

# Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

## Duration: 5 Days

## Prerequisites:

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 the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concepts

These Cisco courses are recommended to help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

## Course Description:

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.1 training helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this training, 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 Adaptive Security Appliance (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 training, including the self-paced material, prepares you for the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications.

## Course Objectives:

After taking this training, you should be able to:

- 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 Internetwork Operating System (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
- 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 basics of cloud computing and common cloud attacks and how to secure cloud environment

## Intended Audience:

- Cisco integrators and partners
- Consulting systems engineer
- Network administrator
- Network designer
- Network engineer
- Network manager
- Security engineer
- Systems engineer
- Technical solutions architect

## Course Outline:

- Describing Information Security Concepts
- Describing Common TCP/IP Attacks
- Describing Common Network Application Attacks
- Describing Common Endpoint Attacks

- Describing Network Security Technologies
- Deploying Cisco ASA Firewall
- Deploying Cisco Firepower Next-Generation Firewall
- Deploying Email Content Security
- Deploying Web Content Security
- Deploying Cisco Umbrella
- Explaining VPN Technologies and Cryptography
- Introducing Cisco Secure Site-to-Site VPN Solutions
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
- Introducing Cisco Secure Remote Access VPN Solutions
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
- Explaining Cisco Secure Network Access Solutions
- Describing 802.1X Authentication
- Configuring 802.1X Authentication
- Describing Endpoint Security Technologies
- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints
- Introducing Network Infrastructure Protection
- Deploying Control Plane Security Controls
- Deploying Layer 2 Data Plane Security Controls
- Deploying Layer 3 Data Plane Security Controls
- Deploying Management Plane Security Controls
- Deploying Traffic Telemetry Methods
- Deploying Cisco Stealthwatch Enterprise
- Describing Cloud and Common Cloud Attacks
- Securing the Cloud
- Deploying Cisco Stealthwatch Cloud
- Describing Software-Defined Networking (SDN)

## Lab outline

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption

## REGISTER NOW!

training@trends.com.ph  
 (+632) 8863-2123  
 www.trendssacademy.com.ph

## COURSE OUTLINE

- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

## REGISTER NOW!

training@trends.com.ph  
(+632) 8863-2123  
www.trendssacademy.com.ph