

---

# Table of Contents

**Introduction** xxxii

**Part I Security Overview and Firewalls** 3

**Chapter 1 Security Threats** 5

Planning for Security	6
Diverse Platforms	6
Security Goals	7
Causes of Security Problems	8
Policy Definitions	9
Policies: Business and Security	9
People	10
Enforcement	10
Change Management	11
Disaster Recovery	11
Computer Technologies	13
Network Protocol Weaknesses	13
Operating System Weaknesses	14
Network Equipment Weaknesses	15
Equipment Configurations	15
Types of Security Threats	16
External and Internal Threats	16
Unstructured and Structured Threats	17
Categories of Threats	18
Reconnaissance Attacks	19
Scanning Attacks	19
Eavesdropping Attacks	20
Access Attacks	22
Unauthorized Access Attack	23
Data-Manipulation Attack	24
Session Attacks	25
Virus, Trojan Horse, and Worm Attacks	29
Denial of Service Attacks	31
Types of DoS Attacks	31
DoS Attack-Prevention Methods	33
Security Solutions	34
Designing a Security Solution	34

The Cisco Security Wheel	35
Secure Your Network	36
Monitor Your Security	36
Test Your Security	37
Improve Your Security	37
Security Checklist	37
Additional Information	38

Summary	38
---------	----

## **Chapter 2** Introduction to Firewalls 41

Firewall Overview	41
Definition of a Firewall	42
Firewall Protection	43
Controlling Traffic and the OSI Reference Model	45
OSI Reference Model Overview	45
Firewalls and the OSI Reference Model	46
Firewall Categories	47
Packet-Filtering Firewalls	47
Filtering Actions	48
Filtering Information	49
Advantages of Packet-Filtering Firewalls	51
Limitations of Packet-Filtering Firewalls	52
Uses for Packet-Filtering Firewalls	53
Stateful Firewalls	53
Problems with Packet-Filtering Firewalls	54
State Table	59
Advantages of Stateful Firewalls	61
Limitations of Stateful Firewalls	61
Uses for Stateful Firewalls	64
Application Gateway Firewalls	64
Authentication Process	65
Authentication Methods	66
Application Gateway Firewall Types	67
Cut-Through Proxy Firewalls	69
Advantages of Application Gateway Firewalls	70
Limitations of Application Gateway Firewalls	70
Other Types of Application Proxy Devices	71
Uses for Application Gateway Firewalls	72
Address-Translation Firewalls	72
Filtering Process	72
Advantages of Address-Translation Firewalls	75
Limitations of Address-Translation Firewalls	75
Uses for Address-Translation Firewalls	76

---

Host-Based Firewalls	76
Advantages of Host-Based Firewalls	77
Limitations of Host-Based Firewalls	78
Uses for Host-Based Firewalls	79
Hybrid Firewalls	79
Firewalls and Other Services	80
Firewall Design	81
Design Guidelines	81
Developing a Security Policy	81
Designing Simple Solutions	82
Using Devices Correctly	82
Creating a Layered Defense	83
Dealing with Internal Threats	84
DMZ	85
DMZ Rules and Traffic Flow	85
DMZ Types	87
Components	91
Perimeter Router Component	91
Firewall Component	92
VPN Component	92
IDS Component	92
Component Placement	94
Simple Firewall System Design	95
Enhanced Firewall System Design	96
Design Considerations	98
Firewall Implementation	99
Security Device Manager	99
Implementing Firewall Features	101
Firewall Administration and Management	101
Cisco IOS Security	102
Cisco IOS Uses	102
Cisco IOS Security Features	103
Cisco IOS Devices and Their Uses	105
When to Use a Cisco IOS Firewall	105
Summary	107

## **Part II Managing Access to Routers 109**

### **Chapter 3 Accessing a Router 111**

Types of Authentication	111
No Password Authentication	112
Static Password Authentication	112
Aging Password Authentication	113

One-Time Password Authentication	114
Token Card Services	115
Methods of User EXEC Access	117
Local Access: Console and Auxiliary	118
Login Authentication Methods	119
Login Connection Timeouts	120
Remote Access	121
VTY (Telnet)	121
Secure Shell	123
Web Browser	127
HTTP with SSL	130
SNMP	139
Privileged EXEC Access	146
Passwords	146
Privilege Levels	146
Restricting Levels	146
Password Levels	149
Local Authentication Database	150
Other Access Items	152
Encrypting Passwords	152
Banners	153
Banner Guidelines	153
Banner Configuration	154
Example Configuration	156
Summary	159
<b>Chapter 4</b> Disabling Unnecessary Services	<b>161</b>
Disabling Global Services	161
Cisco Discovery Protocol	162
TCP and UDP Small Servers	163
Finger	164
IdentD	165
IP Source Routing	166
FTP and TFTP	167
HTTP	167
SNMP	168
Name Resolution	169
BootP	170
DHCP	171
PAD	172
Configuration Autoloading	172

---

Disabling Interface Services	173
CDP on Insecure Interfaces	173
Proxy ARP	174
Directed Broadcasts	176
ICMP Messages	177
ICMP Unreachables	177
ICMP Redirects	178
ICMP Mask Replies	180
Maintenance Operation Protocol	181
VTYs	181
Unused Interfaces	182
Manual Configuration Example of Disabling Services on a Perimeter Router	183
AutoSecure	184
Securing Planes	185
The Management Plane	185
The Forwarding Plane	186
AutoSecure Configuration	187
Starting up AutoSecure	187
Going Through a Sample Script	188
Verifying AutoSecure's Configuration	198
Using Additional Commands	198
Summary	199
<b>Chapter 5 Authentication, Authorization, and Accounting</b>	<b>201</b>
AAA Overview	201
AAA Functions	202
Enabling AAA	202
Security Protocols	203
TACACS+	203
RADIUS	205
Server Groupings	208
Troubleshooting TACACS+ and RADIUS	209
Server Protocol Example Configuration	211
Comparison of TACACS+ and RADIUS	212
Authentication	213
Methods of Authentication	213
Authentication Configuration	216
User EXEC Authentication	216
Privileged EXEC Authentication	217
Username and Password Prompts	218
Login Banners	218
Login Attempts	219

Authentication Troubleshooting	219
Authentication Example	220
Authorization	221
Methods of Authorization	222
Authorization Configuration	222
Executing Commands	223
Executing Configuration Commands	224
Authorization Troubleshooting	224
Authorization Example	225
Accounting	226
Methods of Accounting	226
Accounting Configuration	227
Enabling Accounting	227
Suppressing Null Username Records	229
Enabling Broadcast Accounting	229
Accounting Troubleshooting	230
Accounting Example	230
Secure Copy	231
Preparation for SCP	231
SCP Configuration	232
SCP Troubleshooting	232
SCP Example	232
Summary	233

### **Part III Nonstateful Filtering Technologies 235**

#### **Chapter 6 Access List Introduction 237**

Access List Overview	237
ACLs and Filtering	238
Simple ACL Example	238
Types of ACLs	239
Processing ACLs	241
Conditions	241
Matches on Conditions	241
ACL Flowchart	242
Statement Order in ACLs	243
ACL Rules and Restrictions	246
Placement of ACLs	247
Basic ACL Configuration	249
Creating ACLs	250
Activating ACLs	251
Editing ACLs	252

---

Wildcard Masks	254
Converting a Subnet Mask to a Wildcard Mask	254
Wildcard Mask Mistakes	256
Summary	257
<b>Chapter 7 Basic Access Lists</b>	<b>259</b>
Types of ACLs	259
Standard ACLs	260
Numbered Standard ACLs	261
Named Standard ACLs	262
Standard ACL Examples	263
Extended ACLs	264
Numbered Extended ACLs	264
Named Extended ACLs	273
Extended ACL Examples	273
ACL Verification	278
Fragments and Extended ACLs	280
Fragmentation Process	280
Fragmentation and Filtering Issues	281
Filtering Fragments	282
Fragment Filtering Example	283
Timed ACLs	285
Creating Time Ranges	285
Activating Time Ranges	287
Using Distributed Timed ACLs	287
Example of Timed ACL	288
Additional ACL Features	289
ACL Remarks	290
Logging Updates	291
IP Accounting and ACLs	292
Configuration of Accounting	292
Restriction of Accounting Information	293
Turbo ACLs	295
Sequenced ACLs	296
ACLs and Sequencing	297
Resequencing ACLs	298
Deleting an Entry in a Sequenced ACL	299
Inserting an Entry in a Sequenced ACL	299
Protection Against Attacks	301
Bogon Blocking and Spoofing	301
Ingress Filtering	302
Egress Filtering	305

DoS and Distributed DoS Attacks	307
TCP SYN Floods	307
Smurf and Fraggle Attacks	308
Simple Reconnaissance Attacks	314
Ingress Filtering of ICMP Traffic	314
Egress Filtering of ICMP Traffic	315
Traceroute	316
Distributed DoS Attacks	317
DDoS Components	317
DDoS Process	317
The Five Main DDoS Attacks	319
Trojan Horses	325
Trojan Horse ACLs	325
Other Prevention Methods	327
Worms	327
Solutions to Worm Problems	328
SQL Slammer Worm	328
Deloder Worm	330
The Microsoft RPC Service and Worms	330
Blocking Unnecessary Services	332
An Uphill Battle	332
Instant-Messenger Products	333
AOL Instant Messenger	333
ICQ	334
Microsoft MSN Messenger	335
Yahoo! Messenger	336
Apple iChat	338
File Sharing: Peer-to-Peer Products	338
Prevention and Detection	339
Napster	340
Kazaa and Morpheus	341
Gnutella	343
IMesh	343
WinMX	344
AudioGalaxy	345
eDonkey2000	346
Summary	347

## **Part IV Stateful and Advanced Filtering Technologies 349**

### **Chapter 8 Reflexive Access Lists 351**

Overview of Reflexive ACLs	351
Extended Versus Reflexive ACLs	352
How Extended ACLs Handle Returning ICMP Traffic	352

---

How Extended ACLs Handle Returning UDP Traffic	353
How Extended ACLs Handle Returning TCP Traffic	354
How RACLs Handle Returning Traffic	355
Reflexive ACLs in Action	357
Steps in Processing Traffic	357
Traffic Leaving the Network	358
Building the RACL	358
Traffic Returning to the Network	359
Removing RACL Entries	360
Limitations of Reflexive ACLs	361
Stateful Issues	362
Application Issues	362
Configuring Reflexive ACLs	365
Interface Selection	365
Two-Interface Example	365
Three-Interface Example	366
Configuration Commands	368
Building the RACL	368
Referencing the RACL	371
ACL Activation	372
Optional Commands	373
RACL Verification	373
Reflexive ACL Examples	374
Simple RACL Example	374
Two-Interface RACL Example	375
Three-Interface RACL Example	375
Summary	379
<b>Chapter 9 Context-Based Access Control</b>	<b>381</b>
Cisco IOS Firewall Features	381
CBAC Functions	382
Filtering Traffic	382
Inspecting Traffic	383
Detecting Intrusions	383
Generating Alerts and Audits	383
Operation of CBAC	383
Basic Operation	384
CBAC Enhancements over RACLs	385
TCP Traffic	385
UDP Traffic	386
ICMP Traffic	386
Extra Connections	387

Embedded Addressing Information	387
Application Inspection	389
DoS Detection and Prevention	389
Supported Protocols for CBAC	390
RTSP Applications	390
H.323 Applications	392
Skinny Support	393
SIP Support	394
CBAC Performance	395
Throughput Improvement Feature	396
Connections Per Second Improvement Feature	396
CPU Utilization Improvement Feature	397
CBAC Limitations	397
CBAC Configuration	398
Step 1: Interface Selection	399
Step 2: ACL Configuration	399
Step 3: Global Timeouts	400
Step 4: Port Application Mapping	401
PAM Table	402
PAM Configuration	403
PAM Verification	404
PAM Examples	404
Step 5: Inspection Rules	405
Inspection Rule Components	405
Generic TCP and UDP Inspection	406
ICMP Inspection	407
HTTP Inspection	407
RPC Inspection	408
SMTP Inspection	408
Fragment Inspection	409
Skinny Inspection	409
Step 6: Inspection Activation	410
Step 7: Troubleshooting CBAC	410
show commands	411
debug commands	413
Alerts and Audits	414
CBAC Removal	415
CBAC Examples	415
Simple Example	415
Two-Interface CBAC Example	417
Three-Interface CBAC Example	418
Summary	423

---

<b>Chapter 10</b>	<b>Filtering Web and Application Traffic</b>	<b>425</b>
	Java Applets	425
	Java Inspection	425
	Java Blocking	426
	Java Blocking Example	426
	URL Filtering	428
	Operation of URL Filtering	429
	Advantages and Limitations of URL Filtering	430
	Advantages of URL Filtering	430
	Restrictions of URL Filtering	431
	URL Filtering Implementation	432
	Content Server Location	432
	URL Filtering Setup	433
	URL Filtering Verification	439
	show Commands	440
	debug Commands	442
	URL Filtering Example	442
	Network-Based Application Recognition	444
	Components of QoS	444
	NBAR and Classification	445
	Classification Process	445
	NBAR and Traffic Filtering	447
	Supported Protocols and Applications	447
	NBAR Restrictions and Limitations	451
	Basic NBAR Configuration	451
	Step 1: Enable CEF	452
	Step 2: Specify Nonstandard Ports	452
	Step 3: Classify Traffic	454
	Step 4: Download PDLMS	457
	Step 5: Define a Traffic Policy	458
	Step 6: Activate the Traffic Policy	459
	Step 7: Filter Marked Traffic	459
	NBAR Verification	460
	Class Maps	460
	Policy Maps	460
	Traffic Flow and NBAR	462
	NBAR Examples	463
	NBAR and Code Red	463
	NBAR and Nimda	466
	NBAR and P2P Programs	467
	Summary	469

**Part V Address Translation and Firewalls 471****Chapter 11 Address Translation 473**

- Address Translation Overview 473
  - Private Addresses 473
  - Address Translation 474
    - Advantages of Address Translation 475
    - Disadvantages of Address Translation 475
- How Address Translation Works 476
  - Terms Used in Address Translation 476
  - Performing Address Translation 477
    - Network Address Translation 477
    - Overlapping Addresses 479
    - Address Overloading 480
    - Traffic Distribution and Load Balancing 482
  - Limitations of Address Translation 483
- Address Translation Configuration 484
  - Configuration of NAT 484
    - Static NAT 485
    - Dynamic NAT 487
  - Configuration of PAT 489
  - Configuration of Port Address Redirection 491
  - Dealing with Overlapping Addresses 493
    - Static Translation 494
    - Dynamic Translation 496
  - Configuration of Traffic Distribution 497
  - Configuration of Translation Limits 499
    - Setting Connection Limits 500
    - Setting Timeout Limits 500
  - Verifying and Troubleshooting Address Translation 501
    - show Commands 501
    - clear Commands 503
    - debug ip nat Command 504
- NAT and CBAC Example 505
- Summary 507

**Chapter 12 Address Translation Issues 509**

- Embedded Addressing Information 509
  - Problem with Embedding Addressing Information 510
  - Supported Protocols and Applications 511
  - Nonstandard Port Numbers 512
    - IP NAT Service Configuration 513
    - IP NAT Service Example 513

---

Controlling Address Translation	514
Using ACLs	514
Using Route Maps: Dynamic Translations	515
Problems with ACLs and Address Translation	516
Route Map Configuration	517
Using Route Maps: Static Translations	520
Address Translation and Redundancy	521
Static NAT Redundancy with HSRP	522
HSRP Redundancy Process	522
HSRP Redundancy Configuration	524
HSRP Redundancy Example	525
Stateful Address Translation Failover	526
Stateful Failover Features and Restrictions	526
SNAT with HSRP	527
SNAT Without HSRP	531
SNAT Verification	534
Traffic Distribution with Server Load Balancing	535
SLB Process	536
Load-Balancing Algorithms	538
SLB Advantages and Limitations	540
SLB Configuration	540
Required SLB Commands	541
Optional SLB Commands	542
SLB Verification	544
SLB Example	545
Summary	546

## **Part VI Managing Access Through Routers 549**

### **Chapter 13 Lock-and-Key Access Lists 551**

Lock-and-Key Overview	551
Lock-and-Key and Normal ACLs	551
When to Use Lock-and-Key	552
Lock-and-Key Benefits	552
Lock-and-Key Process	553
Lock-and-Key Configuration	554
Configuration Steps	555
Step 1: Create Your Extended ACL	555
Step 2: Define Your Authentication Method	558
Step 3: Enable Lock-and-Key Authentication	559
Allowing Remote Administration Access	560
Telnet Solution	560

SSH Solution	561
Local Database Solution	562
Verification and Troubleshooting	562

Lock-and-Key Example 563

Summary 565

## **Chapter 14 Authentication Proxy 567**

Introduction to AP 567

AP Features 568

AP Process 569

AP Process Example 570

AP Authentication and JavaScript 572

AP Usage 573

When to Use AP 573

Where to Use AP 573

Limitations of AP 574

AP Configuration 575

Configuring AAA on Your Router 576

Configuring AAA on Your Server 576

AP Service 577

User Authorization Profiles 578

Preparing for HTTP or HTTPS 579

HTTP Configuration Tasks 579

Configuration Tasks for HTTPS 579

Configuring AP Policies 580

AP Policy Definitions 580

AP Policy Activation 581

Tuning AP 582

Protecting Against Access Attacks 583

Verifying and Troubleshooting AP 584

show Commands 584

clear Commands 586

debug Commands 587

AP Examples 587

Simple AP Example 587

Complex AP Example: CBAC and NAT 590

Summary 595

## **Chapter 15 Routing Protocol Protection 597**

Static and Black Hole Routing 597

Static Routes 597

---

Null Routes	598
Policy-Based Routing	601
Interior Gateway Protocol Security	604
Authentication	604
Supported Routing Protocols	605
Authentication Process	605
RIPv2	606
EIGRP	608
OSPF	608
IS-IS	609
Group 1 Steps: Authentication Keys	610
Group 2 Steps: IS-IS Authentication	610
Group 3 Steps: Using Authentication	610
IS-IS Authentication Example	611
Other Tools	612
Passive Interfaces	612
ACL Filters	613
HSRP	614
BGP Security	617
Authentication	617
Route Flap Dampening	618
BGP Routing Example	620
Reverse-Path Forwarding (Unicast Traffic)	625
RPF Process	625
ACL Enhancements	626
Statistics	627
RPF Usage	627
RPF Limitations	628
RPF Configuration	629
RPF Verification	630
Unicast RPF Example	631
Summary	631

## **Part VII Detecting and Preventing Attacks 633**

### **Chapter 16 Intrusion-Detection System 635**

IDS Introduction	635
IDS Implementations	635
Profiles	636
Signatures	636
Complications with IDS Systems	637

IDS Solutions	637
Network-Based Solutions	638
Host-Based Solutions	639
Host-Based Versus Network-Based	640
IDS Concerns	640
Installed Components	640
Detecting Intrusions	641
Responding to Intrusions	641
IDS Signatures	642
Signature Implementations	642
Signature Structures	642
Basic Classification	643
Cisco Signature Categories	643
Cisco Router IDS Solution	644
Signature Support	644
Router IDS Process	651
Memory and Performance Issues	652
IDS Configuration	652
Step 1: Initialization Configuration	652
Step 2: Logging and PostOffice Configuration	653
Step 3: Audit Rule Configuration and Activation	654
Global Policies	655
Specific Policies	655
Signature Policies	655
Protection Policies	656
Policy Activation	656
IDS Verification	657
IDS Example	658
Summary	659
<b>Chapter 17 DoS Protection</b>	<b>661</b>
Detecting DoS Attacks	661
Common Attacks	661
Symptoms of Attacks	662
Examining CPU Utilization to Detect DoS Attacks	663
Using ACLs to Detect DoS Attacks	665
ACL Counters	665
Specific ACL Entries	666
ACL Logging	668
Smurf Example	668

---

Damage Limitations	670
Finding the Attacker	670
Using NetFlow to Detect DoS Attacks	672
NetFlow Overview	672
NetFlow Configuration	673
Examining and Clearing NetFlow Statistics	673
NetFlow and DoS Attacks	675
CEF Switching	678
TCP Intercept	679
TCP SYN Flood Attacks	679
TCP Intercept Modes	679
Intercept Mode	680
Watch Mode	681
TCP Intercept Configuration and Verification	681
Enabling TCP Intercept	681
Defining the Mode	682
Changing the Timers	682
Changing the Thresholds	683
Changing the Drop Method	684
Verifying Your Configuration	684
TCP Intercept Example	686
CBAC and DoS Attacks	687
Timeouts and Thresholds	687
Setting Connection Timeouts	688
Setting Connection Thresholds	688
CBAC DoS Prevention Verification	690
CBAC Example Configuration	690
Rate Limiting	692
ICMP Rate Limiting	692
Using Other Solutions	692
Using the ICMP Rate-Limiting Feature	693
CAR	694
CAR Configuration	694
Verifying CAR	696
Rate Limiting for ICMP and Smurf Attacks	697
Rate Limiting for TCP SYN and Other TCP Floods	698
How to Choose a Rate Limit	698
Rate Limiting for W32.Blaster Worm	699
NBAR	700
Smurf Example	700
W32.Blaster Worm Example	702
Summary	703

<b>Chapter 18</b>	<b>Logging Events</b>	<b>705</b>
	Basic Logging	705
	Log Message Format	706
	Basic Logging Configuration	706
	Enabling Logging	706
	Configuring Synchronous Logging	706
	Logging Destinations	708
	Severity Levels	708
	Line Logging	709
	Internal Buffer Logging	710
	Syslog Server Logging	710
	SNMP Logging	713
	Other Logging Commands	713
	Date and Time Stamps	714
	Sequence Numbers	714
	Rate Limits	715
	Logging Verification	716
	show logging Command	716
	show logging history Command	717
	Logging and Error Counts	718
	Time and Date and the Cisco IOS	718
	Router Time Sources	719
	Hardware Clock	719
	Software Clock	719
	Manual Time and Date Configuration	720
	Time Zone	720
	Daylight Saving Time	720
	Software Clock Settings	721
	Hardware Clock Settings	722
	Network Time Protocol Overview	722
	Time Distribution	722
	Simple Network Time Protocol	723
	Router Client Configuration for NTP	723
	Poll-Based Configuration	724
	Broadcast-Based Configuration	725
	SNTP Configuration	725
	Router Server Configuration for NTP	725
	Distributing Timing Information	726
	Configuring an External Clock	726
	Setting Up the NTP Server	727
	NTP Security	727
	Access Groups	728
	Authentication	728

---

Other NTP Commands	729
NTP Verification	730
NTP Commands	730
SNTP Command	731
NTP Configuration Example	731
Embedded Syslog Manager	732
ESM Overview	733
ESM Filter Modules	733
Input Process	734
Filtering Process	736
Example Filter Modules	737
Introduction to ESM Setup and Configuration	738
Specifying Filter Modules	739
Using Filter Modules	739
Verifying Your ESM Configuration	740
Additional Logging Information	740
What to Look For	741
Additional Tools	741
Rotating Syslog Log Files	741
Examining Log File Contents	742
Summary	743

## **Part VIII Virtual Private Networks 745**

### **Chapter 19 IPsec Site-to-Site Connections 747**

IPsec Preparation	747
Basic Tasks	747
External ACL	749
IKE Phase 1: Management Connection	750
Enabling ISAKMP/IKE	750
Defining IKE Phase 1 Policies	751
Policy Commands	751
Policy Verification	753
IKE Phase 1 Peer Authentication	753
Identity Type	754
Authentication with Preshared Keys	754
Authentication with RSA Encrypted Nonces	755
RSA Manual Key Generation	755
Peer Key Configuration	756
Authentication with Certificates	757
Certificates and CAs	757

Simple Certificate Enrollment Protocol	758
Certificate Revocation List	759
Certificate Enrollment and Configuration Process	759
Removing Your Router's Certificate	765
Removing Your Router's RSA Keys	765

IKE Phase 2: Data Connection	766
Step 1: Building a Crypto ACL	766
Step 2: Creating a Transform Set	767
Transform Set Protection Parameters	767
Transform Set Connection Modes	768
Transform Set Verification	769
Step 3: Creating a Crypto Map	770
Crypto Map Rules	770
Crypto Map Types	771
Static Crypto Map Entries	771
Entry Commands	772
Step 4: Activating a Crypto Map	773
Step 5: Verifying a Crypto Map Configuration	774

IPSec Connection Troubleshooting	775
Examining SAs	775
Using debug Commands	778
Clearing Connections	780

L2L Example	780
-------------	-----

Summary	783
---------	-----

## **Chapter 20** IPSec Remote-Access Connections 785

Remote Access Overview	785
EasyVPN Introduction	786
EasyVPN IPSec Support	787
EasyVPN Features	787
IPSec Remote-Access Connection Process	789
Step 1: The EVC Initiates an IPSec Connection	789
Step 2: The EVC Sends the IKE Phase 1 Policies	790
Step 3: The EVS Accepts an IKE Phase 1 Policy	790
Step 4: The EVS Authenticates the User	790
Step 5: The EVS Performs IKE Mode Config	791
Step 6: The EVS Handles Routing with RRI	791
Step 7: The IPSec Devices Build the Data Connections	793
IPSec Remote-Access EVS Setup	793
Configuration Process	793
Task 1: Authentication Policies	793

Task 2: Group Policies	794
Task 3: IKE Phase 1 Policies	797
Task 4: Dynamic Crypto Maps	798
Overview of Dynamic Crypto Maps	798
Creating a Dynamic Crypto Map	799
Using a Dynamic Crypto Map	800
Verifying a Dynamic Crypto Map	800
Task 5: Static Crypto Map	801
Task 6: Remote-Access Verification	802

IPSec Remote Access Example 802

Summary 805

## **Part IX Case Study 807**

### **Chapter 21 Case Study 809**

Company Profile	809
Corporate Office	809
Perimeter Router	809
Internal Router	811
Branch Office	812
Remote-Access Users	812
Proposal	812
Case Study Configuration	813
Basic Configuration	813
Unnecessary Services and SSH	815
AAA	817
Access Control Lists	820
CBAC and Web Filtering	825
Address Translation	827
Routing	830
Intrusion-Detection System	832
Connection Attacks and CBAC	832
Rate Limiting	833
NTP and Syslog	835
Site-to-Site VPN	836
Remote-Access VPNs	839

Summary 842

**Index 845**