
Implementing Cisco Intrusion Prevention System

Duration: 4 Days **Course Code: IPS**

Overview:

This course aims to provide delegates with the knowledge and skills needed to design, install, configure, and maintain a Cisco IPS sensor for small, medium, and enterprise networks. The course also describes the procedures for managing intrusion prevention system (IPS) alarms.

Target Audience:

The primary audience for this course is as follows: Network designers, Network security administrators, The secondary audience for this course is as follows: Network administrators, Network engineers, Systems engineers

Objectives:

- At the end of the course delegates will be able to;-
 - Explain how the Cisco IPS protects network devices from attacks
 - Install and configure the basic settings on a Cisco IPS 4200 Series Sensor
 - Use the Cisco IDM to configure built-in signatures to meet the requirements of a given security policy
 - Configure some of the more advanced features of the Cisco IPS product line
 - Initialize and install into your environment the rest of the Cisco IPS family of products
 - Use the CLI and the Cisco IDM to obtain system information, and configure the Cisco IPS sensor to allow an SNMP NMS to monitor the Cisco IPS sensor
-

Prerequisites:

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

- Familiarity with networking and security terms and concepts, including completion of the Securing Cisco Network Devices (SND) course
- Strong user-level experience with Microsoft Windows operating systems

Testing and Certification:

Recommended as preparation for exam(s):

- 642-533 IPS - Implementing Cisco Intrusion Prevention System
This course is associated with the CCSP and the Security Specializations
-

Follow-on-Courses:

The following courses are recommended for further study

- CSVPN – Cisco Secure VPN
 - SNRS – Securing Networks with Cisco Routers and Switches
 - SNPA –Securing Networks with PIX and ASA
 - HIPS- Securing Hosts Using Cisco Security Agent.
 - CANAC – Implementing Cisco NAC
 - MARS – Implementing Cisco Security Monitoring , Analysis and Response time
 - SND – Securing Cisco Network Devices
-

Content:

Intrusion Prevention Overview

- Explaining Intrusion Prevention
- Examining Cisco IPS Products
- Examining Cisco IPS Sensor Software Solutions
- Examining Evasive Techniques

Installation of a Cisco IPS 4200 Series Sensor

- Installing a Cisco IPS Sensor Using the CLI
- Using the Cisco IDM
- Configuring Basic Sensor Settings

Cisco IPS Signatures

- Configuring Cisco IPS Signatures and Alerts
- Examining the Signature Engines
- Customizing Signatures

Advanced Cisco IPS Configuration

- Performing Advanced Tuning of Cisco IPS Sensors
- Monitoring and Managing Alarms
Configuring a Virtual Sensor
- Configuring Advanced
Features Configuring Blocking

Additional Cisco IPS Devices

- Installing the Cisco Catalyst 6500 Series IDSM-2
- Initializing the Cisco ASA AIP-SSM

Cisco IPS Sensor Maintenance

- Maintaining Cisco IPS Sensors Managing Cisco IPS Sensors

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