

CCIE Security Expert Level Certification (350-701 SCOR)

Duration: 80 Hours

Certification Level: Expert

Course Overview

The **CCIE Security Expert Level Certification (350-701 SCOR)** is designed for networking professionals who want to validate their expertise in enterprise security, including advanced network security, cloud security, and automation. This course prepares you for the **CCIE Security exam** by covering topics such as secure network infrastructures, VPN technologies, firewalls, and intrusion prevention systems (IPS). Candidates will gain hands-on experience in securing networks and implementing security solutions at the expert level.

Course Objectives

Upon completion of this course, participants will:

- Gain in-depth knowledge of network security concepts
 - Learn to design, implement, and troubleshoot secure network infrastructures
 - Understand VPN technologies, firewalls, and intrusion prevention systems
 - Implement security automation solutions and security monitoring
 - Prepare for the **CCIE Security** certification exam
-

Course Modules

Module 1: Security Concepts and Network Security Fundamentals (10 Hours)

- Overview of security architectures and best practices
- Security policy development and enforcement
- Introduction to security concepts: Confidentiality, Integrity, and Availability (CIA)
- Secure network design principles
- Implementing and managing firewalls, VPNs, and intrusion detection systems (IDS)

Module 2: Threat Defense Technologies (14 Hours)

- Configuring next-generation firewalls (NGFW)
- Understanding and implementing Intrusion Prevention Systems (IPS)
- Site-to-site and remote-access VPN configurations
- Implementing security for mobile users and remote workers
- Advanced threat protection and detection techniques

Module 3: VPN Technologies and Remote Access Solutions (10 Hours)

- IPsec VPNs: Configuration and troubleshooting
- SSL VPN technologies and remote access solutions
- DMVPN (Dynamic Multipoint VPN)
- Cisco AnyConnect and VPN concentrator solutions
- Configuring and securing remote access environments

Module 4: Identity Management and Access Control (10 Hours)

- Identity and access management (IAM) fundamentals
- Implementing Cisco Identity Services Engine (ISE)
- Role-based access control (RBAC)
- AAA (Authentication, Authorization, Accounting) protocols
- Integration of Cisco ISE with external authentication services

Module 5: Secure Network Infrastructure (12 Hours)

- Advanced network security design and implementation
- Layer 2 and Layer 3 security technologies: ACLs, DDoS protection
- Securing routing protocols: OSPF, EIGRP, BGP
- Security in network devices (routers, switches)
- Secure access control and network segmentation

Module 6: Security Automation and Orchestration (8 Hours)

- Introduction to security automation tools
- Automating security configurations with Ansible, Puppet, and Cisco Prime
- Using Cisco Identity Services Engine (ISE) for security policy automation
- Network programmability for security with APIs
- Implementing orchestration solutions for network security

Module 7: Cloud Security (8 Hours)

- Cloud security fundamentals and challenges
- Securing cloud environments and services
- Cisco Cloud Security solutions: Umbrella, Cloudlock, etc.
- Implementing multi-cloud security strategies
- Securing hybrid cloud and cloud-based applications

Module 8: Security Monitoring and Incident Response (8 Hours)

- Security information and event management (SIEM)
- Monitoring and managing security logs and events
- Incident detection and response strategies
- Implementing security monitoring tools (e.g., Cisco Stealthwatch)
- Best practices for handling security incidents and breaches

Module 9: CCIE Lab and Exam Preparation (10 Hours)

- Hands-on practice with real-world security scenarios
- Lab exercises on configuring and securing networks
- Mock exams and practical exercises
- Final exam preparation tips and strategies
- Understanding the CCIE exam format and structure

Target Audience

This course is ideal for:

- Network security engineers looking to specialize in enterprise security
- IT professionals responsible for securing large-scale network infrastructures
- Network administrators and architects aiming for expert-level security certifications
- Those preparing for the **CCIE Security** certification exam