
Implementing Cisco IOS Network Security

Duration: 5 Days **Course Code: IINS**

Overview:

Implementing Cisco IOS Network Security (IINS) v1.0 is an instructor-led course that focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. Delegates will be able to perform the basic tasks required 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.

Target Audience:

This is an ideal course for those individuals looking for an entry level understanding of security on the network.

Objectives:

- **After you complete this course you will be able to:**
 - 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.
-

Prerequisites:

Attendees should meet the following prerequisites:

- [ICND1](#) Interconnecting Cisco Network Devices Part 1
- [ICND2](#) Interconnecting Cisco Network Devices Part 2
- Or
- [CCNABC](#) Cisco CCNA Certification Fast Track Programme

Testing and Certification

Recommended preparation for exam(s):

- [640-553](#) IINS Implementing Cisco IOS Network Security

This exam is required for those delegates wishing to obtain the CCNA Security Concentration Certification

Follow-on-Courses:

Delegates who are focusing on Security may wish to consider the Cisco Certified Security Professional Certification for which the following courses are required.

- SNRS Securing Networks with Cisco Routers and Switches.
- IPS Implementing Cisco Intrusion Prevention System
- SNAF Securing Networks with ASA Fundamentals

Plus **one** elective from the courses below.

- MARS Cisco Security Monitoring, Analysis & Response System
 - CANAC Implementing NAC Appliance (Cisco Clean Access)
 - SNAA Securing Networks with ASA Advance
-

Content:

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

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 PKI
- Examining IPsec Fundamentals
- Building Site-to Site IPsec VPN
- Configuring IPsec on a Site-to Site VPN Using Cisco SDM

Network Security Usind 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

Labs

- 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
- 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
- Lab 3-1: Creating Static Packet Filters Using ACLs
- Lab 3-2: Configuring a Cisco IOS Zone-Based Policy Firewall
- Lab 4-1: Configuring a Site-to-Site IPsec VPN
- Lab 5-1: Configuring Cisco IOS IPS
- Lab 6-1: Using Cisco Catalyst Switch Security Features

Additional Information:

Re-Certification

IINS is part of the Cisco CCNA Security Concentration and is valid for 3 years.

To recertify, pass a CCNA Concentration exam (wireless, security, voice), or pass any 642 - XXX professional level or Cisco Specialist exam (excluding Sales Specialist exams), or pass a current CCIE or CCDE written exam.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 01924 377489

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK