FIREFLY

CONTACT US

# Implementing Cisco IOS Network Security

DURATION: 5 DAYS COURSE CODE: IINS FORMAT: LECTURE/LAB

## COURSE DESCRIPTION

Implementing Cisco Network Security (IINS) v3.0 is a 5-day instructor-led course presented by Cisco Learning Partners to end users and channel partner customers.

The course focuses on security principles and technologies, using Cisco 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.

## WHO SHOULD ATTEND

Network designers

Network, systems, and security engineers

Network and security managers

## 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

## LEARNING OBJECTIVES

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 OUTLINE

1. Security Concepts
    - Threatscape
    - Threat Defense Technologies
    - Security Policy and Basic Security Architectures
    - Cryptographic Technologies
    - Module Summary
    - Module Self-Check
2. Secure Network Devices
    - Implementing AAA
    - Management Protocols and Systems
    - Securing the Control Plane
    - Module Summary
    - Module Self-Check
3. Layer 2 Security
    - Securing Layer 2 Infrastructure
    - Securing Layer 2
    - Protocols Module Summary
    - Module Self-Check
4. Firewall
    - Firewall Technologies
    - Introducing the Cisco ASA v9.2
    - Cisco ASA Access Control and Service Policies
    - Cisco IOS Zone Based Firewall
    - Module Summary
    - Module Self-Check
5. VPN
    - IPsec Technologies
    - Site-to-Site VPN
    - Client Based Remote Access VPN
    - Clientless Remote Access VPN
    - Module Summary
    - Module Self-Check
6. Advanced Topics
    - Intrusion Detection and Protection
    - Endpoint Protection
    - Content Security
    - Advanced Network Security Architectures
    - Module Summary
    - Module Self-Check

## DISCOVERY LABS

1: Configure AAA and Secure Remote Administration
2: Configure Secure Network Management Protocols
3: Configure Secure EIGRP Routing
4: Configure Secure Layer 2 Infrastructure
5: Configure DHCP Snooping and STP Protection
6: Configure Interfaces and NAT on the Cisco ASA
7: Configure Network Access Control with the Cisco ASAl
8: Configure Site-to-Site VPN on IOS
9: Configure AnyConnect Remote Access VPN on ASA
10: Configure Clientless SSL VPN on the ASA