



Practice  
Tests



Flash  
Cards



Glossary



Study  
Planner

# Official Cert Guide

Advance your IT career with hands-on learning

# CCNP Security

Cisco Secure Firewall and  
Intrusion Prevention System

# Special Offers

## **Save 70% on Complete Video Course**

To enhance your preparation, Cisco Press also sells Complete Video Courses for both streaming and download. Complete Video Courses provide you with hours of expert-level instruction mapped directly to exam objectives.

## **Save 80% on Premium Edition eBook and Practice Test**

*The CCNP Security Cisco Secure Firewall and Intrusion Prevention System Official Cert Guide Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

**See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.**

# CCNP Security Cisco Secure Firewall and Intrusion Prevention System Official Cert Guide

## Table of Contents

Cover

Title Page

Copyright Page

Dedications

Contents at a Glance

Contents

Introduction

Part I: General Deployment

Chapter 1 Introduction to Cisco Secure Firewall and IPS

Do I Know This Already? Quiz

Foundation Topics

Evolution of Next-Generation Firewall

Cisco Secure Firewall Solutions

Product Evolution and Lifecycle

Software and Hardware Architecture

Scalability and Resiliency

Clustering

Multi-Instance

High Availability

Resiliency in Connectivity

Summary

Exam Preparation Tasks

# **Table of Contents**

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 2 Deployment of Secure Firewall Virtual**

Do I Know This Already? Quiz

Foundation Topics

Cisco Secure Firewall on a Virtual Platform

- Hosting Environment Settings

- Virtual Resource Allocation

- Software Package Selection

Best Practices

Configuration

- Virtual Network for Management Traffic

- Virtual Network for Data Traffic

- Virtual Machine Creation for Secure Firewall

System Initialization and Validation

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 3 Licensing and Registration**

Do I Know This Already?

Foundation Topics

Cisco Licensing Architecture

- Direct Cloud Access

- On-Premises Server

- Offline Access

Cisco Secure Firewall Licenses

- Feature License

- Export-Controlled License

# **Table of Contents**

Evaluation License

Validation of Licensing

Device Registration

Best Practices for Registration

Configurations on Threat Defense

Configurations on Management Center

Management Communication over the Internet

Validation of Registration

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 4 Firewall Deployment in Routed Mode**

Do I Know This Already? Quiz

Foundation Topics

Routed Mode Essentials

Best Practices for Routed Mode Configuration

Fulfilling Prerequisites

Enabling the Routed Firewall Mode

Configuration of the Routed Interface

Configuring Interfaces with Static IP Addresses

Configuring Interfaces with Automatic IP Addresses

Validation of Interface Configuration

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 5 Firewall Deployment in Transparent Mode**

# **Table of Contents**

Do I Know This Already? Quiz

Foundation Topics

Transparent Mode Essentials

Best Practices for Transparent Mode Configuration

Fulfilling Prerequisites

- Enabling the Transparent Firewall Mode

Configuring Transparent Mode in a Layer 2 Network

- Configuring the Physical and Virtual Interfaces

- Verifying the Interface Status

- Verifying Basic Connectivity and Operations

Deploying a Threat Defense Between Layer 3 Networks

- Selecting a Default Action

- Adding an Access Control Rule for a Routing Protocol

- Creating an Access Control Rule for the SSH Protocol

- Verifying Access Control Lists

Integrated Routing and Bridging (IRB)

Summary

Exam Preparation Tasks

Review All Key Topics

Memory Tables and Lists

Define Key Terms

## **Chapter 6 IPS-Only Deployment in Inline Mode**

Do I Know This Already? Quiz

Foundation Topics

Inline Mode Essentials

- Inline Mode Versus Passive Mode

- Inline Mode Versus Transparent Mode

Best Practices for Inline Mode

Inline Mode Configuration

- Fulfilling Prerequisites

- Interface Setup

# **Table of Contents**

Inline Set Configuration

Verification

Event Analysis in IPS-Only Mode

Summary

Exam Preparation Tasks

Review All Key Topics

Memory Tables and Lists

Define Key Terms

## **Chapter 7 Deployment in Detection-Only Mode**

Do I Know This Already? Quiz

Foundation Topics

Detection-Only Mode Essentials

Passive Monitoring Technology

Interface Modes: Inline, Inline Tap, and Passive

Best Practices for Detection-Only Deployment

Inline Tap Mode

Configuration of Inline Tap Mode

Verification of Inline Tap Configuration

Passive Interface Mode

Configuration of Passive Interface Mode

Configuring Passive Interface Mode on a Threat Defense

Configuring a SPAN Port on a Switch

Verification of Passive Interface Configuration

Event Analysis in Detection-Only Mode

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Part II: Basic Security Operations**

# **Table of Contents**

## **Chapter 8 Capturing Traffic for Advanced Analysis**

Do I Know This Already? Quiz

Foundation Topics

Packet Capture Essentials

Best Practices for Capturing Traffic

Capturing of Packets Using Secure Firewall

Configuration

Verification

Packet Capture versus Packet Tracer

Summary

Exam Preparation Tasks

Review All Key Topics

Memory Tables and Lists

Define Key Terms

## **Chapter 9 Network Discovery Policy**

Do I Know This Already? Quiz

Foundation Topics

Network Discovery Essentials

Application Detectors

Network Discovery Operations

Best Practices for Network Discovery

Fulfilling Prerequisites

Configurations

Reusable Objects

Network Discovery Policy

Verification

Analyzing Application Discovery

Analyzing Host Discovery

Undiscovered New Hosts

Summary

Exam Preparation Tasks



# **Table of Contents**

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 10 Access Control Policy**

Do I Know This Already? Quiz

Foundation Topics

Access Control Policy Essentials

Policy Editor

Rule Editor

Best Practices for Access Control Policy

Access Control Policy Configuration

Fulfilling Prerequisites

Creating Rules

Verification

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 11 Prefilter Policy**

Do I Know This Already? Quiz

Foundation Topics

Prefilter Policy Essentials

Prefilter Policy: Rules and Actions

Bypassing Deep Packet Inspection

Best Practices for a Prefilter Policy

Enabling Bypass Through a Prefilter Policy

Fulfilling Prerequisites

Configuring a Rule in a Prefilter Policy

Invoking a Prefilter Policy into an Access Control Policy

Establishing Trust Through an Access Control Policy

# Table of Contents

Verification

Managing Encapsulated Traffic Inspection

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 12 Security Intelligence

Do I Know This Already? Quiz

Foundation Topics

Security Intelligence Essentials

Best Practices for Security Intelligence

Fulfilling Prerequisites

Automatic Blocking Using Cisco Intelligence Feed

Verifying the Action of Cisco Intelligence Feed

Overriding the Cisco Intelligence Feed Outcome

Instant Blocking Using Context Menu

Adding an Address to the Block List

Deleting an Address from the Block List

Manual Blocking Using Custom List

Enabling Security Intelligence in Monitor-Only Mode

Threat Intelligence Director

Enabling Threat Intelligence Director

Adding Sources and Importing Indicators

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 13 Domain Name System (DNS) Policy

# **Table of Contents**

Do I Know This Already? Quiz

Foundation Topics

DNS Policy Essentials

- Domain Name System (DNS)

- Blocking of a DNS Query Using a Secure Firewall

- DNS Rule Actions

- Actions That Can Interrupt DNS Queries

- Actions That Allow DNS Queries

- Sources of Intelligence

Best Practices for Blocking DNS Queries

Fulfilling Prerequisites

Configuring DNS Policy

- Add a New Rule to a DNS Policy

- Invoke the DNS Policy

Verification

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Chapter 14 URL Filtering**

Do I Know This Already? Quiz

Foundation Topics

URL Filtering Essentials

- Category and Reputation

- URL Database

Fulfilling Prerequisites

Best Practices for URL Filtering Configuration

Enabling URL Filtering

- Blocking URLs of a Certain Category

- Verifying the Operation of a URL Filtering Rule

# Table of Contents

- Allowing a Specific URL
- Analyzing the Default Category Override
- Handling Uncategorized URLs
- Investigating the Uncategorized URLs

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Part III: Advanced Configurations

### Chapter 15 Network Analysis and Intrusion Policies

Do I Know This Already? Quiz

Foundation Topics

Intrusion Prevention System Essentials

- Network Analysis Policy

- Intrusion Policy

- System-Provided Variable Sets

- System-Provided Base Policies

Best Practices for Intrusion Policy Deployment

Configuring a Network Analysis Policy

Configuring an Intrusion Policy

- Creating a Policy with a Default Ruleset

- Incorporating Intrusion Rule Recommendations

- Enabling or Disabling an Intrusion Rule

Setting Up a Variable Set

Policy Deployment

Verification

Summary

Exam Preparation Tasks

Review All Key Topics

# Table of Contents

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 16 Malware and File Policy

Do I Know This Already? Quiz

Foundation Topics

File Policy Essentials

File Type Detection

Malware Analysis

Best Practices for File Policy Configuration

Fulfilling Prerequisites

Configuring a File Policy

Creating a File Policy

Deploying a File Policy

Verification

Analyzing File Events

Analyzing Malware Events

The Management Center Is Unable to Communicate with the Cloud

The Management Center Performs a Cloud Lookup

The Threat Defense Blocks Malware

Overriding a Malware Disposition

Network Trajectory

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 17 Network Address Translation (NAT)

Do I Know This Already? Quiz

Foundation Topics

NAT Essentials

NAT Techniques

# Table of Contents

NAT Rule Types

Best Practices for NAT Deployment

Fulfilling Prerequisites

Configuring NAT

Masquerading a Source Address (Source NAT for Outbound Connection)

Configuring a Dynamic NAT Rule

Verifying the Configuration

Verifying the Operation: Inside to Outside

Verifying the Operation: Outside to Inside

Connecting to a Masqueraded Destination (Destination NAT for Inbound Connection)

Configuring a Static NAT Rule

Verifying the Operation: Outside to DMZ

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 18 Traffic Decryption Policy

Do I Know This Already? Quiz

Foundation Topics

Traffic Decryption Essentials

Overview of SSL and TLS Protocols

Decryption Techniques on Secure Firewall

Best Practices for Traffic Decryption

Configuring a Decryption Policy

PKI Objects

Internal CAs Object

Internal Certs Object

SSL Policy

File Policy

Access Control Policy

Verification

# Table of Contents

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 19 Virtual Private Network (VPN)

Do I Know This Already? Quiz

Foundation Topics

VPN Essentials

Site-to-Site VPN

Remote Access VPN

IPsec Essentials

Mode of Operation

Security Association and Key Exchange

IKEv1

IKEv2

Authentication

Site-to-Site VPN Deployment

Prerequisites

Configurations

Access Control Policy

NAT Policy

Verification

Remote Access VPN Deployment

Prerequisites

Configuration

AnyConnect File

RADIUS Server Group

Certificate Enrollment

Network and IP Address Pool

Remote Access VPN Policy

Verification

# Table of Contents

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 20 Quality of Service (QoS)

Do I Know This Already? Quiz

Foundation Topics

Quality of Service Essentials

Best Practices for Enabling QoS

Fulfilling Prerequisites

Configuring QoS Policy

Verification

Analyzing QoS Events and Statistics

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## Chapter 21 System Logging (Syslog)

Do I Know This Already? Quiz

Foundation Topics

Secure Firewall Logging Essentials

Best Practices for Logging

Prerequisites

Sending Syslog from Threat Defense

Add a Syslog Server on Platform Settings

Enable Logging on Access Control Policy

Verification

Sending Syslog from Management Center



# **Table of Contents**

Create Syslog Alerts

Verification

Correlate Events to Send Syslog Alerts

Troubleshooting Logs

Summary

Exam Preparation Tasks

Review All Key Topics

Complete Tables and Lists from Memory

Define Key Terms

## **Part IV: Conclusion**

### **Chapter 22 Final Preparation**

Getting Ready for the Exam

Tools for Final Review

Exam Day

Practice Tests

Pearson Cert Practice Test Engine and Questions on the Website

Accessing the Pearson Test Prep Software Online

Accessing the Pearson Test Prep Software Offline

Customizing Your Exams

Updating Your Exams

Premium Edition

Chapter-Ending Review Tools

Summary

## **Part V: Appendixes**

Appendix A: Answers to the Do I Know This Already? Questions

Appendix B: CCNP Security Cisco Secure Firewall and Intrusion  
Prevention System Official Cert Guide Updates

## **Glossary**

A

B

# **Table of Contents**

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

Index

Appendix C: Memory Tables

Appendix D: Memory Tables Answer Key

Appendix E: Study Planner