



# Official Cert Guide

Learn, prepare, and practice for exam success



- ▶ Master **CCNP SECURE 642-637** exam topics
- ▶ Assess your knowledge with **chapter-opening quizzes**
- ▶ Review key concepts with **exam preparation tasks**
- ▶ Practice with **realistic exam questions** on the CD-ROM

# CCNP Security SECURE

## 642-637

# 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

<i>Control Plane</i>	43
<i>Data Plane</i>	44
<i>Management Plane</i>	45
Identifying Network Foundation Protection Deployment Models	45
Identifying Network Foundation Protection Feature Availability	48
<i>Cisco Catalyst Switches</i>	48
<i>Cisco Integrated Services Routers (ISR)</i>	49
<i>Cisco Supporting Management Components</i>	50
Exam Preparation	53

## **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 111
  - 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

<i>Task 6: Choose the Login Credentials to Be Used for Authentication</i>	132
<i>Task 7: Create the CSSC Installation Package</i>	133
<i>Network Login</i>	134
<i>Verify and Troubleshoot 802.1X Operations</i>	134
<i>Troubleshooting Flow</i>	134
<i>Successful Authentication</i>	135
<i>Verify Connection Status</i>	135
<i>Verify Authentication on AAA Server</i>	135
<i>Verify Guest/Restricted VLAN Assignment</i>	135
<i>802.1X Readiness Check</i>	135
<i>Unresponsive Supplicant</i>	135
<i>Failed Authentication: RADIUS Configuration Issues</i>	135
<i>Failed Authentication: Bad Credentials</i>	135
<i>Exam Preparation</i>	136

## **Chapter 7 Implementing and Configuring Advanced 802.1X 139**

<i>“Do I Know This Already?” Quiz</i>	139
<i>Foundation Topics</i>	143
<i>Plan the Deployment of Cisco Advanced 802.1X Authentication Features</i>	143
<i>Gathering Input Parameters</i>	143
<i>Deployment Tasks</i>	144
<i>Deployment Choices</i>	144
<i>Configure and Verify EAP-TLS Authentication on Cisco IOS Components and Cisco Secure ACS</i>	145
<i>EAP-TLS with 802.1X Configuration Tasks</i>	145
<i>Configuration Scenario</i>	146
<i>Configuration Choices</i>	146
<i>Task 1: Configure RADIUS Server</i>	147
<i>Task 2: Install Identity and Certificate Authority Certificates on All Clients</i>	147
<i>Task 3: Configure an Identity Certificate on the Cisco Secure ACS Server</i>	147
<i>Task 4: Configure Support of EAP-TLS on the Cisco Secure ACS Server</i>	149
<i>Task 5: (Optional) Configure EAP-TLS Support Using the Microsoft Windows Native Supplicant</i>	151
<i>Task 6: (Optional) Configure EAP-TLS Support Using the Cisco Secure Services Client (CSSC) Supplicant</i>	152

<i>Implementation Guidelines</i>	153
<i>Feature Support</i>	153
<i>Verifying EAP-TLS Configuration</i>	153
<i>Deploying User and Machine Authentication</i>	153
<i>Configuring User and Machine Authentication Tasks</i>	154
<i>Configuration Scenario</i>	154
<i>Task 1: Install Identity and Certificate Authority Certificates on All Clients</i>	155
<i>Task 2: Configure Support of EAP-TLS on Cisco Secure ACS Server</i>	155
<i>Task 3: Configure Support of Machine Authentication on Cisco Secure ACS Server</i>	156
<i>Task 4: Configure Support of Machine Authentication on Microsoft Windows Native 802.1X Supplicant</i>	156
<i>Task 5: (Optional) Configure Machine Authentication Support Using the Cisco Secure Services Client (CSSC) Supplicant</i>	157
<i>Task 6: (Optional) Configure Additional User Support Using the Cisco Secure Services Client (CSSC) Supplicant</i>	158
<i>Implementation Guidelines</i>	158
<i>Feature Support</i>	158
<i>Deploying VLAN and ACL Assignment</i>	159
<i>Deploying VLAN and ACL Assignment Tasks</i>	159
<i>Configuration Scenario</i>	159
<i>Configuration Choices</i>	160
<i>Task 1: Configure Cisco IOS Software 802.1X Authenticator Authorization</i>	160
<i>Task 2: (Optional) Configure VLAN Assignment on Cisco Secure ACS</i>	161
<i>Task 3: (Optional) Configure and Prepare for ACL Assignment on Cisco IOS Software Switch</i>	162
<i>Task 4: (Optional) Configure ACL Assignment on Cisco Secure ACS Server</i>	162
<i>Verification of VLAN and ACL Assignment with Cisco IOS Software CLI</i>	164
<i>Verification of VLAN and ACL Assignment on Cisco Secure ACS</i>	165
<i>Configure and Verify Cisco Secure ACS MAC Address Exception Policies</i>	165
<i>Cisco Catalyst IOS Software MAC Authentication Bypass (MAB)</i>	165

<i>Configuration Tasks</i>	166
<i>Configuration Scenario</i>	166
<i>Tasks 1 and 2: Configure MAC Authentication Bypass on the Switch and ACS</i>	167
<i>Verification of Configuration</i>	168
<i>Implementation Guidelines</i>	168
Configure and Verify Web Authentication on Cisco IOS Software LAN Switches and Cisco Secure ACS	168
<i>Configuration Tasks</i>	169
<i>Configuration Scenario</i>	169
<i>Task 1: Configure Web Authentication on the Switch</i>	169
<i>Task 2: Configure Web Authentication on the Cisco Secure ACS Server</i>	171
<i>Web Authentication Verification</i>	172
<i>User Experience</i>	172
Choose a Method to Support Multiple Hosts on a Single Port	172
<i>Multiple Hosts Support Guidelines</i>	172
<i>Configuring Support of Multiple Hosts on a Single Port</i>	172
Configuring Fail-Open Policies	174
<i>Configuring Critical Ports</i>	174
<i>Configuring Open Authentication</i>	176
Resolve 802.1X Compatibility Issues	176
<i>Wake-on-LAN (WOL)</i>	176
<i>Non-802.1X IP Phones</i>	177
<i>Preboot Execution Environment (PXE)</i>	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
<i>IP Spoofing</i>	186
<i>Slow-Path Denial of Service</i>	186
<i>Traffic Flooding</i>	187
Routed Data Plane Security Technologies	187
<i>Access Control Lists (ACL)</i>	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

**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

<i>PAT Example</i>	281
<i>NAT Configuration</i>	282
<i>Overlapping NAT</i>	287
<i>Exam Preparation</i>	290

## **Chapter 12 Implementing and Configuring Zone-Based Policy Firewalls 295**

“Do I Know This Already?” Quiz	295
Foundation Topics	298
<i>Zone-Based Policy Firewall Overview</i>	298
<i>Zones/Security Zones</i>	298
<i>Zone Pairs</i>	299
<i>Transparent Firewalls</i>	300
<i>Zone-Based Layer 3/4 Policy Firewall Configuration</i>	301
<i>Class Map Configuration</i>	302
<i>Parameter Map Configurations</i>	304
<i>Policy Map Configuration</i>	306
<i>Zone Configuration</i>	308
<i>Zone Pair Configuration</i>	309
<i>Port to Application Mapping (PAM) Configuration</i>	310
<i>Zone-Based Layer 7 Policy Firewall Configuration</i>	312
<i>URL Filter</i>	313
<i>HTTP Inspection</i>	318
<i>Exam Preparation</i>	323

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

“Do I Know This Already?” Quiz	333
Foundation Topics	336
<i>Configuration Choices, Basic Procedures, and Required Input Parameters</i>	336
<i>Intrusion Detection and Prevention with Signatures</i>	337
<i>Sensor Accuracy</i>	339
<i>Choosing a Cisco IOS IPS Sensor Platform</i>	340
<i>Software-Based Sensor</i>	340
<i>Hardware-Based Sensor</i>	340
<i>Deployment Tasks</i>	341
<i>Deployment Guidelines</i>	342
<i>Deploying Cisco IOS Software IPS Signature Policies</i>	342
<i>Configuration Tasks</i>	342

<i>Configuration Scenario</i>	342
<i>Verification</i>	346
<i>Guidelines</i>	347
Tuning Cisco IOS Software IPS Signatures	347
<i>Event Risk Rating System Overview</i>	348
<i>Event Risk Rating Calculation</i>	348
<i>Event Risk Rating Example</i>	349
<i>Signature Event Action Overrides (SEAO)</i>	349
<i>Signature Event Action Filters (SEAF)</i>	349
<i>Configuration Tasks</i>	350
<i>Configuration Scenario</i>	350
<i>Verification</i>	355
<i>Implementation Guidelines</i>	355
Deploying Cisco IOS Software IPS Signature Updates	355
<i>Configuration Tasks</i>	356
<i>Configuration Scenario</i>	356
<i>Task 1: Install Signature Update License</i>	356
<i>Task 2: Configure Automatic Signature Updates</i>	357
<i>Verification</i>	357
Monitoring Cisco IOS Software IPS Events	358
<i>Cisco IOS Software IPS Event Generation</i>	358
<i>Cisco IME Features</i>	358
<i>Cisco IME Minimum System Requirements</i>	359
<i>Configuration Tasks</i>	359
<i>Configuration Scenario</i>	360
<i>Task 2: Add the Cisco IOS Software IPS Sensor to Cisco IME</i>	361
<i>Verification</i>	362
<i>Verification: Local Events</i>	362
<i>Verification: IME Events</i>	363
Cisco IOS Software IPS Sensor	363
<i>Troubleshooting Resource Use</i>	365
<i>Additional Debug Commands</i>	365
Exam Preparation	366
<b>Chapter 14 Introduction to Cisco IOS Site-to-Site Security Solutions</b>	<b>369</b>
“Do I Know This Already?” Quiz	369
Foundation Topics	372
Choose an Appropriate VPN LAN Topology	372

<i>Input Parameters for Choosing the Best VPN LAN Topology</i>	373
<i>General Deployment Guidelines for Choosing the Best VPN LAN Topology</i>	373
Choose an Appropriate VPN WAN Technology	373
<i>Input Parameters for Choosing the Best VPN WAN Technology</i>	374
<i>General Deployment Guidelines for Choosing the Best VPN WAN Technology</i>	376
Core Features of IPsec VPN Technology	376
<i>IPsec Security Associations</i>	377
<i>Internet Key Exchange (IKE)</i>	377
<i>IPsec Phases</i>	377
<i>IKE Main and Aggressive Mode</i>	378
<i>Encapsulating Security Payload</i>	378
Choose Appropriate VPN Cryptographic Controls	379
<i>IPsec Security Associations</i>	379
<i>Algorithm Choices</i>	379
<i>General Deployment Guidelines for Choosing Cryptographic Controls for a Site-to-Site VPN Implementation</i>	381
<i>Design and Implementation Resources</i>	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
<i>Virtual Tunnel Interfaces</i>	390
<i>Input Parameters</i>	392
<i>Deployment Tasks</i>	393
<i>Deployment Choices</i>	393
<i>General Deployment Guidelines</i>	393
Configuring Basic IKE Peering	393
<i>Cisco IOS Software Default IKE PSK-Based Policies</i>	394
<i>Configuration Tasks</i>	394
<i>Configuration Choices</i>	395
<i>Configuration Scenario</i>	395
<i>Task 1: (Optional) Configure an IKE Policy on Each Peer</i>	395
<i>Tasks 2 and 3: Generate and Configure Authentication Credentials on Each Peer</i>	396
<i>Verify Local IKE Sessions</i>	396

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

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

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

<i>“Do I Know This Already?” Quiz</i>	411
<i>Foundation Topics</i>	414
<i>Describe the Concept of a Public Key Infrastructure</i>	414
<i>Manual Key Exchange with Verification</i>	414

<i>Trusted Introducing</i>	414
<i>Public Key Infrastructure: Certificate Authorities</i>	416
<i>X.509 Identity Certificate</i>	417
<i>Certificate Revocation Checking</i>	418
<i>Using Certificates in Network Applications</i>	419
<i>Deployment Choices</i>	420
<i>Deployment Steps</i>	420
<i>Input Parameters</i>	421
<i>Deployment Guidelines</i>	421
<i>Configure, Verify, and Troubleshoot a Basic Cisco IOS Software Certificate Server</i>	421
<i>Configuration Tasks for a Root Certificate Server</i>	422
<i>Configuration Scenario</i>	423
<i>Task 1: Create an RSA Key Pair</i>	423
<i>Task 2: Create a PKI Trustpoint</i>	424
<i>Tasks 3 and 4: Create the CS and Configure the Database Location</i>	424
<i>Task 5: Configure an Issuing Policy</i>	425
<i>Task 6: Configure the Revocation Policy</i>	425
<i>Task 7: Configure the SCEP Interface</i>	426
<i>Task 8: Enable the Certificate Server</i>	426
<i>Cisco Configuration Professional Support</i>	426
<i>Verify the Cisco IOS Software Certificate Server</i>	427
<i>Feature Support</i>	427
<i>Implementation Guidelines</i>	428
<i>Troubleshooting Flow</i>	429
<i>PKI and Time: Additional Guidelines</i>	429
<i>Enroll a Cisco IOS Software VPN Router into a PKI and Troubleshoot the Enrollment Process</i>	429
<i>PKI Client Features</i>	429
<i>Simple Certificate Enrollment Protocol</i>	430
<i>Key Storage</i>	430
<i>Configuration Tasks</i>	430
<i>Configuration Scenario</i>	431
<i>Task 1: Create an RSA Key Pair</i>	431
<i>Task 2: Create an RSA Key Pair</i>	432
<i>Task 3: Authenticate the PKI Certificate Authority</i>	432
<i>Task 4: Create an Enrollment Request on the VPN Router</i>	433

<i>Task 5: Issue the Client Certificate on the CA Server</i>	434
<i>Certificate Revocation on the Cisco IOS Software Certificate Server</i>	434
<i>Cisco Configuration Professional Support</i>	434
<i>Verify the CA and Identity Certificates</i>	435
<i>Feature Support</i>	435
<i>Implementation Guidelines</i>	436
<i>Troubleshooting Flow</i>	436
<i>Configure and Verify the Integration of a Cisco IOS Software VPN Router with Supporting PKI Entities</i>	436
<i>IKE Peer Authentication</i>	436
<i>IKE Peer Certificate Authorization</i>	437
<i>Configuration Tasks</i>	437
<i>Configuration Scenario</i>	437
<i>Task 1: Configure an IKE Policy</i>	438
<i>Task 2: Configure an ISAKMP Profile</i>	438
<i>Task 3: Configure Certificate-Based Authorization of Remote Peers</i>	438
<i>Verify IKE SA Establishment</i>	439
<i>Feature Support</i>	439
<i>Implementation Guidelines</i>	440
<i>Troubleshooting Flow</i>	440
<i>Configuring Advanced PKI Integration</i>	440
<i>Configuring CRL Handling on PKI Clients</i>	441
<i>Using OCSP or AAA on PKI Clients</i>	441
<i>Exam Preparation</i>	442

## **Chapter 17 Deploying DMVPNs 447**

<i>“Do I Know This Already?” Quiz</i>	447
<i>Foundation Topics</i>	451
<i>Understanding the Cisco IOS Software DMVPN Architecture</i>	451
<i>Building Blocks of DMVPNs</i>	452
<i>Hub-and-Spoke Versus On-Demand Fully Meshed VPNs</i>	452
<i>DMVPN Initial State</i>	453
<i>DMVPN Spoke-to-Spoke Tunnel Creation</i>	453
<i>DMVPN Benefits and Limitations</i>	454
<i>Plan the Deployment of a Cisco IOS Software DMVPN</i>	455
<i>Input Parameters</i>	455

<i>Deployment Tasks</i>	455
<i>Deployment Choices</i>	456
<i>General Deployment Guidelines</i>	456
<i>Configure and Verify Cisco IOS Software GRE Tunnels</i>	456
<i>GRE Features and Limitations</i>	456
<i>Point-to-Point Versus Point-to-Multipoint GRE Tunnels</i>	457
<i>Point-to-Point Tunnel Configuration Example</i>	457
<i>Configuration Tasks for a Hub-and-Spoke Network</i>	459
<i>Configuration Scenario</i>	459
<i>Task 1: Configure an mGRE Interface on the Hub</i>	459
<i>Task 2: Configure a GRE Interface on the Spoke</i>	459
<i>Verify the State of GRE Tunnels</i>	460
<i>Configure and Verify a Cisco IOS Software NHRP Client and Server</i>	461
<i>(m)GRE and NHRP Integration</i>	461
<i>Configuration Tasks</i>	461
<i>Configuration Scenario</i>	461
<i>Task 1: Configure an NHRP Server</i>	461
<i>Task 2: Configure an NHRP Client</i>	462
<i>Verify NHRP Mappings</i>	462
<i>Debugging NHRP</i>	463
<i>Configure and Verify a Cisco IOS Software DMVPN Hub</i>	464
<i>Configuration Tasks</i>	464
<i>Configuration Scenario</i>	464
<i>Task 1: (Optional) Configure an IKE Policy</i>	464
<i>Task 2: Generate and/or Configure Authentication Credentials</i>	465
<i>Task 3: Configure an IPsec Profile</i>	465
<i>Task 4: Create an mGRE Tunnel Interface</i>	465
<i>Task 5: Configure the NHRP Server</i>	465
<i>Task 6: Associate the IPsec Profile with the mGRE Interface</i>	466
<i>Task 7: Configure IP Parameters on the mGRE Interface</i>	466
<i>Cisco Configuration Professional Support</i>	466
<i>Verify Spoke Registration</i>	466
<i>Verify Registered Spoke Details</i>	467
<i>Implementation Guidelines</i>	468
<i>Feature Support</i>	468
<i>Configure and Verify a Cisco IOS Software DMVPN Spoke</i>	468

<i>Configuration Tasks</i>	468
<i>Configuration Scenario</i>	469
<i>Task 1: (Optional) Configure an IKE Policy</i>	469
<i>Task 2: Generate and/or Configure Authentication Credentials</i>	469
<i>Task 3: Configure an IPsec Profile</i>	469
<i>Task 4: Create an mGRE Tunnel Interface</i>	470
<i>Task 5: Configure the NHRP Client</i>	470
<i>Task 6: Associate the IPsec Profile with the mGRE Interface</i>	470
<i>Task 7: Configure IP Parameters on the mGRE Interface</i>	471
<i>Verify Tunnel State and Traffic Statistics</i>	471
Configure and Verify Dynamic Routing in a Cisco IOS Software DMVPN	471
<i>EIGRP Hub Configuration</i>	472
<i>OSPF Hub Configuration</i>	473
<i>Hub-and-Spoke Routing and IKE Peering on Spoke</i>	473
<i>Full Mesh Routing and IKE Peering on Spoke</i>	474
Troubleshoot a Cisco IOS Software DMVPN	474
<i>Troubleshooting Flow</i>	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
<i>VPN Failure Modes</i>	484
<i>Partial Failure of the Transport Network</i>	484
<i>Partial or Total Failure of the Service Provider (SP) Transport Network</i>	485
<i>Partial or Total Failure of a VPN Device</i>	485
<i>Deployment Guidelines</i>	485
Use Routing Protocols for VPN Failover	486
<i>Routing to VPN Tunnel Endpoints</i>	486
<i>Routing Protocol Inside the VPN Tunnel</i>	486
<i>Recursive Routing Hazard</i>	487
<i>Routing Protocol VPN Topologies</i>	487
<i>Routing Tuning for Path Selection</i>	487
<i>Routing Tuning for Faster Convergence</i>	488

Choose the Most Optimal Method of Mitigating Failure in a VTI-Based VPN	488
<i>Path Redundancy Using a Single-Transport Network</i>	489
<i>Path Redundancy Using Two Transport Networks</i>	489
<i>Path and Device Redundancy in Single-Transport Networks</i>	489
<i>Path and Device Redundancy with Multiple-Transport Networks</i>	489
Choose the Most Optimal Method of Mitigating Failure in a DMVPN	490
<i>Recommended Architecture</i>	490
<i>Shared IPsec SAs</i>	490
<i>Configuring a DMVPN with a Single-Transport Network</i>	490
<i>Configuring a DMVPN over Multiple-Transport Networks</i>	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
<i>Peer Authentication and Policy Provisioning</i>	502
<i>GET VPN Traffic Exchange</i>	504
<i>Packet Security Services</i>	504
<i>Key Management Architecture</i>	505
<i>Rekeying Methods</i>	505
<i>Traffic Encapsulation</i>	507
<i>Benefits and Limitations</i>	507
Plan the Deployment of a Cisco IOS Software GET VPN	508
<i>Input Parameters</i>	508
<i>Deployment Tasks</i>	508
<i>Deployment Choices</i>	509
<i>Deployment Guidelines</i>	509
Configure and Verify a Cisco IOS Software GET VPN Key Server	509
<i>Configuration Tasks</i>	509
<i>Configuration Choices</i>	510
<i>Configuration Scenario</i>	510
<i>Task 1: (Optional) Configure an IKE Policy</i>	511
<i>Task 2: Generate and/or Configure Authentication Credentials</i>	511
<i>Task 3: Generate RSA keys for Rekey Authentication</i>	511

<i>Task 4: Configure a Traffic Protection Policy on the Key Server</i>	512
<i>Task 5: Enable and Configure the GET VPN Key Server Function</i>	512
<i>Task 6: (Optional) Tune the Rekeying Policy</i>	513
<i>Task 7: Create and Apply the GET VPN Crypto Map</i>	513
<i>Cisco Configuration Professional Support</i>	514
<i>Verify Basic Key Server Settings</i>	514
<i>Verify the Rekey Policy</i>	514
<i>List All Registered Members</i>	515
<i>Implementation Guidelines</i>	515
<i>Configure and Verify Cisco IOS Software GET VPN Group Members</i>	515
<i>Configuration Tasks</i>	516
<i>Configuration Choices</i>	516
<i>Configuration Scenario</i>	516
<i>Task 1: Configure an IKE Policy</i>	516
<i>Task 2: Generate and/or Configure Authentication Credentials</i>	517
<i>Task 3: Enable the GET VPN Group Member Function</i>	518
<i>Task 4: Create and Apply the GET VPN Crypto Map</i>	518
<i>Task 5: (Optional) Configure a Fail-Closed Policy</i>	518
<i>Cisco Configuration Professional Support</i>	519
<i>Verify Registration of the Group Member</i>	519
<i>Implementation Guidelines</i>	519
<i>Troubleshooting Flow</i>	519
<i>Configure and Verify High-Availability Mechanisms in a GET VPN</i>	520
<i>Network Splits and Network Merges</i>	521
<i>Configuration Tasks</i>	521
<i>Configuration Scenario</i>	521
<i>Task 1: Distribute the Rekey RSA Key Pair</i>	522
<i>Task 2: Configure a Full Mesh of Key Server IKE Peering</i>	522
<i>Task 3: Configure COOP</i>	522
<i>Tasks 4 and 5: Configure Traffic Protection Policy and Multiple Key Servers on Group Members</i>	523
<i>Verify IKE Peering</i>	523
<i>Verify COOP Peering</i>	523

*Implementation Guidelines* 524

*Troubleshooting Flow* 524

*Exam Preparation* 525

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

<i>Task 5: (Optional) Configure Gateway High Availability</i>	545
<i>Gateway Verification</i>	545
<i>Implementation Guidelines</i>	546
Configure and Verify Client Authentication and Policies on the SSL VPN Gateway	546
<i>Gateway, Contexts, and Policy Groups</i>	546
<i>Basic User Authentication Overview</i>	546
<i>Configuration Tasks</i>	547
<i>Configuration Scenario</i>	547
<i>Task 1: Create and Apply a Default Policy</i>	548
<i>Task 2: Enable User Authentication Using Local AAA</i>	548
<i>Implementation Guidelines</i>	548
Configure and Verify Full Tunneling Connectivity on the Cisco IOS SSL VPN Gateway	549
<i>Configuration Tasks</i>	549
<i>Configuration Scenario</i>	549
<i>Task 1: Enable Full Tunneling Access</i>	549
<i>Task 2: Configure Local IP Address Assignment</i>	550
<i>Task 3: (Optional) Configure Client Configuration</i>	551
<i>Task 4: (Optional) Configure Split Tunneling</i>	551
<i>Task 5: (Optional) Configure Access Control</i>	551
<i>Cisco Configuration Professional Support</i>	552
Install and Configure the Cisco AnyConnect Client	552
<i>AnyConnect 2.4–Supported Platforms</i>	553
<i>Configuration Tasks</i>	553
<i>Configuration Scenario</i>	553
<i>Task 1: Enable Full Tunneling Access</i>	553
<i>Task 2: Verify Server Certificate Authentication Chain</i>	554
<i>Task 3: Configure Basic AnyConnect Profile Settings</i>	554
<i>Task 4: Establish the SSL VPN Connection</i>	554
<i>Client-Side Verification</i>	554
<i>Gateway-Side Verification</i>	555
<i>Cisco Configuration Professional</i>	556
Configure and Verify Clientless Access on the Cisco IOS SSL VPN Gateway	556
<i>Basic Portal Features</i>	556
<i>Cisco Secure Desktop for Clientless Access</i>	557
<i>Port Forwarding Overview</i>	557

<i>Port Forwarding Benefits and Limitations</i>	558
<i>Portal ACLs</i>	558
<i>Configuration Tasks</i>	558
<i>Configuration Scenario</i>	559
<i>Task 1: Enable Full Tunneling Access</i>	560
<i>Task 2: (Optional) Configure Port Forwarding</i>	560
<i>Task 3: (Optional) Configure Cisco Secure Desktop</i>	561
<i>Task 4: (Optional) Configure Access Control</i>	561
<i>Basic Portal Verification</i>	562
<i>Web Application Access</i>	562
<i>File Server Access</i>	562
<i>Port Forwarding Access</i>	562
<i>Cisco Secure Desktop Verification</i>	563
<i>Gateway-Side Verification</i>	563
<i>Troubleshoot the Basic SSL VPN Operation</i>	563
<i>Port Forwarding Access</i>	563
<i>Troubleshooting Flow (VPN Establishment)</i>	563
<i>Troubleshooting Flow (Data Flow)</i>	563
<i>Gateway-Side Issue</i>	564
<i>Client-Side Issues: Certificates</i>	564
<i>Exam Preparation</i>	565

## **Chapter 21 Deploying Remote Access Solutions Using EZVPNs 569**

<i>“Do I Know This Already?” Quiz</i>	569
<i>Foundation Topics</i>	572
<i>Plan the Deployment of a Cisco IOS Software EZVPN</i>	572
<i>Solution Components</i>	573
<i>Deployment Tasks</i>	573
<i>Input Parameters</i>	574
<i>Deployment Guidelines</i>	574
<i>Configure and Verify a Basic Cisco IOS Software VTI-Based EZVPN Server</i>	575
<i>Group Pre-Shared Key Authentication</i>	575
<i>Extended Authentication (XAUTH) Overview</i>	575
<i>Configuration Groups and ISAKMP Profiles</i>	576
<i>Configuration Tasks</i>	576
<i>Configuration Scenario</i>	576
<i>Task 1: (Optional) Verify an IKE Policy</i>	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

## **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

**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**