CCIE Security v4.0 Practice Labs

Natalie Timms

Cisco Press

CCIE Security v4.0 Practice Labs

Natalie Timms, CCIE No. 37959

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCIE Security v4.0 Practice Labs

Natalie Timms, CCIE No. 37959

Published by:

Pearson Education, Inc.
800 East 96th Street
Indianapolis, IN 46240 USA

ISBN-13: 978-1-58714-414-1

ISBN-10: 1-58714-414-X

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Internetwork Expert (CCIE) Security Lab 4.0 Exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

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	Business Operation Manager, Cisco Press: Jan Cornelssen
Associate Publisher: Dave Dusthimer	Senior Development Editor: Christopher Cleveland
Acquisition Editor: Denise Lincoln	Managing Editor: Sandra Schroeder
Senior Project Editor: Tonya Simpson	Technical Editors: Tim Rowley, Tyson Scott
Proofreader: Paula Lowell	Editorial Assistant: Vanessa Evans
Cover Designer: Mark Shirar	Composition: Mary Sudul

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Contents

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

Practice Lab 1

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 1-1 *Administration*

Hostname	ASA1
Enable Password	cisco

Table 1-2 *Context Admin*

Physical Interface	Logical Name	VLAN	config-url
GigabitEthernet0/2.2	mgmt (management traffic only)	102	disk0:/admin.cfg

Table 1-3 *Context c1*

Physical Interface	Logical Name	VLAN	config-url
GigabitEthernet0/0	outside	80	disk0:/c1.cfg
GigabitEthernet0/2.1	inside	101	

Table 1-4 *Context c2*

Physical Interface	Logical Name	VLAN	config-url
GigabitEthernet0/0	outside	80	disk0:/c2.cfg
GigabitEthernet0/1	dmz	90	
GigabitEthernet0/3	inside	100	

Table 1-5 *Context Initialization Details*

Context	Interface	IP Address/Mask	Nameif	Security Level
admin	GigabitEthernet0/2.2	192.168.1.20/24	mgmt	100
c1	GigabitEthernet0/0	10.50.80.20/24	outside	0
	GigabitEthernet0/2.1	192.168.2.20/24	inside	100
c2	GigabitEthernet0/0	10.50.80.30/24	outside	0
	GigabitEthernet0/1	10.50.90.20/24	dmz	50
	GigabitEthernet0/3	10.50.100.20/24	inside	100

Table 1-6 *Routing Details*

Context	Type	Network Prefix	Next Hop
c1	Default	0.0.0.0/0	10.50.80.6
c2	Default	0.0.0.0/0	10.50.80.6
admin	Default	0.0.0.0/0	192.168.1.5
c2	Static	10.10.0.0/16	10.50.100.2

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*

Hostname	ASA2
Enable Password	cisco

Table 1-8 *Interface Initialization Details*

Interface	IP Address/Mask	Nameif	Security Level
GigabitEthernet0/0	10.50.50.20/24	outside	0
GigabitEthernet0/2	10.50.40.20/24	inside	100
GigabitEthernet0/3	10.50.30.20/24	dmz	50

Table 1-9 *Static Routing Details*

Interface	Type	Network Prefix	Next Hop
dmz	Static	10.3.3.0/24	10.50.30.3
dmz	Static	10.4.4.0/24	10.50.30.4

Table 1-10 *OSPF Routing Details*

Interface	Area	Network Prefix	Network Mask
outside	0	10.50.50.0	255.255.255.0
dmz	1	10.50.30.0	255.255.255.0
inside	2	10.50.40.0	255.255.255.0

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:

```
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:

```
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

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.18.106.0/24  0.0.0.0                  0         32768 ?
*> 172.18.107.0/24  10.50.40.7               0             0 107 ?

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

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.18.106.0/24  10.50.70.6               0             0 106 ?
*> 172.18.107.0/24  0.0.0.0                  0         32768 ?
```

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

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.50.50.20       1   FULL/BDR        00:00:32    10.50.40.20     GigabitEthernet0/1

ASA2# show ospf neighbor inside

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.18.107.7      1   FULL/DR         0:00:38     10.50.40.7      inside
```

```
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 (switchport 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*

Parameter	Settings
Hostname	IPS
Management	Configure the command and control Management0/0 interface in VLAN 101
Sensor IP address	192.168.2.100/24
Default gateway	192.168.2.20
Sensor ACL	192.168.2.0
Telnet	Enable Telnet management

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*

Parameter	Settings	Virtual Sensor Name
Physical interface	GigabitEthernet0/2	vs0
Inline VLAN pair	Vlan1 70 (VLAN70) Vlan2 50 (VLAN50)	

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*

Parameter	Name	Settings	Switch VLANS	Virtual Sensor Name
Interface Pair	ipair	GigabitEthernet0/0, GigabitEthernet0/1	60 80	vs1

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."

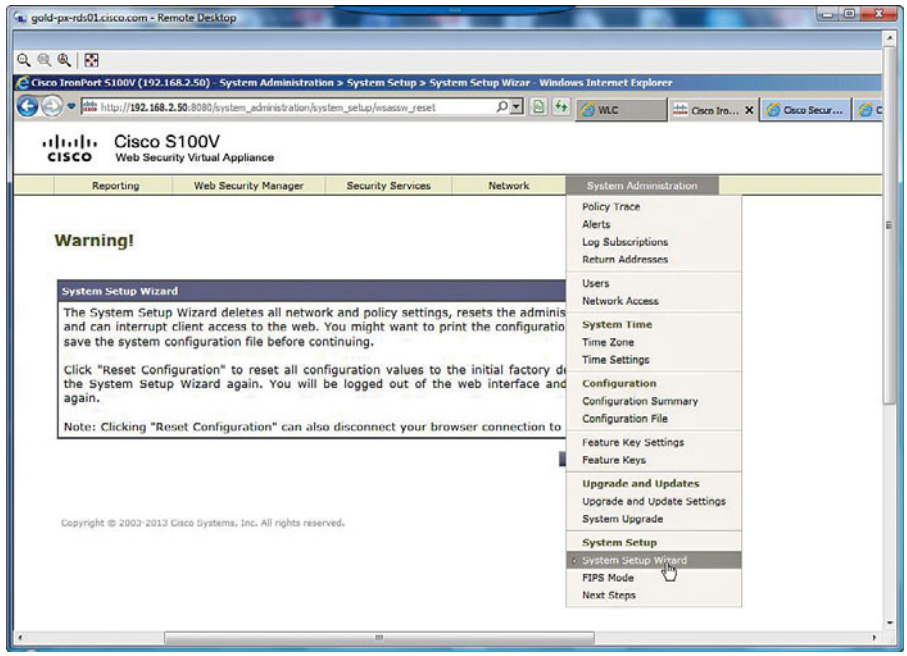

Figure 1-1 *WSA System Setup Wizard*

Table 1-14 *WSA Initialization Parameters*

Parameter	Settings
Hostname	wsa.cisco.com
Interfaces	Management (M1) to be used for data and management
IP address	192.168.2.50/24
Default gateway	192.168.2.20
System Information	username: admin; password: ironport; email: fred@foobar.com; timezone: America/United States/Los Angeles (this will vary)
NTP server	192.168.2.5
DNS	192.168.2.25
L4 Traffic Monitoring	Duplex TAP:T1 (In/Out)

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
```