

Implementing Cisco IOS Network Security

Overview

The Implementing Cisco IOS Network Security (IINS) course focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features and technologies as examples.

The course covers security controls of Cisco IOS devices as well as a functional introduction to the Cisco ASA adaptive security appliance. Using instructor-led discussion, lecture, and hands-on lab exercises, this course allows students to perform basic tasks to secure a small branch office network using Cisco IOS security features that are available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASA appliances.

Pre-request: The knowledge and skills that a learner must have before attending this course are as follows:

- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- CCENT, CCNA Routing and Switching or any Cisco CCIE Certification

To gain the prerequisite skills and knowledge, Cisco strongly recommends the knowledge of the following courses:

- Interconnecting Cisco Networking Devices Part 1 (ICND1)

Course duration: 40 Hours

Objective

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe the components of a comprehensive network security policy that can be used to counter threats against IT systems, within the context of a security policy life cycle
- Develop and implement security countermeasures that are aimed at protecting network elements as part of the network infrastructure
- Deploy and maintain threat control and containment technologies for perimeter security in small and midsize networks
- Describe secure connectivity strategies and technologies using VPNs, as well as configure site-to-site and remote-access VPNs using Cisco IOS features

Course Content:

Networking Security Fundamentals

- Introducing Networking Security Concepts
- Understanding Security Policies Using a Life-Cycle Approach
- Building a Security Strategy for Borderless Networks

Protecting the Network Infrastructure

- Introducing Cisco Network Foundation Protection
- Protecting the Network Infrastructure Using Cisco Configuration Professional
- Securing the Management Plane on Cisco IOS Devices
- Configuring AAA on Cisco IOS Devices Using Cisco Secure ACS
- Securing the Data Plane on Cisco Catalyst Switches
- Securing the Data Plane in IPv6 Environments

Threat Control and Containment

- Planning a Threat Control Strategy
- Implementing Access Control Lists for Threat Mitigation
- Understanding Firewall Fundamentals
- Implementing Cisco IOS Zone-Based Policy Firewalls
- Configuring Basic Firewall Policies on Cisco ASA Appliances
- Understanding IPS Fundamentals
- Implementing Cisco IOS IPS

Secure Connectivity

- Understanding the Fundamentals of VPN Technologies
- Introducing Public Key Infrastructure
- Examining IPsec Fundamentals
- Implementing Site-to-Site VPNs on Cisco IOS Routers
- Implementing SSL VPNs Using Cisco ASA Appliances

Target Audience

This course is designed for:

- Network Designers
- Network Administrators
- Network Engineers
- Network Managers
- Systems Engineers