
CONTENTS

Introduction	xxi
Part I Introduction to Network Security	I
Chapter I Understanding Network Security Threats	3
Identify the Need for Network Security	4
Identify the Causes of Network Security Problems	5
Technology Weakness	6
Policy Weakness	7
Configuration Weakness	8
The Four Primary Types of Network Threats	8
Unstructured Threats	8
Structured Threats	9
Internal Threats	10
External Threats	10
The Four Primary Types of Network Attack	11
Reconnaissance Attacks	11
Access Attacks	14
Denial of Service (DoS) Attacks	16
Data Manipulation Attacks	20
Cisco AVVID and SAFE Strategies	22
AVVID	22
SAFE	23
Cisco Security Wheel	23
Network Security Policy	25
Why Create a Network Security Policy	25
The Balancing Act	26
A Security Policy Is to Be Shared	28
Who Should Help Create the Security Policy?	29
Assets and Threats	30
Evaluating a Network Security Policy	32
Example of a Network Security Policy	35
Securing the Network	35
Wireless Communication Policy	36
Monitoring Network Security	37
Improving Network Security	38
Chapter Review	39
Questions	40
Answers	44

Chapter 2	Securing the Network	47
	Secure Network Design Example	48
	Inside Network	49
	Outside Network	49
	Demilitarized Zone (DMZ)	49
	Securing Network Devices	50
	Physically Secure the Devices	50
	Securing Administrative Access	50
	Using Access Control Lists to Secure the Network	57
	Standard ACLs	57
	Extended Access Lists	64
	Named Access Lists	66
	Time-Based Access Lists	66
	Chapter Review	71
	Questions	71
	Answers	74
Part II	Securing the Network Perimeter	75
Chapter 3	Cisco AAA Security Technology	77
	The Cisco AAA Model	78
	NAS Servers	78
	Why Authenticate?	79
	AAA Benefits	82
	TACACS+, RADIUS, and Kerberos Support	83
	AAA System Components	88
	AAA as Facilitator	88
	Authentication	92
	Authorization	96
	Accounting	99
	Testing AAA Configuration	103
	The show Commands	103
	The debug Commands	103
	Chapter Review	104
	Questions	105
	Answers	107
Chapter 4	Cisco Secure ACS and TACACS+/RADIUS Technologies	109
	Describe Cisco Secure ACS	110
	CiscoSecure ACS for Windows and UNIX	110
	Features and Architecture of Cisco Secure ACS for Windows	111
	Features and Benefits	111
	Cisco Secure ACS Benefits	112
	Cisco Secure ACS for Windows Internal Architecture	113
	System Performance	117
	Features of CiscoSecure ACS for UNIX	118
	Features and Benefits	118
	Preparing to Install UNIX ACS	119

Installing Cisco Secure ACS 3.0 for Windows	119
Hardware Requirements	120
Operating System Requirements	120
Third-Party Software Requirements	120
NAS Minimum IOS Requirements	121
Network Requirements	121
Back Up Server Data	121
Gathering Information Required During Installation	122
Administering and Troubleshooting Cisco Secure ACS for Windows	122
Navigation Bar	123
Configuration Area	125
Display Area	125
Accessing the HTML Interface	125
Suggested Configuration Sequence	128
TACACS+ Overview	132
Configuring Cisco Secure ACS and TACACS+	133
Configure NAS to TACACS+ Server Communication	134
Verifying TACACS+	136
The show Commands	136
The debug Commands	136
Configure NAS to RADIUS Server Communication	137
Chapter Review	138
Questions	139
Answers	141
Chapter 5 Securing Cisco Perimeter Routers	143
Perimeter Router Terms and Concepts	143
Simple Secure Network Design	144
Eavesdropping	147
Router Solutions	147
Hub and Switch Issues	149
Limit Unneeded TCP/IP and Other Services	150
TCP and UDP “Small Services”	150
Finger	150
NTP	150
CDP	150
Denial of Service Attacks	150
Controlling Directed Broadcasts	151
Flood Management	151
Antispoofing with RPF Checks	152
Unauthorized Access	152
Address Filtering	152
Dynamic (Lock-and-Key) Access Lists	152
Reflexive Access Lists	157
Lack of Legal IP Addresses	161
NAT Technology and Terminology	162
Static NAT	163
Dynamic NAT	165
Dynamic NAT with Overloading (PAT)	167
Rerouting Attacks	169

Event Logging on Perimeter Routers	170
Access List Violation Logs	171
Chapter Review	171
Questions	172
Answers	174
Chapter 6 IOS Firewall Feature Set—CBAC	175
Introduction to Cisco IOS Firewall	175
Router-Based Firewall Functionality	176
Integration with Cisco IOS Software	176
Feature Summary	178
Context-Based Access Control (CBAC)	179
Quick Access List Review	179
CBAC Advantages	179
CBAC Limitations	181
CBAC Process	181
Configuring CBAC	182
IOS Firewall Management	198
Command Line Interface	198
ConfigMaker	199
Chapter Review	200
Questions	201
Answers	203
Chapter 7 IOS Firewall—Intrusion Detection System	205
Intrusion Detection System (IDS)	205
IOS Firewall Intrusion Detection System	206
Devices Supporting the IOS Firewall IDS Features	206
Cisco IDS Attack Signatures	208
Cisco Secure IDS Director Support	209
Performance Implications	210
IOS IDS vs. Cisco Secure IDS	210
Cisco IOS Firewall IDS Configuration Task List	211
Initializing the IOS Firewall IDS	212
The ip audit smtp spam Command	212
The ip audit po max-events Command	212
Initializing the Post Office	212
The ip audit notify Command	213
The ip audit po local Command	214
The ip audit po remote Command	215
Creating and Applying Audit Rules	216
Creating an Audit Rule	217
Apply the Audit Rule to the Interface(s)	220
Verifying the IDS Configuration	222
The show ip audit statistics Command	222
The show ip audit configuration Command	223
The show ip audit interface Command	223
The show ip audit all Command	224
Chapter Review	224
Questions	225
Answers	227

Chapter 8	IOS Firewall—Authentication Proxy	229
	Cisco IOS Firewall Authentication Proxy	229
	How the Authentication Proxy Works	230
	Applying the Authentication Proxy	232
	Comparison with the Lock-and-Key Feature	233
	Compatibility with Other Features	233
	Security Vulnerability Issues	236
	Before Configuring Authentication Proxy	236
	Authentication Proxy Configuration Task List	238
	AAA Server Configuration	238
	AAA Router Configuration	244
	Enable AAA	244
	Define the Security Server	244
	Define Login Authentication Methods List	249
	Enable Authorization Proxy (auth-proxy) for AAA	250
	Activate Authentication Proxy Accounting	251
	ACL Entry for Return Traffic from the AAA Server	252
	Configuring the HTTP Server	253
	Authentication Proxy Configuration on the Router	254
	The ip auth-proxy auth-cache-time Command	254
	The ip auth-proxy auth-proxy-banner Command	255
	The ip auth-proxy name Command	255
	The auth-proxy Interface Configuration	257
	Verify Authentication Proxy Configuration	257
	The auth-proxy Cache	258
	The debug Commands	259
	CBAC Configuration	259
	Chapter Review	260
	Questions	260
	Answers	263
Part III	Virtual Private Networks (VPNs)	265
Chapter 9	Cisco IOS IPSec Introduction	267
	Virtual Private Networks	268
	Remote-Access	269
	Site-to-Site	270
	Layer 2 VPNs	271
	Layer 3 VPNs	272
	Other VPN Implementations	273
	Why Use VPNs?	274
	VPN Analogy	274
	Tunneling Protocols	275
	Layer Two Forwarding (L2F) Protocol	276
	Layer 2 Tunneling Protocol (L2TP)	276
	Generic Routing Encapsulation (GRE)	276
	How IPSec Works	276
	Cisco IOS IPSec Technologies	277
	IPSec Security Overview	278

Transport and Tunnel Mode	281
IPSec Transforms and Transform Sets	286
Cisco IOS Cryptosystem Components	288
How Encryption Works	288
Cryptography Types	290
Encryption Alternatives	290
Hashing	292
Diffie-Hellman Key Agreement (DH)	293
Security Association (SA)	294
IKE SAs versus IPSec SAs	295
Five Steps of IPSec Revisited	296
Step 1—Determine Interesting Traffic	296
Step 2—IKE Phase One	297
Step 3—IKE Phase Two	300
Step 4—IPSec Data Transfer	301
Step 5—Session Termination	301
IPSec Support in Cisco Systems Products	301
Chapter Review	302
Questions	303
Answers	305
Chapter 10 Cisco IOS IPSec for Preshared Keys	307
Configure IPSec Encryption Tasks	307
Task 1 Prepare for IKE and IPSec	309
Task 2 Configure IKE	317
Task 3 Configure IPSec	321
Task 4 Test and Verify IPSec	329
Configuring IPSec Manually	333
Configuring IPSec Manually Is Not Recommended	334
Chapter Review	335
Questions	336
Answers	339
Chapter 11 Cisco IOS IPSec Certificate Authority Support	341
CA Support Overview	341
Digital Certificates	342
Certificate Distribution	343
IPSec with CAs	344
How CA Certs Are Used by IPSec Peers	344
Cisco IOS CA Standards	345
Simple Certificate Enrollment Protocol (SCEP)	345
CA Servers Interoperable with Cisco Routers	346
Enroll a Device with a CA	348
Configure CA Support Tasks	348
Task 1—Prepare for IKE and IPSec	349
Task 2—Configure CA Support	351
Task 3—Configure IKE	369
Task 4—Configure IPSec	371
Task 5—Test and Verify IPSec	372

RSA Encrypted Nonces Overview	372
Task 2—Configure RSA Keys	373
Chapter Review	374
Questions	377
Answers	379
Chapter 12 Cisco IOS Remote Access Using Cisco Easy VPN	381
Introduction to Cisco Easy VPN	381
Cisco Easy VPN Server	382
Client Connection Process	382
Cisco Easy VPN Remote	383
Split Tunneling	384
Cisco VPN 3.6 Client	385
How the VPN Client Works	385
Connection Technologies	385
Easy VPN Server Configuration Tasks	386
Preconfiguring the Cisco VPN 3.6 Client	386
Creating a New Connection Entry	387
Trying Out the New Connection	389
Customizing the Connection	390
Management Center for VPN Routers	392
Features and Benefits	393
Router MC Server Requirements	394
Router MC Client Requirements	394
Router MC User Permissions	395
Easy VPN Remote Phase Two	396
Supported VPN Servers	396
Phase Two Features	396
Cisco VPN Firewall Feature for VPN Client	402
Overview of Software Client Firewall Feature	402
Defining a Client Firewall Policy	403
The Are You There Feature	403
The Central Policy Protection Feature	404
Client/Server Feature	406
Client Firewall Statistics	407
Chapter Review	408
Questions	409
Answers	411
Chapter 13 Cisco VPN Hardware Overview	413
Cisco Products Enable a Secure VPN	413
What's New?	414
Cisco VPN 3002 Client Devices	414
Cisco VPN 3002 Client Models	415
Client and Network Extension Modes	416
Standards Supported	417
Cisco VPN 3002 Hardware Client Features	417
Cisco VPN 3000 Concentrator Devices	419
Cisco VPN 3000 Concentrator Models	419

Standards Supported	423
Cisco VPN 3000 Concentrator Features	424
VPN 3000 Concentrator Client Support	426
Chapter Review	429
Questions	430
Answers	432
Chapter 14 Cisco VPN 3000 Remote Access Networks	435
VPN Concentrator User Interfaces and Startup	436
Quick Configuration	437
Command-Line Interface (CLI) Basics	439
Concentrator Manager (Web Interface)	443
VPN Concentrators in IPSec VPN Implementations	450
Remote Access Networks	451
LAN-to-LAN Networks	451
Remote Access VPNs with Preshared Keys	452
Preshared Keys	453
Initial Configuration	454
Setting the Public Interface	455
Defining the Default Gateway (Optional)	456
Adding the Static Routes	458
General System Information	459
Define Inside Address Assignment Method	459
Define Inside Address Pool for Remote Users	461
Configuring Groups and Users	461
Other Configuration Options	473
Digital Certificates	477
Certificate Types	477
VPN Concentrator and Certificates	477
Enrolling and Installing Certificates	478
Using SCEP to Manage Certificates	479
Using the Certificates	484
Configure Cisco VPN Client Support	486
VPN Client Autoinitiation Feature	487
The vpnclient.ini File	487
Preparation	488
Configuration	488
VPN 3000 Configuration	489
Administer and Monitor Remote Access Networks	489
Administration	489
Monitoring	494
Chapter Review	495
Questions	496
Answers	499
Chapter 15 Configuring Cisco VPN 3002 Remote Clients	501
The VPN 3002 in the Network	502
VPN Modes	503
IPSec VPNs	504
Configuring the 3002 Device	506

Command-Line Interface (CLI)	506
The Hardware Client Manager (Web Interface)	511
Common Configuration Tasks	515
Upgrading the Software	515
Quick Configuration	517
System Status	519
PPPoE Support	519
Basic Configuration for the VPN 3002	521
Set the System Time, Date, and Time Zone	522
Optional—Upload an Existing Configuration File	523
Configure the Private Interface	523
Configure the Public Interface	526
Configure the IPSec	527
Choose Client (PAT) Mode or Network Extension Mode	528
Configure DNS	529
Configure Static Routes	529
Change the Admin Password	530
Modifying Options	531
Other VPN 3002 Software Features	532
Interactive Hardware Client Authentication	532
Individual User Authentication	533
LEAP Bypass	535
IPSec Backup Servers	536
IPSec Server Load Balancing	537
H.323 Support in PAT Mode	540
Simple Certificate Enrollment Protocol (SCEP)	541
XML Management	542
Reverse Route Injection (RRI)	542
AES Support and Diffie-Hellman Group 5	543
Push Banner to VPN 3002	544
Delete with Reason	544
Auto-Update Feature	546
VPN 3002 Hardware Clients	546
Cisco VPN Software Clients	546
Configuring Auto-Update	546
Chapter Review	547
Questions	549
Answers	551
Chapter 16 Cisco VPN 3000 LAN-to-LAN Networks	553
The VPN Concentrators in LAN-to-LAN VPNs	553
Chapter Scenario	555
LAN-to-LAN Networks with Preshared Keys	555
Configure Network Lists	556
Define the IKE Proposals (Optional)	560
Create the Tunnel	561
LAN-to-LAN Networks with Digital Certificates	566
NAT Issues	567
NAT Transparency	568
IPSec over TCP	569
IPSec over NAT-T	570

IPSec over UDP	571
LAN-to-LAN VPN with Overlapping Network Addresses	572
LAN-to-LAN Routing	575
Default Gateways	576
Reverse Route Injection	577
Virtual Router Redundancy Protocol	578
Chapter Review	581
Questions	582
Answers	584
 Part IV PIX Firewalls	585
 Chapter 17 CiscoSecure PIX Firewalls	587
Firewall and Firewall Security Systems	587
Packet Filter	588
Proxy Filter	589
Stateful Packet Filter	589
CiscoSecure PIX Firewall Technology	589
PIX Adaptive Security Algorithm	591
The PIX Firewall Family	592
Tested and Certified	595
VPN Support	595
PIX Management Options	596
Cisco Mobile Office Support	596
Cisco Catalyst 6500 Implementation	596
Basic PIX Firewall Configuration	597
PIC Command-Line Interface	597
The nameif Command	599
The interface Command	599
The ip address Command	601
The nat Command	601
The global Command	602
The route Command	604
Chapter Review	604
Questions	605
Answers	607
 Chapter 18 Getting Started with the Cisco PIX Firewall	609
Basic PIX Firewall Configuration	609
Verifying Configuration and Traffic	612
ICMP Traffic to the Firewall	612
The show icmp Command	614
The debug icmp trace Command	614
Time Setting and NTP Support	614
How NTP Works	614
NTP and PIX Firewalls	615
Syslog Configuration	617
The logging Commands	618
FTP and URL Logging	620
Verifying and Monitoring Logging	621

DHCP Server Configuration	625
Configuring the DHCP Server Feature	626
DHCP Client	631
Using NAT/PAT with DHCP Client	632
Firewalls as a DHCP Client and Server	632
Chapter Review	633
Questions	634
Answers	637
Chapter 19 Access Through the PIX Firewall	639
Adaptive Security Algorithm	639
Security Levels	640
Stateful System	642
Translations	643
Connections	643
Translations and Connections	644
Transport Protocols	646
Static Translations	649
Network Address Translation	654
Port Address Translations (PAT)	658
Using NAT and PAT Together	659
Names and Name Commands	659
Configuring DNS Support	660
Access Control Lists (ACLs)	661
Using Access Lists	661
Access-Group Statement	662
Basic ACL Statements	662
ICMP ACL Statements	663
TurboACL	664
Downloadable ACLs	666
Content Filtering	668
ActiveX Blocking	669
Java Blocking	669
Websense Filtering	670
Object Grouping	673
Overview of Object Grouping	673
Getting Started with Group Objects	674
Configuring Object Groups with ACLs	675
Nested Object Groups	676
Conduit Statements	676
Configuring Conduits	677
PIX Routing Configuration	678
The Route Command	678
Routing Options	680
Multicast Traffic	682
Chapter Review	682
Questions	683
Answers	685
Chapter 20 Advanced PIX Firewall Features	687
Remote Access	687
Telnet Access	688

HTTP Access	689
Secure Shell (SSH) Access	690
AAA Support for Telnet, HTTP, and SSH Sessions	691
AAA on the PIX Firewall	691
Defining the AAA Server	691
Local User Database	693
Configuring AAA Features	695
Access Lists with AAA	699
Command-Level Authorization	700
Firewall Privilege Levels	701
Configuring Cisco Secure ACS for Windows	702
Advanced Protocol Handling	702
Application Inspection	702
The fixup protocol Command	703
Supported Applications and Protocols	704
Fixup Protocol Examples	706
Other Supported Protocols and Applications	709
Attack Guards	710
DNS Control	711
Flood Defender	711
FragGuard and Virtual Reassembly	712
TCP Intercept	714
Unicast Reverse Path Forwarding	714
ActiveX Blocking, Java Filtering, and URL Filtering	715
Intrusion Detection	715
Define Default Audit Actions	716
Disabling Individual Signatures	716
Create Named Audit Rules	717
Apply the Audit Rule to the Interface(s)	717
PIX Firewall IDS Syslog Messages	718
Shunning	718
Managing SNMP Services	719
PIX Firewall SNMP Support	719
SNMP Contact and Location	720
SNMP Management Station	721
SNMP Community Key	721
Enabling SNMP Traps	722
Verify SNMP Configuration	722
Logging to the SNMP Management Station	722
Chapter Review	723
Questions	724
Answers	726
Chapter 21 Firewalls and VPN Features	729
Pix Firewall Enables a Secure VPN	729
IPSec VPN Establishment	731
Five Steps of IPSec	731
IPSec Configuration Tasks	732
Task 1: Prepare to Configure VPN Support	732
Task 2: Configure IKE Parameters	733

Task 3: Configure IPSec Parameters	740
Task 4: Test and Verify VPN Configuration	747
Cisco VPN Client	748
Client Mode	748
Network Extension Mode	748
Establishing Preliminary Connectivity	749
Easy VPN Remote Configuration	749
Scale PIX Firewall VPNs	750
Network Management Options	750
PPPoE and the PIX Firewall	752
Chapter Review	754
Configuring IPSec	754
Configuring IPSec for RSA Encrypted Nonces	757
Configuring CA Support Tasks	757
Questions	760
Answers	763
Chapter 22 Managing and Maintaining the PIX Firewall	765
PDM Overview	765
Versions and Device Support	767
PDM Operating Requirements	767
PIX Firewall Requirements	767
Workstation Requirements	768
Cisco Secure Policy Manager Considerations	769
Web Browser Considerations	769
Prepare for PDM	771
Installing PDM on a PIX Firewall	771
Minimum PIX Configuration	772
Starting PDM	772
Using the PDM Startup Wizard	774
Using PDM to Configure the PIX Firewall	775
Using PDM to Create a Site-to-Site VPN	776
Using PDM to Create a Remote Access VPN	780
CiscoWorks Management Center for PIX Firewalls (PIX MC)	783
System Requirements	783
PIX Failover Feature	784
Understanding Failover	785
Failover Configuration with Failover Cable	789
LAN-Based Failover Configuration	792
Verifying Failover Configuration	793
Password Recovery	794
Before Getting Started	794
PIX Devices with a Floppy Drive	795
PIX Devices Without a Floppy Drive	796
Upgrading the PIX OS	797
Older Upgrade Methods	798
Chapter Review	800
Questions	801
Answers	803

Part V	Intrusion Detection Systems (IDS)	805
Chapter 23	Intrusion Detection System Overview	807
	Security Threats	807
	Internal Threats	808
	External Threats	808
	Unstructured Threats	809
	Structured Threats	809
	The Attack Types and Phases	809
	Attack Types	810
	Attack Phases	811
	Intrusion Detection Systems Overview	816
	Host- and Network-Based IDSs	817
	IDS Triggers	821
	Summary	827
	Questions	829
	Answers	832
Chapter 24	Cisco Secure Intrusion Detection System	835
	CIDS Operations and Functionality	836
	Monitoring	836
	Analyzing	841
	Communications	841
	Centralized Alarm Display and Management	845
	Sensor Response	848
	CIDS Architecture	850
	CIDS Software Architecture	851
	CIDS Commands	860
	CIDS Directory Structure	861
	CIDS Log Files	863
	Chapter Review	866
	Questions	867
	Answers	871
Chapter 25	Sensor Installation and Configuration	873
	Sensor Deployment Considerations	873
	Network Entry Points	874
	Network Size and Complexity	877
	The Amount and Type of Traffic	877
	Sensor Installation	878
	Connecting to Your Network Sensor Appliance	878
	Sensor Bootstrap	880
	IDS Device Manager	885
	Connecting to the IDS Device Manager	886
	IDS Device Manager GUI Interface	887
	Device Area Configuration	890
	Configuration Area	894
	Monitoring Area	911
	Administration Area	912
	Chapter Review	917

Questions	918
Answers	919
Chapter 26 Signature and Alarm Management	921
CIDS Signatures	922
Signature Series	922
Signature Implementations	924
Signature Structure	925
Signature Classes	926
Signature Types	927
Signature Severity	929
Event Viewer	930
Managing Alarms	931
Event Viewer Customization	936
Preference Settings	938
Chapter Review	940
Review Questions	941
Answers	943
 Part VI Cisco SAFE Implementation	 945
Chapter 27 Cisco SAFE Implementation	947
Preparation Documents	947
Exam Topics	948
Security Fundamentals	948
Architectural Overview	948
Cisco Security Portfolio	948
SAFE Small Network Design	949
SAFE Medium Network Design	949
SAFE Remote-User Network Implementation	949
Skills Required for the Exam	950
Chapter Review	950
Questions	951
Answers	954
 Appendix A Access Control Lists	 955
Access List Basics	955
Two-Step Process	956
Numbered ACL Common Characteristics	957
The Numbers Matter	957
Standard Access Lists	958
Building a Standard ACL	958
Verifying ACLs	963
Show Run Command	963
Show Access-Lists Command	964
Show IP Interfaces Command	964
Extended Access Lists	965
Creating an Extended Access List	965
Named Access Lists	971

Appendix B About the CD	975
System Requirements	975
LearnKey Online Training	975
Installing and Running MasterExam	976
MasterExam	976
Electronic Book	976
Lab Exercises	976
Help	976
Removing Installation(s)	977
Technical Support	977
LearnKey Technical Support	977
 Index	 979