Implementing and Operating Cisco Security Core Technologies

Duration: 5 Days Course Code: SCOR Version: 2.0

Overview:

The Implementing and Operating Cisco Security Core Technologies (SCOR) 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 Secure Firewall ASA and Cisco Secure Firewall Threat Defense; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Network Analytics and and Cisco Secure Cloud Analytics features.

Please note that this course is a combination of Instructor-Led and Self-Paced Study - 5 days in the classroom and approx 3 days of self study. The self-study content will be provided as part of the digital courseware that you will recieve at the beginning of the course and should be part of your preparation for the exam.

This course is worth 64 Continuing Education (CE) Credits

Target Audience:

Security individuals who need to be able to implement and operate core security technologies including network security, cloud security, content security, endpoint protection and detection, secure network access, visibility and enforcements.

Objectives:

- **After completing this course you should 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
- 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

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
- Describe how to secure cloud environment
- Describe the deployment of Cisco Secure Cloud Analytics
- Describe basics of software-defined networks and network programmability

Prerequisites:

Attendees should meet the following prerequisites:

- 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
- CCNA - Implementing and Administering Cisco Solutions

Testing and Certification

Recommended as preparation for the following exams:

- **350-701 -** Implementing and Operating Cisco Security Core Technologies (SCOR 350-701)

This is the core exam for the Cisco CCNP Security certification, in order to gain the CCNP Security certification you will also need to pass **one** of the concentration exams.

Follow-on-Courses:

- SAUI - Implementing Automation for Cisco Security Solutions
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention
- SFWIPA - Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention
- SISE - Implementing and Configuring Cisco Identity Services Engine
- SVPN - Implementing Secure Solutions with Virtual Private Networks
- SESA - Securing Email with Cisco Email Security Appliance
- SWSA - Securing the Web with Cisco web Security Appliance

Content:

Network Security Technologies

- Defense-in-Depth Strategy
- Defending Across the Attack Continuum
- Network Segmentation and Virtualization Overview
- Stateful Firewall Overview
- Cisco IOS Zone-Based Policy 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 (VPN) Technology Overview
- Network Security Device Form Factors Overview

Cisco Secure Firewall ASA Deployment

- Cisco Secure Firewall ASA Deployment Types
- Cisco Secure Firewall ASA Interface Security Levels
- Cisco Secure Firewall ASA Objects and Object Groups
- Network Address Translation
- Cisco Secure Firewall ASA Interface ACLs
- Cisco Secure Firewall ASA Global ACLs
- Cisco Secure Firewall ASA Advanced Access Policies
- Cisco Secure Firewall ASA High Availability Overview

Cisco Secure Firewall Threat Defense Basics

- Cisco Secure Firewall Threat Defense Deployments
- Cisco Secure Firewall Threat Defense Packet Processing and Policies
- Cisco Secure Firewall Threat Defense Objects
- Cisco Secure Firewall Threat Defense NAT
- Cisco Secure Firewall Threat Defense Prefilter Policies
- Cisco Secure Firewall Threat Defense Access Control Policies
- Cisco Secure Firewall Threat Defense Security Intelligence
- Cisco Secure Firewall Threat Defense Discovery Polices

Cisco Cisco Secure Firewall Threat Defense IPS, Malware and File Policies

Remote Access SSL VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense

- Remote Access Configuration Concepts
- Connection Profiles
- Group Policies
- Cisco Secure Firewall ASA Remote Access VPN Configuration
- Cisco Secure Firewall Threat Defense Remote Access VPN Configuration

Describing Information Security Concepts (Self-Study)

- Information Security Overview
- Assets, Vulnerabilities and Countermeasures
- Managing Risk
- Vulnerability Assessment
- Understanding CVSS

Describe Common TCP/IP Attacks (Self-Study)

- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- ICMP 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

Describe Common Network Application Attacks (Self-Study)

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

Common Endpoint Attacks (Self-Study)

- 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

Control Plane Security Controls (Self-Study)

- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection
- Routing Protocol Security

Layer 2 Data Plane Security Controls (Self-Study)

- 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

Layer 3 Data Plane Security Controls (Self-Study)

- Infrastructure Antispoofing ACLs
- Unicast Reverse Path Forwarding
- IP Source Guard

Management Plane Security Controls (Self-Study)

- Cisco Secure Management Access
- Simple Network Management Protocol Version 3
- Secure Access to Cisco Devices
- AAA or Management Access

Traffic Telemetry Methods (Self-Study)

- Network Time Protocol
- Device and Network Events Logging and Export
- Network Traffic Monitoring Using NetFlow

Cisco Secure Network Analytics Deployment (Self-Study)

- Cisco Secure Network Analytics Overview
- Cisco Secure Network Analytics Required Components
- Flow Stitching and Deduplication
- Cisco Secure Network Analytics Optional Components
- Cisco Secure Network Analytics and ISE Integration
- Cisco Secure Network Analytics with Global Threat Alerts
- Cisco Encrypted Traffic Analytics (ETA)
- Host Groups
- Security Events and Alarms
- Host, Role and Default Policies

Cloud Computing and Cloud Security

- Cisco Secure Firewall Threat Defense IPS Policies
- Cisco Secure Firewall Threat Defense Malware and File Policies

Cisco Secure Email Gateway Basics

- Cisco Secure Email Overview
- SMTP Overview
- Email Pipeline Overview
- Public and Private Listeners
- Host Access Table Overview
- Recipient Access Table Overview

Cisco Secure Email Policy Configuration

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

Cisco Secure Web Appliance Deployment

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

VPN Technologies and Cryptography Concepts

- VPN Definition
- VPN Types
- Secure Communication and Cryptographic Services
- Keys in Cryptography
- Public Key Infrastructure

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

Cisco IOS VTI-Based Point-to-Point IPsec VPNs

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

Point-to-Point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense

- Point-to-Point VPNs on the Cisco Secure

Cisco Umbrella Deployment (Self-Study)

- Cisco Umbrella Capabilities
- Cisco Umbrella Identities and Policies Overview
- Cisco Umbrella DNS Security
- Cisco Umbrella Investigate Overview
- Cisco Umbrella Secure Web Gateway
- Cisco Umbrella CASB Functionalities

Endpoint Security Technologies (Self-Study)

- Host-Based Personal Firewall
- Host-Based Anti-Virus
- Host-Based Intrusion Prevention System
- Application Allowed Lists and Blocked Lists
- Host-Based Malware Protection
- Sandboxing Overview
- File Integrity Checking

Cisco Secure Endpoint (Self-study)

- Cisco Secure Endpoint Architecture
- Cisco Secure Endpoint Engines
- Retrospective Security with Cisco Secure Endpoint
- Cisco Secure Endpoint Device and File Trajectory
- Managing Cisco Secure Endpoint for Endpoints

Cisco Secure Network Access Solutions (Self-study)

- Cisco Secure Network Access
- Cisco Secure Network Access Components
- AAA Role in Cisco Secure Network Access Solution
- Cisco ISE
- Cisco TrustSec

Describing 802.1X Authentication (Self-study)

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

Configuring 802.1X Authentication (Self-study)

- Cisco Catalyst Switch 802.1X Configuration
- Cisco IBNS 2.0 Configuration on Cisco Catalyst Switch
- Cisco WLC 802.1X Configuration
- Cisco ISE 802.1X Configuration
- Supplicant 802.1x Configuration
- Cisco Central Web Authentication

Network Infrastructure Protection (Self-Study)

(Self-Study)

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the Cloud
- Cloud Deployment Models
- Patch Management in the Cloud
- Security Assessment in the Cloud

Cloud Security (Self-Study)

- Cisco Threat-Centric Approach to Network Security
- Cloud Physical Environment Security
- Application and Workload Security
- Cloud Management and API Security
- Network Functions Virtualization (NFV) and Virtual Network Function (VNF)
- Cisco NFV Examples
- Reporting and Threat Visibility in Cloud
- Cloud Access Security Broker
- Cisco Cloudlock
- OAuth and OAuth Attacks

Cisco Secure Cloud Analytics Deployment (Self-Study)

- Cisco Secure Cloud Analytics for Public Cloud Monitoring
- Cisco Secure Cloud Analytics for Private Network Monitoring
- Cisco Secure Cloud Analytics Operations

Software-Defined Networking (Self-Study)

- Software-Defined Networking Concepts
- Network Programmability and Automation
- Cisco Platforms and APIs
- Basic Python Scripts for Automation

Labs

- Discovery Lab 1: Configure Network Settings And NAT On Cisco Secure Firewall ASA
- Discovery Lab 2: Configure Cisco Secure Firewall ASA Access Control Policies
- Discovery Lab 3: Configure Cisco Secure Firewall Threat Defense NAT
- Discovery Lab 4: Configure Cisco Secure Firewall Threat Defense Access Control Policy
- Discovery Lab 5: Configure Cisco Secure Firewall Threat Defense Discovery and IPS Policy
- Discovery Lab 6: Configure Cisco Secure Firewall Threat Defense Malware and File Policy
- Discovery Lab 7: Configure Listener, HAT, and RAT on Cisco Secure Email Gateway
- Discovery Lab 8: Configure Cisco Secure Email Policies
- Discovery Lab 9: Configure Proxy Services, Authentication, and HTTPS Decryption

Firewall ASA and Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall ASA Point-to-Point VPN Configuration
- Cisco Secure Firewall Threat Defense Point-to-Point VPN Configuration

Cisco Secure Remote Access VPN Solutions

- Remote Access VPN Components
- Remote Access VPN Technologies
- SSL Overview

- 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

- Discovery Lab 10: Enforce Acceptable Use Control and Malware Protection
- Discovery Lab 11: Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Discovery Lab 12: Configure Point-to-Point VPN between the Cisco Secure Firewall Threat Defense Devices
- Discovery Lab 13: Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
- Discovery Lab 14: Examine Cisco Umbrella Dashboard and DNS Security
- Discovery Lab 15: Explore Cisco Umbrella Secure Web Gateway and Cloud-Delivered Firewall
- Discovery Lab 16: Explore Cisco Umbrella CASB Functionalities
- Discovery Lab 17: Explore Cisco Secure Endpoint
- Discovery Lab 18: Perform Endpoint Analysis Using Cisco Secure Endpoint Console
- Discovery Lab 19: Explore File Ransomware Protection by Cisco Secure Endpoint Console
- Discovery Lab 20: Explore Secure Network Analytics v7.4.2
- Discovery Lab 21: Explore Global Threat Alerts Integration and ETA Cryptographic Audit
- Discovery Lab 22: Explore Cloud Analytics Dashboard and Operations
- Discovery Lab 23: Explore Secure Cloud Private and Public Cloud Monitoring

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/