

## CCNA Security

**NOTE:** This Exam is Retired. On February 24, 2020, Cisco released a new consolidated CCNA exam, the Cisco Certified Network Associate (200-301 CCNA). [Click for to visit the new certification page.](#)

This new update replaces the following certifications:

- CCNA Cloud
- CCNA Collaboration
- CCNA Data Center
- CCDA
- CCNA Industrial
- CCNA Routing and Switching
- CCNA Security
- CCNA Service Provider
- CCNA Wireless

SecureNinja's CCNA Security (Cisco Certified Network Associate Security) training and certification boot camp in Washington, DC prepares you for the arduous Cisco 210-260 IINS exam and focuses on security principles and technologies, using Cisco security products to provide hands-on examples. Using instructor-led discussions, extensive hands-on lab exercises, and supplemental materials, this course allows learners to understand common security concepts, and deploy basic security techniques utilizing a variety of popular security appliances within a "real-life" network infrastructure.

### Course Completion

Upon completion of the course, students will have the knowledge and skills to:

- Describe common network security concepts
- Secure routing and switching infrastructure
- Deploy basic authentication, authorization and accounting services
- Deploy basic firewalling services
- Deploy basic site-to-site and remote access VPN services
- Describe the use of more advanced security services such as intrusion protection, content security, and identity management

### Topics Covered

1. SecurityConcepts
2. SecureNetworkDevices
3. Layer2Security
4. Firewall
5. VPN
6. advanced topics

## **Pre-requisites**

The knowledge and skills that a learner must have before attending this course are as follows:

Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1).

Working knowledge of the Windows operating system.

## **Required Exam**

210-260 IINS

This exam tests the candidate's knowledge of secure network infrastructure, understanding core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web, and email content security, and endpoint security. This exam validates skills for installation, troubleshooting, and monitoring of a secure network to maintain integrity, confidentiality, and availability of data and devices.

## **Course Length**

40 Hours

## **Follow on Course**

- Security+
- CEH
- CISSP