

Document Generated: 06/30/2024

Learning Style: On Demand

Provider: Cisco

Difficulty: Intermediate

Course Duration: 40 Hours

Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 - On Demand



Course Information

About this course:

This course helps you prepare for the Cisco CCNP Security and CCIE Security

certifications and for senior-level security roles. It will teach you the skills and technologies you need to implement core Cisco security solutions, providing you advanced threat protection against cybersecurity attacks. You will also learn security for cloud and content, networks, endpoint protection, secure network access, visibility, and enforcements. With extensive hands-on experience, you will learn to deploy Cisco Firepower® Next-Generation Firewall and Cisco Adaptive Security Appliance (Cisco ASA) Firewall; configure access control policies, mail policies, and 802.1X Authentication; and more. The course will also provide introductory practice on Cisco Stealthwatch® Enterprise and Cisco Stealthwatch Cloud threat detection features.

Upon completing this course, you will be fully prepared to take the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam, passing which will lead to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications.

Course Objective:

After taking this course, you should be able to:

- 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
- 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 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
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy 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
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Audience:

- Systems engineers
- Consulting systems engineers
- Technical solutions architects
- Security engineers
- Network engineers, designers, administrators, and managers
- Cisco integrators and partners

Prerequisite:

To fully benefit from this course, you should have the following knowledge and skills:

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA®) v1.0 course
- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of Microsoft Windows
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concepts

This Cisco course is recommended to help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA) v1.0

Course Outline:

Describing Information Security Concepts*

Information Security Overview
Managing Risk
Vulnerability Assessment
Understanding CVSS

Describing Common TCP/IP Attacks*

Legacy TCP/IP Vulnerabilities
IP Vulnerabilities
ICMP Vulnerabilities
TCP Vulnerabilities
UDP Vulnerabilities
Attack Surface and Attack Vectors
Reconnaissance Attacks
Access Attacks
Man-In-The-Middle Attacks
Denial of Service and Distributed Denial of Service Attacks
Reflection and Amplification Attacks
Spoofing Attacks
DHCP Attacks

Describing Common Network Application Attacks*

- Password Attacks
- DNS-Based Attacks
- DNS Tunneling
- Web-Based Attacks
- HTTP 302 Cushioning
- Command Injections
- SQL Injections
- Cross-Site Scripting and Request Forgery
- Email-Based Attacks

Describing Common Endpoint Attacks*

- Buffer Overflow
- Malware
- Reconnaissance Attack
- Gaining Access and Control
- Gaining Access via Social Engineering
- Gaining Access via Web-Based Attacks
- Exploit Kits and Rootkits
- Privilege Escalation
- Post-Exploitation Phase
- Angler Exploit Kit

Describing Network Security Technologies

- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Stateful Firewall Overview
- Security Intelligence Overview
- Threat Information Standardization
- Network-Based Malware Protection Overview
- IPS Overview
- Next Generation Firewall Overview
- Email Content Security Overview
- Web Content Security Overview
- Threat Analytic Systems Overview
- DNS Security Overview
- Authentication, Authorization, and Accounting Overview
- Identity and Access Management Overview
- Virtual Private Network Technology Overview
- Network Security Device Form Factors Overview

Deploying Cisco ASA Firewall

- Cisco ASA Deployment Types
- Cisco ASA Interface Security Levels
- Cisco ASA Objects and Object Groups

- Network Address Translation
- Cisco ASA Interface ACLs
- Cisco ASA Global ACLs
- Cisco ASA Advanced Access Policies
- Cisco ASA High Availability Overview

Deploying Cisco Firepower Next-Generation Firewall

- Cisco Firepower NGFW Deployments
- Cisco Firepower NGFW Packet Processing and Policies
- Cisco Firepower NGFW Objects
- Cisco Firepower NGFW NAT
- Cisco Firepower NGFW Prefilter Policies
- Cisco Firepower NGFW Access Control Policies
- Cisco Firepower NGFW Security Intelligence
- Cisco Firepower NGFW Discovery Policies
- Cisco Firepower NGFW IPS Policies
- Cisco Firepower NGFW Malware and File Policies

Deploying Email Content Security

- Cisco Email Content Security Overview
- SMTP Overview
- Email Pipeline Overview
- Public and Private Listeners
- Host Access Table Overview
- Recipient Access Table Overview
- Mail Policies Overview
- Protection Against Spam and Graymail
- Anti-virus and Anti-malware Protection
- Outbreak Filters
- Content Filters
- Data Loss Prevention
- Email Encryption

Deploying Web Content Security

- Cisco WSA Overview
- Deployment Options
- Network Users Authentication
- HTTPS Traffic Decryption
- Access Policies and Identification Profiles
- Acceptable Use Controls Settings
- Anti-Malware Protection

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
- Keys in Cryptography
- Public Key Infrastructure

Introducing Cisco Secure Site-to-Site VPN Solutions

- Site-to-Site VPN Topologies
- IPsec VPN Overview
- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

Deploying Cisco IOS VTI-Based Point-to-Point

- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec IKEv2 VPN Configuration

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
- SSL Overview

Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW

- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies
- Cisco ASA Remote Access VPN Configuration
- Cisco Firepower NGFW Remote Access VPN Configuration

Explaining Cisco Secure Network Access Solutions

- Cisco Secure Network Access

Cisco Secure Network Access Components
AAA Role in Cisco Secure Network Access Solution
Cisco Identity Services Engine
Cisco TrustSec

Describing 802.1X Authentication

802.1X and EAP
EAP Methods
Role of RADIUS in 802.1X Communications
RADIUS Change of Authorization

Configuring 802.1X Authentication

Cisco Catalyst Switch 802.1X Configuration
Cisco WLC 802.1X Configuration
Cisco ISE 802.1X Configuration
Supplicant 802.1x Configuration
Cisco Central Web Authentication

Describing Endpoint Security Technologies*

Host-Based Personal Firewall
Host-Based Anti-Virus
Host-Based Intrusion Prevention System
Application Whitelists and Blacklists
Host-Based Malware Protection
Sandboxing Overview
File Integrity Checking

Deploying Cisco AMP for Endpoints*

Cisco AMP for Endpoints Architecture
Cisco AMP for Endpoints Engines
Retrospective Security with Cisco AMP
Cisco AMP Device and File Trajectory
Managing Cisco AMP for Endpoints

Introducing Network Infrastructure Protection*

Identifying Network Device Planes
Control Plane Security Controls
Management Plane Security Controls
Network Telemetry
Layer 2 Data Plane Security Controls
Layer 3 Data Plane Security Controls

Deploying Control Plane Security Controls*

Infrastructure ACLs

Control Plane Policing
Control Plane Protection
Routing Protocol Security

Deploying Layer 2 Data Plane Security Controls*

Overview of Layer 2 Data Plane Security Controls
VLAN-Based Attacks Mitigation
STP Attacks Mitigation
Port Security
Private VLANs
DHCP Snooping
ARP Inspection
Storm Control
MACsec Encryption

Deploying Layer 3 Data Plane Security Controls*

Infrastructure Antispoofing ACLs
Unicast Reverse Path Forwarding
IP Source Guard

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your LinkedIn profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

[Find Out More](#) or [See List Of Badges](#)