



Course Outline

Implementing Cisco IOS Network Security (IINS) v1.0

Duration: 5 days (30 hours)

Learning Objectives:

- Develop a comprehensive network security policy to counter threats against information security.
- Configure routers on the network perimeter with Cisco IOS Software security features.
- Configure a Cisco IOS zone-based firewall to perform basic security operations on a network.
- Configure site-to-site VPNs using Cisco IOS features.
- Configure IPS on Cisco network routers.
- Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic.

Target Audience:

Channel Partner/Reseller, Customers, Employees

Prerequisites:

- Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1).
- Working knowledge of the Windows operating system.

Topics Covered:

- Module 1: Introduction to Network Security Principles
- Module 2: Perimeter Security
- Module 3: Network Security Using Cisco IOS Firewalls
- Module 4: Site-to-Site VPNs
- Module 5: Network Security Using Cisco IOS IPS
- Module 6: LAN, SAN, Voice, and Endpoint Security Overview