

Contents

Foreword xxiii

Introduction xxiv

Part I An Overview of Network Security 2

Chapter 1 Network Security Essentials 5

“Do I Know This Already?” Quiz 5

Foundation Topics 9

Definition of Network Security 9

Balancing Business Need with Security Requirement 9

Security Policies 9

Security Policy Goals 12

Security Guidelines 13

Management Must Support the Policy 13

The Policy Must Be Consistent 13

The Policy Must Be Technically Feasible 14

The Policy Should Not Be Written as a Technical Document 14

The Policy Must Be Implemented Globally Throughout the Organization 14

The Policy Must Clearly Define Roles and Responsibilities 15

The Policy Must Be Flexible Enough to Respond to Changing Technologies and Organizational Goals 15

The Policy Must Be Understandable 15

The Policy Must Be Widely Distributed 16

The Policy Must Specify Sanctions for Violations 16

The Policy Must Include an Incident Response Plan for Security Breaches 16

Security Is an Ongoing Process 17

Network Security as a Process 17

Network Security as a Legal Issue 18

Foundation Summary 19

Security Policies 19

Security Policy Goals 19

Security Guidelines 20

Network Security as a Process 20

Q&A 21

Chapter 2 Attack Threats Defined and Detailed 23

“Do I Know This Already?” Quiz 23

Foundation Topics 27

Vulnerabilities 27

Self-Imposed Vulnerabilities 27

Lack of Effective Policy 28

Configuration Weakness 29

Technology Weakness 30

	Threats	31
	Intruder Motivation	31
	<i>Lack of Understanding of Computers or Networks</i>	31
	<i>Intruding for Curiosity</i>	32
	<i>Intruding for Fun and Pride</i>	32
	<i>Intruding for Revenge</i>	32
	<i>Intruding for Profit</i>	32
	<i>Intruding for Political Purposes</i>	33
	Types of Attacks	33
	<i>Reconnaissance Attacks</i>	34
	<i>Access Attacks</i>	34
	<i>DoS Attacks</i>	36
	Foundation Summary	37
	Vulnerabilities	37
	<i>Self-Imposed Vulnerabilities</i>	37
	Threats	38
	<i>Intruder Motivation</i>	38
	Types of Attacks	39
	Q&A	40
Chapter 3	Defense in Depth	43
	“Do I Know This Already?” Quiz	43
	Foundation and Supplemental Topics	46
	Overview of Defense in Depth	46
	<i>Components Used for Defense in Depth</i>	47
	<i>Physical Security</i>	51
	Foundation Summary	52
	Q&A	54
Part II	Managing Cisco Routers	56
Chapter 4	Basic Router Management	59
	“Do I Know This Already?” Quiz	59
	Foundation Topics	63
	Router Configuration Modes	63
	Accessing the Cisco Router CLI	66
	<i>Configuring CLI Access</i>	68
	Cisco IOS Firewall Features	69
	Foundation Summary	71
	Router Configuration Modes	71
	Accessing the Cisco Router CLI	72
	Cisco IOS Firewall Features	72
	Q&A	75

Chapter 5 Secure Router Administration 79

“Do I Know This Already?” Quiz 79

Foundation Topics 83

Privilege Levels 83

Securing Console Access 84

Configuring the Enable Password 84

enable secret 86

service password-encryption 87

Configuring Multiple Privilege Levels 87

Warning Banners 89

Interactive Access 90

Securing vty Access 90

Secure Shell (SSH) Protocol 91

Setting Up a Cisco IOS Router or Switch as an SSH Client 91

Port Security for Ethernet Switches 92

Configuring Port Security 93

Foundation Summary 95**Q&A 96****Part III Authentication, Authorization, and Accounting (AAA) 98****Chapter 6 Authentication 101**

“Do I Know This Already?” Quiz 101

Foundation Topics 104

Authentication 104

Configuring Line Password Authentication 104

Configuring Username Authentication 105

Remote Security Servers 105

TACACS Overview 106

RADIUS Overview 107

Kerberos Overview 109

PAP and CHAP Authentication 109

PAP 110

CHAP 110

MS-CHAP 111

Foundation Summary 112**Q&A 113****Chapter 7 Authentication, Authorization, and Accounting 115**

“Do I Know This Already?” Quiz 115

Foundation Topics 119

AAA Overview 119

Authentication 119

Authorization 120

Accounting 120

	Configuring AAA Services	120
	<i>Configuring AAA Authentication</i>	121
	<i>Configuring Login Authentication Using AAA</i>	122
	<i>Enabling Password Protection at the Privileged Level</i>	123
	<i>Configuring PPP Authentication Using AAA</i>	124
	<i>Configuring AAA Authorization</i>	125
	<i>Configuring AAA Accounting</i>	128
	Troubleshooting AAA	130
	Foundation Summary	133
	Q&A	134
Chapter 8	Configuring RADIUS and TACACS+ on Cisco IOS Software	137
	“Do I Know This Already?” Quiz	137
	Foundation Topics	140
	Configuring TACACS+ on Cisco IOS	140
	<i>TACACS+ Authentication Examples</i>	141
	<i>TACACS+ Authorization Example</i>	143
	<i>TACACS+ Accounting Example</i>	143
	<i>AAA TACACS+ Troubleshooting</i>	144
	<i>debug aaa authentication</i>	144
	<i>debug tacacs</i>	145
	<i>debug tacacs events</i>	145
	Configuring RADIUS on Cisco IOS	146
	<i>RADIUS Authentication and Authorization Example</i>	148
	<i>RADIUS Authentication, Authorization, and Accounting Example</i>	148
	<i>Testing and Troubleshooting RADIUS Configuration</i>	150
	Foundation Summary	153
	Q&A	154
Chapter 9	Cisco Secure Access Control Server	157
	“Do I Know This Already?” Quiz	157
	Foundation Topics	161
	Cisco Secure ACS for Windows	161
	<i>Authentication</i>	162
	<i>Authorization</i>	164
	<i>Accounting</i>	165
	Administration	165
	Cisco Secure ACS for Windows Architecture	166
	<i>CSAdmin</i>	167
	<i>CSAuth</i>	167
	<i>CSDBSync</i>	168
	<i>CSLog</i>	168
	<i>CSMon</i>	168
	<i>CS Tacacs and CS Radius</i>	168
	Cisco ACS for UNIX	169

Foundation Summary 171

Q&A 172

Chapter 10 Administration of Cisco Secure Access Control Server 175

“Do I Know This Already?” Quiz 175

Foundation Topics 178

Basic Deployment Factors for Cisco Secure ACS 178

Hardware Requirements 178

Operating System Requirements 178

Browser Compatibility 179

Installing Cisco Secure ACS 179

Suggested Deployment Sequence 181

Troubleshooting Cisco Secure ACS for Windows 182

Authentication Problems 183

Troubleshooting Authorization Problems 183

Administration Issues 183

Foundation Summary 185

Q&A 186

Part IV The Cisco IOS Firewall Feature Set 188

Chapter 11 Securing the Network with a Cisco Router 191

“Do I Know This Already?” Quiz 191

Foundation Topics 194

Simple Network Management Protocol (SNMP) 194

Controlling Interactive Access Through a Browser 195

Disabling Directed Broadcasts 196

Routing Protocol Authentication 197

Small Server Services 198

Disabling Finger Services 198

Disabling Network Time Protocol (NTP) 199

Disabling Cisco Discovery Protocol (CDP) 199

Foundation Summary 200

Q&A 201

Chapter 12 Access Lists 203

“Do I Know This Already?” Quiz 203

Foundation Topics 207

What Are Access Lists 207

When to Configure Access Lists 208

Types of IP ACLs 208

Standard IP ACLs 208

Extended IP ACLs 212

Reflexive ACLs 212

Time-Based ACLs 213

Configuring ACLs on a Router 214

	Foundation Summary	216
	Q&A	217
Chapter 13	The Cisco IOS Firewall	219
	“Do I Know This Already?” Quiz	219
	Foundation Topics	222
	The Cisco IOS Firewall Feature Set	222
	<i>Authentication Proxy</i>	223
	<i>DoS Protection</i>	224
	<i>Logging and Audit Trail</i>	224
	<i>Intrusion Detection</i>	224
	<i>Port-To-Application Mapping</i>	225
	<i>System-Defined Port Mapping</i>	225
	<i>User-Defined Port Mapping</i>	227
	<i>Host-Specific Port Mapping</i>	227
	Foundation Summary	228
	Q&A	229
Chapter 14	Context-Based Access Control (CBAC)	231
	“Do I Know This Already?” Quiz	231
	Foundation Topics	235
	Content-Based Access Control	235
	<i>DoS Detection and Protection</i>	235
	<i>Alerts and Audit Trails</i>	236
	<i>How CBAC Works</i>	236
	<i>UDP Sessions</i>	237
	<i>ACL Entries</i>	238
	<i>CBAC Restrictions</i>	238
	<i>Supported Protocols</i>	238
	<i>Memory and Performance Impact</i>	239
	Configuring CBAC	239
	<i>Select an Interface</i>	239
	<i>Configure IP ACLs at the Interface</i>	240
	<i>Configure Global Timeouts and Thresholds</i>	240
	<i>Define an Inspection Rule</i>	241
	<i>Configure Generic TCP and UDP Inspection</i>	243
	<i>Configure Java Inspection</i>	243
	<i>Apply the Inspection Rule to an Interface</i>	244
	Verifying and Debugging CBAC	244
	<i>Debugging Context-Based Access Control</i>	244
	<i>Generic debug Commands</i>	245
	<i>Transport Level debug Commands</i>	245
	<i>CBAC Configuration Example</i>	245
	Foundation Summary	247
	Q&A	248

Chapter 15 Authentication Proxy and the Cisco IOS Firewall 251

“Do I Know This Already?” Quiz 251

Foundation Topics 255

Understanding Authentication Proxy 255

How Authentication Proxy Works 255

What Authentication Proxy Looks Like 256

Authentication Proxy and the Cisco IOS Firewall 258

Configuring Authentication Proxy on the Cisco IOS Firewall 258

Authentication Proxy Configuration Steps 259

Step 1: Configure AAA 260

Step 2: Configure the HTTP Server 261

Step 3: Configure the Authentication Proxy 261

Step 4: Verify the Authentication Proxy Configuration 262

Authentication Proxy Configuration Examples 263

Using Authentication Proxy with TACACS+ 266

Step 1: Complete the Network Configuration 267

Step 2: Complete the Interface Configuration 268

Step 3: Complete the Group Setup 269

Using Authentication Proxy with RADIUS 270

Limitations of Authentication Proxy 272

Foundation Summary 274

Q&A 276

Chapter 16 Intrusion Detection and the Cisco IOS Firewall 279

“Do I Know This Already?” Quiz 279

Foundation Topics 283

Cisco IOS Firewall IDS Features 283

Compatibility with the CSIDS 284

Cisco IOS Firewall IDS Configuration 285

Initialize the Cisco IOS Firewall IDS on the Router 286

Configuring the Notification Type 286

Configure the IOS Firewall IDS and Central Management Post Office Parameters 286

Define the Protected Network 288

Configure the Router Maximum Queue for Alarms 288

Configure Info and Attack Signatures 288

Create and Apply Audit Rules 290

Configure the Default Actions 290

Create the IDS Audit Rule 291

Create the IDS Audit Exclusions 291

Apply the IDS Audit Rule 292

Add the Cisco IOS Firewall IDS to the Centralized Management 292

Verifying the Cisco IOS Firewall IDS Configuration 292

Cisco IOS Firewall IDS Deployment Strategies 295

Foundation Summary 296

Q&A 298

Part V Virtual Private Networks 300

Chapter 17 Building a VPN Using IPSec 303

“Do I Know This Already?” Quiz 303

Foundation Topics 307

Configuring a Cisco Router for IPSec Using Preshared Keys 309

How IPSec Works 309

Step 1: Select the IKE and IPSec Parameters 310

Define the IKE (Phase 1) Policy 311

Define the IPSec Policies 313

Verify the Current Router Configuration 317

Verify Connectivity 317

Ensure Compatible Access Lists 318

Step 2: Configure IKE 318

Enable IKE 319

Create the IKE Policy 319

Configure Preshared Key 319

Verify the IKE Configuration 320

Step 3: Configure IPSec 321

Create the IPSec Transform Set 322

Configure IPSec SA Lifetimes 323

Create the Crypto ACLs 323

Create the Crypto Map 324

Apply the Crypto Map to the Correct Interface 325

Step 4: Test and Verify the IPSec Configuration 326

Configuring Manual IPSec 328

Configuring IPSec Using RSA Encrypted Nonces 328

Configure the RSA Keys 329

Plan the Implementation Using RSA Keys 329

Configure the Router Host Name and Domain Name 330

Generate the RSA Keys 330

Enter Your Peer RSA Public Keys 330

Verify the Key Configuration 331

Manage the RSA Keys 332

Foundation Summary 333

Configure a Cisco Router for IPSec Using Preshared Keys 333

Verifying the IKE and IPSec Configuration 334

Explain the Issues Regarding Configuring IPSec Manually and Using RSA Encrypted Nonces 335

Q&A 336

Chapter 18 Scaling a VPN Using IPSec with a Certificate Authority 339

“Do I Know This Already?” Quiz 339

Foundation Topics 343

- Advanced IPSec VPNs Using Cisco Routers and CAs 343
 - Overview of Cisco Router CA Support 343*
 - Configuring the Cisco Router for IPSec VPNs Using CA Support 345*
 - Step 1: Select the IKE and IPSec Parameters 345*
 - Step 2: Configure the Router CA Support 346*
 - Step 3: Configure IKE Using RSA Signatures 353*
 - Step 4: Configure IPSec 354*
 - Step 5: Test and Verify the Configuration 355*

Foundation Summary 356

- Advanced IPSec VPNs Using Cisco Routers and CAs 356

Q&A 357**Chapter 19 Configuring Remote Access Using Easy VPN 359**

- “Do I Know This Already?” Quiz 359

Foundation Topics 362

- Describe the Easy VPN Server 362
 - Easy VPN Server Functionality 363*
 - Configuring the Easy VPN Server 364*
 - Prepare the Router for Easy VPN Server 365*
 - Configure the Group Policy Lookup 366*
 - Create the ISAKMP Policy for the Remote VPN Clients 366*
 - Define a Group Policy for a Mode Configuration Push 367*
 - Create the Transform Set 368*
 - Create the Dynamic Crypto Maps with Reverse Route Injection (RRI) 368*
 - Apply the Mode Configuration to the Dynamic Crypto Map 369*
 - Apply the Dynamic Crypto Map to the Interface 369*
 - Enable IKE DPD 370*
 - Configure xauth 370*
 - Easy VPN Modes of Operation 371*

Foundation Summary 372

- Describe the Easy VPN Server 372
 - Easy VPN Server Functionality 372*
 - Configuring the Easy VPN Server 372*
 - Easy VPN Modes of Operation 375*

Q&A 376**Chapter 20 Scaling Management of an Enterprise VPN Environment 379**

- “Do I Know This Already?” Quiz 379

Foundation Topics 383

- Managing Enterprise VPN Routers 383
 - CiscoWorks 2000 383*
 - VPN/Security Management Solution (VMS) 385*
 - Management Center for VPN Routers (Router MC) 385*
 - Concepts of the Router MC 386*

<i>Supported Tunneling Technologies</i>	388
<i>Router MC Integration with CiscoWorks Common Services</i>	389
<i>Installation and Login to Router MC</i>	389
<i>Connecting to the Router MC</i>	392
<i>Router MC Workflow</i>	392

Foundation Summary 395

Managing Enterprise VPN Routers	395
---------------------------------	-----

Q&A 398

Part VI Scenarios 400

Chapter 21 Final Scenarios 403

Task 1: Secure the Routers at All Locations	404
<i>Change All Administrative Access on All the Routers</i>	405
<i>Configure Local Database Authentication Using AAA</i>	406
<i>Configure a Secure Method for Remote Access of the Routers</i>	406
<i>Disable Unnecessary Services</i>	407
<i>Implement ACLs for Antispoofing Purposes</i>	408
Task 2: Secure Site-to-Site Connectivity	409
<i>Define VPN Configuration Parameters</i>	409
<i>Configure the IKE Parameters</i>	411
<i>Configure the IPSec Parameters</i>	413
<i>Configure ACLs</i>	414
<i>Create and Apply Crypto Maps</i>	414
Task 3: Configure CA Support	416
<i>Configure Host Name and Domain Name</i>	416
<i>Configure NTP</i>	417
<i>Enroll with the CA</i>	418
Task 4: Secure Remote Access	419
Task 5: Secure the Enterprise Network	420
<i>Implement the Cisco IOS Firewall IDS</i>	420
<i>Implement Authentication Proxy</i>	423
<i>Implement CBAC</i>	424

Appendix Answers to the “Do I Know This Already?” Quizzes and Q&A Sections 427

Chapter 1	427
“Do I Know This Already?” Quiz	427
Q&A	427
Chapter 2	429
“Do I Know This Already?” Quiz	429
Q&A	430
Chapter 3	432
“Do I Know This Already?” Quiz	432
Q&A	432

Chapter 4	433
<i>“Do I Know This Already?” Quiz</i>	433
Q&A	433
Chapter 5	435
<i>“Do I Know This Already?” Quiz</i>	435
Q&A	435
Chapter 6	437
<i>“Do I Know This Already?” Quiz</i>	437
Q&A	437
Chapter 7	438
<i>“Do I Know This Already?” Quiz</i>	438
Q&A	438
Chapter 8	440
<i>“Do I Know This Already?” Quiz</i>	440
Q&A	440
Chapter 9	441
<i>“Do I Know This Already?” Quiz</i>	441
Q&A	442
Chapter 10	443
<i>“Do I Know This Already?” Quiz</i>	443
Q&A	443
Chapter 11	444
<i>“Do I Know This Already?” Quiz</i>	444
Q&A	445
Chapter 12	446
<i>“Do I Know This Already?” Quiz</i>	446
Q&A	446
Chapter 13	448
<i>“Do I Know This Already?” Quiz</i>	448
Q&A	448
Chapter 14	449
<i>“Do I Know This Already?” Quiz</i>	449
Q&A	449
Chapter 15	451
<i>“Do I Know This Already?” Quiz</i>	451
Q&A	451
Chapter 16	452
<i>“Do I Know This Already?” Quiz</i>	452
Q&A	453
Chapter 17	454
<i>“Do I Know This Already?” Quiz</i>	454
Q&A	454

Chapter 18	456
<i>“Do I Know This Already?” Quiz</i>	456
Q&A	456
Chapter 19	457
<i>“Do I Know This Already?” Quiz</i>	457
Q&A	457
Chapter 20	458
<i>“Do I Know This Already?” Quiz</i>	458
Q&A	459

Glossary	463
----------	-----

Index	472
-------	-----