

# Table of Contents

Introduction xvii

## **Chapter 1** All About the Cisco Certified Security Professional 3

How This Book Can Help You Pass the CCSP Cisco Secure VPN Exam 5

Overview of CCSP Certification and Required Exams 5

The Cisco Secure VPN Exam 6

Topics on the Cisco Secure VPN Exam 8

Recommended Training Path for the CCSP Certification 10

Using This Book to Pass the Exam 11

Final Exam Preparation Tips 11

## **Chapter 2** Overview of VPN and IPSec Technologies 15

How to Best Use This Chapter 15

“Do I Know This Already?” Quiz 16

Cisco VPN Product Line 21

Enabling VPN Applications Through Cisco Products 21

Typical VPN Applications 21

Using Cisco VPN Products 26

An Overview of IPSec Protocols 36

The IPSec Protocols 39

Security Associations 46

Existing Protocols Used in the IPSec Process 47

Authenticating IPSec Peers and Forming Security Associations 54

Combining Protocols into Transform Sets 54

Establishing VPNs with IPSec 57

Step 1: Interesting Traffic Triggers IPSec Process 59

Step 2: Authenticate Peers and Establish IKE SAs 61

Step 3: Establish IPSec SAs 61

Step 4: Allow Secured Communications 61

Step 5: Terminate VPN 62

Table of Protocols Used with IPSec 63

IPSec Preconfiguration Processes 65

Creating VPNs with IPSec 65

**Chapter 3 Cisco VPN 3000 Concentrator Series Hardware Overview 79**

How to Best Use This Chapter	79
“Do I Know This Already?” Quiz	80
Major Advantages of Cisco VPN 3000 Series Concentrators	85
Ease of Deployment and Use	87
Performance and Scalability	87
Security	90
Fault Tolerance	94
Management Interface	94
Ease of Upgrades	99
Cisco Secure VPN Concentrators: Comparison and Features	100
Cisco VPN 3005 Concentrator	101
Cisco VPN 3015 Concentrator	102
Cisco VPN 3030 Concentrator	103
Cisco VPN 3060 Concentrator	104
Cisco VPN 3080 Concentrator	104
Cisco VPN 3000 Concentrator Series LED Indicators	105
Cisco Secure VPN Client Features	108
Cisco VPN 3002 Hardware Client	108
Cisco VPN Client	109
Table of Cisco VPN 3000 Concentrators	111
Table of Cisco VPN 3000 Concentrator Capabilities	112

**Chapter 4 Configuring Cisco VPN 3000 for Remote Access Using Preshared Keys 125**

How to Best Use This Chapter	125
“Do I Know This Already?” Quiz	126
Using VPNs for Remote Access with Preshared Keys	132
Unique Preshared Keys	132
Group Preshared Keys	133
Wildcard Preshared Keys	133
VPN Concentrator Configuration	134
Cisco VPN 3000 Concentrator Configuration Requirements	135
Cisco VPN 3000 Concentrator Initial Configuration	136
Configuring IPSec with Preshared Keys Through the VPN 3000 Concentrator Series Manager	152
Advanced Configuration of the VPN Concentrator	169

Installing and Configuring the VPN Client	174
Overview of the VPN Client	174
VPN Client Features	175
VPN Client Installation	177
VPN Client Configuration	181
Types of Preshared Keys	186
VPN 3000 Concentrator CLI Quick Configuration Steps	186
VPN 3000 Concentrator Browser-Based Manager Quick Configuration Steps	187
VPN Client Installation Steps	187
VPN Client Configuration Steps	188
VPN Client Program Options	188
Limits for Number of Groups and Users	189
Complete Configuration Table of Contents	189
Complete Administration Table of Contents	192
Complete Monitoring Table of Contents	193
Scenario 4-1	207
Scenario 4-2	208
Scenario 4-1 Answers	210
Scenario 4-2 Answers	211

## **Chapter 5** Configuring Cisco VPN 3000 for Remote Access Using Digital Certificates 215

How to Best Use This Chapter	216
“Do I Know This Already?” Quiz	217
Digital Certificates and Certificate Authorities	221
The CA Architecture	221
Simple Certificate Enrollment Process Authentication Methods	228
CA Vendors and Products that Support Cisco VPN Products	231
Digital Certificate Support Through the VPN 3000 Concentrator Series Manager	232
Certificate Generation and Enrollment	232
Certificate Validation	237
Certificate Revocation Lists	237
IKE Configuration	239

Configuring the VPN Client for CA Support	241
PKCS #10 Certificate Request Fields	245
X.509 Identity Certificate Fields	245
Types of Digital Certificates	246
Types of CA Organization	246
Certificate Validation and Authentication Process	246
Internet-Based Certificate Authorities	247
Certificate Management Applications	247
Scenario 5-1	255
Scenario 5-2	255
Scenario 5-1 Answers	256
Scenario 5-2 Answers	257
<b>Chapter 6</b> Configuring the Cisco VPN Client Firewall Feature	259
How to Best Use This Chapter	259
“Do I Know This Already?” Quiz	260
Cisco VPN Client Firewall Feature Overview	265
Firewall Configuration Overview	267
The Stateful Firewall (Always On) Feature	267
The Are You There Feature	269
Configuring Firewall Filter Rules	269
Name, Direction, and Action	273
Protocol and TCP Connection	273
Source Address and Destination Address	274
TCP/UDP Source and Destination Ports	274
ICMP Packet Type	276
Configuring the Stateful Firewall	276
Configuring the VPN Concentrator for Firewall Usage	277
Firewall Setting	278
Firewall	279
Custom Firewall	279
Firewall Policy	280

Monitoring VPN Client Firewall Statistics	281
Enabling Automatic Client Update Through the Cisco VPN 3000 Concentrator Series Manager	283
Cisco VPN Client Firewall Feature Overview	285
Stateful Firewall (Always On) Feature	287
Cisco Integrated Client	288
Centralized Protection Policy	288
Are You There Feature	288
Configuring Firewall Filter Rules	288
Action	289
Configuring the Stateful Firewall	290
Configuring the VPN Concentrator for Firewall Usage	290
Firewall	291
Firewall Policy	291
Monitoring VPN Client Firewall Statistics	291
Scenario 6-1	299
Scenario 6-1 Answers	299

## **Chapter 7** Monitoring and Administering the VPN 3000 Series Concentrator 303

How Best to Use This Chapter	303
“Do I Know This Already?” Quiz	304
Administering the Cisco VPN 3000 Series Concentrator	307
Administer Sessions	310
Software Update	310
System Reboot	313
Ping	315
Monitoring Refresh	315
Access Rights	316
File Management	322
Certificate Manager	323
Monitoring the Cisco VPN 3000 Series Concentrator	324
Routing Table	326
Event Log Screen	326
System Status	327

Sessions	328
Statistics	330
Administering the Cisco VPN 3000 Series Concentrator	338
Administer Sessions	340
Software Update	341
Concentrator	342
Clients	342
System Reboot	343
Ping	344
Monitoring Refresh	344
Access Rights	345
Administrators	345
Access Control List	346
Access Settings	347
AAA Servers	347
Authentication	347
File Management	347
Certificate Manager	347
Monitoring the Cisco VPN 3000 Series Concentrator	348
System Status	349
Sessions	349
Top Ten Lists	350
Statistics	351
MIB II Statistics	352
<b>Chapter 8</b> Configuring Cisco 3002 Hardware Client for Remote Access	359
How to Best Use This Chapter	360
“Do I Know This Already?” Quiz	361
Configure Preshared Keys	366
Verify IKE and IPSec Configuration	368
Setting debug Levels	369
Configuring VPN 3002 Hardware Client and LAN Extension Modes	371
Split Tunneling	374

Unit and User Authentication for the VPN 3002 Hardware Client	375
Configuring the Head-End VPN Concentrator	376
Configuring Unit and User Authentication	380
Interactive Hardware Client and Individual User Authentication	381
Configure Preshared Keys	386
Troubleshooting IPSec	386
Client and LAN Extension Modes	387
Split Tunnel	387
Configuring Individual User Authentication on the VPN 3000 Concentrator	388
Scenario 8-1	395
Scenario 8-2	396
Scenario 8-1 Answers	397
Scenario 8-2 Answers	397

## **Chapter 9** Configuring Scalability Features of the VPN 3002 Hardware Client 399

How to Best Use This Chapter	399
“Do I Know This Already?” Quiz	400
VPN 3002 Hardware Client Reverse Route Injection	407
Setting Up the VPN Concentrator Using RIPv2	407
Setting Up the VPN Concentrator Using OSPF	408
Configuring VPN 3002 Hardware Client Reverse Route Injection	409
VPN 3002 Hardware Client Backup Servers	412
VPN 3002 Hardware Client Load Balancing	414
Overview of Port Address Translation	416
IPSec on the VPN 3002 Hardware Client	418
IPSec Over TCP/IP	418
UDP NAT Transparent IPSec (IPSec Over UDP)	419
Troubleshooting a VPN 3002 Hardware Client IPSec Connection	420
Configuring Auto-Update for the VPN 3002 Hardware Client	423
Monitoring Auto-Update Events	426
Table of RRI Configurations	429
Backup Servers	429
Load Balancing	430

Comparing NAT and PAT 430

IPSec Over TCP/IP 430

IPSec Over UDP 431

Troubleshooting IPSec 431

Auto-Update 431

Scenario 9-1 440

Scenario 9-1 Answers 441

## **Chapter 10** Cisco VPN 3000 LAN-to-LAN with Preshared Keys 443

How to Best Use This Chapter 444

“Do I Know This Already?” Quiz 445

Overview of LAN-to-LAN VPN 449

LAN-to-LAN Configuration 449

Configuring Network Lists 449

Creating a Tunnel with the LAN-to-LAN Wizard 451

SCEP Overview 454

Certificate Management 454

Root Certificate Installation via SCEP 455

Maximum Certificates 464

Enrollment Variables 464

## **Chapter 11** Scenarios 473

Example Corporation 473

Site Descriptions 474

Detroit 474

Portland 474

Seattle 474

Memphis 474

Richmond 475

Terry and Carol 475

Scenario 11-1—The Basics 475

IKE Policy 475

IPSec Policy 476

Scenario 11-2—Portland 476



Scenario 11-3—Seattle	476
Scenario 11-4—Memphis	476
Scenario 11-5—Richmond	477
Scenario 11-6—Terry and Carol	477
Scenario 11-1 Answers	478
IKE Policy	478
IPSec Policy	479
Scenario 11-2 Answers	479
Detroit VPN 3030 Concentrator and Router (Generic for All)	479
Detroit VPN 3030 Concentrator for Portland	480
Portland VPN 3002 Hardware Client	481
Scenario 11-3 Answers	482
Detroit VPN 3030 Concentrator for Seattle	482
Seattle VPN 3002 Hardware Client	482
Scenario 11-4 Answers	483
Detroit VPN 3030 Concentrator for Memphis	483
Memphis VPN 3005 Concentrator and Router	483
Scenario 11-5 Answers	484
Detroit VPN 3030 Concentrator for Richmond	484
Richmond VPN 3005 Concentrator and Router	484
Scenario 11-6 Answers	484
Detroit VPN 3030 Concentrator for Terry and Similar Users	485
Terry VPN Client and Browser	485
Detroit VPN 3030 Concentrator for Carol and Similar Users	485
Carol VPN Client and Browser	486

<b>Appendix A</b>	Answers to the “Do I Know This Already?” Quizzes and Q&A Sections	489
-------------------	---	-----

<b>Index</b>	551
--------------	-----