COMPUTER LEARNING CENTRE
EDUCATE | INNOVATE | EMPOWER

CISCO PARTNER Learning



Implementing and Operating Cisco Security Core Technologies (SCOR)

What you'll learn in this course

The **Implementing andOperatingCiscoSecurityCoreTechnologies (SCOR)** v2.0 course helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcements. You will get extensive hands-on experience deploying Cisco Firepower® Next-Generation Firewall and Cisco Adaptive Security Appliance (ASA) Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch® Enterprise and Cisco Stealthwatch Cloud threat detection features.

This course, including the self-paced material, prepares you for the exam, **Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)**, which leads to the new **CCNP Security, CCIE Security**, and the **CiscoC ertified Specialist- Security Core** certifications. This course also earns you 64 Continuing Education (CE) credits toward recertification.

Course duration

Instructor-ledtraining: 5days in the classroom with hands-on lab practice, plus the equivalent of 3 days of self-paced material

- Virtual instructor-led training: 5 days of web-based classes with hands-on lab practice plus the equivalent of 3 days of self-paced material
- E-learning: Equivalent of 8 days of content with videos, practice, and challenges

How you'll benefit

Thiscourse willhelpyou:

- Gain hands-on experience implementing core security technologies, and learn best practices using Cisco security solutions
- Prepare for the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam
- Qualify for professional and expert-level security job roles
- Earn 64 CE credits toward recertification

© 2022 Cisco and/or its affiliates. All rights reserved.

Who should enroll

- Ciscointegratorsandpartners
- Consulting systems engineer
- Network administrator
- Network designer
- Network engineer
- Network manager
- Security engineer
- Systems engineer
- Technical solutions architect

What to expect in the exam

This coursewillhelp youprepare totakethe**Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)** exam. This exam tests a candidate's knowledge of implementing and operating core security technologies.

After you pass 350-701 SCOR:

- You earn the **Cisco Certified Specialist - Security Core** certification
- You satisfy the core requirement for CCNP Security and CCIE Security.

  To complete your **CCNP Security** certification, pass one of the security concentration exams. To complete your **CCIE Security** certification, pass the **CCIES ecurity** v6.0 LabExam

Technology areas

- Security

Course details

Objectives

After taking this course, you should be able to:

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication

© 2022 Cisco and/or its affiliates. All rights reserved.

- Provide basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Recommended knowledge and training

- To fully benefit from this course, you should have the following knowledge and skills:
- Skills and knowledge equivalent to those learned in**I mplementing and Administering Cisco Solutions (CCNA®)** v1.0 course
- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concepts

These Cisco courses are recommended to help you meet these prerequisites:

- **Implementing and Administering Cisco Solutions (CCNA)**

Outline

- Describing Information Security Concepts*

  -Information Security Overview

  -Assets, Vulnerabilities, and Countermeasures

  - Managing Risk

- Describing Common TCP/IP Attacks*

  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities

  - Internet Control Message Protocol (ICMP) Vulnerabilities

- Describing Common Network Application Attacks*

  - Password Attacks

  -Domain Name System (DNS)-Based Attacks

  - DNS Tunneling

- Describing Common Endpoint Attacks*

  - Buffer Overflow

  - Malware

  - Reconnaissance Attack

© 2022 Cisco and/or its affiliates. All rights reserved.

- Describing Network Security Technologies
  - Defense-in-Depth Strategy
  - Defending Across the Attack Continuum
  - Network Segmentation and Virtualization Overview
- Deploying Cisco ASA Firewall
  - Cisco ASA Deployment Types
  - Cisco ASA Interface Security Levels
  - Cisco ASA Objects and Object Groups
- Deploying Cisco Firepower Next-Generation Firewall
  - Cisco Firepower NGFW Deployments
  - Cisco Firepower NGFW Packet Processing and Policies
  - Cisco Firepower NGFW Objects
- Deploying Email Content Security
  - Cisco Email Content Security Overview
  - Simple Mail Transfer Protocol (SMTP) Overview
  - Email Pipeline Overview
- Deploying Web Content Security
  - Cisco Web Security Appliance (WSA) Overview
  - Deployment Options
  - Network Users Authentication
- Deploying Cisco Umbrella*
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
- Explaining VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
- Introducing Cisco Secure Site-to-Site VPN Solutions
  - Site-to-Site VPN Topologies
  - IPsec VPN Overview
  - IPsec Static Crypto Maps
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration

© 2022 Cisco and/or its affiliates. All rights reserved.

- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Cisco ASA Point-to-Point VPN Configuration
  - Cisco Firepower NGFW Point-to-Point VPN Configuration
- Introducing Cisco Secure Remote Access VPN Solutions
  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - Secure Sockets Layer (SSL) Overview
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Remote Access Configuration Concepts
  - Connection Profiles
  - Group Policies
- Explaining Cisco Secure Network Access Solutions
  - Cisco Secure Network Access
  - Cisco Secure Network Access Components
  - AAA Role in Cisco Secure Network Access Solution
- Describing 802.1X Authentication
  - 802.1X and Extensible Authentication Protocol (EAP)
  - EAP Methods
  - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- Configuring 802.1X Authentication
  - Cisco Catalyst® Switch 802.1X Configuration
  - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
  - Cisco Identity Services Engine (ISE) 802.1X Configuration
- Describing Endpoint Security Technologies*
  - Host-Based Personal Firewall
  - Host-Based Anti-Virus
  - Host-Based Intrusion Prevention System
- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*
  - Cisco AMP for Endpoints Architecture
  - Cisco AMP for Endpoints Engines
  - Retrospective Security with Cisco AMP
- Introducing Network Infrastructure Protection*
  - Identifying Network Device Planes
  - Control Plane Security Controls
  - M anagement Plane Security Controls
- Deploying Control Plane Security Controls*
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection

© 2022 Cisco and/or its affiliates. All rights reserved.

- Deploying Layer 2 Data Plane Security Controls*
  - Overview of Layer 2 Data Plane Security Controls
  - Virtual LAN (VLAN)-Based Attacks Mitigation
  - Spanning Tree Protocol (STP) Attacks Mitigation
- Deploying Layer 3 Data Plane Security Controls*
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding
  - IP Source Guard
- Deploying Management Plane Security Controls*
  - Cisco Secure Management Access
  - Simple Network Management Protocol Version 3
  - Secure Access to Cisco Devices
- Deploying Traffic Telemetry Methods*
  - Network Time Protocol
  - Device and Network Events Logging and Export
  - Network Traffic Monitoring Using NetFlow
- Deploying Cisco Stealthwatch Enterprise*
  - Cisco Stealthwatch Offerings Overview
  - Cisco Stealthwatch Enterprise Required Components
  - Flow Stitching and Deduplication
- Describing Cloud and Common Cloud Attacks*
  - Evolution of Cloud Computing
  - Cloud Service Models
  - Security Responsibilities in Cloud
- Securing the Cloud*
  - Cisco Threat-Centric Approach to Network Security
  - Cloud Physical Environment Security
  - Application and Workload Security
- Deploying Cisco Stealthwatch Cloud*
  - Cisco Stealthwatch Cloud for Public Cloud Monitoring
  - Cisco Stealthwatch Cloud for Private Network Monitoring
  - Cisco Stealthwatch Cloud Operations
- Describing Software-Defined Networking (SDN*)
  - Software-Defined Networking Concepts
  - Network Programmability and Automation
  - Cisco Platforms and APIs

* This section is self-study material that you can complete at your own pace if you are taking the instructor-led version of this course.

© 2022 Cisco and/or its affiliates. All rights reserved.

How to enroll

To enroll in the SCOR course or explore our larger catalog of courses on Cisco Digital Learning, contact us at: info.africa@clc-training.com

Lab outline

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

COMPUTER LEARNING CENTRE
EDUCATE | INNOVATE | EMPOWER

CISCO PARTNER Learning

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) **SCOR_v2.0**C22-743407-04 03/22