
Implementing Cisco Intrusion Prevention System

Duration: 5 Days **Course Code: IPS**

Overview:

The Implementing Cisco Intrusion Prevention System (IPS) course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. It is a five-day instructor-led course aimed at providing network security engineers with the knowledge and skills needed to deploy Cisco IPS-based security solutions. Successful graduates will be able to reduce risk to the IT infrastructure and applications using Cisco IPS features, and provide detailed operations support for the Cisco IPS.

Target Audience:

This course is designed for: Channel Partner / Reseller Customer Employee

Objectives:

- Upon completing this course, the learner will be able to meet these overall objectives:
 - Evaluate products and deployment architectures for the Cisco IPS product line.
 - Perform an initial implementation of a Cisco IPS sensor.
 - Implement an initial security policy using a Cisco IPS sensor according to local policies and environmental requirements.
 - Deploy customized policies to adapt Cisco IPS traffic analysis and response to the target environment.
 - Implement a basic Cisco IPS data management and analysis solution.
 - Implement complex Cisco IPS policy virtualization, high availability, and high performance solutions according to policy and environmental requirements.
 - Perform the initial setup of, and maintain specific Cisco IPS hardware.
-

Prerequisites:

The knowledge and skills that a learner must have before attending this course:

- Working knowledge of the Microsoft Windows operating system
To gain the prerequisite skills and knowledge, Cisco strongly recommends the knowledge of the following courses:
- Interconnecting Cisco Network Devices 1 (ICND1)
- Interconnecting Cisco Network Devices 2 (ICND2)
- Implementing Cisco IOS Network Security (IINS)

Testing and Certification

Recommended as preparation for:

- 642-627 - Implementing Cisco Intrusion Prevention System
IPS is one of the courses required for the **Cisco Certified Network Professional (CCNP) Security** Certification.
-

Follow-on-Courses:

- Securing Networks with Cisco Routers and Switches (SECURE)
 - Deploying Cisco ASA Firewall Solutions (FIREWALL)
 - Deploying Cisco ASAVPN Solutions (VPN)
-

Content:

Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

- Evaluating Intrusion Prevention and Intrusion Detection Systems
- Choosing Cisco IPS Software, Hardware, and Supporting Applications
- Evaluating Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-Evasive Countermeasures
- Choosing a Network IPS and IDS Deployment Architecture

Installing and Maintaining Cisco IPS Sensors

- Integrating the Cisco IPS Sensor into a Network
- Performing the Cisco IPS Sensor Initial Setup
- Managing Cisco IPS Devices

Applying Cisco IPS Security Policies

- Configuring Basic Traffic Analysis
- Implementing Cisco IPS Signatures and Responses
- Configuring Cisco IPS Signature Engines and the Signature Database
- Deploying Anomaly-Based Operation

Adapting Traffic Analysis and Response to the Environment

- Customizing Traffic Analysis
- Managing False Positives and False Negatives
- Improving Alarm and Response Quality

Managing and Analyzing Events

- Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors
- Managing and Investigating Events Using Cisco IPS Manager Express
- Using Cisco IME Reporting and Notifications
- Integrating Cisco IPS with Cisco Security Manager and Cisco Security MARS
- Using the Cisco IntelliShield Database and Services

Deploying Virtualization, High Availability, and High Performance Solutions

- Using Cisco IPS Virtual Sensors
- Deploying Cisco IPS for High Availability and High Performance

Configuring and Maintaining Specific Cisco IPS Hardware

- Configuring and Maintaining the Cisco ASA AIP-SSM and AIP-SSC-5 Modules
- Configuring and Maintaining the Cisco ISR IPS AIM and IPS NME Modules
- Configuring and Maintaining the Cisco IDSM-2

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya