



Enhanced Network Solutions Group

Systems Integration • Learning Solutions • CIO Consulting
Managed Outsourcing • Healthcare Solutions • Security Solutions

7224 Engle Road - Fort Wayne, IN 46804 - Phone: (260) 432-1364 - Fax: (260) 432.3168

IPS Implementing Cisco Intrusion Prevention System

IPS Rev 04.10

4 days

Description

Securing Networks Using Intrusion Prevention Systems (IPS) v6.0 is an update to Securing Networks Using Intrusion Prevention Systems (IPS) v5.0, an instructor-led course on using the Cisco Intrusion Detection System v5.0 product to protect network systems from intrusions and security threats. The course covers important new IPS 6.0 features. The IPS 6.0 course takes a task-oriented approach to teaching the skills to deploy, configure, and administer Cisco IPS sensors.

Prerequisites

- *Experience configuring Cisco IOS software*
- *Certification as a CCNA or the equivalent knowledge*
- *Basic knowledge of the Windows operating system*
- *Familiarity with networking and security terms and concepts (concepts are learned in prerequisite training or by reading industry publications)*

Course Objectives

After completing this course, the learner will be able to meet these overall objectives:

- *Deploy, configure, and administer Cisco IPS sensors to protect network devices as well as efficiently manage IPS alarms*

Course Outline

Lesson 1: Intrusion Prevention Overview

Lesson 2: Getting Started with the IPS Command

Line Interface

Lab Exercise: Getting Started with the IPS

Command Line Interface

Lesson 3: Using the IPS Device Manager

Lab Exercise: Using the IPS Device Manager

Lesson 4: Basic Sensor Configuration

Lab Exercise: Basic Sensor Configuration

Lesson 5: Cisco Intrusion Prevention System

Signatures and Alarms

Lab Exercise: Signatures and Alarms

Lesson 6: Signature Engines

Lesson 7: Signature Configuration

Lab Exercise: Signature Configuration

Lesson 8: Tuning the Sensor

Lab Exercise: Tuning the Sensor Using IDM

Lesson 9: Alarm Monitoring and Management

Lab Exercise: Alarm Monitoring and Management

Lesson 10: Configuring Blocking

Lab Exercise: Configuring Blocking

Lesson 11: Cisco Intrusion Detection System Module

Lesson 12: Capturing Network Traffic

Lesson 13: Maintaining Sensors

Lesson 14: Verifying System Configuration

Lab Exercise: Verifying System Configuration

Lesson 15: Configuring Anomaly Detection, Passive OS Fingerprinting, and CSA Collaboration



Advanced Infrastructure Solutions
Information Worker Solutions
Learning Solutions
Unified Communication Solutions

