

Implementing Cisco Network Security (IINS) 3.0

Length: 5 Days

Prerequisites:

- 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

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 completion of the course, students will have the knowledge and skills to:

- 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

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
-