Contents at a Glance

Introduction xxxiii

Part I Network Security Technologies Overview

Chapter 1 Network Security Fundamentals 3

Chapter 2 Network Security Threats 21

Chapter 3 Network Foundation Protection (NFP) Overview 39

Chapter 4 Configuring and Implementing Switched Data Plane Security Solutions 57

Chapter 5 802.1X and Cisco Identity-Based Networking Services (IBNS) 91

Chapter 6 Implementing and Configuring Basic 802.1X 109

Chapter 7 Implementing and Configuring Advanced 802.1X 139

Part II Cisco IOS Foundation Security Solutions

Chapter 8 Implementing and Configuring Cisco IOS Routed Data Plane Security 183

Chapter 9 Implementing and Configuring Cisco IOS Control Plane Security 219

Chapter 10 Implementing and Configuring Cisco IOS Management Plane Security 245

Chapter 11 Implementing and Configuring Network Address Translation (NAT) 275

Chapter 12 Implementing and Configuring Zone-Based Policy Firewalls 295

Chapter 13 Implementing and Configuring IOS Intrusion Prevention System (IPS) 333

Chapter 14 Introduction to Cisco IOS Site-to-Site Security Solutions 369

Chapter 15 Deploying VTI-Based Site-to-Site IPsec VPNs 387

Part III Cisco IOS Threat Detection and Control

Chapter 16 Deploying Scalable Authentication in Site-to-Site IPsec VPNs 411

Chapter 17 Deploying DMVPNs 447

Chapter 18 Deploying High Availability in Tunnel-Based IPsec VPNs 481

Chapter 19 Deploying GET VPNs 499

Part IV Managing and Implementing Cisco IOS Site-to-Site Security Solutions

Part V Managing and Implementing Cisco IOS Secure Remote Access Solutions

Chapter 20 Deploying Remote Access Solutions Using SSL VPNs 529

Chapter 21 Deploying Remote Access Solutions Using EZVPNs 569

Part VI Exam Preparation

Chapter 22 Final Preparation 591

Part VII Appendixes

Appendix A Answers to Chapter DIKTA Quizzes and Fill in the Blanks Questions 599

Appendix B CCNP Security 642-637 SECURE Exam Updates, Version 1.0 621

Index 622

Elements Available on CD

Appendix C Memory Tables

Appendix D Memory Table Answers

Glossary

Contents

Introduction xxxiii

Part I Network Security Technologies Overview

Chapter 1 Network Security Fundamentals 3

"Do I Know This Already?" Quiz 3

Foundation Topics 7

Defining Network Security 7

Building Secure Networks 7

Cisco SAFE 9

SCF Basics 9

SAFE/SCF Architecture Principles 12

SAFE/SCF Network Foundation Protection (NFP) 14

SAFE/SCF Design Blueprints 14

SAFE Usage 15

Exam Preparation 17

Chapter 2 Network Security Threats 21

"Do I Know This Already?" Quiz 21

Foundation Topics 24

Vulnerabilities 24

Self-Imposed Network Vulnerabilities 24

Intruder Motivations 29

Lack of Understanding of Computers or Networks 30

Intruding for Curiosity 30

Intruding for Fun and Pride 30

Intruding for Revenge 30

Intruding for Profit 31

Intruding for Political Purposes 31

Types of Network Attacks 31

Reconnaissance Attacks 32

Access Attacks 33

DoS Attacks 35

Exam Preparation 36

Chapter 3 Network Foundation Protection (NFP) Overview 39

"Do I Know This Already?" Quiz 39

Foundation Topics 42

Overview of Device Functionality Planes 42

Control Plane 43

Data Plane 44

Management Plane 45

Identifying Network Foundation Protection Deployment Models 45

Identifying Network Foundation Protection Feature Availability 48

Cisco Catalyst Switches 48

Cisco Integrated Services Routers (ISR) 49

Cisco Supporting Management Components 50

Exam Preparation 53

Part II Cisco IOS Foundation Security Solutions

Chapter 4 Configuring and Implementing Switched Data Plane Security Solutions 57

"Do I Know This Already?" Quiz 57

Foundation Topics 60

Switched Data Plane Attack Types 60

VLAN Hopping Attacks 60

CAM Flooding Attacks 61

MAC Address Spoofing 63

Spanning Tree Protocol (STP) Spoofing Attacks 63

DHCP Starvation Attacks 66

DHCP Server Spoofing 67

ARP Spoofing 67

Switched Data Plane Security Technologies 67

Port Configuration 67

Port Security 71

Root Guard, BPDU Guard, and PortFast 74

DHCP Snooping 75

Dynamic ARP Inspection (DAI) 77

IP Source Guard 79

Private VLANs (PVLAN) 80

Exam Preparation 84

Chapter 5 802.1X and Cisco Identity-Based Networking Services (IBNS) 91

"Do I Know This Already?" Quiz 91

Foundation Topics 94

Identity-Based Networking Services (IBNS) and IEEE 802.1x Overview 94

IBNS and 802.1x Enhancements and Features 94

802.1x Components 96

802.1x Interworking 97

Extensible Authentication Protocol (EAP) 97

EAP over LAN (EAPOL) 98

EAP Message Exchange 99

Port States 100

Port Authentication Host Modes 101

EAP Type Selection 102

EAP–Message Digest Algorithm 5 102

Protected EAP w/MS-CHAPv2 102

Cisco Lightweight EAP 103

EAP–Transport Layer Security 104

EAP–Tunneled Transport Layer Security 104

EAP–Flexible Authentication via Secure Tunneling 105

Exam Preparation 106

Chapter 6 Implementing and Configuring Basic 802.1X 109

"Do I Know This Already?" Quiz 109

Foundation Topics 112

Plan Basic 802.1X Deployment on Cisco Catalyst IOS Software 112

Gathering Input Parameters 113

Deployment Tasks 113

Deployment Choices 114

General Deployment Guidelines 114

Configure and Verify Cisco Catalyst IOS Software 802.1X Authenticator 115

Configuration Choices 115

Configuration Scenario 115

Verify Basic 802.1X Functionality 121

Configure and Verify Cisco ACS for EAP-FAST 121

Configuration Choices 122

Configuration Scenario 122

Configure the Cisco Secure Services Client 802.1X Supplicant 128

Task 1: Create the CSSC Configuration Profile 128

Task 2: Create a Wired Network Profile 128

Tasks 3 and 4: (Optional) Tune 802.1X Timers and Authentication Mode 130

Task 5: Configure the Inner and Outer EAP Mode for the Connection 131

Task 6: Choose the Login Credentials to Be Used for Authentication 132

Task 7: Create the CSSC Installation Package 133

Network Login 134

Verify and Troubleshoot 802.1 X Operations 134

Troubleshooting Flow 134

Successful Authentication 135

Verify Connection Status 135

Verify Authentication on AAA Server 135

Verify Guest/Restricted VLAN Assignment 135

802.1X Readiness Check 135

Unresponsive Supplicant 135

Failed Authentication: RADIUS Configuration Issues 135

Failed Authentication: Bad Credentials 135

Exam Preparation 136

Chapter 7 Implementing and Configuring Advanced 802.1X 139

"Do I Know This Already?" Quiz 139

Foundation Topics 143

Plan the Deployment of Cisco Advanced 802.1X Authentication Features 143

Gathering Input Parameters 143

Deployment Tasks 144

Deployment Choices 144

Configure and Verify EAP-TLS Authentication on Cisco IOS Components and Cisco Secure ACS 145

EAP-TLS with 802.1X Configuration Tasks 145

Configuration Scenario 146

Configuration Choices 146

Task 1: Configure RADIUS Server 147

Task 2: Install Identity and Certificate Authority Certificates on All Clients 147

Task 3: Configure an Identity Certificate on the Cisco Secure ACS Server 147

Task 4: Configure Support of EAP-TLS on the Cisco Secure ACS Server 149

Task 5: (Optional) Configure EAP-TLS Support Using the Microsoft Windows Native Supplicant 151

Task 6: (Optional) Configure EAP-TLS Support Using the Cisco Secure Services Client (CSSC) Supplicant 152

Implementation Guidelines 153

Feature Support 153

Verifying EAP-TLS Configuration 153

Deploying User and Machine Authentication 153

Configuring User and Machine Authentication Tasks 154

Configuration Scenario 154

Task 1: Install Identity and Certificate Authority Certificates on All Clients 155

Task 2: Configure Support of EAP-TLS on Cisco Secure ACS Server 155

Task 3: Configure Support of Machine Authentication on Cisco Secure ACS Server 156

Task 4: Configure Support of Machine Authentication on Microsoft Windows Native 802.1X Supplicant 156

Task 5: (Optional) Configure Machine Authentication Support Using the Cisco Secure Services Client (CSSC) Supplicant 157

Task 6: (Optional) Configure Additional User Support Using the Cisco Secure Services Client (CSSC) Supplicant 158

Implementation Guidelines 158

Feature Support 158

Deploying VLAN and ACL Assignment 159

Deploying VLAN and ACL Assignment Tasks 159

Configuration Scenario 159

Configuration Choices 160

Task 1: Configure Cisco IOS Software 802.1X Authenticator Authorization 160

Task 2: (Optional) Configure VLAN Assignment on Cisco Secure ACS 161

Task 3: (Optional) Configure and Prepare for ACL Assignment on Cisco IOS Software Switch 162

Task 4: (Optional) Configure ACL Assignment on Cisco Secure ACS Server 162

Verification of VLAN and ACL Assignment with Cisco IOS Software CLI 164

Verification of VLAN and ACL Assignment on Cisco Secure ACS 165

Configure and Verify Cisco Secure ACS MAC Address Exception Policies 165

Cisco Catalyst IOS Software MAC Authentication Bypass (MAB) 165

Configuration Tasks 166

Configuration Scenario 166

Tasks 1 and 2: Configure MAC Authentication Bypass on the Switch and ACS 167

Verification of Configuration 168

Implementation Guidelines 168

Configure and Verify Web Authentication on Cisco IOS Software LAN Switches and Cisco Secure ACS 168

Configuration Tasks 169

Configuration Scenario 169

Task 1: Configure Web Authentication on the Switch 169

Task 2: Configure Web Authentication on the Cisco Secure ACS Server 171

Web Authentication Verification 172

User Experience 172

Choose a Method to Support Multiple Hosts on a Single Port 172

Multiple Hosts Support Guidelines 172

Configuring Support of Multiple Hosts on a Single Port 172

Configuring Fail-Open Policies 174

Configuring Critical Ports 174

Configuring Open Authentication 176

Resolve 802.1X Compatibility Issues 176

Wake-on-LAN (WOL) 176

Non-802.1X IP Phones 177

Preboot Execution Environment (PXE) 177

Exam Preparation 178

~~Part II Cisco IOS Foundation Security Solutions~~

Chapter 8 Implementing and Configuring Cisco IOS Routed Data Plane Security 183

"Do I Know This Already?" Quiz 183

Foundation Topics 186

Routed Data Plane Attack Types 186

IP Spoofing 186

Slow-Path Denial of Service 186

Traffic Flooding 187

Routed Data Plane Security Technologies 187

Access Control Lists (ACL) 187

Flexible Packet Matching 196

Flexible NetFlow 203

Unicast Reverse Path Forwarding (Unicast RPF) 209

Exam Preparation 212

Chapter 9 Implementing and Configuring Cisco IOS Control Plane Security 219

"Do I Know This Already?" Quiz 219

Foundation Topics 222

Control Plane Attack Types 222

Slow-Path Denial of Service 222

Routing Protocol Spoofing 222

Control Plane Security Technologies 222

Control Plane Policing (CoPP) 222

Control Plane Protection (CPPr) 226

Routing Protocol Authentication 232

Exam Preparation 237

Chapter 10 Implementing and Configuring Cisco IOS Management Plane Security 245

"Do I Know This Already?" Quiz 245

Foundation Topics 248

Management Plane Attack Types 248

Management Plane Security Technologies 248

Basic Management Security and Privileges 248

SSH 254

SNMP 256

CPU and Memory Thresholding 261

Management Plane Protection 262

AutoSecure 263

Digitally Signed Cisco Software 265

Exam Preparation 267

Part III Cisco IOS Threat Detection and Control

Chapter 11 Implementing and Configuring Network Address Translation (NAT) 275

"Do I Know This Already?" Quiz 275

Foundation Topics 278

Network Address Translation 278

Static NAT Example 280

Dynamic NAT Example 280

PAT Example 281

NAT Configuration 282

Overlapping NAT 287

Exam Preparation 290

Chapter 12 Implementing and Configuring Zone-Based Policy Firewalls 295

"Do I Know This Already?" Quiz 295

Foundation Topics 298

Zone-Based Policy Firewall Overview 298

Zones/Security Zones 298

Zone Pairs 299

Transparent Firewalls 300

Zone-Based Layer 3/4 Policy Firewall Configuration 301

Class Map Configuration 302

Parameter Map Configurations 304

Policy Map Configuration 306

Zone Configuration 308

Zone Pair Configuration 309

Port to Application Mapping (PAM) Configuration 310

Zone-Based Layer 7 Policy Firewall Configuration 312

URL Filter 313

HTTP Inspection 318

Exam Preparation 323

Chapter 13 Implementing and Configuring IOS Intrusion Prevention System (IPS) 333

"Do I Know This Already?" Quiz 333

Foundation Topics 336

Configuration Choices, Basic Procedures, and Required Input Parameters 336

Intrusion Detection and Prevention with Signatures 337

Sensor Accuracy 339

Choosing a Cisco IOS IPS Sensor Platform 340

Software-Based Sensor 340

Hardware-Based Sensor 340

Deployment Tasks 341

Deployment Guidelines 342

Deploying Cisco IOS Software IPS Signature Policies 342

Configuration Tasks 342

Configuration Scenario 342
Verification 346
Guidelines 347
Tuning Cisco IOS Software IPS Signatures 347
Event Risk Rating System Overview 348
Event Risk Rating Calculation 348
Event Risk Rating Example 349
Signature Event Action Overrides (SEAO) 349
Signature Event Action Filters (SEAF) 349
Configuration Tasks 350
Configuration Scenario 350
Verification 355
Implementation Guidelines 355
Deploying Cisco IOS Software IPS Signature Updates 355
Configuration Tasks 356
Configuration Scenario 356
Task 1: Install Signature Update License 356
Task 2: Configure Automatic Signature Updates 357
Verification 357
Monitoring Cisco IOS Software IPS Events 358
Cisco IOS Software IPS Event Generation 358
Cisco IME Features 358
Cisco IME Minimum System Requirements 359
Configuration Tasks 359
Configuration Scenario 360
Task 2: Add the Cisco IOS Software IPS Sensor to Cisco IME 361
Verification 362
Verification: Local Events 362
Verification: IME Events 363
Cisco IOS Software IPS Sensor 363
Troubleshooting Resource Use 365
Additional Debug Commands 365
Exam Preparation 366

Part IV Managing and Implementing Cisco IOS Site-to-Site Security Solutions

Chapter 14 Introduction to Cisco IOS Site-to-Site Security Solutions 369
"Do I Know This Already?" Quiz 369
Foundation Topics 372
Choose an Appropriate VPN LAN Topology 372

Input Parameters for Choosing the Best VPN LAN Topology 373

General Deployment Guidelines for Choosing the Best VPN LAN Topology 373

Choose an Appropriate VPN WAN Technology 373

Input Parameters for Choosing the Best VPN WAN Technology 374

General Deployment Guidelines for Choosing the Best VPN WAN Technology 376

Core Features of IPsec VPN Technology 376

IPsec Security Associations 377

Internet Key Exchange (IKE) 377

IPsec Phases 377

IKE Main and Aggressive Mode 378

Encapsulating Security Payload 378

Choose Appropriate VPN Cryptographic Controls 379

IPsec Security Associations 379

Algorithm Choices 379

General Deployment Guidelines for Choosing Cryptographic Controls for a Site-to-Site VPN Implementation 381

Design and Implementation Resources 382

Exam Preparation 383

Chapter 15 Deploying VTI-Based Site-to-Site IPsec VPNs 387

"Do I Know This Already?" Quiz 387

Foundation Topics 390

Plan a Cisco IOS Software VTI-Based Site-to-Site VPN 390

Virtual Tunnel Interfaces 390

Input Parameters 392

Deployment Tasks 393

Deployment Choices 393

General Deployment Guidelines 393

Configuring Basic IKE Peering 393

Cisco IOS Software Default IKE PSK-Based Policies 394

Configuration Tasks 394

Configuration Choices 395

Configuration Scenario 395

Task 1: (Optional) Configure an IKE Policy on Each Peer 395

Tasks 2 and 3: Generate and Configure Authentication Credentials on Each Peer 396

Verify Local IKE Sessions 396

Verify Local IKE Policies 396
Verify a Successful Phase 1 Exchange 397
Implementation Guidelines 397
Troubleshooting IKE Peering 397
Troubleshooting Flow 397
Configuring Static Point-to-Point IPsec VTI Tunnels 398
Default Cisco IOS Software IPsec Transform Sets 398
Configuration Tasks 398
Configuration Choices 399
Configuration Scenario 399
Task 1: (Optional) Configure an IKE Policy on Each Peer 399
Task 2: (Optional) Configure an IPsec Transform Set 399
Task 3: Configure an IPsec Protection Profile 400
Task 4: Configure a Virtual Tunnel Interface (VTI) 400
Task 5: Apply the Protection Profile to the Tunnel Interface 401
Task 6: Configure Routing into the VTI Tunnel 401
Implementation Guidelines 401
Verify Tunnel Status and Traffic 401
Troubleshooting Flow 402
Configure Dynamic Point-to-Point IPsec VTI Tunnels 403
Virtual Templates and Virtual Access Interfaces 403
ISAKMP Profiles 404
Configuration Tasks 404
Configuration Scenario 404
Task 1: Configure IKE Peering 405
Task 2: (Optional) Configure an IPsec Transform Set 405
Task 3: Configure an IPsec Protection Profile 405
Task 4: Configure a Virtual Template Interface 406
Task 5: Map Remote Peer to a Virtual Template Interface 406
Verify Tunnel Status on the Hub 407
Implementation Guidelines 407
Exam Preparation 408

~~**Part III Cisco IOS Threat Detection and Control**~~

Chapter 16 Deploying Scalable Authentication in Site-to-Site IPsec VPNs 411
“Do I Know This Already?” Quiz 411
Foundation Topics 414
Describe the Concept of a Public Key Infrastructure 414
Manual Key Exchange with Verification 414

Trusted Introducing 414

Public Key Infrastructure: Certificate Authorities 416

X.509 Identity Certificate 417

Certificate Revocation Checking 418

Using Certificates in Network Applications 419

Deployment Choices 420

Deployment Steps 420

Input Parameters 421

Deployment Guidelines 421

Configure, Verify, and Troubleshoot a Basic Cisco IOS Software Certificate Server 421

Configuration Tasks for a Root Certificate Server 422

Configuration Scenario 423

Task 1: Create an RSA Key Pair 423

Task 2: Create a PKI Trustpoint 424

Tasks 3 and 4: Create the CS and Configure the Database Location 424

Task 5: Configure an Issuing Policy 425

Task 6: Configure the Revocation Policy 425

Task 7: Configure the SCEP Interface 426

Task 8: Enable the Certificate Server 426

Cisco Configuration Professional Support 426

Verify the Cisco IOS Software Certificate Server 427

Feature Support 427

Implementation Guidelines 428

Troubleshooting Flow 429

PKI and Time: Additional Guidelines 429

Enroll a Cisco IOS Software VPN Router into a PKI and Troubleshoot the Enrollment Process 429

PKI Client Features 429

Simple Certificate Enrollment Protocol 430

Key Storage 430

Configuration Tasks 430

Configuration Scenario 431

Task 1: Create an RSA Key Pair 431

Task 2: Create an RSA Key Pair 432

Task 3: Authenticate the PKI Certificate Authority 432

Task 4: Create an Enrollment Request on the VPN Router 433

Task 5: Issue the Client Certificate on the CA Server 434

Certificate Revocation on the Cisco IOS Software Certificate Server 434

Cisco Configuration Professional Support 434

Verify the CA and Identity Certificates 435

Feature Support 435

Implementation Guidelines 436

Troubleshooting Flow 436

Configure and Verify the Integration of a Cisco IOS Software VPN Router with Supporting PKI Entities 436

IKE Peer Authentication 436

IKE Peer Certificate Authorization 437

Configuration Tasks 437

Configuration Scenario 437

Task 1: Configure an IKE Policy 438

Task 2: Configure an ISAKMP Profile 438

Task 3: Configure Certificate-Based Authorization of Remote Peers 438

Verify IKE SA Establishment 439

Feature Support 439

Implementation Guidelines 440

Troubleshooting Flow 440

Configuring Advanced PKI Integration 440

Configuring CRL Handling on PKI Clients 441

Using OCSP or AAA on PKI Clients 441

Exam Preparation 442

Chapter 17 Deploying DMVPNs 447

"Do I Know This Already?" Quiz 447

Foundation Topics 451

Understanding the Cisco IOS Software DMVPN Architecture 451

Building Blocks of DMVPNs 452

Hub-and-Spoke Versus On-Demand Fully Meshed VPNs 452

DMVPN Initial State 453

DMVPN Spoke-to-Spoke Tunnel Creation 453

DMVPN Benefits and Limitations 454

Plan the Deployment of a Cisco IOS Software DMVPN 455

Input Parameters 455

Deployment Tasks 455

Deployment Choices 456

General Deployment Guidelines 456

Configure and Verify Cisco IOS Software GRE Tunnels 456

GRE Features and Limitations 456

Point-to-Point Versus Point-to-Multipoint GRE Tunnels 457

Point-to-Point Tunnel Configuration Example 457

Configuration Tasks for a Hub-and-Spoke Network 459

Configuration Scenario 459

Task 1: Configure an mGRE Interface on the Hub 459

Task 2: Configure a GRE Interface on the Spoke 459

Verify the State of GRE Tunnels 460

Configure and Verify a Cisco IOS Software NHRP Client and Server 461

(m)GRE and NHRP Integration 461

Configuration Tasks 461

Configuration Scenario 461

Task 1: Configure an NHRP Server 461

Task 2: Configure an NHRP Client 462

Verify NHRP Mappings 462

Debugging NHRP 463

Configure and Verify a Cisco IOS Software DMVPN Hub 464

Configuration Tasks 464

Configuration Scenario 464

Task 1: (Optional) Configure an IKE Policy 464

Task 2: Generate and/or Configure Authentication Credentials 465

Task 3: Configure an IPsec Profile 465

Task 4: Create an mGRE Tunnel Interface 465

Task 5: Configure the NHRP Server 465

Task 6: Associate the IPsec Profile with the mGRE Interface 466

Task 7: Configure IP Parameters on the mGRE Interface 466

Cisco Configuration Professional Support 466

Verify Spoke Registration 466

Verify Registered Spoke Details 467

Implementation Guidelines 468

Feature Support 468

Configure and Verify a Cisco IOS Software DMVPN Spoke 468

Configuration Tasks 468

Configuration Scenario 469

Task 1: (Optional) Configure an IKE Policy 469

Task 2: Generate and/or Configure Authentication Credentials 469

Task 3: Configure an IPsec Profile 469

Task 4: Create an mGRE Tunnel Interface 470

Task 5: Configure the NHRP Client 470

Task 6: Associate the IPsec Profile with the mGRE Interface 470

Task 7: Configure IP Parameters on the mGRE Interface 471

Verify Tunnel State and Traffic Statistics 471

Configure and Verify Dynamic Routing in a Cisco IOS Software DMVPN 471

EIGRP Hub Configuration 472

OSPF Hub Configuration 473

Hub-and-Spoke Routing and IKE Peering on Spoke 473

Full Mesh Routing and IKE Peering on Spoke 474

Troubleshoot a Cisco IOS Software DMVPN 474

Troubleshooting Flow 475

Exam Preparation 476

Chapter 18 Deploying High Availability in Tunnel-Based IPsec VPNs 481

"Do I Know This Already?" Quiz 481

Foundation Topics 484

Plan the Deployment of Cisco IOS Software Site-to-Site IPsec VPN High-Availability Features 484

VPN Failure Modes 484

Partial Failure of the Transport Network 484

Partial or Total Failure of the Service Provider (SP) Transport Network 485

Partial or Total Failure of a VPN Device 485

Deployment Guidelines 485

Use Routing Protocols for VPN Failover 486

Routing to VPN Tunnel Endpoints 486

Routing Protocol Inside the VPN Tunnel 486

Recursive Routing Hazard 487

Routing Protocol VPN Topologies 487

Routing Tuning for Path Selection 487

Routing Tuning for Faster Convergence 488

Choose the Most Optimal Method of Mitigating Failure in a VTI-Based VPN 488

Path Redundancy Using a Single-Transport Network 489

Path Redundancy Using Two Transport Networks 489

Path and Device Redundancy in Single-Transport Networks 489

Path and Device Redundancy with Multiple-Transport Networks 489

Choose the Most Optimal Method of Mitigating Failure in a DMVPN 490

Recommended Architecture 490

Shared IPsec SAs 490

Configuring a DMVPN with a Single-Transport Network 490

Configuring a DMVPN over Multiple-Transport Networks 493

Exam Preparation 495

Chapter 19 Deploying GET VPNs 499

"Do I Know This Already?" Quiz 499

Foundation Topics 502

Describe the Operation of a Cisco IOS Software GET VPN 502

Peer Authentication and Policy Provisioning 502

GET VPN Traffic Exchange 504

Packet Security Services 504

Key Management Architecture 505

Rekeying Methods 505

Traffic Encapsulation 507

Benefits and Limitations 507

Plan the Deployment of a Cisco IOS Software GET VPN 508

Input Parameters 508

Deployment Tasks 508

Deployment Choices 509

Deployment Guidelines 509

Configure and Verify a Cisco IOS Software GET VPN Key Server 509

Configuration Tasks 509

Configuration Choices 510

Configuration Scenario 510

Task 1: (Optional) Configure an IKE Policy 511

Task 2: Generate and/or Configure Authentication Credentials 511

Task 3: Generate RSA keys for Rekey Authentication 511

Task 4: Configure a Traffic Protection Policy on the Key Server 512

Task 5: Enable and Configure the GET VPN Key Server Function 512

Task 6: (Optional) Tune the Rekeying Policy 513

Task 7: Create and Apply the GET VPN Crypto Map 513

Cisco Configuration Professional Support 514

Verify Basic Key Server Settings 514

Verify the Rekey Policy 514

List All Registered Members 515

Implementation Guidelines 515

Configure and Verify Cisco IOS Software GET VPN Group Members 515

Configuration Tasks 516

Configuration Choices 516

Configuration Scenario 516

Task 1: Configure an IKE Policy 516

Task 2: Generate and/or Configure Authentication Credentials 517

Task 3: Enable the GET VPN Group Member Function 518

Task 4: Create and Apply the GET VPN Crypto Map 518

Task 5: (Optional) Configure a Fail-Closed Policy 518

Cisco Configuration Professional Support 519

Verify Registration of the Group Member 519

Implementation Guidelines 519

Troubleshooting Flow 519

Configure and Verify High-Availability Mechanisms in a GET VPN 520

Network Splits and Network Merges 521

Configuration Tasks 521

Configuration Scenario 521

Task 1: Distribute the Rekey RSA Key Pair 522

Task 2: Configure a Full Mesh of Key Server IKE Peering 522

Task 3: Configure COOP 522

Tasks 4 and 5: Configure Traffic Protection Policy and Multiple Key Servers on Group Members 523

Verify IKE Peering 523

Verify COOP Peering 523

Implementation Guidelines 524

Troubleshooting Flow 524

Exam Preparation 525

~~**Part IV Managing and Implementing Cisco IOS Site-to-Site Security Solutions**~~

Part V Managing and Implementing Cisco IOS Secure Remote Access Solutions

Chapter 20 Deploying Remote Access Solutions Using SSL VPNs 529

"Do I Know This Already?" Quiz 529

Foundation Topics 533

Choose an Appropriate Remote Access VPN Technology 533

Cisco IOS Software Remote Access VPN Options 533

Full Tunneling Remote Access SSL VPN: Features 533

Full Tunneling Remote Access SSL VPN: Benefits and Limitations 534

Clientless Remote Access SSL VPN: Features 534

Clientless SSL VPN: Benefits and Limitations 535

Software Client Remote Access IPsec VPN (EZVPN): Features 535

Hardware Client Remote Access IPsec VPN (EZVPN): Features 536

Remote Access IPsec VPN: Benefits and Limitations 536

VPN Access Methods: Use Cases 536

Choose Appropriate Remote Access VPN Cryptographic Controls 537

SSL/TLS Refresher 537

Algorithm Choices in Cisco SSL Remote Access VPNs 539

IKE Remote Access VPN Extensions 539

Algorithm Choices in Cisco IPsec Remote Access VPNs 540

Deploying Remote Access Solutions Using SSL VPNs 541

Solution Components 541

Deployment Tasks 541

Input Parameters 542

Configure and Verify Common SSL VPN Parameters 542

Configuration Tasks 543

Configuration Choices 543

Configuration Scenario 543

Task 1: (Optional) Verify SSL VPN Licensing 544

Task 2: Provision an Identity Server SSL/TLS Certificate to the ISR 544

Task 3: Enable the SSL VPN Gateway and Context 544

Task 4: Configure and Tune SSL/TLS Settings 545

Task 5: (Optional) Configure Gateway High Availability 545

Gateway Verification 545

Implementation Guidelines 546

Configure and Verify Client Authentication and Policies on the SSL VPN Gateway 546

Gateway, Contexts, and Policy Groups 546

Basic User Authentication Overview 546

Configuration Tasks 547

Configuration Scenario 547

Task 1: Create and Apply a Default Policy 548

Task 2: Enable User Authentication Using Local AAA 548

Implementation Guidelines 548

Configure and Verify Full Tunneling Connectivity on the Cisco IOS SSL VPN Gateway 549

Configuration Tasks 549

Configuration Scenario 549

Task 1: Enable Full Tunneling Access 549

Task 2: Configure Local IP Address Assignment 550

Task 3: (Optional) Configure Client Configuration 551

Task 4: (Optional) Configure Split Tunneling 551

Task 5: (Optional) Configure Access Control 551

Cisco Configuration Professional Support 552

Install and Configure the Cisco AnyConnect Client 552

AnyConnect 2.4–Supported Platforms 553

Configuration Tasks 553

Configuration Scenario 553

Task 1: Enable Full Tunneling Access 553

Task 2: Verify Server Certificate Authentication Chain 554

Task 3: Configure Basic AnyConnect Profile Settings 554

Task 4: Establish the SSL VPN Connection 554

Client-Side Verification 554

Gateway-Side Verification 555

Cisco Configuration Professional 556

Configure and Verify Clientless Access on the Cisco IOS SSL VPN Gateway 556

Basic Portal Features 556

Cisco Secure Desktop for Clientless Access 557

Port Forwarding Overview 557

Port Forwarding Benefits and Limitations 558

Portal ACLs 558

Configuration Tasks 558

Configuration Scenario 559

Task 1: Enable Full Tunneling Access 560

Task 2: (Optional) Configure Port Forwarding 560

Task 3: (Optional) Configure Cisco Secure Desktop 561

Task 4: (Optional) Configure Access Control 561

Basic Portal Verification 562

Web Application Access 562

File Server Access 562

Port Forwarding Access 562

Cisco Secure Desktop Verification 563

Gateway-Side Verification 563

Troubleshoot the Basic SSL VPN Operation 563

Port Forwarding Access 563

Troubleshooting Flow (VPN Establishment) 563

Troubleshooting Flow (Data Flow) 563

Gateway-Side Issue 564

Client-Side Issues: Certificates 564

Exam Preparation 565

Chapter 21 Deploying Remote Access Solutions Using EZVPNs 569

"Do I Know This Already?" Quiz 569

Foundation Topics 572

Plan the Deployment of a Cisco IOS Software EZVPN 572

Solution Components 573

Deployment Tasks 573

Input Parameters 574

Deployment Guidelines 574

Configure and Verify a Basic Cisco IOS Software VTI-Based EZVPN Server 575

Group Pre-Shared Key Authentication 575

Extended Authentication (XAUTH) Overview 575

Configuration Groups and ISAKMP Profiles 576

Configuration Tasks 576

Configuration Scenario 576

Task 1: (Optional) Verify an IKE Policy 577

Task 2: Configure an IPsec Transform Set and Profile 577

Task 3: Configure a Dynamic VTI Template 577

Task 4: Create a Client Configuration Group 578

Task 5: Create an ISAKMP Profile 578

Tasks 6 and 7: Configure and Enable User Authentication 579

Cisco Configuration Professional Support 579

Implementation Guidelines 580

Configure the Cisco VPN Client 580

Configuration Tasks 580

Configuration Scenario 580

Task 1: Install the Cisco VPN Client Software 580

Task 2: Configure the VPN Client Connection Entry 580

Task 3: Establish the EZVPN Connection 581

Client-Side Verification 581

Gateway-Side Verification 581

Configure and Verify VTI-Based EZVPN Remote Client Functionality on the Cisco ISR 582

EZVPN Remote Modes 582

Configuration Tasks 583

Configuration Scenario 583

Task 1: Configure EZVPN Remote Profile 583

Task 2: Designate EZVPN Interface Roles 584

Implementation Guidelines 584

Configure and Verify EZVPN Server and VPN Client PKI Features 585

Head-End PKI Configuration 585

VPN Client Configuration: SCEP Enrollment 585

VPN Client Enrollment Verification 586

VPN Client Configuration: Profile 586

Troubleshoot Basic EZVPN Operation 587

Troubleshooting Flow: VPN Session Establishment 587

Troubleshooting Flow: VPN Data Flow 587

Exam Preparation 588

Part VI Exam Preparation

Chapter 22 Final Preparation 591

Tools for Final Preparation 591

Pearson Cert Practice Test Engine and Questions on the CD 591

Install the Software from the CD 592

Activate and Download the Practice Exam 592

Activating Other Exams 593

Premium Edition 593

Cisco Learning Network 593

Memory Tables 593

Chapter-Ending Review Tools 594

Suggested Plan for Final Review/Study 594

Step 1: Review the Key Topics, the DIKTA Questions, and the Fill in the Blanks Questions 595

Step 2: Complete the Memory Tables 595

Step 3: Do Hands-On Practice 595

Step 4: Build Configuration Checklists 596

Step 5: Use the Exam Engine 596

Part VII Appendixes

Appendix A Answers to Chapter DIKTA Quizzes and Fill in the Blanks Questions 599

Appendix B CCNP Security 642-637 SECURE Exam Updates, Version 1.0 621

Index 622

Elements Available on CD

Appendix C Memory Tables

Appendix D Memory Table Answers

Glossary