FIREFLY

CONTACT US

Implementing and Operating Cisco Security Core Technologies

DURATION: 5 DAYS COURSE CODE: SCOR FORMAT: LECTURE/LAB

COURSE DESCRIPTION

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 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 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, helps prepare you to take the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications.

WHO SHOULD ATTEND

Security Engineer

Network Engineer

Network Designer

Network Administrator

Systems Engineer

Consulting Systems Engineer

Technical Solutions Architect

Cisco Integrators/Partners

Network Manager

Cisco integrators and partners

PREREQUISITES

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 the Windows operating system

Working knowledge of Cisco IOS networking and concepts

Familiarity with basics of networking security concepts

LEARNING OBJECTIVES

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 IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco FirePower NGFW

Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and EAP authentication

Provide basic understanding of endpoint security and describe AMP for Endpoints architecture and basic features

Examine various defenses on Cisco devices that protect the control and management planes

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

COURSE OUTLINE

1. Describing Information Security Concepts*

- Information Security Overview
- Managing Risk
- Vulnerability Assessment
- Understanding CVSS

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

COURSE OUTLINE

- Mail Policies Overview
- Protection Against Spam and Graymail
- Anti-virus and Anti-malware Protection
- Outbreak Filters
- Content Filters
- Data Loss Prevention
- Email Encryption

9. 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
10. Deploying Cisco Umbrella*
    - Cisco Umbrella Architecture
    - Deploying Cisco Umbrella
    - Cisco Umbrella Roaming Client
    - Managing Cisco Umbrella
    - Cisco Umbrella Investigate Overview
11. Explaining VPN Technologies and Cryptography
    - VPN Definition
    - VPN Types
    - Secure Communication and Cryptographic Services
    - Keys in Cryptography
    - Public Key Infrastructure
12. 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
13. Deploying Cisco IOS VTI-Based Point-to-Point
    - Cisco IOS VTIs
    - Static VTI Point-to-Point IPsec IKEv2 VPN Configuration
14. 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
15. Introducing Cisco Secure Remote Access VPN Solutions
    - Remote Access VPN Components
    - Remote Access VPN Technologies
    - SSL Overview
16. 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
17. 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
18. Describing 802.1X Authentication
    - 802.1X and EAP
    - EAP Methods
    - Role of RADIUS in 802.1X Communications
    - RADIUS Change of Authorization
19. 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
20. 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
21. 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

COURSE OUTLINE

22. 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
23. Deploying Control Plane Security Controls*
    - Infrastructure ACLs
    - Control Plane Policing
    - Control Plane Protection
    - Routing Protocol Security
24. 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
25. Deploying Layer 3 Data Plane Security Controls*
    - Infrastructure Antispoofing ACLs
    - Unicast Reverse Path Forwarding
    - IP Source Guard

DISCOVERY LABS

1: Configure Network Settings And NAT On Cisco ASA
2: Configure Cisco ASA Access Control Policies
3: Configure Cisco Firepower NGFW NAT
4: Configure Cisco Firepower NGFW Access Control Policy
5: Configure Cisco Firepower NGFW Discovery and IPS Policy
6: Configure Cisco NGFW Malware and File Policy
7: Configure Listener, HAT, and RAT on Cisco ESA
8: Configure Mail Policies
9: Configure Proxy Services, Authentication, and HTTPS Decryption
10: Enforce Acceptable Use Control and Malware Protection
11: Examine the Umbrella Dashboard
12: Examine Cisco Umbrella Investigate
13: Explore DNS Ransomware Protection by Cisco Umbrella
14: Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
15: Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
16: Configure Remote Access VPN on the Cisco Firepower NGFW
17: Explore Cisco AMP for Endpoints
18: Perform Endpoint Analysis Using AMP for Endpoints Console
19: Explore File Ransomware Protection by Cisco AMP for Endpoints Console
20: Explore Cisco Stealthwatch Enterprise v6.9.3
21: Explore CTA in Stealthwatch Enterprise v7.0
22: Explore the Cisco Cloudlock Dashboard and User Security
23: Explore Cisco Cloudlock Application and Data Security
24: Explore Cisco Stealthwatch Cloud
25: Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors