CCNA Security Certification (Exam 210-260 IINS) (Coming Soon)

Modality: Self-Paced Learning

Duration: No

SUBSCRIPTION: Learn, Master, Master Plus

About this course:

The Cisco Certified Network Associate Security (CCNA Security) will enable you attain associate-level knowledge and skills required to secure Cisco networks.
In this course you will learn about the design, implementation, and monitoring of a comprehensive security policy using Cisco IOS security features and technologies as examples. You will also learn about security controls of Cisco IOS devices as well as a functional introduction to the Cisco Adaptive Security Appliance (ASA). This course enables you to perform basic tasks to secure a network using Cisco IOS security features, which are available through web-based GUIs on the Cisco ASA, and the command-line interface (CLI) on Cisco routers and switches.
Site-to-site virtual private network (VPN) configuration is covered on both the Cisco IOS and the Cisco ASA. Modern malware examples are included in this course as are cryptographic techniques using stronger hashing and encryption algorithms. Current versions of Cisco IOS, Cisco ASA, and Cisco AnyConnect are featured.

This certification is a DoD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

Exam:

This Course prepares you for the following exam:

- 210-260 IINS

Course Objective:

- 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
- Advanced security services such as intrusion protection, content security and identity management
- Develop a comprehensive network security policy to counter threats against information security
- Configure routers with Cisco IOS software security features, including management and reporting functions
- Bootstrap the Cisco ASA Firewall for use in a production network
- Configure the Cisco ASA Firewall for remote access to a Secure Sockets Layer (SSL) VPN

- Configure a Cisco IOS zone-based firewall (ZBF) to perform basic security operations on a network
- Configure site-to-site VPNs using Cisco IOS features
- Configure security features on IOS switches to mitigate various Layer 2 and Layer 3 attacks
- How a network can be compromised using freely available tools
- Implement line passwords, and enable passwords and secrets
- Examine authentication, authorization, and accounting (AAA) concepts and features using the local database as well as Cisco Secure ACS 5.2
- Configure packet filtering on the perimeter router

Audience:

- Network designers
- Network, systems, and security engineers
- Network and security managers

Job Roles associated with CCNA Security certification:

- Security engineer **$87,470**
- Network security engineer **$86,633**
- Network administrator **$62,181**
- Network engineer **$76,768**
- Senior network engineer **$97,615**
- Information security analyst **$68,991**
- Systems engineer (computer networking / IT) **$72,700**

Prerequisite:

- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

Course Outline:

Module 1. Security Concepts

- Threatscape
- Threat defense technologies
- Security policy and basic security architectures
- Cryptographic technologies

Module 2. Secure Network Devices

- Implementing AAA
- Management protocols and systems
- Securing the control plane

Module 3. Layer 2 Security

- Securing Layer 2 infrastructures
- Securing Layer 2 protocols

Module 4. Firewall

- Firewall technologies
- Introducing the Cisco ASA v9.2
- Cisco ASA access control and service policies
- Cisco IOS zone-based firewall

Module 5. VPN

- IPsec technologies
- Site-to-site VPN
- Client-based remote access VPN
- Clientless remote access VPN

Module 6. Advanced Topics

- Intrusion detection and protection
- Endpoint protection
- Content security
- Advanced network security architectures
- Classroom Live Labs

Lab 1: Exploring Cryptographic Technologies

Lab 2: Configure and Verify AAA

Lab 3: Configuration Management Protocols

Lab 4: Securing Routing Protocols

Lab 5: VLAN Security and ACLs on Switches

Lab 6: Port Security and Private VLAN Edge

Lab 7: Securing DHCP, ARP, and STP

Lab 8: Explore Firewall Technologies

Lab 9: Cisco ASA Interfaces and NAT

Lab 10: Access Control Using the Cisco ASA

Lab 11: Exploring Cisco IOS Zone-Based Firewall

Lab 12: Explore IPsec Technologies

Lab 13: IOS-Based Site-to-Site VPN

Lab 1: ASA-Based Site-to-Site VPN

Lab 14: Remote Access VPN: ASA and AnyConnect

Lab 15: Clientless Remote Access VPN

Lab 16: Configure AAA and Secure Remote Administration

Lab 17: Configure Secure Network Management Protocols

Lab 18: Configure Secure EIGRP Routing

Lab 19: Configure Secure Layer 2 Infrastructure

Lab 20: Configure DHCP Snooping and STP Protection

Lab 21: Configure Interfaces and NAT on the Cisco ASA

Lab 22: Configure Network Access Control with the Cisco ASA

Lab 23: Configure Site-to-Site VPN on IOS

Lab 24: Configure AnyConnect Remote Access VPN on ASA

Lab 25: Configure Clientless SSL VPN on the ASA