

Contents

Foreword	xxxiii
Part I Introduction to Network Security & Firewalls	1
Chapter 1 Introduction to Information Security	3
Introduction	4
Insecurity and the Internet	4
Defining Information Security	6
Common Information Security Concepts	8
Knowledge Is Power	8
Think Like a Thief	9
Removing Intrusion Opportunities	9
Threats and Attacks	10
Physical Security	10
Network Security	11
Recognizing Network Security Threats	12
Understanding Intruder Motivations	13
Recreational Hackers	13
Profit-Motivated Hackers	13
Vengeful Hackers	14
Hybrid Hackers	15
Categorizing Security Solutions	15
Back to Basics: TCP/UDP Well-Known Ports	15
IP Half-Scan Attack	16
Source-Routing Attack	17
Other Protocol Exploits	17
System and Software Exploits	17
Trojans, Viruses, and Worms	18
Classifying Specific Types of Attacks	20
Social Engineering Attacks	20
Protecting Your Network Against Social Engineers	21
Denial-of-Service Attacks	22
Scanning and Spoofing	28
Security Policies	31
Preventing Intentional Internal Security Breaches	31
Tactical Planning	31
Designating Responsibility for Network Security	32
Responsibility for Developing the Security Plan and Policies	32
Responsibility for Implementing and Enforcing the Security Plan and Policies	32
Designing the Corporate Security Policy	33
Developing an Effective Password Policy	33
Designing a Comprehensive Security Plan	36
Evaluating Security Needs	38

Assessing the Type of Business	38
Assessing the Type of Data	38
Assessing the Network Connections	39
Assessing Management Philosophy	39
Understanding Security Ratings	40
Legal Considerations	41
Addressing Security Objectives	41
Know Your Users	41
Control Your Users	41
Hiring and Human Resource Policies	42
Creating a Security Policy	42
Educating Network Users on Security Issues	42
Protecting Information Technology	45
Improving Security	45
Protecting the Servers	46
Keeping Workstations Secure	46
Protecting Network Devices	46
Using SSL and Secure Shell	47
Testing Security	47
Other Hardware Security Devices	49
Monitoring Activity	49
Detecting Internal Breaches	50
Preventing Unauthorized External Intrusions and Attacks	50
Summary	52
Chapter 2 Firewall Concepts	53
Introduction	54
Defining a Firewall	54
Types of Firewalls	55
Packet Filters	56
Stateful Inspection Packet Filters	56
Application Proxies	57
Networking and Firewalls	58
Firewall Interfaces: Inside, Outside, and DMZ	58
Firewall Policies	61
Address Translation	62
Static Translation	63
Dynamic Translation	63
Port Address Translation	64
Virtual Private Networking	64
Popular Firewalls	66
Hardware-Based Firewalls	67
The Cisco PIX Firewall	68
Nokia Firewall	69
Firewall Software	69
Check Point FW-1	69
Darren Reed's IPFilter	70
Microsoft ISA Server	70
Summary	71
Chapter 3 DMZ Concepts, Layout, and Conceptual Design	73
Introduction	74
DMZ Basics	74
DMZ Concepts	78

Traffic Flow Concepts	84
Networks with and without DMZs	88
Pros and Cons of DMZ Basic Designs	89
DMZ Design Fundamentals	90
Why Design Is So Important	90
Putting It All Together: A Business Case Study	91
Designing End-to-End Security for Data Transmission between Hosts on the Network	92
Traffic Flow and Protocol Fundamentals	93
DMZ Protocols	93
Designing for Protection in Relation to the Inherent Flaws of TCP/IPv4	94
Public and Private IP Addressing	94
Ports	95
Using Firewalls to Protect Network Resources	96
Using Screened Subnets to Protect Network Resources	97
Securing Public Access to a Screened Subnet	97
Traffic and Security Risks	98
Application Servers in the DMZ	99
Domain Controllers in the DMZ	99
RADIUS-Based Authentication Servers in the DMZ	100
VPN DMZ Design Concepts	100
Advanced Risks	101
Business Partner Connections	101
Extranets	102
Web and FTP Sites	102
E-Commerce Services	102
E-Mail Services	103
Advanced Design Strategies	103
Advanced DMZ Design Concepts	103
Remote Administration Concepts	104
Authentication Design	106
DMZ High Availability and Failover	106
DMZ Server Cluster	106
The PIX Failover Services	107
What Causes Failover to Occur	109
Summary	110
Chapter 4 Introduction to Intrusion Detection Systems	111
Introduction	112
What Is Intrusion Detection?	112
Network IDS	114
Host-Based IDS	115
Distributed IDS	115
What Is an Intrusion?	117
Why Are Intrusion Detection Systems Important?	118
Why Are Attackers Interested in Me?	118
Where Does an IDS Fit with the Rest of My Security Plan?	119
Doesn't My Firewall Serve as an IDS?	119
Where Else Should I Be Looking for Intrusions?	120
Backdoors and Trojans	121
What Else Can Be Done with Intrusion Detection?	122
Monitoring Database Access	122
Monitoring DNS Functions	123

E-Mail Server Protection	123
Using an IDS to Monitor My Company Policy	123
Summary	124
PartII Solaris & Linux Firewalls	125
Chapter 5 Implementing a Firewall with Ipchains and Iptables	127
Introduction	128
Understanding the Need for a Firewall	129
Building a Personal Firewall	130
Understanding Packet Filtering Terminology	130
Choosing a Linux Firewall Machine	131
Protecting the Firewall	131
Deploying IP Forwarding and Masquerading	132
Masquerading	134
Configuring Your Firewall to Filter Network Packets	136
Customized Packet Filtering	137
Configuring the Kernel	137
Packet Accounting	137
Understanding Tables and Chains in a Linux Firewall	138
Built-In Targets and User-Defined Chains	139
Specifying Interfaces	139
Setting Policies	140
Using Ipchains to Masquerade Connections	143
Iptables Masquerading Modules	143
Using Iptables to Masquerade Connections	144
Iptables Modules	145
Exercise: Masquerading Connections Using Ipchains or Iptables	145
Logging Packets at the Firewall	146
Setting Log Limits	146
Adding and Removing Packet Filtering Rules	147
ICMP Types	147
Exercise: Creating a Personal Firewall and Creating a User-Defined Chain	149
Redirecting Ports in Ipchains and Iptables	151
Configuring a Firewall	151
Setting a Proper Foundation	152
Creating Anti-Spoofing Rules	152
Counting Bandwidth Usage	155
Listing and Resetting Counters	156
Setting Type of Service (ToS) in a Linux Router	156
Setting ToS Values in Ipchains and Iptables	157
Using and Obtaining Automated Firewall Scripts and Graphical Firewall Utilities	159
Weighing the Benefits of a Graphical Firewall Utility	160
Firewall Works in Progress	160
Exercise: Using Firestarter to Create a Personal Firewall	161
Exercise: Using Advanced Firestarter Features	167
Summary	169
Chapter 6 Maintaining Open Source Firewalls	171
Introduction	172
Testing Firewalls	172
IP Spoofing	173
Open Ports/Daemons	173
Monitoring System Hard Drives, RAM, and Processors	174
Suspicious Users, Logins, and Login Times	174
Check the Rules Database	175

Verify Connectivity with Company Management and End Users	175
Port Scans	176
Using Telnet, Ipchains, Netcat, and SendIP to Probe Your Firewall	176
Ipchains	177
Telnet	177
Using Multiple Terminals	178
Netcat	178
Sample Netcat Commands	179
Additional Netcat Commands	180
Using Netcat	181
SendIP: The Packet Forger	182
SendIP Syntax	182
Using SendIP to Probe a Firewall	184
Understanding Firewall Logging, Blocking, and Alert Options	185
Firewall Log Daemon	186
Obtaining firelogd	186
Syntax and Configuration Options	186
Message Format	187
Customizing Messages	188
Reading Log Files Generated by Other Firewalls	189
Configuring and Compiling firelogd	190
fwlogwatch	191
fwlogwatch Modes	191
fwlogwatch Options and Generating Reports	192
Generating an HTML-Based Firewall Log with fwlogwatch	195
Automating fwlogwatch	195
The fwlogwatch Configuration File	196
Notification Options	197
Response Options	199
Configuring fwlogwatch to Send Automatic Alerts and Block Users	201
Using fwlogwatch with CGI Scripts	202
Obtaining More Information	203
Viewing the Results	204
Using cron and fwlogwatch CGI Scripts to Generate an Automatic HTML Report	205
Additional fwlogwatch Features	207
Obtaining Additional Firewall Logging Tools	207
Summary	209
Chapter 7 Configuring Solaris as a Secure Router and Firewall	211
Introduction	212
Configuring Solaris as a Secure Router	212
Reasoning and Rationale	212
Routing Conditions	213
The S30network.sh Script	214
The S69inet Script	214
Configuring for Routing	215
A Seven-Point Checklist	216
Security Optimization	218
Security Implications	219
Minimal Installation	219
Minimal Services	219
Minimal Users	220
Minimal Dynamic Information	220
Minimal Cleartext Communication	220

Unconfiguring Solaris Routing	220
A Three-Point Checklist	221
Routing IP Version 6	222
Configuration Files	222
The hostname6.interface File	222
The ndpd.conf File	223
The ipnodes File	224
The nsswitch.conf File	225
IPv6 Programs	225
The in.ndpd Program	225
The in.ripngd Program	226
The ifconfig Command	227
IPv6 Router Procedure	227
Stopping IPv6 Routing	228
Method 1: Rebooting the System	228
Method 2: Not Rebooting the System	228
IP Version 6 Hosts	229
Automatic Configuration	229
Manual Configuration	230
The ipnodes File	230
DNS	231
Configuring Solaris as a Secure Gateway	231
Configuring Solaris as a Firewall	232
General Firewall Theory	232
General Firewall Design	233
SunScreen Lite	234
IP Filter	234
Using NAT	235
Summary	236
Part III PIX Firewalls	239
Chapter 8 Introduction to PIX Firewalls	241
Introduction	242
PIX Firewall Features	242
Embedded Operating System	242
The Adaptive Security Algorithm	243
State	244
Security Levels	246
How ASA Works	246
Technical Details for ASA	246
User Datagram Protocol	250
Advanced Protocol Handling	251
VPN Support	251
URL Filtering	252
NAT and PAT	252
High Availability	254
PIX Hardware	254
Models	254
PIX 501	254
PIX 506	256
PIX 506E	256
PIX 515	256
PIX 515E	256

PIX 520	257
PIX 525	257
PIX 535	257
The Console Port	257
Software Licensing and Upgrades	259
Licensing	261
Upgrading Software	261
Password Recovery	262
The Command-Line Interface	264
Factory Default Configurations	264
PIX 501 and 506E	264
PIX 515E, 525, and 535	264
Administrative Access Modes	265
Basic Commands	267
Hostname and Domain Name	268
Configuring Interfaces	268
Static Routes	269
Password Configuration	270
Managing Configurations	271
The write Command	271
The copy Command	271
The configure Command	272
Resetting the System	273
The reload Command	273
Summary	274
Chapter 9 Passing Traffic	277
Introduction	278
Allowing Outbound Traffic	278
Configuring Dynamic Address Translation	278
Identity NAT and NAT Bypass	282
Blocking Outbound Traffic	284
Access Lists	284
Outbound/Apply	290
Allowing Inbound Traffic	292
Static Address Translation	292
Access Lists	293
Conduits	294
ICMP	295
Port Redirection	295
TurboACLs	296
Object Grouping	297
Configuring and Using Object Groups	297
ICMP-Type Object Groups	298
Network Object Groups	298
Protocol Object Groups	299
Service Object Groups	299
Case Study	301
Access Lists	302
Conduits and Outbound/Apply	305
Summary	308
Chapter 10 Advanced PIX Configurations	309
Introduction	310

Handling Advanced Protocols	310
File Transfer Protocol	314
Active vs. Passive Mode	314
Domain Name Service	318
Simple Mail Transfer Protocol	320
Hypertext Transfer Protocol	321
Remote Shell	322
Remote Procedure Call	323
Real-Time Streaming Protocol, NetShow, and VDO Live	324
SQL*Net	328
H.323 and Related Applications	328
Skinny Client Control Protocol	331
Session Initiation Protocol	331
Internet Locator Service and Lightweight Directory Access Protocol	333
Filtering Web Traffic	334
Filtering URLs	334
Websense and N2H2	335
Fine-Tuning and Monitoring the Filtering Process	337
Active Code Filtering	339
Filtering Java Applets	341
Filtering ActiveX Objects	341
DHCP Functionality	341
DHCP Clients	342
DHCP Servers	343
Cisco IP Phone-Related Options	347
Other Advanced Features	347
Fragmentation Guard	347
AAA Floodguard	349
SYN Floodguard	349
The TCP Intercept Feature in PIX v5.3 and Later	350
Reverse-Path Forwarding	351
Unicast Routing	353
Static and Connected Routes	353
Routing Information Protocol	355
Stub Multicast Routing	357
SMR Configuration with Clients on a More Secure Interface	358
SMR Configuration with Clients on a Less Secure Interface	360
Access Control and Other Options	361
PPPoE	362
Summary	365
Chapter 11 Troubleshooting and Performance Monitoring	367
Introduction	368
Troubleshooting Hardware and Cabling	368
Troubleshooting PIX Hardware	370
Troubleshooting PIX Cabling	378
Troubleshooting Connectivity	381
Checking Addressing	382
Checking Routing	384
Failover Cable	388
Checking Translation	389
Checking Access	392
Troubleshooting IPsec	396
IKE	398

IPsec	401
Capturing Traffic	404
Displaying Captured Traffic	405
Display on the Console	405
Display to a Web Browser	406
Downloading Captured Traffic	406
Support Options as Troubleshooting Tools	407
Monitoring and Troubleshooting Performance	408
CPU Performance Monitoring	408
The show cpu usage Command	410
The show processes Command	410
The show perfinon Command	411
Memory Performance Monitoring	413
The show memory Command	413
The show xlate Command	413
The show conn Command	413
The show block Command	414
Network Performance Monitoring	414
The show interface Command	414
The show traffic Command	415
Identification (IDENT) Protocol and PIX Performance	415
Summary	417
Part IV Check Point NG and Nokia IP Series Appliances	419
Chapter 12 Installing and Configuring VPN-1/FireWall-1 Next Generation	421
Introduction	422
Before You Begin	422
Obtaining Licenses	423
Securing the Host	424
Disabling Services	425
Routing and Network Interfaces	426
Enabling IP Forwarding	428
Configuring DNS	428
Preparing for VPN-1/FireWall-1 NG	429
Administrators	433
GUI Clients	434
Upgrading from a Previous Version	434
Installing Check Point VPN-1/FireWall-1 NG on Windows	435
Installing from CD	435
Configuring Check Point VPN-1/FireWall-1 NG on Windows	444
Licenses	444
Administrators	446
GUI Clients	449
Certificate Authority Initialization	450
Installation Complete	452
Getting Back to Configuration	453
Uninstalling Check Point VPN-1/FireWall-1 NG on Windows	455
Uninstalling VPN-1 & FireWall-1	456
Uninstalling SVN Foundation	458
Uninstalling Management Clients	459
Installing Check Point VPN-1/FireWall-1 NG on Solaris	460
Installing from CD	460
Configuring Check Point VPN-1/FireWall-1 NG on Solaris	465

Licenses	466
Administrators	467
GUI Clients	469
SNMP Extension	470
Group Permission	471
Certificate Authority Initialization	471
Installation Complete	473
Unload defaultfilter Script	474
Getting Back to Configuration	475
Uninstalling Check Point VPN-1/FireWall-1 NG on Solaris	476
Uninstalling VPN-1 & FireWall-1	477
Uninstalling SVN Foundation	480
Uninstalling Management Clients	482
Installing Check Point VPN-1/FireWall-1 NG on Nokia	483
Installing the VPN-1/FireWall-1 NG Package	483
Upgrading IPSO Images	483
Installing VPN-1/FireWall-1 NG	484
Configuring VPN-1/FireWall-1 NG on Nokia	487
Summary	489
Chapter 13 Using the Graphical Interface	491
Introduction	492
Managing Objects	492
Network Objects	493
Workstation	494
Network	496
Domain	497
OSE Device	498
Embedded Device	499
Group	500
Logical Server	501
Address Range	502
Gateway Cluster	503
Dynamic Object	503
Services	504
TCP	505
UDP	506
RPC	506
ICMP	507
Other	508
Group	508
DCE-RPC	509
Resources	509
Uniform Resource Identifier	509
URI for QoS	510
SMTP	510
FTP	510
Open Platform for Security Applications	510
Servers	510
Radius	510
Radius Group	511
TACACS	511
Defender	511
Lightweight Database Access Protocol Account Unit	512

Certificate Authority	512
SecuRemote DNS	513
Internal Users	513
Time	513
Group	514
Scheduled Event	514
Virtual Link	514
Adding Rules	515
Rules	515
Adding Rules	515
Source	516
Destination	516
Service	516
Action	516
Track	517
Install On	517
Time	518
Comment	518
Global Properties	518
FW-1 Implied Rules	518
Viewing Implied Rules	519
SYNDefender	519
Security Server	520
Authentication	520
VPN-1	520
Desktop Security	520
Visual Policy Editor	520
Gateway High Availability	521
Management High Availability	521
Stateful Inspection	521
LDAP Account Management	521
Network Address Translation	521
ConnectControl	521
Open Security Extension	521
Log and Alert	521
SecureUpdate	521
Log Viewer	524
Column Selections	525
System Status	525
Summary	527
Chapter 14 Creating a Security Policy	529
Introduction	530
Reasons for a Security Policy	530
How to Write a Security Policy	531
Security Design	533
Firewall Architecture	533
Writing the Policy	534
Introduction	535
Guidelines	535
Standards	535
Procedures	536
Deployment	537
Enforcement	537

Modifications or Exceptions	537
Implementing a Security Policy	537
Default and Initial Policies	537
Translating Your Policy into Rules	538
Defining a Firewall Object	540
Define Rule Base	544
Manipulating Rules	547
Cut and Paste Rules	547
Disable Rules	548
Delete Rules	548
Hiding Rules	548
Drag and Drop	549
Querying the Rule Base	549
Policy Options	549
Verify	550
Install	550
Uninstall	550
View	550
Access Lists	550
Install Users Database	551
Management High Availability	551
Installing a Security Policy	551
Policy Files	552
Summary	554
Chapter 15 Advanced Configurations	555
Introduction	556
Check Point High Availability (CPHA)	556
Enabling High Availability	556
Failing Over	559
Firewall Synchronization	560
Single Entry Point VPN Configurations (SEP)	562
Gateway Configuration	563
Policy Configuration	567
Multiple Entry Point VPN Configurations (MEP)	567
Overlapping VPN Domains	568
Gateway Configuration	571
Overlapping VPN Domains	572
Other High Availability Methods	574
Routing Failover	574
Hardware Options	575
Summary	576
Chapter 16 Configuring Virtual Private Networks	577
Introduction	578
Encryption Schemes	578
Encryption Algorithms; Symmetric versus Asymmetric Cryptography	579
Key Exchange Methods: Tunneling versus In-Place Encryption	580
Hash Functions and Digital Signatures	581
Certificates and Certificate Authorities	582
Types of VPNs	582
VPN domains	582
Configuring an FWZ VPN	582
Defining Objects	583

Local Gateway	583
Remote Gateway	584
Adding VPN Rules	584
FWZ Limitations	586
Configuring an IKE VPN	586
Defining Objects	586
Local Gateway	586
Remote Gateway	587
Adding VPN Rules	588
Testing the VPN	590
Debugging VPNs	591
Considerations for External Networks	592
Configuring a SecuRemote VPN	593
Local Gateway Object	593
User Encryption Properties	594
FWZ	594
IKE	594
Client Encryption Rules	595
Installing SecuRemote Client Software	596
Using SecuRemote Client Software	598
Making Changes to Objects_5_0.C Stick	599
Secure Domain Login	600
VPN Management	600
Summary	601
Chapter 17 Overview of the Nokia Security Platform	603
Introduction	604
Introducing the Nokia IP Series Appliances	604
Enterprise Models	605
IP120	605
IP330	606
IP400 Series	607
IP530	608
IP650	609
IP700	610
Administration Made Easy	611
Summary	614
Chapter 18 Configuring the Check Point Firewall	615
Introduction	616
Preparing for the Configuration	616
Obtaining Licenses	617
Configuring Your Host Name	618
Understanding FireWall-1 Options	618
Configuring the Firewall	620
Installing the Package	620
Enabling the Package	621
Environment and Path	622
VPN-1 and FireWall-1 Directory Structure	622
IP Forwarding and Firewall Policies	623
Unload InitialPolicy Script	625
Running cpconfig	626
Licenses	628
Administrators	629

Management Clients	631
Certificate Authority Initialization	633
Installation Complete	636
Getting Back to Configuration	636
Testing the Configuration	638
Testing GUI Client Access	638
Pushing and Fetching Policy	641
FireWall-1 Command Line	645
Upgrading the Firewall	645
Upgrading from 4.1 SP6 to NG FP2	646
Upgrading from NG FP2 to NG FP3	648
Backing Out from NG to 4.1	648
Summary	650
Chapter 19 Introducing the Voyager Web Interface	651
Introduction	652
Basic System Configuration, Out of the Box	652
Front Screen	653
Navigating Voyager	653
Configuring Basic Interface Information	654
IP Addresses	654
Speed and Duplex	657
Confirming Interface Status	657
Adding a Default Gateway	659
Setting the System Time, Date, and Time Zone	660
Time and Date	660
Configuring the Network Time Protocol	661
Configuring Domain Name System and Host Entries	662
DNS	663
The Hosts Table	664
Configuring a Mail Relay	665
Configuring System Event Notification	665
Configuring the System for Security	666
Enabling SSH Access	666
SSH Versions 1 and 2	667
Host Keys	667
Authorized Keys	668
Starting the Daemon	668
Disabling Telnet Access	669
An Alternative to FTP	669
Securing FTP	670
Configuring Secure Socket Layer	671
Creating the Self-Signed Certificate	671
Enabling HTTPS for Voyager	672
Understanding Configuration Options	674
Interface Configuration	674
System Configuration	674
SNMP	675
IPv6	675
Reboot, Shut Down System	675
Security and Access Configuration	676
Fault Management Configuration	676
Routing Configuration	676
Traffic Management	677
Router Services	678

Summary	679
Chapter 20 Basic System Administration	681
Introduction	682
Rebooting the System	682
Managing Packages	683
Installing New Packages	683
Voyager	684
The Command Line	686
Enabling and Disabling Packages	688
Removing Packages	689
Managing IPSO Images	689
Upgrading to a New IPSO	690
Installing with newimage	692
Deleting Images	693
Managing Users and Groups	694
Users	694
The admin User	694
The monitor User	695
Other Users	695
Groups	696
Configuring Static Routes	699
System Backup and Restore	700
Configuration Sets	700
Making Backups	701
Restoring Backups	704
System Logging	705
Local System Logging	706
Remote Logging	706
Audit Logs	707
Scheduling Tasks Using cron	708
Summary	710
Chapter 21 High Availability and Clustering	713
Introduction	714
Designing Your Cluster	714
Why Do You Need a Cluster?	714
Resilience	714
Increased Capacity	714
High Availability or Load Sharing?	715
Load Sharing	715
High Availability	715
Clustering and Check Point	715
Operating System Platform	715
Clustering and Stateful Inspection	715
Desire for Stickiness	716
Location of Management Station	716
A Management Station on a Cluster-Secured Network	716
Management Station on Internal Network	718
Connecting the Cluster to Your Network : Hubs or Switches?	719
FireWall-1 Features, Single Gateways versus Clusters: The Same, But Different	719
Network Address Translation	719
Security Servers	720
Remote Authentication Servers	721

External VPN Partner Configuration	721
Installing FireWall-1 NG FP3	721
Checking the Installation Prerequisites	721
Installation Options	722
Installation Procedure	723
Check Point ClusterXL	727
Configuring ClusterXL in HA New Mode	727
Prerequisites for Installing ClusterXL in HA New Mode	727
Configuration of ClusterXL HA New Mode	729
Testing ClusterXL in HA New Mode	743
Test 1: Pinging the Virtual IP Address of Each Interface	743
Test 2: Using SmartView Status to Examine the Status of the Cluster Members	744
Test 3: FTP Session Through the Cluster When an Interface Fails	745
Command-Line Diagnostics on ClusterXL	745
How Does ClusterXL HA New Mode Work?	748
ClusterXL HA New Mode Failover	749
ClusterXL Failover Conditions	752
Special Considerations for ClusterXL in HA New Mode	755
Network Address Translation	755
Configuring ClusterXL in HA Legacy Mode	758
Configuring ClusterXL in Load-Sharing Mode	759
Prerequisites for Configuring ClusterXL in Load-Sharing Mode	759
Configuration of ClusterXL in Load-Sharing Mode	759
Testing ClusterXL in Load-Sharing Mode	759
Test 1: Pinging the Virtual IP Address for Each Interface	759
Test 2: Using SmartView Status to Examine the Status of the Cluster Members	760
Test 3: FTPing through ClusterXL Load Sharing During Failover	760
Command-Line Diagnostics for ClusterXL	761
How ClusterXL Works in Load-Sharing Mode	764
ClusterXL Load-Sharing Mode Failover	765
Special Considerations for ClusterXL in Load-Sharing Mode	767
Network Address Translation	767
User Authentication and One-Time Passcodes	767
Nokia IPSO Clustering	768
Nokia Configuration	768
A Few Points about Installing an Initial Configuration of NG FP3 on Nokia IPSO	769
Check Point FireWall-1 Configuration for a Nokia Cluster	769
Configuring the Gateway Cluster Object	770
Nokia Cluster Configuration on Voyager	774
Voyager Configuration	774
Testing the Nokia Cluster	778
Test 1: Pinging the Virtual IP Address of Each Interface	778
Test 2: Determining the Status of Each Member in the Cluster	779
Test 3: FTPing through a Load-Sharing Nokia Cluster During Interface Failure	781
Command-Line Stats	782
How Nokia Clustering Works	784
Nokia Cluster Failover	786
Nokia Failover Conditions	787
Special Considerations for Nokia Clusters	787
Network Address Translation	787
Defining the Cluster Object Topology	788
Nokia IPSO VRRP Clusters	788
Nokia Configuration	788

Nokia VRRP Configuration on Voyager	790
Voyager Configuration	791
Testing the Nokia VRRP Cluster	794
Test 1: Pinging the Virtual IP Address for Interface	794
Test 2: Finding Which Member Responds to Administrative Connections to the VIPs	795
Test 3: Determining the Status of Each Member in the Cluster	795
Test 4: FTPing through a VRRP Cluster During Interface Failure	796
Command-Line Stats	796
How VRRP Works	796
Special Considerations for Nokia VRRP Clusters	798
Network Address Translation	798
Connections Originating from a Single Member in the Cluster	799
Third-Party Clustering Solutions	799
Clustering and HA Performance Tuning	799
Data Throughput or Large Number of Connections	799
Improving Data Throughput	800
Improving for Large Number of Connections	802
Final Tweaks to Get the Last Drop of Performance	807
Summary	808
Part V ISA Server	811
Chapter 22 ISA Server Deployment Planning and Design	813
Introduction	814
ISA Deployment: Planning and Designing Issues	814
Assessing Network and Hardware Requirements	814
System Requirements	815
Software Requirements	815
Processor Requirements	815
Multiprocessor Support	816
RAM Configuration	817
Disk Space Considerations	818
Cache Size Considerations	818
Logging and Reporting	820
Network Interface Configuration	820
Active Directory Implementation	825
Mission-Critical Considerations	826
Hard Disk Fault Tolerance	826
Mirrored Volumes (Mirror Sets)	827
RAID 5 Volumes (Stripe Sets with Parity)	828
Network Fault Tolerance	831
Server Fault Tolerance	831
Bastion Host Configuration	834
Planning the Appropriate Installation Mode	834
Installing in Firewall Mode	835
Installing in Cache Mode	835
Installing in Integrated Mode	836
Planning for a Stand-Alone or an Array Configuration	837
Planning ISA Client Configuration	838
The Firewall Service Client	838
The Web Proxy Client	840
The Secure NAT Client	840
Assessing the Best Solution for Your Network	841
Internet Connectivity and DNS Considerations	842

Level of Service	842
External Interface Configuration	843
DNS Issues	844
Summary	845
Chapter 23 ISA Server Installation	847
Introduction	848
Putting Together Your Flight Plan	848
Installation Files and Permissions	848
CD Key and Product License	849
Active Directory Considerations	849
Server Mode	850
Disk Location for ISA Server Files	850
Internal Network IDs and the Local Address Table	851
ISA Server Features Installation	851
Performing the Installation	852
Installing ISA Server: A Walkthrough	852
Upgrading a Stand-Alone Server to an Array Member: A Walkthrough	860
Performing the Enterprise Initialization	861
Backing Up a Configuration and Promoting a Stand-Alone Server to an Array Member	863
Changes Made After ISA Server Installation	868
Migrating from Microsoft Proxy Server 2.0	868
What Gets Migrated and What Doesn't	869
Functional Differences between Proxy Server 2.0 and ISA Server	870
Learn the ISA Server Vocabulary	873
Upgrading Proxy 2.0 on the Windows 2000 Platform	874
Upgrading a Proxy 2.0 Installation on Windows NT 4.0	876
A Planned Upgrade from Windows NT 4.0 Server to Windows 2000	877
Summary	879
Chapter 24 Managing ISA Server	881
Introduction	882
Understanding Integrated Administration	882
The ISA Management Console	882
Adding ISA Management to a Custom MMC	884
The Components of the ISA MMC	885
The ISA Console Objects	891
ISA Wizards	904
The Getting Started Wizard	905
Rules Wizards	905
VPN Wizards	906
Performing Common Management Tasks	906
Configuring Object Permissions	906
Default Permissions	906
Special Object Permissions	907
Setting Permissions on ISA Objects	908
Managing Array Membership	908
Creating a New Array	908
Adding and Removing Computers	909
Promoting a Stand-Alone ISA Server	910
Using Monitoring, Alerting, Logging, and Reporting Functions	910
Creating, Configuring, and Monitoring Alerts	910
Viewing Alerts	911
Creating and Configuring Alerts	911

Refreshing the Display	915
Event Messages	915
Monitoring Sessions	915
Using Logging	917
Logging to a File	917
Logging to a Database	918
Configuring Logging	919
Generating Reports	922
Creating Report Jobs	922
Viewing Generated Reports	926
Configuring Sort Order for Report Data	930
Saving Reports	931
Configuring the Location for Saving the Summary Database	931
Understanding Remote Administration	932
Installing the ISA Management Console	933
Managing a Remote Standalone Computer	933
Remotely Managing an Array or Enterprise	934
Using Terminal Services for Remote Management of ISA	934
Installing Terminal Services on the ISA Server	935
Installing Terminal Services Client Software	936
Summary	939
Chapter 25 Optimizing, Customizing, Integrating, and Backing Up ISA Server	941
Introduction	942
Optimizing ISA Server Performance	942
Establishing a Baseline and Monitoring Performance	943
How Baselines Are Used	943
Defining Threshold Values	944
Using the Performance Monitor Tools	945
Addressing Common Performance Issues	964
Addressing Network Bandwidth Issues	965
Addressing Load-Balancing Issues	968
Cache Configuration Issues	970
Editing the Windows 2000 Registry to Tune ISA Performance Settings	973
Customizing ISA Server	975
Using the ISA Server Software Developer's Kit	975
Administration Scripts	975
Sample Filters	977
Using Third-Party Add-Ons	978
Types of Add-On Programs	978
Overview of Available Add-On Programs	979
Integrating ISA Server with Other Services	980
Understanding Interoperability with Active Directory	980
Stand-Alone versus Array Member	980
The Active Directory Schema	981
ISA Server and Domain Controllers	981
Understanding Interoperability with Routing and Remote Access Services	981
RRAS Components	982
RRAS and ISA Server	982
Understanding Interoperability with Internet Information Server	983
IIS Functionality	983
Publishing IIS to the Internet	983
Understanding Interoperability with IPsec	984
How IPsec Works	984
How IPsec Is Configured in Windows 2000	985
IPsec and ISA Server	986

Integrating an ISA Server into a Windows NT 4.0 Domain	987
Backing Up and Restoring the ISA Configuration	987
Backup Principles	987
Backing Up and Restoring Stand-Alone Server Configurations	988
Backing Up and Restoring Array and Enterprise Configurations	989
Backing Up and Restoring an Array Configuration	989
Backing Up and Restoring an Enterprise Configuration	991
Summary	992
Chapter 26 Troubleshooting ISA Server	993
Introduction	994
Troubleshooting Guidelines	994
The Five Steps of Troubleshooting	994
Information Gathering	995
Analysis	996
Solution Implementation	996
Assessment	996
Documentation	997
ISA Server and Windows 2000 Diagnostic Tools	997
ISA Server Troubleshooting Resources	999
Troubleshooting ISA Server Installation and Configuration Problems	1005
Hardware and Software Compatibility Problems	1005
ISA Server Doesn't Meet Minimum System Requirements	1005
ISA Server Exhibits Odd Behavior When Windows 2000 NAT Is Installed	1006
Internal Clients Are Unable to Access External Exchange Server	1006
Initial Configuration Problems	1007
Unable to Renew DHCP Lease	1007
Failure of Services to Start After Completing Installation	1007
Inability to Join Array	1008
Inability to Save LAT Entry	1008
ISA Server Control Service Does Not Start	1008
Troubleshooting Authentication and Access Problems	1009
Authentication Problems	1009
User's HTTP Request Is Sometimes Allowed, Although a Site and Content Rule Denies Access	1010
Failure to Authenticate Users of Non-Microsoft Browsers	1010
Error Message When Using Pass-Through Authentication with NTLM	1011
Access Problems	1012
Inability of Clients to Browse External Web Sites	1012
Problems with Specific Protocols or Protocol Definitions	1012
Inability of Clients to PING External Hosts	1013
Redirection of URL Results in Loop Condition	1013
Ability of Clients to Continue Using a Specific Protocol After Disabling of Rule	1013
Dial-Up and VPN Problems	1014
Inability of ISA Server to Dial Out to the Internet	1014
Dial-Up Connection Is Dropped	1014
Inability of PPTP Clients to Connect Through ISA Server	1015
Troubleshooting ISA Client Problems	1015
Client Performance Problems	1015
Slow Client Connection: SecureNAT Clients	1015
Slow Internal Connections: Firewall Clients	1016
Client Connection Problems	1017
Inability of Clients to Connect Via Modem	1017
Inability of SecureNAT Clients to Connect to the Internet	1017
Inability of Clients to Connect to External SSL Sites	1017
Inability of SecureNAT Clients to Connect Using Computer Names	1018
Inability of SecureNAT Clients to Connect to Specific Port Due to a Timeout	1018

Troubleshooting Caching and Publishing Problems	1019
Caching Problems	1019
All Web Objects Not Being Cached	1019
Web Proxy Service Does Not Start	1020
Publishing Problems	1020
Inability of Clients to Access Published Web Server	1020
Inability of External Clients to Send E-Mail Via Exchange Server	1021
Summary	1023

Chapter 27 Advanced Server Publishing with ISA Server 1025

Introduction	1026
Disabling Socket Pooling	1029
Disabling Web and FTP Service Socket Pooling	1031
Disabling SMTP and NNTP Service Socket Pooling	1032
Disabling IIS Services on the ISA Server	1032
Server Publishing	1033
Publishing Terminal Services on the Internal Network	1034
Publishing Terminal Services on an Alternate Port	1035
Publishing Terminal Services on the ISA Server	1038
Publishing Terminal Services on the ISA Server Using Packet Filters	1038
Publishing Terminal Services on Both the ISA Server and Internal Network	1040
Publishing TSAC Sites	1041
Installing the TSAC Software on the Web Server	1042
Publishing the TSAC Web Server	1042
Publishing the Terminal Server	1045
Connecting to the TSAC Web Site and the Terminal Server	1046
Publishing TSAC Sites on an Alternate Port	1049
Publishing FTP Servers on the Internal Network	1049
Publishing FTP Servers on Alternate Ports	1051
Publishing FTP Servers Co-Located on the ISA Server	1057
Method One: Creating Packet Filters	1058
Method Two: Server and Web Publishing Rules	1060
Using Web Publishing Rules to Allow Secure FTP Access	1064
Configuring the Incoming Web Requests Listener	1064
Creating the Destination Set for the FTP Site	1066
Publishing the FTP Site with a Web Publishing Rule	1066
Publishing HTTP and HTTPS (SSL) Servers with Server Publishing Rules	1068
Configuring the Incoming Web Requests Listener to Prevent Port Contention	1069
Create an HTTP Server Protocol Definition	1070
Create the HTTP Server Publishing Rule	1071
Publishing pcAnywhere on the Internal Network	1071
Creating the pcAnywhere Protocol Definitions	1072
Creating the pcAnywhere Server Publishing Rules	1073
Web Publishing	1074
Incoming Web Request Listeners	1075
Destination Sets	1075
Public DNS Entries	1076
Private DNS Entries	1077
Terminating an SSL Connection at the ISA Server	1078
Creating a Stand-Alone Root Certificate Server	1079
Creating an Enterprise Root Certificate Server	1086

Exporting the Web Site Certificate and Importing the Certificate into the ISA Server Certificate Store	1088
Bridging SSL Connections	1091
Bridging SSL Connections as HTTP	1092
Bridging SSL Connections as SSL	1094
Secure FTP Connections Using SSL	1099
Publishing a Certificate Server	1100
Summary	1103
Chapter 28 Protecting Mail Services with ISA Server	1105
Introduction	1106
Configuring Mail Services on the ISA Server	1107
Publishing the IIS SMTP Service on the ISA Server	1107
Configuring the SMTP Service	1108
Configuring the SMTP Server Publishing Rule	1111
Message Screener on the ISA Server	1114
Publishing Exchange Server on the ISA Server	1117
Installing Windows 2000	1119
Configuring DNS Server Forward and Reverse Lookup Zones	1122
Promoting the Machine to a Domain Controller	1124
Installing ISA Server	1127
Installing Exchange Server	1128
Disabling Socket Pooling for the Exchange Services	1129
Configure Server Publishing Rules to Publish the Exchange Services	1132
Secure Services Publishing	1135
Configure Services “Publishing” with Packet Filters	1140
Publishing Outlook Web Access on the ISA Server	1141
Configure the SSL Listening Port on the Default Web Site	1142
Configure Authentication Methods on the OWA Folders	1142
Force a Secure Channel to the OWA Folders	1144
Configuring the Incoming Web Requests Listener and the Web Publishing Rule	1144
Configuring User Rights on the Domain Controller	1147
Connecting to the OWA Site	1148
Troubleshooting Notes on Publishing OWA on the ISA Server	1149
Message Screener on the ISA Server and Exchange Server	1150
Disable the SMTP Service	1151
Disable the ISA Server Services	1151
Configure the New SMTP Virtual Server	1151
Restart the ISA Server Services	1153
Restart the SMTP Service	1153
Notes on the SMTP Message Screener on the Exchange Server Configuration	1154
Configuring Mail Services on the Internal Network	1155
Publishing Exchange Server on the Internal Network	1155
Exchange RPC Publishing	1157
How Exchange RPC Publishing Works	1158
Preparing the Infrastructure for Exchange RPC Publishing	1160
Publishing Outlook Web Access on the Internal Network Exchange Server	1165
Message Screener on the Internal Network Exchange Server	1166
GFI’s Mail Security and Mail Essentials for SMTP Servers	1169
MailSecurity Versions	1170
Installing MailSecurity for SMTP Gateways	1170
Configuring MailSecurity	1173
Summary	1179

Part VI Intrusion Detection	1181
Chapter 29 Introducing Snort	1183
Introduction	1184
What Is Snort?	1185
Snort System Requirements	1186
Hardware	1186
Operating System	1187
Other Software	1187
Exploring Snort's Features	1188
Packet Sniffer	1189
Preprocessor	1190
Detection Engine	1191
Alerting/Logging Component	1192
Using Snort on Your Network	1194
Snort's Uses	1195
Using Snort as a Packet Sniffer and Logger	1195
Using Snort as an NIDS	1199
Snort and Your Network Architecture	1199
Snort and Switched Networks	1202
Pitfalls When Running Snort	1204
False Alerts	1205
Upgrading Snort	1205
Security Considerations with Snort	1205
Snort Is Susceptible to Attacks	1205
Securing Your Snort System	1206
Summary	1208
Chapter 30 Installing Snort	1209
Introduction	1210
A Brief Word about Linux Distributions	1210
Debian	1211
Slackware	1211
Gentoo	1211
Installing PCAP	1212
Installing libpcap from Source	1214
Configure, Make, Make Install Defined	1216
Installing libpcap from RPM	1217
Installing Snort	1218
Installing Snort from Source	1218
Customizing Your Installation: Editing the snort.conf File	1219
Enabling Features via configure	1221
Installing Snort from RPM	1221
Installation on the MS Windows Platform	1223
Detailed Component Selection Options	1225
Installing Bleeding-Edge Versions of Snort	1225
The CVS System	1226
Summary	1227
Chapter 31 Combining Firewalls and IDS	1229
Introduction	1230
Policy-Based IDS	1230
Defining a Network Policy for the IDS	1231
An Example of Policy-Based IDS	1235
Policy-Based IDS in Production	1240
Inline IDS	1243

Where Did the Inline IDS for Snort Come From?	1243
Installation of Snort in Inline Mode	1244
Using Inline IDS to Protect Your Network	1258
Is Inline IDS the Tool for Me?	1260
IDS Functionality on the PIX Firewall	1261
Supported Signatures	1261
Configuring Auditing for the PIX with an IDS	1264
Disabling Signatures	1265
Configuring Shunning	1266
Summary	1267
Index	1270