Learning Services

Cisco Training on Demand

Implementing Cisco Network Security (IINS)

Overview
Implementing Cisco® Network Security (IINS) Version 3.0 is a Cisco Training on Demand course. It is in the curriculum for the CCNA® Security certification. It provides you with an understanding of common security concepts and how to deploy basic security techniques using a variety of popular security appliances in a real-life network infrastructure.

This course provides a foundational understanding of the current threat landscape and threat-defense technologies used today, and security policy and architectures. The IINS course prepares you to work in a network security role working with various technologies, such as cryptography, identity management, firewalls, and infrastructure protection.

Interested in purchasing this course in volume at discounts for your company? Contact ctod-sales@cisco.com.

Duration
The IINS Cisco Training on Demand course is a self-paced course based on the 5-day instructor-led training version. It consists of 21 sections of instructor video and text totaling more than 11 hours of instruction, along with interactive activities, 26 hands-on lab exercises, content review questions, and challenge questions.

Target Audience
This course is designed for network security specialists, security technicians, security administrators, network security support engineers, principle system engineers, Cisco Channel Partners, and those preparing for the 210-260 IINS exam.
Objectives

After completing this course, you should be able to:

- Describe common network security concepts
- Secure routing and switching infrastructure
- Deploy basic authentication, authorization, and accounting services
- Deploy basic firewaling 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 Prerequisites

The knowledge and skills recommended before attending this course are:

- 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.

Course Outline

- Course Introduction
- Section 1: Threatscape
- Section 2: Threat-Defense Technologies
- Section 3: Security Policy and Basic Security Architectures
- Section 4: Cryptographic Technologies
- Section 5: AAA
- Section 6: Management Protocols and Systems
- Section 7: Securing the Control Plane
- Section 8: Securing Layer 2 Infrastructure
- Section 9: Securing Layer 2 Protocols
- Section 10: Firewall Technologies
- Section 11: Introducing the Cisco ASA Version 9.2
- Section 12: Cisco ASA Access Control and Service Policies
- Section 13: Cisco IOS Zone-Based Firewall
- Section 14: IPsec Technologies
- Section 15: Site-to-Site VPN
- Section 16: Client-Based Remote-Access VPN
- Section 17: Clientless Remote-Access VPN
- Section 18: Intrusion Detection and Protection
- Section 19: Endpoint Protection
- Section 20: Content Security
- Section 21: Advanced Network Security Architectures

**Labs Outline**

This course contains 26 hands-on lab exercises.

**Figure 1.** Topology for All Labs in Implementing Cisco Network Security

The labs included in this course are:

- Discovery Lab 4.14: Exploring Cryptographic Technologies
- Discovery Lab 5.11: Configure and Verify AAA
- Challenge Lab 5.12: Configure AAA and Secure Remote Administration
- Discovery Lab 6.16: Configuration Management Protocols
- Challenge Lab 6.17: Configure Secure Network Management Protocols
- Discovery Lab 7.8: Securing Routing Protocols
- Challenge Lab 7.9: Configure Secure EIGRP Routing
- Discovery Lab 8.17: VLAN Security and ACLs on Switches
- Discovery Lab 8.18: Port Security and Private VLAN Edge
- Challenge Lab 8.19: Configure Secure Layer 2 Infrastructure
- Discovery Lab 9.11: Securing DHCP, ARP, and STP
- Challenge Lab 9.12: Configure DHCP Snooping and STP Protection
- Discovery Lab 10.8: Explore Firewall Technologies
● Discovery Lab 11.12: Cisco ASA Interfaces and NAT
● Challenge Lab 11.13: Configure Interfaces and NAT on the Cisco ASA
● Discovery Lab 12.7: Access Control Using the Cisco ASA
● Challenge Lab 12.8: Configure Network Access Control with the Cisco ASA
● Discovery Lab 13.9: Exploring Cisco IOS Zone-Based Firewall
● Discovery Lab 14.14: Explore IPsec Technologies
● Discovery Lab 15.12: Cisco IOS-Based Site-to-Site VPN
● Discovery Lab 15.13: Cisco ASA-Based Site-to-Site VPN
● Challenge Lab 15.14: Configure a Site-to-Site VPN on IOS
● Discovery Lab 16.9: Remote-Access VPN: Cisco ASA and Cisco AnyConnect
● Challenge Lab 16.10: Configure AnyConnect Remote Access VPN on ASA
● Discovery Lab 17.11: Clientless Remote-Access VPN
● Challenge Lab 17.12: Configure Clientless SSL VPN on the ASA

Cisco Capital Financing Helps You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.