

Implementing Cisco Intrusion Prevention System (IPS) v6.0

Days: 3

Associated Certification: CCSP

Prerequisites

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

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

Course Content

Securing Networks Using Intrusion Prevention Systems (IPS) v6.0 is an update to Securing Networks Using Intrusion Prevention Systems (IPS) v5.0, an existing five-day 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.

Course Objectives

Learners will 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
- Lesson 2: Lab Exercise Getting Started with the IPS Command Line Interface
- Lesson 3: Using the IPS Device Manager
- Lesson 3: Lab Exercise Using the IPS Device Manager
- Lesson 4: Basic Sensor Configuration
- Lesson 4: Lab Exercise Basic Sensor Configuration
- Lesson 5: Cisco Intrusion Prevention System Signatures and Alarms
- Lesson 5: Lab Exercise Signatures and Alarms
- Lesson 6: Signature Engines
- Lesson 7: Signature Configuration
- Lesson 7: Lab Exercise Signature Configuration
- Lesson 8: Tuning the Sensor
- Lesson 8: Lab Exercise Tuning the Sensor Using IDM
- Lesson 9: Alarm Monitoring and Management
- Lesson 9: Lab Exercise Alarm Monitoring and Management
- Lesson 10: Configuring Blocking
- Lesson 10: 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
- Lesson 14: Lab Exercise Verifying System Configuration
- Lesson 14: Lab Exercise Verifying System Configuration
- Lesson 15: Configuring Anomaly Detection, Passive OS fingerprinting, and CSA Collaboration

Who Should Attend

- Channel Partner / Reseller
- Customer
- Employee