CCIE Security v4.0
Practice Labs

Natalie Timms, CCIE No. 37959

Cisco Press
800 East 96th Street
Indianapolis, IN 46240
Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger
Associate Publisher: Dave Dusthimer
Acquisition Editor: Denise Lincoln
Senior Project Editor: Tonya Simpson
Proofreader: Paula Lowell
Cover Designer: Mark Shirar

Business Operation Manager, Cisco Press: Jan Cornelssen
Senior Development Editor: Christopher Cleveland
Managing Editor: Sandra Schroeder
Technical Editors: Tim Rowley, Tyson Scott
Editorial Assistant: Vanessa Evans
Composition: Mary Sudul

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.
About the Author

Natalie Timms, CCIE No. 37959, is a former program manager with the CCIE certification team at Cisco, managing exam curricula and content for the CCIE Security track before becoming an independent consultant.

Natalie has been involved with computer networking for more than 20 years, much of which was spent with Cisco. Natalie has contributed at the IETF standards level and has written many technical papers, and is also a Cisco Press author and U.S. patent holder.

Natalie has also been a technical instructor in the Asia-Pacific region for Wellfleet Communications/Bay Networks, and is the winner of multiple Cisco Live Distinguished Speaker awards.

Natalie has a CCIE Security certification and a bachelor’s degree in computer science and statistics from Macquarie University in Sydney, Australia.
About the Technical Reviewers

Tim Rowley, CCIE No. 25960 (Security/Wireless), CWNE No. 124, CCSI No. 33858, CISSP, is a consultant within the Cisco Global Security Services. He is responsible for design, implementation, and support of customer networks with a focus on network security and wireless. Tim regularly contributes to the development of certification exams and the related training material, including CCNA, CCNP, and CCIE security and wireless. He has a passion for technical development and enjoys helping others achieve their certification goals.

Tyson Scott, Triple CCIE No. 13513, is a consulting systems engineer for Cisco Systems with more than 14 years in the IT industry. He has traveled the globe delivering learning solutions to the Cisco certification community, specializing in CCIE Security and CCIE Routing and Switching. Today, he helps to deliver leading security solutions in the state, local government, and education verticals.
Dedication

I have been so very fortunate to be surrounded by people who have always encouraged me to march to the beat of my own drum. To my husband, Randy, I give my love and gratitude for letting me be me; never being in my face yet always being there. To my parents, Helen and Denis, thank you for putting up with my craziness and patiently waiting for me to find my niche in life. I am Russian passion tempered with an Aussie sense of humor. And to my brother, Mick, you have always been the “little” brother I looked up to both in stature and knowing who you wanted to be.

Finally, this book is also dedicated to all those who strive to be the best they can be.

Acknowledgments

I would like to thank the folks at Cisco Press, Denise Lincoln and Brett Bartow, for inviting me to contribute, and Chris Cleveland, for wading through pages of edits and not imploding.

To my technical editors, Tyson Scott and Tim Rowley, I appreciate all you have done to help me complete this book. You guys are network rock stars and I bow at your feet.

I need to acknowledge Scott Fanning, who for so many years was my partner in crime at Cisco. Scott, you helped foster my love for security technologies, all-night coding sessions, Tim Hortons Coffee, and ice hockey. I'm so proud of all you have achieved.

So many others have helped and supported me over the years, and kicked my ass when required; it is impossible to list everyone who has made an impact in my life. I hope I can pay it forward.

Sometimes, inspiration comes in the most unexpected way, even a Cake Pop.
## Contents at a Glance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>xxiii</td>
</tr>
<tr>
<td><strong>Part I</strong> Lab Topology Components, Cabling, and Routing and Switching Configuration</td>
<td>1</td>
</tr>
<tr>
<td><strong>Part II</strong> Practice Lab 1</td>
<td></td>
</tr>
<tr>
<td>Practice Lab 1</td>
<td>19</td>
</tr>
<tr>
<td>Practice Lab 1 Solutions</td>
<td>51</td>
</tr>
<tr>
<td><strong>Part III</strong> Practice Lab 2</td>
<td></td>
</tr>
<tr>
<td>Practice Lab 2</td>
<td>205</td>
</tr>
<tr>
<td>Practice Lab 2 Solutions</td>
<td>233</td>
</tr>
<tr>
<td><strong>Part IV</strong> Appendices</td>
<td></td>
</tr>
<tr>
<td>Manual Configuration Guide</td>
<td>401</td>
</tr>
<tr>
<td>Preparing for the CCIE Exam</td>
<td>411</td>
</tr>
<tr>
<td>Sample Written Exam Questions and Answers</td>
<td>417</td>
</tr>
</tbody>
</table>
Contents

Introduction  xxiii

Part I  Lab Topology Components, Cabling, and Routing and Switching Configuration  1

Equipment List  2
General Guidelines  4
Prelab Setup Instructions  5
  Catalyst Switchport Cabling Diagram  5
  Lab Topology Diagram  7
  Lab Guide Addressing Scheme  8
  Lab Guide IP Routing Details  11
  VPN Solutions Diagrams  15
  Initial Device Configurations  18
Final Configuration Files  18
CCIE Security Exam Study and Preparation Tips  18
  CCIE Security Written Exam  18

Part II  Practice Lab 1  19

Section 1  Perimeter Security and Services  19
Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode  19
  Notes  21
Exercise 1.2: Configure Routing and Basic Access on ASA2  21
  Notes  22
Exercise 1.3: Configure IP Services on ASA1  22
  Task 1: Configure Network Object NAT  23
  Task 2: Configure Twice NAT  23
  Task 3: Configure and Troubleshoot NTP Services Using Authentication  23
  Task 4: Configure Support for IPv6 in IPv4 Tunneling Through ASA1  23
Exercise 1.4: Configure IP Routing Security on ASA2  23
  Task 1: BGP Connectivity Through the ASA2  24
  Task 2: OSPF Authentication for Routing Update Security  24

Section 2  Intrusion Prevention and Content Security  25
Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance  25
  Task 1: Initialize the Cisco IPS Sensor  25
  Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode  26
Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode 27
Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode 27
Exercise 2.2: Initialize the Cisco WSA 27
Exercise 2.3: Enable Web Content Features on the Cisco WSA 29
  Task 1: Configure WCCPv2 Proxy Support on the WSA (Client) and ASA1 (Server) 29
  Task 2: Configure Proxy Bypass on the WSA 30
  Task 3: Create a Custom URL Access Policy on the WSA 30

Section 3  Secure Access  30
Exercise 3.1: Configure and Troubleshoot IPsec EZVPN 30
Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3 32
Exercise 3.3: Configure Security Features on the Cisco WLC 33
  Task 1: Initialize the WLC and Establish Control over the Cisco Access Points (AP) 33
  Task 2: Enable IP Services on the WLC to Enhance Security 35
  Task 3: Creating and Assigning Security Policy to WLANs and Users 35
Exercise 3.4: Configure the Cisco IOS Certificate Server 36

Section 4  System Hardening and Availability 37
Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch 37
Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in Cisco IOS 38
Exercise 4.3: Configure Control Plane Policing (CoPP) 39
Exercise 4.4: Troubleshoot Management Plane Protection 39
Exercise 4.5: Device Hardening on the Cisco WLC 40
  Task 1: Disable SSID Broadcasting 40
  Task 2: Protect the WLC Against Associating with a Rogue AP 40
  Task 3: Enable Infrastructure Management Frame Protection on the WLC 40
  Task 4: Enable Encryption for CAPWAP Packets 40
  Task 5: Create a Rate Limiting Policy for Guest Users on the Guest WLAN 40

Section 5  Threat Identification and Mitigation  41
Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel 41
Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch 41
Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching 42
Exercise 5.4: Application Protocol Protection 43
Section 6: Identity Management  43
Exercise 6.1: Configure Router Command Authorization and Access Control  43
Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+  45
Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs  45
   Exercise 6.3a: Authentication and Authorization Using MAB  45
   Exercise 6.3b: Authentication and Authorization Using 802.1X  47

Part II  Practice Lab 1 Solutions  51

Section 1  Perimeter Security and Services  51
Solution and Verification for Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode  51
   Skills Tested  51
   Solution and Verification  52
      Basic Parameters  52
      Admin Context Parameters  53
      Context c1 Parameters  54
      Context c2 Parameters  56
   ASA1 Configuration  57
   Tech Notes  60
Solution and Verification for Exercise 1.2: Configure Routing and Basic Access on ASA2  62
   Skills Tested  62
   Solution and Verification  62
      Configuration  66
   Tech Notes  67
Solution and Verification for Exercise 1.3: Configure IP Services on ASA1  68
   Skills Tested  68
   Solution and Verification  68
      Task 1: Network Object NAT  69
      Task 2: Twice NAT  69
      Task 3: NTP with Authentication  70
      Task 4: Tunneling ipv6ip  71
   Configuration  71
   Tech Notes  72
Solution and Verification for Exercise 1.4: Configure IP Routing Security on ASA2 77
Skills Tested 77
Solution and Verification 77

Task 1: BGP Connectivity Through ASA2 77
Task 2: OSPF Authentication for Routing Update Security 78

Configuration 79
Tech Notes 80

Section 2 Intrusion Prevention and Content Security 80

Solution and Verification for Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance 80
Skills Tested 80
Solution and Verification 81

Task 1: Initialize the Cisco IPS 81
Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode 82
Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode 83
Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode 83

Configuration 84
Tech Notes 85

Solution and Verification for Exercise 2.2: Initialize the Cisco WSA 86
Skills Tested 86
Solution and Verification 86
Tech Notes 88

Solution and Verification for Exercise 2.3: Enable Web Content Features on the Cisco WSA 89
Skills Tested 89
Solution and Verification 89

Task 1: Configure WCCPv2 Proxy Support on the Cisco WSA (Client) and the Cisco ASA (Server) 90
Task 2: Configure Proxy Bypass on the Cisco WSA 91
Task 3: Create a Custom URL Access Policy on the Cisco WSA 92

Configuration 92
Tech Notes 92

WCCP Support Across Cisco Products 92
Transparent Proxy Versus Explicit Proxy 92
Connection Assignment and Redirection 93
Service Groups 94
Section 3  Secure Access  95

Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec EZVPN  95
Skills Tested  95
Solution and Verification  95
Configuration  100
Tech Notes  101

Initiating the EZVPN Tunnel  101
Split Tunnel Options  101

EZVPN Client Modes of Operation in Cisco IOS  102
Client U-Turn Versus IPsec Hairpinning  102
External Versus Internal Policy  102

Solution and Verification for Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3  103
Skills Tested  103
Solution and Verification  103

NHRP Spoke Registration  104
Spoke-to-Spoke Connection from R4 to R3  108
Verification  113
Configuration  121
Tech Notes  123

DMVPNv1  123
DMVPNv2  124
DMVPNv3  125

Solution and Verification for Exercise 3.3: Configure Security Features on the Cisco WLC  127
Task 1: Initialize the Cisco WLC and Establish Control over the Cisco Access Points  127
Task 2: Enable IP Services on the Cisco WLC to Enhance Security  128
Task 3: Creating and Assigning Security Policy to WLANs and Users  129

Configuration  132

Solution and Verification for Exercise 3.4: Configure the Cisco IOS Certificate Server  132
Skills Tested  132
Solution and Verification  133
Configuration  135
Tech Notes  135
Section 4  System Hardening and Availability  136

Solution and Verification for Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch  136
  Skills Tested  136
  Solution and Verification  136
  Configuration  138
  Tech Notes  138
  SPAN Versus RSPAN  138
  SPAN and RSPAN Terminology and Guidelines  138
  VLAN-Based SPAN  139

Solution and Verification for Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in Cisco IOS  140
  Skills Tested  140
  Solution and Verification  140
  Configuration  143
  Tech Notes  144

Solution and Verification for Exercise 4.3: Configure Control Plane Policing (CoPP)  145
  Skills Tested  145
  Solution and Verification  145
  Verification  146
  Configuration  150
  Tech Notes  151
  Router Planes  151
  CoPP Versus CPPr  152

Solution and Verification for Exercise 4.4: Troubleshoot Management Plane Protection  153
  Skills Tested  153
  Solution and Verification  153
  Configuration  154

Solution and Verification for Exercise 4.5: Device Hardening on the Cisco WLC  154
  Skills Tested  154
  Solution and Verification  154
  Task 1: Disable SSID Broadcasting  155
  Task 2: Protect the WLC Against Associating with a Rogue AP  155
  Task 3: Enable Infrastructure Management Frame Protection on the Cisco WLC  156
Task 4: Enable Encryption for CAPWAP Packets  157
Task 5: Create a Rate Limiting Policy for Guest Users on the Guest WLAN  157
Configuration  158
Tech Notes  159
Summary of Wireless Attacks  159
Management Frame Protection via 802.11w  160

Section 5  Threat Identification and Mitigation  160
Solution and Verification for Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel  161
Skills Tested  161
Solution and Verification  161
Configuration  163
Solution and Verification for Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch  164
Skills Tested  164
Solution and Verification  164
Configuration  166
Tech Notes  166
DHCP Implementation Notes  167
DHCP Option 82  167
DHCP Snooping and the DHCP Server on Cisco IOS Routers  168
Solution and Verification for Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching  169
Skills Tested  169
Solution and Verification  169
Configuration  171
Solution and Verification for Exercise 5.4: Application Protocol Protection  171
Skills Tested  171
Solution and Verification  171
Configuration  173

Section 6  Identity Management  174
Solution and Verification for Exercise 6.1: Configure Router Command Authorization and Access Control  174
Skills Tested  174
Solution and Verification 174
ACS Solution 177
Configuration 183
Tech Notes 184
Tracing the Command Authorization Process 184
Understanding AAA and Login on the Router Lines 186
Test AAA Commands 188
AAA Accounting 189
Solution and Verification for Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+ 189
Skills Tested 189
Solution and Verification 189
CiscoSecure ACS Configuration 190
Configuration 193
Tech Notes 193
Solution and Verification for Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs 193
Skills Tested 193
Verification: Part A 195
Verification: Part B 196
Configuration 197
Cisco ISE Configuration 198
Tech Notes 203

Part III Practice Lab 2 205
Section 1 Perimeter Security 205
Exercise 1.1: Configure a Redundant Interface on ASA2 205
Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1 206
Exercise 1.3: Configuring Advanced Network Protection on the ASA 206
  Task 1: Botnet Traffic Filtering on ASA1 206
  Task 2: Threat Detection on ASA2 207
  Task 3: IP Audit on ASA1 207
Exercise 1.4: Configure IPv6 on ASA2 207
Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging 208
Section 2  Intrusion Prevention and Content Security  209
Exercise 2.1: Configuring Custom Signatures on the Cisco IPS Sensor  209
  Custom Signature to Track OSPF TTL  209
  Custom Signature to Identify and Deny Large ICMP Packets  210
  Custom Signature to Identify and Deny an ICMP Flood Attack  210
Exercise 2.2: Enable Support for HTTPS on the Cisco WSA  211
Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP  212
Exercise 2.4: Guest User Support on the Cisco WSA  213

Section 3  Secure Access  214
Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6  214
Exercise 3.2: Troubleshoot and Configure GETVPN  216
Exercise 3.3: SSL Client and Clientless VPNs  218
Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes  219
Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access (Client to Server)  221

Section 4  System Hardening and Availability  222
Exercise 4.1: BGP TTL-Security Through the Cisco ASA  222
Exercise 4.2: Configure and Troubleshoot Control Plane Protection  223
Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS  223

Section 5  Threat Identification and Mitigation  223
Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA  223
Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks  224
Exercise 5.3: Identifying and Protecting Against SYN Attacks  224
Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow  225

Section 6  Identity Management  226
Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB  227
  Part A: Configuring SGTs on the Cisco ISE  227
  Part B: Dynamically Assigning SGTs via 802.1X and MAB  227
  Task 1: Cisco Access Point as an 802.1X Supplicant with SGTs  227
  Task 2: Cisco IP Phone Using MAB and SGTs  228
  Part C: Create the SGA Egress Policy  229
Exercise 6.2: Cisco TrustSec—NDAC and MACsec 230
Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP 231

Part III Practice Lab 2 Solutions 233

Section 1 Perimeter Security 233

Solution and Verification for Exercise 1.1: Configure a Redundant Interface on ASA2 233
Skills Tested 233
Solution and Verification 233
Configuration 236

Solution and Verification for Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1 236
Skills Tested 236
Solution and Verification 236
Configuration 239
Tech Notes 240

Solution and Verification for Exercise 1.3: Configuring Advanced Network Protection on the ASA 240
Skills Tested 240
Solution and Verification 241
Task 1: Botnet Traffic Filtering on ASA1 241
Task 2: Threat Detection on ASA2 243
Task 3: IP Audit 243
Configuration 244
Tech Notes 245

Solution and Verification for Exercise 1.4: Configure IPv6 on ASA2 246
Skills Tested 246
Solution and Verification 246
Configuration 248
Tech Notes 248
IPv6 Addressing Review 248
IPv6 Addressing Notation 249
IPv6 Address Types 249
IPv6 Address Allocation 251
IPv6 Addressing Standards 251

Solution and Verification for Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging 252
Skills Tested 252
Section 2  Intrusion Prevention and Content Security  263

Solution and Verification for Exercise 2.1: Configuring Custom Signatures on the Cisco IPS Sensor  263
Skills Tested  263
Solution and Verification  263
  Custom Signature to Track OSPF TTL  264
  Custom Signature to Identify and Deny Large ICMP Packets  265
  Custom Signature to Identify and Deny an ICMP Flood Attack  266
Configuration  268
Tech Notes  270
  Risk Ratings  270
  Understanding Threat Rating  271

Solution and Verification for Exercise 2.2: Enable Support for HTTPS on the Cisco WSA  272
Skills Tested  272
Solution and Verification  272

Configuration  274

Solution and Verification for Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP  274
Skills Tested  274
Solution and Verification  274

Solution and Verification for Exercise 2.4: Guest User Support on the Cisco WSA  278
Skills Tested  278
Solution and Verification  278

WSA Configuration  279

Section 3  Secure Access  280

Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6  280
Skills Tested  280
Solution and Verification  280

Configuration  286
Tech Notes 289
Tip and Tricks 289
Static VTIs for IPv6 Using Preshared Keys 289

Solution and Verification for Exercise 3.2: Troubleshoot and Configure GETVPN 290
Skills Tested 290
Solution and Verification 290
Verify Network Connectivity 292
Configure and Verify the COOP Key Servers 293
Configure and Verify the Group Members 298
Configure and Verify DPD and Authorization 302
Configuration 303
Tech Notes 308
Key Server Design Considerations for IKE 308
Key Server Design Considerations for IPsec 309
Key Server Design Considerations for Traffic Encryption Key Lifetime 309
Key Server Design Considerations for ACLs in a Traffic Encryption Policy 310
Key Server Design Considerations for Key Encryption Key Lifetime 311
Rekey Retransmit Interval 311
Time-Based Antireplay 311
Key Server Design Considerations for Authentication Policies for GM Registration 312
Implementing Rekeying Mechanisms 312
Unicast Rekeying 313
Implementing Multicast Rekeying with No ASA Considerations 313
Implementing Multicast Rekeying Through the ASA in Routed Mode 314

Solution and Verification for Exercise 3.3: SSL Client and Clientless VPNs 315
Skills Tested 315
Solution and Verification 315
Configuration 321
Tech Notes 323
Importing Third-Party Trusted CA Certificates 323
Default Group Policy and Attribute Inheritance 328
Solution and Verification for Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes 328
Skills Tested 328
Solution and Verification 328
Configuration 332
Tech Notes 334
IKEv2 Smart Defaults 334
IKEv2 Anti-Clogging Cookie 334
RADIUS Tunnel Attributes and IKEv2 335

Solution and Verification for Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access (Client to Server) 337
Skills Tested 337
Solution and Verification 337
Configuration 341
Tech Notes 343
Debugging FlexVPN 343
Understanding IKEv2 Routing Options 348

Section 4 System Hardening and Availability 349

Solution and Verification for Exercise 4.1: BGP TTL-Security through the Cisco ASA 349
Skills Tested 349
Solution and Verification 349
Configuration 351
Tech Notes 351

Solution and Verification for Exercise 4.2: Configure and Troubleshoot Control Plane Protection 352
Skills Tested 352
Solution and Verification 352
Configuration 354
Tech Notes 354

Solution and Verification for Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS 354
Skills Tested 354
Solution and Verification 355
Configuration 356
Section 5  Threat Identification and Mitigation  357

Solution and Verification for Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA  357
Skills Tested  357
Solution and Verification  357
Configuration  358
Tech Notes  359

Understanding Unicast Reverse Path Forwarding in Cisco IOS: Technology Overview  359

Understanding Unicast Reverse Path Forwarding: Deployment Guidelines  359

Understanding Unicast Reverse Path Forwarding: Other Guidelines  360

Solution and Verification for Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks  361
Skills Tested  361
Solution and Verification  361
Configuration  362

Solution and Verification for Exercise 5.3: Identifying and Protecting Against SYN Attacks  362
Skills Tested  362
Solution and Verification  362
Configuration  363
Tech Notes  364

Configuring Maximum Connections  364

TCP Intercept and Limiting Embryonic Connections  364

Solution and Verification for Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow  365
Skills Tested  365
Solution and Verification  365
Configuration  369
Tech Notes  370

Configuring a NetFlow Exporter  370
Comparing NetFlow Types  370
Migrating from Traditional Netflow to Flexible Netflow  371
Section 6  Identity Management  372
Solution and Verification for Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB  372
Skills Tested  372
Solution and Verification  372
Part A: Configuring SGTs on the Cisco ISE  373
Part B: Dynamically Assigning SGT’s via 802.1X and MAB  374
Part C: Create the SGA Egress Policy  376
Configuration  377
Tech Notes  378
IP Device Tracking  378
Solution and Verification for Exercise 6.2: Cisco TrustSec—NDAC and MACsec  378
Skills Tested  378
Solution and Verification  378
Configuration  389
Tech Notes  390
Protected Access Credential  390
MACsec Overview  391
Solution and Verification for Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP  393
Skills Tested  393
Solution and Verification  393
Configuration  398
Tech Notes  399
SXP on the Cisco WLC  399
Summary of Secure Group Access Features  400

Part IV  Appendices
Appendix A  Manual Configuration Guide  401
Cisco Catalyst Switches: SW1, SW2  401
Cisco Routers R1, R2, R3, R4, R5, R6, R7  402
Cisco Router R6: Also Used as the CME Server  403
Cisco ASA Appliances ASA1, ASA2  403
Cisco WLC  405
Cisco IPS Sensor  406
Cisco WSA  407
Appendix B  Preparing for the CCIE Exam  411
CCIE Certification Process  411
CCIE Security Written Exam  411
CCIE Security Lab Exam  412
Planning Resources  413
Assessing Strengths and Weaknesses  414
Training, Practice Labs, and Boot Camps  414
Books and Online Materials  414
Lab Preparation  415
Lab Exam Tips  415
A Word on Cheating...  416

Appendix C  Sample Written Exam Questions and Answers  417
Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (`|`) separate alternative, mutually exclusive elements.

- Square brackets (`[ ]`) indicate an optional element.

- Braces (`{ }`) indicate a required choice.

- Braces within brackets (`{{ }}`) indicate a required choice within an optional element.

Introduction

For more than ten years, the CCIE program has identified networking professionals with the highest level of expertise. Fewer than 3 percent of all Cisco certified professionals actually achieve CCIE status. The majority of candidates who take the exam fail at the first attempt because they are not fully prepared; they generally find that their study plan did not match what was expected of them in the exam. These practice exercises are indicative of the types of questions you can expect in an actual exam. Completion of these exercises with a solid understanding of the solutions will be an indication of whether you are ready to schedule your lab or you need to reevaluate your study plan.

Exam Overview

The CCIE qualification consists of two separate exams, a two-hour written exam and an eight-hour hands-on lab exam that includes troubleshooting questions. Written exams are computer-based multiple-choice exams lasting two hours and available at hundreds of authorized testing centers worldwide. The written exam is designed to test your theoretical knowledge to ensure you are ready to take the lab exam; as such, you are eligible to schedule the lab exam only after you have passed the written exam. Having purchased this publication, it is assumed that you have passed the written exam and are ready to practice for the lab exam. The lab exam is an eight-hour hands-on exam in which you are required to configure a series of complex scenarios in strict accordance to the questions—it’s tough but achievable. Current exam blueprint content information can be found at the following URL:

https://learningnetwork.cisco.com/community/certifications/ccie_security
Study Roadmap

Taking the lab exam is all about experience: You can’t expect to take it and pass after just completing your written exam, relying on your theoretical knowledge. You must spend countless hours of rack time configuring features and learning how protocols interact with one another. To be confident enough to schedule your lab exam, review the following outlined points.

Assessing Your Strengths

Using the content blueprint, determine your experience and knowledge in the major topic areas. For areas of strength, practicing for speed should be your focus. For weak areas, you might need training or book study in addition to practice.

Study Materials

Choose lab materials that provide configuration examples and take a hands-on approach. Look for materials approved or provided by Cisco and its Learning Partners.

Hands-On Practice

Build and practice your lab scenarios on a per-topic basis. Go beyond the basics and practice additional features. Learn the show and debug commands along with each topic. If a protocol has multiple ways of configuring a feature, practice all of them.

Cisco Documentation

Make sure you can navigate Cisco documentation with confidence because you will have limited access to cisco.com when you take the lab exam.

Further Study Information and Exam-Taking Tips

Appendix B of this guide outlines additional study information and reviews exam preparation and exam-taking tips and guidelines.
This page intentionally left blank
Section 1: Perimeter Security and Services

Securing the perimeter around important networks and devices is a fundamental part of network protection. In this section, you are asked to implement firewall services that include not only traditional features, such as Network Address Translation (NAT) and traffic inspection, but also secured routing features. This section focuses on initializing and configuring the Cisco Adaptive Security Appliance (ASA) in both single- and multi-context modes. Connectivity through perimeter devices must be verified before moving on to other exercises in this guide.

Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode

ASA1 must be configured as a multi-context firewall using a shared outside interface. In addition, context c1 and the admin context will be using VLANs for logical segregation on a physical interface. The logical placement of ASA1 is shown in the network topology presented in Diagram 2 in Part I.

Table 1-1 through Table 1-6 outline the initialization requirements.

Use names and addresses exactly as outlined. Remember that names are case sensitive.

<table>
<thead>
<tr>
<th>Table 1-1</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ASA1</td>
</tr>
<tr>
<td>Enable Password</td>
<td>cisco</td>
</tr>
</tbody>
</table>
Table 1-2  *Context Admin*

<table>
<thead>
<tr>
<th>Physical Interface</th>
<th>Logical Name</th>
<th>VLAN</th>
<th>config-url</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/2.2</td>
<td>mgmt (management traffic only)</td>
<td>102</td>
<td>disk0:/admin.cfg</td>
</tr>
</tbody>
</table>

Table 1-3  *Context c1*

<table>
<thead>
<tr>
<th>Physical Interface</th>
<th>Logical Name</th>
<th>VLAN</th>
<th>config-url</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0</td>
<td>outside</td>
<td>80</td>
<td>disk0:/c1.cfg</td>
</tr>
<tr>
<td>GigabitEthernet0/2.1</td>
<td>inside</td>
<td>101</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-4  *Context c2*

<table>
<thead>
<tr>
<th>Physical Interface</th>
<th>Logical Name</th>
<th>VLAN</th>
<th>config-url</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0</td>
<td>outside</td>
<td>80</td>
<td>disk0:/c2.cfg</td>
</tr>
<tr>
<td>GigabitEthernet0/1</td>
<td>dmz</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet0/3</td>
<td>inside</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-5  *Context Initialization Details*

<table>
<thead>
<tr>
<th>Context</th>
<th>Interface</th>
<th>IP Address/Mask</th>
<th>Nameif</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>GigabitEthernet0/2.2</td>
<td>192.168.1.20/24</td>
<td>mgmt</td>
<td>100</td>
</tr>
<tr>
<td>c1</td>
<td>GigabitEthernet0/0</td>
<td>10.50.80.20/24</td>
<td>outside</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GigabitEthernet0/2.1</td>
<td>192.168.2.20/24</td>
<td>inside</td>
<td>100</td>
</tr>
<tr>
<td>c2</td>
<td>GigabitEthernet0/0</td>
<td>10.50.80.30/24</td>
<td>outside</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>GigabitEthernet0/1</td>
<td>10.50.90.20/24</td>
<td>dmz</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>GigabitEthernet0/3</td>
<td>10.50.100.20/24</td>
<td>inside</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 1-6  *Routing Details*

<table>
<thead>
<tr>
<th>Context</th>
<th>Type</th>
<th>Network Prefix</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1</td>
<td>Default</td>
<td>0.0.0.0/0</td>
<td>10.50.80.6</td>
</tr>
<tr>
<td>c2</td>
<td>Default</td>
<td>0.0.0.0/0</td>
<td>10.50.80.6</td>
</tr>
<tr>
<td>admin</td>
<td>Default</td>
<td>0.0.0.0/0</td>
<td>192.168.1.5</td>
</tr>
<tr>
<td>c2</td>
<td>Static</td>
<td>10.10.0.0/16</td>
<td>10.50.100.2</td>
</tr>
</tbody>
</table>
Notes

- To validate your configuration, ensure that all interfaces in all contexts are up. You should ensure that Internet Control Message Protocol (ICMP) is permitted through each context to test connectivity and routing to the major subnets in the topology. You may use `permit icmp any any` for this purpose. Refer to Part I of this guide for information on the network addressing used in the topology.

- You might need to add or modify the configuration of switches and routers to ensure you have full connectivity.

- Some subnets might not be accessible until the configuration of ASA2 (see Exercise 1.2) and the Cisco IPS sensor (Exercise 2.1) is complete.

- The subinterface used for management traffic (admin context) must connect to inside secure hosts for management purposes only.

For the solution and verification information of this lab exercise, see “Solution and Verification for Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode.”

Exercise 1.2: Configure Routing and Basic Access on ASA2

In this exercise, ASA2 should be configured in single-context routed mode with support for Open Shortest Path First (OSPF). Table 1-7 through Table 1-10 provide the necessary configuration details. Use names exactly as they are shown; remember that they are case sensitive. You will not need to change any of the OSPF parameters on neighboring routers. Refer to Diagram 2 and Diagram 3 in Part I for device placement, addressing, and routing details.

Table 1-7  Administration

<table>
<thead>
<tr>
<th>Hostname</th>
<th>ASA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>cisco</td>
</tr>
</tbody>
</table>

Table 1-8  Interface Initialization Details

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/Mask</th>
<th>Nameif</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0</td>
<td>10.50.50.20/24</td>
<td>outside</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet0/2</td>
<td>10.50.40.20/24</td>
<td>inside</td>
<td>100</td>
</tr>
<tr>
<td>GigabitEthernet0/3</td>
<td>10.50.30.20/24</td>
<td>dmz</td>
<td>50</td>
</tr>
</tbody>
</table>
### Table 1-9  *Static Routing Details*

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Network Prefix</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>dmz</td>
<td>Static</td>
<td>10.3.3.0/24</td>
<td>10.50.30.3</td>
</tr>
<tr>
<td>dmz</td>
<td>Static</td>
<td>10.4.4.0/24</td>
<td>10.50.30.4</td>
</tr>
</tbody>
</table>

### Table 1-10  *OSPF Routing Details*

<table>
<thead>
<tr>
<th>Interface</th>
<th>Area</th>
<th>Network Prefix</th>
<th>Network Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>outside</td>
<td>0</td>
<td>10.50.50.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>dmz</td>
<td>1</td>
<td>10.50.30.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>inside</td>
<td>2</td>
<td>10.50.40.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

#### Notes

- To validate your configuration, ensure that all interfaces are up. You should ensure that ICMP is permitted through the firewall to test connectivity and routing to the major subnets in the topology. Refer to Part I of this guide for information on the network addressing used in the topology.
- You might need to add or modify the configuration of switches and routers to ensure you have full connectivity.
- Some subnets might not be accessible until the configuration of ASA1 (in Exercise 1.1) and the Cisco IPS sensor (in Exercise 2.1) is completed.

For the solution and verification information of this lab exercise, see “Solution and Verification for Exercise 1.2: Configure Routing and Basic Access on ASA2.”

### Exercise 1.3: Configure IP Services on ASA1

This exercise has four tasks that build on the initial configuration of ASA1 Exercise 1.1. You may use any names for configuration elements such as access lists or objects, unless otherwise specified. Note that because the version of software currently running on ASA1 is post 8.3, the NAT configuration tasks will require the use of objects. Refer to Diagram 2 and Diagram 3 in Part I for device placement and addressing details.

- Task 1: Configure Network Object NAT
- Task 2: Configure Twice NAT
- Task 3: Configure and Troubleshoot NTP Services Using Authentication
- Task 4: Configure Support for IPv6 in IPv4 Tunneling Through ASA1
Task 1: Configure Network Object NAT
Use network object NAT to translate 10.50.90.5/32 on R5 to 10.50.80.50/32 in the appropriate context. This translation must allow bidirectional communication.

Task 2: Configure Twice NAT
Using Twice NAT, create a policy that will translate network 10.50.100.0/24 to the range 10.50.80.100–10.50.80.150 if the destination is 10.50.50.0/24. Translation for this task is unidirectional.

Task 3: Configure and Troubleshoot NTP Services Using Authentication
Network Time Protocol (NTP) on ASA1 using authentication is required with the NTP master service, which is partially configured on SW1 as follows:

```plaintext
SW1# show run | begin ntp
ntp authentication-key 1 md5 cisco
ntp source Vlan102
ntp access-group peer 1
ntp master 2
```

Complete the configuration and troubleshoot any issues using the following outputs to verify your solution:

```plaintext
ASA1# show ntp associations detail
192.168.1.5 configured, authenticated, our_master, sane, valid, stratum 2

ASA1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.5
```

Task 4: Configure Support for IPv6 in IPv4 Tunneling Through ASA1
Enable support for the ipv6ip tunnel configured between the tunnel endpoints 10.50.80.6 (R6) and 10.50.90.5 (R5). This configuration will be important for the completion of Exercise 5.1.

For the solution and verification information of this lab exercise, see “Solution and Verification for Exercise 1.3: Configure IP Services on ASA1.”

Exercise 1.4: Configure IP Routing Security on ASA2
There are two tasks in this exercise that will focus on configuring the ASA2 to support dynamic routing protocols. Refer to Diagram 3 for routing protocol and addressing details.
Task 1: BGP Connectivity Through the ASA2

External Border Gateway Protocol (eBGP) has been preconfigured on R7 and R6 in Autonomous Systems 107 and 106, respectively. The BGP peering function cannot establish a session between these two routers through ASA2. Configure a solution that will enable the BGP peers to establish a connection. The following outputs can be used to verify your solution:

R6# show ip bgp
BGP table version is 3, local router ID is 172.18.106.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 172.18.106.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*&gt; 172.18.107.0/24</td>
<td>10.50.40.7</td>
<td>0</td>
<td>0</td>
<td>107    ?</td>
<td></td>
</tr>
</tbody>
</table>

R7# show ip bgp
BGP table version is 5, local router ID is 172.18.107.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 172.18.106.0/24</td>
<td>10.50.70.6</td>
<td>0</td>
<td>0</td>
<td>106    ?</td>
<td></td>
</tr>
<tr>
<td>*&gt; 172.18.107.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>

Task 2: OSPF Authentication for Routing Update Security

MD5 authentication is required in OSPF area 2. Configure a solution for this area only, and ensure that OSPF routing information is still correctly exchanged between neighbors. Use the key cisco123.

The following outputs will verify your solution:

R7# show ip ospf neighbor

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.50.50.20</td>
<td>1</td>
<td>FULL/BDR</td>
<td>00:00:32</td>
<td>10.50.40.20</td>
<td>GigabitEthernet0/1</td>
</tr>
</tbody>
</table>

ASA2# show ospf neighbor inside

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.18.107.7</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:38</td>
<td>10.50.40.7</td>
<td>inside</td>
</tr>
</tbody>
</table>
ASA2# show ospf
Area 2
   Number of interfaces in this area is 1
   Area has message digest authentication

R7# show ip ospf
   Area 2
   Number of interfaces in this area is 2 (1 loopback)
   Area has message digest authentication

For the solution and verification information of this lab exercise, see “Solution and Verification for Exercise 1.4: Configure IP Routing Security on ASA2.”

Section 2: Intrusion Prevention and Content Security

This section covers tasks applicable to some specialized Cisco appliances, the Intrusion Prevention Sensor (IPS) and the Web Services Appliance (WSA). Both devices will be initialized and deployed into the network topology as shown in Diagram 1 and Diagram 2 in Part I. The single IPS appliance will be logically partitioned using various deployment modes of operation to service distinct traffic flows in the network. The WSA will handle redirected traffic of interest via Web Cache Communication Protocol (WCCP) from the Cisco ASA. It is important to verify whether traffic is correctly flowing through the appliances before moving on to other exercises in the lab.

Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance

The exercise has four tasks.

You will be required to initialize the Cisco Intrusion Prevention Sensor (IPS) appliance and make it accessible from its management interface, and then deploy the sensor in three different interface modes: Inline VLAN pair, Inline Interface pair, and Promiscuous.

The Lab Topology diagram (Diagram 2 in Part I) depicts three IPS devices; however, only one physical IPS sensor exists in the network. This requires you to pay special attention to the switches in the topology to ensure switch ports are correctly configured (switch-port modes, VLANs, and so on) to support each of the three logical/virtual sensors (refer to Diagram 1 in Part I).

Use names and details exactly as they appear in the tables.

Task 1: Initialize the Cisco IPS Sensor

Use the parameters in Table 1-11 to complete the task of initializing the sensor.
### Table 1-11  Initialization Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>IPS</td>
</tr>
<tr>
<td>Management</td>
<td>Configure the command and control Management0/0 interface in VLAN 101</td>
</tr>
<tr>
<td>Sensor IP address</td>
<td>192.168.2.100/24</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.2.20</td>
</tr>
<tr>
<td>Sensor ACL</td>
<td>192.168.2.0</td>
</tr>
<tr>
<td>Telnet</td>
<td>Enable Telnet management</td>
</tr>
</tbody>
</table>

Verify the Cisco IPS sensor configuration using the following:

- The username and password for the Cisco IPS console are ciscoips and 123cisco123. Do not change them. Use the console to initialize the Cisco IPS sensor appliance using the details in this table.

- Ensure that the Management0/0 interface is up and functioning (refer to the Lab Topology diagram). You can modify the Cisco Catalyst switch configuration if required.

- Ensure that the Cisco IPS sensor can ping the default gateway:

  ```
  IPS# ping 192.168.2.5
  ```

- Ensure that the following ping and Telnet connection is successful from SW1:

  ```
  SW1# telnet 192.168.2.100
  ```

### Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode

Configure the Cisco IPS sensor appliance for the Inline VLAN pair as shown in Table 1-12.

### Table 1-12  Inline VLAN Pair Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Settings</th>
<th>Virtual Sensor Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>GigabitEthernet0/2</td>
<td>vs0</td>
</tr>
<tr>
<td>Inline VLAN pair</td>
<td>Vlan1 70 (VLAN70)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan2 50 (VLAN50)</td>
<td></td>
</tr>
</tbody>
</table>
Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode

Configure the Cisco IPS sensor appliance for the Inline Interface pair as shown in Table 1-13.

Table 1-13  *Inline Interface Pair Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Name</th>
<th>Settings</th>
<th>Switch VLANS</th>
<th>Virtual Sensor Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Pair</td>
<td>ipair</td>
<td>GigabitEthernet0/0, GigabitEthernet0/1</td>
<td>60 80</td>
<td>vs1</td>
</tr>
</tbody>
</table>

Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode

Configure the Cisco IPS sensor appliance for promiscuous mode on GigabitEthernet 0/3 and assign it to virtual sensor vs2.

For the solution and verification information of this lab exercise, see “Solution and Verification for Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance.”
Figure 1-1  WSA System Setup Wizard

Table 1-14  WSA Initialization Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>wsa.cisco.com</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Management (M1) to be used for data and management</td>
</tr>
<tr>
<td>IP address</td>
<td>192.168.2.50/24</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.2.20</td>
</tr>
<tr>
<td>System Information</td>
<td>username: admin; password: ironport; email: <a href="mailto:fred@foobar.com">fred@foobar.com</a>; timezone: America/United States/Los Angeles (this will vary)</td>
</tr>
<tr>
<td>NTP server</td>
<td>192.168.2.25</td>
</tr>
<tr>
<td>DNS</td>
<td>192.168.2.25</td>
</tr>
<tr>
<td>L4 Traffic Monitoring</td>
<td>Duplex TAP:T1 (In/Out)</td>
</tr>
</tbody>
</table>

Accept all other defaults.

From ASA1/c1, verify whether you can ping the M1 interface of the Cisco WSA:

ASA1/c1# ping 192.168.2.50