

Implementing and Operating Cisco Security Core Technologies 2.0

Duration: 40 Hours (5 Days)

Overview

The **Implementing and Operating Cisco Security Core Technologies (SCOR)** training helps you gain the skills and technologies needed to implement core Cisco security solutions. This training will ready you to provide advanced threat protection against cybersecurity attacks and prepare you for senior-level security roles.

This training prepares you for the 350-701 SCOR v1.1 exam. If passed, you earn the Cisco Certified Specialist - Security Core certification and satisfy the core exam requirement for the Cisco Certified Network Professional (CCNP) Security and Cisco Certified Internetwork Expert (CCIE) Security certifications. This training also earns you 64 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training will help you:

- Gain hands-on experience implementing core security technologies and learn best practices using Cisco security solutions
- Qualify for professional and expert-level security job roles
- Prepare for the 350-701 SCOR v1.1 exam
- Earn 64 CE credits towards recertification

This course prepares you to take the exam:

350-701 SCOR core exam

What to expect in the exam

Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) v1.1 is a 120-minute exam associated with the Cisco Certified Specialist - Security Core certification and satisfies the core exam requirement for the CCNP Security and CCIE Security certifications.

This exam tests your knowledge of implementing and operating core security technologies, including:

- Network security
- Cloud security
- Content security
- Endpoint protection and detection
- Secure network access
- Visibility and enforcement

Who Should Enroll

- Security Engineers
- Network Engineers
- Network Designers
- Network Administrators
- Systems Engineers
- Consulting Systems Engineers
- Technical Solutions Architects
- Cisco Integrators and Partners
- Network Managers
- Program Managers
- Project Managers

Technology areas

- Security

Training overview

Objectives

- Describe information security concepts and strategies within the network
- Describe security flaws in the transmission protocol/internet protocol (TCP/IP) and how they can be used to attack networks and hosts
- Describe network application-based attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Deploy Cisco Secure Firewall Threat Defense basic configurations
- Deploy Cisco Secure Firewall Threat Defense IPS, malware, and fire policies
- Deploy Cisco Secure Email Gateway basic configurations
- Deploy Cisco Secure Email Gateway policy configurations
- Describe and implement basic web content security features and functions provided by Cisco Secure Web Appliance
- Describe various attack techniques against the endpoints

- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Provide basic understanding of endpoint security and be familiar with common endpoint security technologies
- Describe Cisco Secure Endpoint architecture and basic features
- Describe Cisco Secure Network Access solutions
- Describe 802.1X and extensible authentication protocol (EAP) authentication
- Configure devices for 802.1X operations
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions
- Deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs
- Configure point-to-point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Describe Cisco secure remote access connectivity solutions
- Deploy Cisco secure remote access connectivity solutions
- Provide an overview of network infrastructure protection controls
- Examine various defenses on Cisco devices that protect the control plane
- Configure and verify Cisco IOS software layer 2 data plane controls
- Configure and verify Cisco IOS software and Cisco ASA layer 3 data plane controls
- Examine various defenses on Cisco devices that protect the management plane
- Describe the baseline forms of telemetry recommended for network infrastructure and security devices
- Describe deploying Cisco Secure Network Analytics
- Describe basics of cloud computing and common cloud attacks
- Describe how to secure cloud environment
- Describe the deployment of Cisco Secure Cloud Analytics
- Describe basics of software-defined networks and network programmability

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 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 skills can be found in the following Cisco Learning Offering:

- Implementing and Administering Cisco Solutions (CCNA®)

Outline

- Network Security Technologies
- Cisco Secure Firewall ASA Deployment
- Cisco Secure Firewall Threat Defense Basics
- Cisco Secure Firewall Threat Defense IPS, Malware, and File Policies
- Cisco Secure Email Gateway Basics
- Cisco Secure Email Policy Configuration
- Cisco Secure Web Appliance Deployment
- VPN Technologies and Cryptography Concepts
- Cisco Secure Site-to-Site VPN Solutions
- Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Point-to-Point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Cisco Secure Remote-Access VPN Solutions
- Remote-Access SSL VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Describing Information Security Concepts
- Describe Common TCP/IP Attacks
- Describe Common Network Application Attacks
- Common Endpoint Attacks
- Cisco Umbrella Deployment
- Endpoint Security Technologies

- Cisco Secure Endpoint
- Cisco Secure Network Access Solutions
- 802.1X Authentication
- 802.1X Authentication Configuration
- Network Infrastructure Protection
- Control Plane Security Solutions
- Layer 2 Data Plane Security Controls
- Layer 3 Data Plane Security Controls
- Management Plane Security Controls
- Traffic Telemetry Methods
- Cisco Secure Network Analytics Deployment
- Cloud Computing and Cloud Security
- Cloud Security
- Cisco Secure Cloud Analytics Deployment
- Software-Defined Networking

Lab outline

- Configure Network Settings and NAT on Cisco Secure Firewall ASA
- Configure Cisco Secure Firewall ASA Access Control Policies
- Configure Cisco Secure Firewall Threat Defense NAT
- Configure Cisco Secure Firewall Threat Defense Access Control Policy
- Configure Cisco Secure Firewall Threat Defense Discovery and IPS Policy
- Configure Cisco Secure Firewall Threat Defense Malware and File Policy
- Configure Listener, HAT, and RAT on Cisco Email Secure Email Gateway
- Configure Cisco Secure Email Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between Cisco Secure Firewall Threat Defense Devices
- Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
- Examine Cisco Umbrella Dashboard and DNS Security

- Examine Cisco Umbrella Secure Web Gateway and Cloud-Delivered Firewall
- Explore Cisco Umbrella CASB Functionalities
- Explore Cisco Secure Endpoint
- Perform Endpoint Analysis Using Cisco Secure Endpoint Console
- Explore File Ransomware Protection by Cisco Secure Endpoint Console
- Explore Secure Network Analytics v7.4.2
- Explore Global Threat Alerts Integration and ETA Cryptographic Audit
- Explore Cloud Analytics Dashboard and Operations
- Explore Secure Cloud Private and Public Cloud Monitoring