IMPLEMENTING CISCO IOS NETWORKING SECURITY (IINS V3.0)

Course number : 123

Overview

Implementing Cisco Network Security (IINS) v3.0 is a 5-day instructor-led course focusing 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.

EXAM INFORMATION:

- Course tuition does not include an exam voucher.

CERTIFICATION INFORMATION:

- To earn Cisco Security certfication, you must past the Cisco 210-260 IINS exam.

REDEEM YOUR CISCO LEARNING CREDITS (CLCS):

- This course is eligible for Cisco Learning Credit (CLC) redemption.
- Want to learn more about Cisco CLCs? **Click to view our CLCs infographic**.

What you'll learn

- 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

Who should attend

Pre-requis

- Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1)
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- To participate in the hands-on labs in this class, you need to bring a laptop computer with the following:
  - Windows 7 or 8.1 or 10 is recommended. Mac OSX 10.6 or greater is supported as well.
  - Intel Celeron or better processors are preferred.
  - 1 GB or more of RAM
  - Browser Requirements: Internet Explorer 10 or greater or Mozilla Firefox. (Safari and Mozilla Firefox for Mac OSX)
    Note: Our labs currently cannot run on Microsoft Edge (Windows 10) due to it not supporting Extensions/Add-ons or Google Chrome due to Java being removed from the platform itself.
  - All students are required to have administrator rights to their PCs and cannot be logged in to a domain using any Group Policies that will limit their machine's capabilities.
    If you do not have administrator rights to your PC, you at least need permissions to download, install, and run Cisco Any Connect Client and Java.
  - If you are participating in a WebEx event, it is highly recommended to take this class at a location that has bandwidth speeds at a minimum of 1 Mbps bandwidth speeds.
  - All PCs require the latest Java Runtime Environment, which can be downloaded from www.java.com.

Outline

Security Concepts

- Threatscape
- Threat Defense Technologies
- Security Policy and Basic Security Architectures
- Cryptographic Technologies
- Module Summary
- Module Self-Check

Secure Network Devices

- Implementing AAA
- Management Protocols and Systems
- Securing the Control Plane
- Module Summary
- Module Self-Check

Layer 2 Security

- Securing Layer 2 Infrastructure
- Securing Layer 2 Protocols
- Module Summary
- Module Self-Check

Firewall

- Firewall Technologies
- Introducing the Cisco ASA v9.2
- Cisco ASA Access Control and Service Policies
- Cisco IOS Zone Based Firewall
- Module Summary
- Module Self-Check

VPN

- IPsec Technologies
- Site-to-Site VPN
- Client Based Remote Access VPN
- Clientless Remote Access VPN
- Module Summary
- Module Self-Check

Advanced Topics

- Intrusion Detection and Protection
- Lesson 2: Endpoint Protection
- Lesson 3: Content Security
- Lesson 4: Advanced Network Security Architectures
- Lesson 5: Module Summary
- Lesson 6: Module Self-Check

Schedule

Location Dates Status

Tuition

IN CLASSROOM OR ONLINE PRIVATE TEAM TRAINING

STANDARD	**$3895**
GOVERNMENT	**$3895**

Contact Us »

FAQ

Certification