Cisco 210-260 IINS Implementing Cisco Network Security

Cisco CCNA Security

210-260 IINS Implementing Cisco Network Security 3.0

About this Course:

- 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.

Course Goals:

- 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

The Course is Designed to:

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

Course Format:


Attendance Course


Online (Live) Remote

Course language option: You can choose the language in which the training will be conducted – Bulgarian or English. All our instructors are fluent in English.

Learning materials: in electronic format (Learning materials are in English) included in the price with unlimited access.

Lab environment: each student has his own lab environment where the exercises are conducted, part of the course.

Course Duration:

- 5 working days (09:00 – 17:00) or 40 hoursSaturday and Sunday 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
  Monday and Wednesday 19:00 – 23:00
  Tuesday and Thursday 19:00 – 23:00

Payments:

An application for an invoice is accepted at the time of enrollment in the respective course.

An invoice is issued within 7 days of confirming the payment.

Next Class:

Notice
There are no upcoming events.
For more information, use the contact format. We will contact you to confirm the data.

Prerequisites:

- Skills and equivalent knowledge of those available in Connecting Cisco Network Devices Part 1

(ICND1)Working knowledge of the Windows operating systemWorking knowledge of Cisco iOS

The course prepares for the following certification levels:

- CCNA Security 210-260