Implementing Cisco IOS Network Security

Duration: 5 Days **Course Code: IINS** **Version: 2.0**

Overview:

This is a five-day instructor-led course that focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features and technologies as examples. The course covers security controls of Cisco IOS devices as well as a functional introduction to the Cisco ASA adaptive security appliance. Using instructor-led discussion, lecture, and hands-on lab exercises, this course provides delegates with the knowledge and skills required to perform the basic tasks to secure a small branch office network using Cisco IOS security features that are available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASA appliances.

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:**
- Describe the components of a comprehensive network security policy that can be used to counter threats against IT systems, within the context of a security policy life cycle
- Develop and implement security countermeasures that are aimed at protecting network elements as part of the network infrastructure
- Deploy and maintain threat control and containment technologies for perimeter security in small and midsize networks
- Describe secure connectivity strategies and technologies using VPNs, as well as configure site-to-site and remote-access VPNs using Cisco IOS features

Prerequisites:

Attendees should meet the following prerequisites:

- **ICND1** - Interconnecting Cisco Network Devices Part 1 is recommended

Testing and Certification

Recommended preparation for exam(s):

- **640-554** - IINS Implementing Cisco IOS Network Security

Delegates wishing to obtain the CCNA SecurityCertification will also need to have passed the ICND1 exam or the CCNA Routing and Switching composite exam.

Follow-on-Courses:

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

- **SECURE** - Securing Networks with Cisco Routers and Switches
- **FIREWALL** - Deploying Cisco ASA Firewall Solutions
- **VPN** - Deploying Cisco ASA VPN Solutions
- **IPS** - Implementing Cisco Intrusion Prevention System

Content:

Networking Security Fundamentals

- Introducing Networking Security Concepts
- Understanding Security Policies Using a Life-Cycle Approach
- Building a Security Strategy for Borderless Networks

Protecting the Network Infrastructure

- Introducing Cisco Network Foundation Protection
- Protecting the Network Infrastructure Using Cisco Configuration Professional
- Securing the Management Plane on Cisco IOS Devices
- Configuring AAA on Cisco IOS Devices Using Cisco Secure ACS
- Securing the Data Plane on Cisco Catalyst Switches
- Securing the Data Plane in IPv6 Environments

Threat Control and Containment

- Planning a Threat Control Strategy
- Implementing Access Control Lists for Threat Mitigation
- Understanding Firewall Fundamentals
- Implementing Cisco IOS Zone-Based Policy Firewalls
- Configuring Basic Firewall Policies on Cisco ASA Appliances
- Understanding IPS Fundamentals
- Implementing Cisco IOS IPS

Secure Connectivity

- Understanding the Fundamentals of VPN Technologies
- Introducing Public Key Infrastructure
- Examining IPsec Fundamentals
- Implementing Site-to-Site VPNs on Cisco IOS Routers
- Implementing SSL VPNs Using Cisco ASA Appliances

Labs

- Lab 2-1: Hardening Network Elements Using Cisco Configuration Professional
- Lab 2-2: Securing Administrative Access to Cisco Routers
- Lab 2-3: Configuring AAA on Cisco Routers and Switches to Use Cisco Secure ACS
- Lab 2-4: Configuring Data Plane Security on Layer 2 Switches
- Lab 3-1: Using ACLs to Implement a Threat Containment Strategy
- Lab 3-2: Implementing Cisco IOS Zone-Based Firewall
- Lab 3-3: Implementing Basic Network Connectivity Using Cisco ASDM on the Cisco ASA Appliance
- Lab 3-4: Configuring Cisco IOS IPS
- Lab 4-1: Configuring Site-to-Site IPsec VPNs
- Lab 4-2: Configuring SSL VPNs on Cisco ASA Appliances Using Cisco ASDM

Additional Information:

Re-Certification
CCNA Security certifications are valid for three years. To recertify, pass ONE of the following before the certification expiration date:Pass the current IINS exam or Pass any current Associate-level exam except for ICND1or Pass any current Cisco Specialist exam (excluding Sales Specialist exams, MeetingPlace Specialist exams, Implementing Cisco TelePresence Installations (ITI) exams, Cisco Leading Virtual Classroom Instruction exams, or any 650 online exams), or Pass any current CCIE Written Exam, or Pass the current CCDE Written Exam OR current CCDE Practical Exam, or Pass the Cisco Certified Architect (CCAr) interview AND the CCAr board review to extend lower certifications

Further Information:

For More information, or to book your course, please Call/Email us on : - +254 713 027 191

KENYA - training.kenya@clclearningafrica.com

TANZANIA - training.tanzania@clclearningafrica.com

UGANDA - training.uganda@clclearningafrica.com

RWANDA - training.rwanda@clclearningafrica.com

BURUNDI - training.burundi@clclearningafrica.com

ETHOPIA - training.ethopia@clclearningafrica.com