Official Cert Guide

Study Planner

# CCNP and CCIE Security Core

## SCOR 350-701

2nd Edition

ciscopress.com

Omar Santos

# Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **ciscopress.com/register**.
2. Enter the **print book ISBN:** 9780138221263.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated in your account under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log in to the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

# CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

## Table of Contents

Cover
Title Page
Copyright Page
Contents at a Glance
Contents
Introduction
Chapter 1 Cybersecurity Fundamentals
    Do I Know This Already? Quiz
    Foundation Topics
    Introduction to Cybersecurity
        Cybersecurity vs. Information Security (InfoSec)
        The NIST Cybersecurity Framework
        Additional NIST Guidance and Documents
        The International Organization for Standardization (ISO)
    Defining What Are Threats, Vulnerabilities, and Exploits
        What Is a Threat?
        What Is a Vulnerability?
        What Is an Exploit?
        Risk, Assets, Threats, and Vulnerabilities
        Defining Threat Actors
        Understanding What Threat Intelligence Is
        Viruses and Worms

Pearson

# Table of Contents

Types and Transmission Methods

Malware Payloads

Trojans

Trojan Types

Trojan Ports and Communication Methods

Trojan Goals

Trojan Infection Mechanisms

Effects of Trojans

Distributing Malware

Ransomware

Covert Communication

Keyloggers

Spyware

Analyzing Malware

Static Analysis

Dynamic Analysis

Common Software and Hardware Vulnerabilities

Injection Vulnerabilities

SQL Injection

HTML Injection

Command Injection

Authentication-based Vulnerabilities

Credential Brute-Force Attacks and Password Cracking

Session Hijacking

Default Credentials

Insecure Direct Object Reference Vulnerabilities

Cross-site Scripting (XSS)

Cross-site Request Forgery

Server-side Request Forgery

Cookie Manipulation Attacks

# Table of Contents

- Race Conditions
- Unprotected APIs
- Typical Attacks Against Artificial Intelligence (AI) and Machine Learning
- Return-to-LibC Attacks and Buffer Overflows
- OWASP Top 10
- Security Vulnerabilities in Open-Source Software

Confidentiality, Integrity, and Availability

- What Is Confidentiality?
- What Is Integrity?
- What Is Availability?
- Talking About Availability, What Is a Denial-of-Service (DoS) Attack?
- Access Control Management

Cloud Security Threats

- Cloud Computing Issues and Concerns
- Cloud Computing Attacks
- Cloud Computing Security

IoT Security Threats

- IoT Protocols
- Hacking IoT Implementations

An Introduction to Digital Forensics and Incident Response

- ISO/IEC 27002:2013 and NIST Incident Response Guidance
- What Is an Incident?
- False Positives, False Negatives, True Positives, and True Negatives
- Incident Severity Levels
- How Are Incidents Reported?
- What Is an Incident Response Program?
- The Incident Response Plan
- The Incident Response Process
- Tabletop Exercises and Playbooks

# Table of Contents

Information Sharing and Coordination

Computer Security Incident Response Teams

Product Security Incident Response Teams (PSIRTs)

The Common Vulnerability Scoring System (CVSS)

The Stakeholder-Specific Vulnerability Categorization (SSVC)

National CSIRTs and Computer Emergency Response Teams (CERTs)

Coordination Centers

Incident Response Providers and Managed Security Service Providers (MSSPs)

Key Incident Management Personnel

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 2 Cryptography

Do I Know This Already? Quiz

Foundation Topics

Introduction to Cryptography

Ciphers

Keys

Block and Stream Ciphers

Symmetric and Asymmetric Algorithms

Hashes

Hashed Message Authentication Code

Digital Signatures

Key Management

Next-Generation Encryption Protocols

IPsec

# Table of Contents

Post-Quantum Cryptography

SSL and TLS

Fundamentals of PKI

Public and Private Key Pairs

More About Keys and Digital Certificates

Certificate Authorities

Root Certificates

Identity Certificates

X.500 and X.509v3

Authenticating and Enrolling with the CA

Public Key Cryptography Standards

Simple Certificate Enrollment Protocol

Revoking Digital Certificates

Digital Certificates in Practice

PKI Topologies

Single Root CA

Hierarchical CA with Subordinate CAs

Cross-Certifying CAs

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 3 Software-Defined Networking Security and Network Programmability

Do I Know This Already? Quiz

Foundation Topics

Software-Defined Networking (SDN) and SDN Security

Traditional Networking Planes

# Table of Contents

- So Whats Different with SDN?
- Introduction to the Cisco ACI Solution
- VXLAN and Network Overlays
- Micro-Segmentation
- Open-Source Initiatives
- More About Network Function Virtualization
- NFV MANO
- Contiv
- ThousandEyes Integration
- Cisco Digital Network Architecture (DNA)
- Cisco DNA Policies
- Cisco DNA Group-Based Access Control Policy
- Cisco DNA IP-Based Access Control Policy
- Cisco DNA Application Policies
- Cisco DNA Traffic Copy Policy
- Cisco DNA Center Assurance Solution
- Cisco DNA Center APIs
- Cisco DNA Security Solution
- Cisco DNA Multivendor Support

Introduction to Network Programmability

- Modern Programming Languages and Tools
- DevNet
- Getting Started with APIs
- REST APIs
- Using Network Device APIs
- YANG Models
- NETCONF
- RESTCONF
- OpenConfig and gNMI

Exam Preparation Tasks

# Table of Contents

Review All Key Topics

Define Key Terms

Review Questions

Chapter 4 Authentication, Authorization, Accounting (AAA) and Identity Management

Do I Know This Already? Quiz

Foundation Topics

Introduction to Authentication, Authorization, and Accounting

The Principle of Least Privilege and Separation of Duties

Authentication

Authentication by Knowledge

Authentication by Ownership or Possession

Authentication by Characteristic

Multifactor Authentication

Duo Security

Zero Trust and BeyondCorp

Single Sign-On

JWT

SSO and Federated Identity Elements

Authorization

Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

Role-Based Access Control (RBAC)

Rule-Based Access Control

Attribute-Based Access Control

Accounting

Infrastructure Access Controls

Access Control Mechanisms

# Table of Contents

- AAA Protocols
  - RADIUS
  - TACACS+
  - Diameter
  - 802.1X
  - Network Access Control List and Firewalling
  - VLAN ACLs
  - Security GroupBased ACL
  - Downloadable ACL
- Cisco Identity Services Engine (ISE)
  - Cisco Platform Exchange Grid (pxGrid)
  - Cisco ISE Context and Identity Services
  - Cisco ISE Profiling Services
  - Cisco ISE Identity Services
  - Cisco ISE Authorization Rules
  - Cisco TrustSec
  - Posture Assessment
  - Change of Authorization (CoA)
- Configuring TACACS+ Access
- Configuring RADIUS Authentication
  - Configuring 802.1X Authentication
- Additional Cisco ISE Design Tips
  - Advice on Sizing a Cisco ISE Distributed Deployment
- Exam Preparation Tasks
- Review All Key Topics
- Define Key Terms
- Review Questions

Chapter 5 Network Visibility and Segmentation

# Table of Contents

Do I Know This Already? Quiz

Foundation Topics

Introduction to Network Visibility

NetFlow

- The Network as a Sensor and as an Enforcer
- What Is a Flow?
- NetFlow for Network Security and Visibility
- NetFlow for Anomaly Detection and DDoS Attack Mitigation
- Data Leak Detection and Prevention
- Incident Response, Threat Hunting, and Network Security Forensics
- Traffic Engineering and Network Planning
- NetFlow Versions

IP Flow Information Export (IPFIX)

- IPFIX Architecture
- Understanding IPFIX Mediators
- IPFIX Templates
- Option Templates
- Understanding the Stream Control Transmission Protocol (SCTP)
- Exploring Application Visibility and Control and NetFlow
- Application Recognition
- Metrics Collection and Exporting

NetFlow Deployment Scenarios

- NetFlow Deployment Scenario: User Access Layer
- NetFlow Deployment Scenario: Wireless LAN
- NetFlow Deployment Scenario: Internet Edge
- NetFlow Deployment Scenario: Data Center
- NetFlow Deployment Scenario: NetFlow in Site-to-Site and Remote VPNs

Cisco Secure Network Analytics and Cisco Secure Cloud Analytics

- Cisco Secure Cloud Analytics

# Table of Contents

On-Premises Monitoring with Cisco Secure Cloud Analytics

Cisco Secure Cloud Analytics Integration with Meraki and Cisco Umbrella

Exploring the Cisco Secure Network Analytics Dashboard

Threat Hunting with Cisco Secure Network Analytics

Cisco Cognitive Intelligence and Cisco Encrypted Traffic Analytics (ETA)

What Is Cisco ETA?

What Is Cisco Cognitive Intelligence?

NetFlow Collection Considerations and Best Practices

Determining the Flows per Second and Scalability

Configuring NetFlow in Cisco IOS and Cisco IOS-XE

Simultaneous Application Tracking

Flexible NetFlow Records

Flexible NetFlow Key Fields

Flexible NetFlow Non-Key Fields

NetFlow Predefined Records

User-Defined Records

Flow Monitors

Flow Exporters

Flow Samplers

Flexible NetFlow Configuration

Configure a Flow Record

Configure a Flow Monitor for IPv4 or IPv6

Configure a Flow Exporter for the Flow Monitor

Apply a Flow Monitor to an Interface

Flexible NetFlow IPFIX Export Format

Configuring NetFlow in NX-OS

Introduction to Network Segmentation

Data-Driven Segmentation

Application-Based Segmentation

# Table of Contents

Micro-Segmentation with Cisco ACI

Segmentation with Cisco ISE

The Scalable Group Tag Exchange Protocol (SXP)

SGT Assignment and Deployment

Initially Deploying 802.1X and/or TrustSec in Monitor Mode

Active Policy Enforcement

Cisco ISE TrustSec and Cisco ACI Integration

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 6 Infrastructure Security

Do I Know This Already? Quiz

Foundation Topics

Securing Layer 2 Technologies

VLAN and Trunking Fundamentals

What Is a VLAN?

Trunking with 802.1Q

Lets Follow the Frame, Step by Step

What Is the Native VLAN on a Trunk?

So, What Do You Want to Be? (Asks the Port)

Understanding Inter-VLAN Routing

What Is the Challenge of Only Using Physical Interfaces?

Using Virtual Sub Interfaces

Spanning Tree Fundamentals

The Solution to the Layer 2 Loop

STP Is Wary of New Ports

Improving the Time Until Forwarding

# Table of Contents

Common Layer 2 Threats and How to Mitigate Them

- Do Not Allow Negotiations
- Layer 2 Security Toolkit
- BPDU Guard
- Root Guard
- Port Security
- CDP and LLDP
- DHCP Snooping
- Dynamic ARP Inspection

Network Foundation Protection

- The Importance of the Network Infrastructure
- The Network Foundation Protection Framework
- Interdependence
- Implementing NFP

Understanding and Securing the Management Plane

- Best Practices for Securing the Management Plane

Understanding the Control Plane

- Best Practices for Securing the Control Plane

Understanding and Securing the Data Plane

- Best Practices for Protecting the Data Plane
- Additional Data Plane Protection Mechanisms

Securing Management Traffic

- What Is Management Traffic and the Management Plane?
- NETCONF and RESTCONF vs. SNMP
- Beyond the Console Cable
- Management Plane Best Practices
- Password Recommendations
- Using AAA to Verify Users
- Router Access Authentication

# Table of Contents

- The AAA Method List
- Role-Based Access Control
- Custom Privilege Levels
- Limiting the Administrator by Assigning a View
- Encrypted Management Protocols
- Using Logging Files
- Understanding NTP
- Protecting Cisco IOS, Cisco IOS-XE, Cisco IOS-XR, and Cisco NX-OS Files
- Implementing Security Measures to Protect the Management Plane
- Implementing Strong Passwords
- User Authentication with AAA
- Using the CLI to Troubleshoot AAA for Cisco Routers
- RBAC Privilege Level/Parser View
- Implementing Parser Views
- SSH and HTTPS

Implementing Logging Features

- Configuring Syslog Support

Configuring NTP

Securing the Network Infrastructure Device Image and Configuration Files

Securing the Data Plane in IPv6

- Understanding and Configuring IPv6
- The Format of an IPv6 Address
- Understanding the Shortcuts
- Did We Get an Extra Address?
- IPv6 Address Types
- Configuring IPv6 Routing
- Moving to IPv6
- Developing a Security Plan for IPv6
- Best Practices Common to Both IPv4 and IPv6

# Table of Contents

Threats Common to Both IPv4 and IPv6

Cisco Secure Firewall

The Focus on IPv6 Security

New Potential Risks with IPv6

IPv6 Best Practices

IPv6 Access Control Lists

Securing Routing Protocols and the Control Plane

Minimizing the Impact of Control Plane Traffic on the CPU

Details about CoPP

Details about CPPr

Securing Routing Protocols

Implementing Routing Update Authentication on OSPF

Implementing Routing Update Authentication on EIGRP

Implementing Routing Update Authentication on RIP

Implementing Routing Update Authentication on BGP

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 7 Cisco Secure Firewall

Do I Know This Already? Quiz

Foundation Topics

Introduction to Cisco Secure Firewall

Cisco Firewall History and Legacy

Introducing the Cisco ASA

The Cisco ASA FirePOWER Module

Cisco Secure Firewall: Formerly known as Cisco Firepower Threat Defense (FTD)

Cisco Secure Firewall

# Table of Contents

- Cisco Secure Firewall Migration Tool
- Cisco Secure Firewall Threat Defense Virtual
- Cisco Secure Firewall Cloud Native
- Cisco Secure Firewall ISA3000
- Cisco Secure WAF and Bot Protection
- SD-WAN, Firewall Capabilities, and the Cisco Integrated Services Routers (ISRs)
- Introduction to Cisco Secure Intrusion Prevention (NGIPS)
- Surveying the Cisco Secure Firewall Management Center (FMC)
- Cisco SecureX
- Exploring the Cisco Firepower Device Manager (FDM)
- Cisco Defense Orchestrator

Comparing Network Security Solutions That Provide Firewall Capabilities

Deployment Modes of Network Security Solutions and Architectures That Provide Firewall Capabilities

- Routed vs. Transparent Firewalls
- Security Contexts
- Single-Mode Transparent Firewalls
- Surveying the Cisco Secure Firewall Deployment Modes
- Cisco Secure Firewall Interface Modes
- Inline Pair
- Inline Pair with Tap
- Passive Mode
- Passive with ERSPAN Mode
- Additional Cisco Secure Firewall Deployment Design Considerations

High Availability and Clustering

- Clustering

Implementing Access Control

- Implementing Access Control Lists in Cisco ASA

# Table of Contents

Cisco ASA Application Inspection

To-the-Box Traffic Filtering in the Cisco ASA

Object Grouping and Other ACL Features

Standard ACLs

Time-Based ACLs

ICMP Filtering in the Cisco ASA

Network Address Translation in Cisco ASA

Cisco ASA Auto NAT

Implementing Access Control Policies in the Cisco Firepower Threat Defense

Cisco Firepower Intrusion Policies

Variables

Platform Settings Policy

Cisco NGIPS Preprocessors

Cisco Secure Malware Defense

Security Intelligence, Security Updates, and Keeping Firepower Software Up to Date

Security Intelligence Updates

Keeping Software Up to Date

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 8 Virtual Private Networks (VPNs)

Do I Know This Already? Quiz

Foundation Topics

Virtual Private Network (VPN) Fundamentals

An Overview of IPsec

IKEv1 Phase 1

# Table of Contents

- IKEv1 Phase 2
- NAT Traversal (NAT-T)
- IKEv2
- SSL VPNs
- Cisco Secure Client Mobility

Deploying and Configuring Site-to-Site VPNs in Cisco Routers

- Traditional Site-to-Site VPNs in Cisco IOS and Cisco IOS-XE Devices
- Tunnel Interfaces
- GRE over IPsec
- More About Tunnel Interfaces
- Multipoint GRE (mGRE) Tunnels
- DMVPN
- GETVPN
- FlexVPN
- Debug and Show Commands to Verify and Troubleshoot IPsec Tunnels

Configuring Site-to-Site VPNs in Cisco ASA Firewalls

- Step 1: Enable ISAKMP in the Cisco ASA
- Step 2: Create the ISAKMP Policy
- Step 3: Set Up the Tunnel Groups
- Step 4: Define the IPsec Policy
- Step 5: Create the Crypto Map in the Cisco ASA
- Step 6: Configure Traffic Filtering (Optional)
- Step 7: Bypass NAT (Optional)
- Step 8: Enable Perfect Forward Secrecy (Optional)
- Additional Attributes in Cisco Site-to-Site VPN Configurations

Configuring Remote-Access VPNs in the Cisco ASA

- Configuring IPsec Remote-Access VPN in the Cisco ASA

Configuring Clientless Remote Access SSL VPNs in the Cisco ASA

- Cisco ASA Remote-Access VPN Design Considerations

# Table of Contents

- Pre-SSL VPN Configuration Steps
- Understanding the Remote-Access VPN Attributes and Policy Inheritance Model
- Configuring Clientless SSL VPN Group Policies
- Configuring the Tunnel Group for Clientless SSL VPN
- Configuring User Authentication for Clientless SSL VPN
- Enabling Clientless SSL VPN
- Configuring WebType ACLs
- Configuring Application Access in Clientless SSL VPNs

Configuring Client-Based Remote-Access SSL VPNs in the Cisco ASA

- Setting Up Tunnel and Group Policies
- Deploying the Cisco Secure Client
- Understanding Split Tunneling
- Understanding DTLS

Configuring Remote-Access VPNs in Cisco Secure Firewall

- Using the Remote Access VPN Policy Wizard
- Troubleshooting Cisco Secure Firewall Remote-Access VPN Implementations

Configuring Site-to-Site VPNs in the Cisco Secure Firewall

Cisco SD-WAN

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 9 Securing the Cloud

Do I Know This Already? Quiz

Foundation Topics

What Is Cloud and What Are the Cloud Service Models?

DevOps, Continuous Integration (CI), Continuous Delivery (CD), and DevSecOps

# Table of Contents

The Waterfall Development Methodology

The Agile Methodology

DevOps

CI/CD Pipelines

The Serverless Buzzword

Container Orchestration

A Quick Introduction to Containers and Docker

Kubernetes

Microservices and Micro-Segmentation

DevSecOps

Describing the Customer vs. Provider Security Responsibility for the Different Cloud Service Models

Patch Management in the Cloud

Security Assessment in the Cloud and Questions to Ask Your Cloud Service Provider

Cisco Umbrella

The Cisco Umbrella Architecture

Secure Internet Gateway

Cisco Umbrella Investigate

Cisco Secure Email Threat Defense

Forged Email Detection

Sender Policy Framework

Email Encryption

Cisco Secure Email Threat Defense for Office 365

Cisco Attack Surface Management (Formerly Cisco Secure Cloud Insights)

Cisco Secure Cloud Analytics

AppDynamics Cloud Monitoring

Cisco Secure Workload

# Table of Contents

Cisco Secure Workload Agents

Application Dependency Mapping

Cisco Secure Workload Forensics Feature

Cisco Secure Workload Security Dashboard

Cisco XDR

Introducing the XDR Concept

Exploring the Cisco XDR Solution

Cisco XDR Threat Intelligence and Automation

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 10 Content Security

Do I Know This Already? Quiz

Foundation Topics

Content Security Fundamentals

Cisco Async Operating System (AsyncOS)

Cisco Secure Web Appliance

The Cisco Secure Web Appliance Proxy

Cisco Secure Web Appliance in Explicit Forward Mode

Cisco Secure Web Appliance in Transparent Mode

Configuring WCCP in a Cisco ASA to Redirect Web Traffic to a Cisco Secure Web Appliance

Configuring WCCP on a Cisco Switch

Configuring the Cisco Secure Web Appliance to Accept WCCP Redirection

Traffic Redirection with Policy-Based Routing

Cisco Secure Web Appliance Security Services

Deploying Web Proxy IP Spoofing

Configuring Policies in the Cisco Secure Web Appliance

# Table of Contents

Cisco Secure Web Appliance Reports

Cisco Secure Email

Reviewing a Few Email Concepts

Cisco Secure Email Deployment

Cisco Secure Email Listeners

SenderBase

The Recipient Access Table (RAT)

Cisco Secure Email Data Loss Prevention

SMTP Authentication and Encryption

Domain Keys Identified Mail (DKIM)

Cisco Content Security Management Appliance (SMA)

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 11 Endpoint Protection and Detection

Do I Know This Already? Quiz

Foundation Topics

Introduction to Endpoint Protection and Detection

Endpoint Threat Detection and Response (ETDR) and Endpoint Detection and Response (EDR)

Cisco Secure Endpoint

Outbreak Control

IP Blacklists and Whitelists

Cisco Secure Endpoint Application Control

Exclusion Sets

Cisco Secure Endpoint Connectors

Cisco Secure Endpoint Policies

# Table of Contents

Cisco Secure Client AMP Enabler

Cisco Secure Endpoint Engines

Cisco Secure Endpoint Reporting

Cisco Threat Response

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 12 Final Preparation

Hands-on Activities

Suggested Plan for Final Review and Study

Summary

Chapter 13 CCNP and CCIE Security Core SCOR (350-701) Exam Updates

The Purpose of This Chapter

About Possible Exam Updates

Impact on You and Your Study Plan

News about the Next Exam Release

Updated Technical Content

Appendix A: Answers to the Do I Know This Already? Quizzes and Q&A Sections

Glossary

A

B

C

D

E

# Table of Contents

F

G

H

I

K

M

N

O

P

R

S

T

U

W

X

Z

Index

Online Element

Appendix B Study Planner