CCNA Security Boot Camp: Implementing Cisco IOS Network Security (IINS) (CS-CCNA-Sec)

Modality: Virtual Classroom

Duration: 4 Days

CLC: 35 Units

About the course:

The CCNA Security educational plan emphasizes core security advancements, troubleshooting, installation, monitoring, and technologies of network devices to maintain confidentiality, integrity, and accessibility of devices and data, and competency in the innovation that Cisco utilizes in its security system.

The certification of CCNA Security is a piece of the DOD 8570 directive.

This boot camp incorporates vouchers for exam and sets you up for the below tests:

- 210-260 IINS

Salary Estimate:

The normal compensation for an analyst of Cisco Systems Network Security is $70,000 every year.

This boot camp incorporates below progressions:

Cisco IINS - Implementing IOS Network Security

Course Objectives:

After finishing this course, the student will have the ability to match these goals:

1. Define the concepts of common network security
2. Secure infrastructure for switching and routing
3. Deploy basic services of accounting, authorization, and, authentication
4. Deploy basic services for firewalling
5. Organize basic remote access VPN and site-to-site services
6. Describe the usage of more progressive services for security, for example, content security, intrusion protection, and identity management

Targeted Audience:

This course intended Targeted Audience are the students who wish to prove themselves network associates in the network security domain and also have information that is comprised in the course of ICND1 - Interconnecting Cisco Networking Devices Part 1.

Prerequisites:

Any certification of CCIE or any substantial certification of Cisco CCNA, CCENT, Routing, and Switching can go about as a prerequisite.

Course Outline:

- **Module 1: Describe common network security concepts**
- **Module 2: Secure routing and switching infrastructure**
- **Module 3: Deploy basic authentication, authorization and accounting services**
- **Module 4: Deploy basic firewalling services**
- **Module 5: Deploy basic site-to-site and remote access VPN services**
- **Module 6: Describe the use of more advanced security services such as intrusion protection, content security and identity management**