

Implementing Cisco IOS Network Security

Course Code: IINS

Duration: 5

Overview

Implementing Cisco IOS Network Security (IINS) v1.0 is an instructor-led course presented by Cisco training partners to their end-user customers. This five day course focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. Learners will be able to perform basic tasks to secure a small branch type office network using Cisco IOS security features available through web-based GUI's (Cisco Router and Security Device Manager [SDM]) and the command-line interface (CLI's) on the Cisco routers and switches.

Pre-Requisites

Before attending this course delegates must have completed the following

- ICND1, Interconnecting Cisco Network Devices Part 1
- ICND2, Interconnecting Cisco Network Devices Part 2
- Or
- CCNABC, Cisco CCNA Certification Fast Track Programme

It is also recommended that before attending this training delegates would have a basic knowledge of Cisco lifecycle deployment, SONA, Wireless standards (IEEE), wireless regulator environment (FCC, ETSI, etc) and wireless certification organisation (WIFI alliance)

Target Audience

The Primary audience for this course is as follows;

Network Designers

Network Administrators

Network Engineers

Network Managers

Systems Engineers

Objectives

Upon completing this course, the learner will be able to meet these overall objectives;

- Develop a comprehensive network security policy to counter threats against information security.

- Configure routers on the network perimeter with Cisco IOS Software Security features.
- Configure a Cisco IOS zone-based firewall to perform basic security operations on a network.
- Configure site-to-site VPN's using Cisco IOS features
- Configure IPS on Cisco Network routers
- Configure LAN devices to control access, resist attacks, shield other network devices and systems and protect the integrity and confidentiality of network traffic.

Content

Introduction to Network Security Principles

- Examining Network Security Fundamentals
- Examining Network Attack Methodologies
- Examining Operations Security
- Examining Operations Security
- Building Cisco Self-Defending Networks

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

Network Security Using Cisco IOS Firewalls

- Introducing Firewall Technologies
- Creating Static Packet Filters Using ACL's
- Configuring Cisco IOS Zone-based Policy Firewall

Site-to-Site VPN's

- Examining Cryptographic Services
- Examining Symmetric Encryption
- Examining Cryptographic Hashes and Digital Signatures
- Examining Asymmetric Encryption and KPI
- Examining IPsec Fundamentals
- Building Site-to Site IPsec VPN
- Configuring IPsec on a Site-to Site VPN Using Cisco SDM

Network Security Using Cisco IOS IPS

- Introducing IPS Technologies
- Configuring Cisco IOS IPS Using Cisco SDM

LAN, SAN, Voice and Endpoint Security Overview

- Examining Endpoint Security
- Examining SAN Security
- Examining Voice Security
- Migrating Layer 2 Attacks

Certification

This course will prepare delegates for the following exam(s);
640-553 -IINS Implementing Cisco IOS Network Security