Cisco Certified Network Professional (CCNP) Security

Price	Duration	Delivery Methods
$3,195.00	5 Daytime Classes Or 10 Evening Classes	Virtual, In-Person, Private Group,

CAREER SKILLS+™

Course Description:

This specialized training program is designed for network security professionals who are interested in enhancing their skills and knowledge in securing Cisco networks. The course covers in-depth concepts and practices necessary to secure network environments against modern threats, vulnerabilities, and attacks. Participants will be prepared for the CCNP Security certification, focusing on core security technologies and various specialized areas through concentration exams.

Certification Preparation:

The course prepares participants for the core exam, 350-701 SCOR (Implementing and Operating Cisco Security Core Technologies), as well as guidance on choosing and preparing for one of the concentration exams.

Learning Mode: Hybrid (Instructor-Led and Self-Paced)

Duration: Varied, typically between 5-10 days of instructor-led training supplemented by extensive self-study.

Materials Provided: Extensive digital courseware, including simulation and lab exercises.

Who Should Attend

This course is tailored for network security engineers, security administrators, and IT personnel who manage and secure network devices in Cisco environments.

Course Objectives

Core Security Concepts: Master the fundamentals of network security, policies, and defense strategies.
Secure Network Design: Learn how to design and implement secure network infrastructures.
Threat Defense: Implement advanced threat defense mechanisms in Cisco environments.
Secure Connectivity: Set up secure connectivity solutions like VPNs and end-to-end encryption.
Content Security: Manage and secure network access to content, including email and web traffic.
Endpoint Protection: Deploy technologies for endpoint protection including firewalls and intrusion prevention systems (IPS).
Network Visibility and Enforcement: Utilize tools to enhance visibility and enforce security policies across the network.

Course Prerequisites

Knowledge Requirements: Understanding of network fundamentals, and basic knowledge of security concepts.
Certifications: CCNA Security or any CCIE certification can serve as a prerequisite.
Experience: Practical experience with network security, including implementing and configuring security solutions.

Agenda

1. Lessons

Introduction to Network Security Principles
Implementing Secure Network Architectures

Configuring Cisco Firewall Technologies and Intrusion Prevention Systems
Deploying Secure Connectivity: VPNs and Encryption
Managing Identity Services and Access Control
Advanced Threat Protection and Secure Network Management
Integration of Cloud and Content Security Solutions
Using Cisco's Advanced Security Tools and Technologies
Security Automation and Programmability

2. Lab Outline

Configuring and Managing Cisco ASA and Firepower Services
Implementing and Troubleshooting VPNs
Deploying Cisco ISE for Network Access and Identity Management
Setting Up Intrusion Prevention Systems and Advanced Malware Protection
Implementing and Monitoring Content Security Policies
Utilizing Cisco Stealthwatch for Network Visibility and Threat Detection
Integrating Cloud Security with Cisco Umbrella
Automating Security Tasks with Cisco Security APIs