Implementing Cisco Network Security (IINS) 3.0

Length: 5 Days

Prerequisites: This course is designed for students that have knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1), Interconnecting Cisco Networking Devices Part 2 (ICND2), working knowledge of the Windows Operating System, and knowledge of Cisco IOS networking and concepts.

About this course: Implementing Cisco Network Security (IINS) v3.0 is a 5-day instructor-led course to end users. The course focuses on security principles and technologies, using 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. Upon completing this course, you will be able to meet these 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
- Technical Features of the Course
- Network security principles
- Firewalls, IPSs, router ACLs
- Encryption and VPNs
- IOS security features and Secure Device Manager
- LAN, SAN, Voice, and Endpoint Security

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
- Lab 2-1: Hardening Network Elements Using Cisco Configuration Professional
- Lab 2-2: Securing Administrative Access to Cisco Routers

- Lab 2-3: Configuring AAA on Cisco Routers and Switches to Use Cisco Secure ACS
- Lab 2-4: Configuring Data Plane Security on Layer 2 Switches

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
- Lab 3-1: Using ACLs to Implement a Threat Containment Strategy
- Lab 3-2: Implementing Cisco IOS Zone-Based Firewalls
- Lab 3-3: Implementing Basic Network Connectivity Using Cisco ASDM on the Cisco ASA Appliance
- Lab 3-4: Configuring 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
- Lab 4-1: Configuring Site-to-Site IPsec VPNs
- Lab 4-2: Configuring SSL VPNs on Cisco ASA Appliances Using Cisco ASDM