6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

Implementing and Operating Cisco Security Core Technologies (SCOR)

In this **Implementing and Operating Cisco Security Core Technologies**course provides a comprehensive, hands-on introduction to modern Cisco security technologies used to protect enterprise, campus, remote, and cloud-based networks. The curriculum begins with core network security and information security concepts, including common TCP/IP, application, and endpoint attacks, establishing a strong foundation for understanding today's threat landscape. Students are then guided through the architecture, deployment, and policy configuration of Cisco Secure Firewall platforms, including Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense, with focused coverage on access control, NAT, intrusion prevention, malware protection, and file policies. VPN technologies are explored in depth, covering cryptographic fundamentals, site-to-site IPsec solutions, VTI-based tunnels, and secure remote-access VPNs using both ASA and Threat Defense platforms.

The course extends beyond perimeter security to address email, web, endpoint, and DNS-layer protection using Cisco Secure Email Gateway, Cisco Secure Web Appliance, Cisco Umbrella, and Cisco Secure Endpoint. Learners gain practical experience configuring email security policies, web proxy services, HTTPS decryption, acceptable use controls, and malware protection, while also exploring endpoint detection, ransomware protection, and endpoint analysis workflows. Network access control and infrastructure protection are covered through detailed examination of 802.1X authentication, control plane security, and Layer 2 and Layer 3 data plane protections, ensuring students understand how to secure the network fabric itself.

Advanced visibility and analytics capabilities are introduced through traffic telemetry methods, Cisco Secure Network Analytics, and Cisco Secure Cloud Analytics, providing insight into encrypted traffic analysis, global threat intelligence, and anomaly detection across on-premises and cloud environments. The course concludes with coverage of cloud computing and cloud security principles, software-defined networking security considerations, and integrated security operations across private and public cloud deployments. A robust lab program reinforces all concepts, allowing students to configure, deploy, and analyze real Cisco security technologies in practical scenarios, equipping them with the skills needed to design, implement, and operate secure enterprise and cloud networks.

How You'll Benefit

This course 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 toward recertification

Price :

$4295.00

Duration :

5 Days

Certification Exam:

350-701

CE Credit: 64

Objective

Upon completing this course, the student will be able to:

- 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

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 Attend

The primary audience for this course is as follows:

- 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

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®)

Course Outline

Course 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