

350-701 – SCOR – Cisco – CCNP Security – Implementing and Operating Cisco Security Core Technologies

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

Cisco 350-701 SCOR – CCNP Security Core

About this Course

- You will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also gives you a foundation in network programmability, automation, and software-defined networking.

Course Goals:

- After taking this course, 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
-

Audience:

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

Course Format



Classroom



Virtual Online



Video Archive (24/7)



Certificate of
Course Completion

Course Duration

- 5 days (monday – friday 09:00 – 17:00)

or

- **40 hours in after hours**
- sat. sun. 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
- mon./wed. 19:00 – 23:00
- tue./thu. 19:00 – 23:00

Payments



Next Class:

■ Notice

There are no upcoming events.

Prerequisites:

- Before taking this course, you should have:
 - 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) v1.0**

**This course can be used to prepare for
the following exams:**

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