yet A Valid Scheme: SKIP 342
10.14: Peer Failed to Reply 342

10.15: GUI Crashes When Editing Encryption Keys 343
10.16: ISAKMP AddNegotiation: Try to Handle Too Many Negotiations 344
10.17: Debugging Interoperability Issues with IKE 345
10.18: Traceroute Does Not Appear to Work through a VPN 345
10.19: VPN Fails When Transferring Large Packets 345
Summary 346
Sample Configurations 346
A Three-Site VPN 346
Adding a Business Partner to the VPN Mesh 350
Switching the Spokane Firewall to a Gateway Cluster Configuration 356

Chapter 11 **SecuRemote and Secure Client** **365**

Introduction 365
A Word about Licensing 366
Steps to Configure SecuRemote on FireWall-1 367
Choosing an Encryption Scheme 367
Configuring Firewall Workstation Object for SecuRemote 368
Creating Users for Use with SecuRemote 369
Client Encryption Rules 371
Desktop Security 373
Installing Secure Client 376
High-Availability and Multiple Entry Point Configurations 379
Hybrid Authentication Mode for IKE 382
Microsoft Networking and Secure Client 384
Frequently Asked Questions 386
11.1: Can I Use SecuRemote If My Client Is Subject to NAT? 386
11.2: How Do I Initiate an Encrypted Session to a SecuRemote Client? 389
11.3: What If My SecuRemote Client Must Pass through a FireWall-1 Gateway? 390
11.4: How Can I Use SecuRemote When I Am behind a Proxy? 392
11.5: How Do I Disable SecuRemote at Boot? 392
11.6: How Do I Automate SecuRemote Configurations? 393

11.7: How Can I Configure Secure Client to Access DNS or WINS Servers Inside My Encryption Domain without Manually Configuring the Clients? 393

11.8: Can I Share an Internet Connection and Use SecuRemote? 395

Troubleshooting 396

11.9: SecuRemote Client Needs NAT or a Proxy 396

11.10: SecuRemote Communication Ports Are Blocked 396

11.11: ISP Uses a Custom Adapter to Connect 397

11.12: Problems Adding the New Site 397

11.13: Encapsulation and Packet Sizes 397

11.14: Windows NT and File Permissions 399

11.15: Mixing NICs and Dial-up Adapters 399

Summary 402

Sample Configurations 402

A Simple Client-to-Site VPN 402

Secure Client with Gateway Clusters 406

Multiple Entry Point Secure Client 409

Chapter 12 **High Availability** **415**

State Synchronization's Role in High Availability 415

UDP State Synchronization 417

How Do I Know State Synchronization Is Working? 418

What Are the Limitations of State Synchronization? 418

Implementing High Availability 419

Asymmetric Routing 420

HA Solution Providers 421

Load Balancing 422

Summary 430

Chapter 13 **INSPECT** **431**

What Is INSPECT? 431

Basic INSPECT Syntax 432

Conditions 434

Constants 436

Registers 436

Manipulating Table Entries 437

Creating Your Own Tables 438

How Your Rulebase Is Converted to INSPECT 438

Services of Type Other 443

Sample INSPECT Code 443

Allowing Outbound Connections to SecuRemote Clients 443

Point-to-Point Tunneling Protocol (PPTP) 444

Allowing a Connection Based on a Previous Connection 445

HTTP 445

Ping and Traceroute 448

Different Rules for Different Interfaces 448

Changing Your Default Filter 448

fw monitor 450

Summary 452

AppendixA: **Securing Your Bastion Host** **453**

Appendix B: **`firewall-1.conf` File for Use with OpenLDAP v1** **469**

Appendix C: **`firewall1.schema` File for Use with OpenLDAP v2** **473**

Appendix D: **Complete Program for Stateful Inspection of HTTP** **477**

Appendix E: **Complete Program for Stateful Inspection of Ping and Traceroute** **479**

Appendix F: **INSPECT Script for Different Policies on Different Interfaces** **487**

Appendix G: **Sample `defaultfilter.pf` File** **489**

Appendix H: **Sample Internet Usage Policy** **491**

Appendix I: **Performance Tuning** **495**

Appendix J: **Other Resources** **503**

Appendix K: **Further Reading** **507**

Index **509**