

Cisco® Implementing Cisco® IOS Network Security (IINS)

Course Outlines

Cisco® Implementing Cisco® IOS Network Security (IINS)

Days of Training: 5

Overview

Students will focus on comprehensive security policies and how they affect networks, and perform tasks to secure the office network using Cisco IOS security features through web-based GUIs and the command-line interface on the Cisco routers and switches.

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.

Cisco® Interconnecting Cisco® Networking Devices Part 2 (ICND2)
Cisco® Interconnecting Cisco® Networking Devices Part 1 (ICND1)

Next Steps

Cisco® Securing Networks with ASA Fundamentals (SNAF)
Cisco® Implementing Cisco® Intrusion Prevention System (IPS)
Cisco® Implementing Cisco® NAC Appliance (CANAC)
Cisco® Implementing Cisco® Security Monitoring, Analysis and Response System (MARS)
Cisco® Securing Networks with Cisco® Routers and Switches (SNRS)
Cisco® Securing Networks with ASA Advanced (SNAA)

3392CWEE-ILT

Lesson 1: Introduction to Network

Security Principles

Examining Network Security Fundamentals
Examining Network Attack Methodologies
Examining Operations Security
Understanding and Developing a Comprehensive Network Security Policy
Building Cisco Self-Defending Networks
Lab 1-1: Embedding a Secret Message Using Steganography
Lab 1-2: Scanning a Computer System Using Testing Tools
Lab 1-3: Scanning a Network Using Testing Tools

Lesson 2: Perimeter Security

Securing Administrative Access to Cisco Routers
Introducing Cisco SDM
Configuring AAA on a Cisco Router Using the Local Database
Configuring AAA on a Cisco Router to Use Cisco Secure ACS
Implementing Secure Management and Reporting
Locking Down the Router
Lab 2-1: Securing Administration Access to Cisco Routers
Lab 2-2: Configuring AAA on Cisco Routers to Use the Local Database
Lab 2-3: Configuring AAA on Cisco Routers to Use Cisco Secure ACS
Lab 2-4: Implementing Secure Management and Reporting
Lab 2-5: Using Cisco SDM One-Step Lockdown and Security Audit

Lesson 3: Network Security Using

Cisco IOS Firewalls

Introducing Firewall Technologies
Creating Static Packet Filters Using ACLs
Configuring Cisco IOS Zone-Based Policy Firewall
Lab 3-1: Creating Static Packet Filters Using ACLs
Lab 3-2: Configuring a Cisco IOS Zone-Based Policy Firewall

Lesson 4: Site-to-Site VPNs

Examining Cryptographic Services
Examining Symmetric Encryption
Examining Cryptographic Hashes and Digital Signatures
Examining Asymmetric Encryption and PKI
Examining IPsec Fundamentals
Building a Site-to-Site IPsec VPN
Configuring IPsec on a Site-to-Site VPN Using Cisco SDM
Lab 4-1: Configuring a Site-to-Site IPsec VPN

Lesson 5: Network Security Using

Cisco IOS IPS

Introducing IPS Technologies
Configuring Cisco IOS IPS Using Cisco SDM
Lab 5-1: Configuring Cisco IOS IPS

Lesson 6: LAN, SAN, Voice, and Endpoint Security

Overview

Examining Endpoint Security
Examining SAN Security
Examining Voice Security
Mitigating Layer 2 Attacks
Lab 6-1: Using Cisco Catalyst Switch Security Features