Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)

Duration: 5 days

Course Overview

Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System is an instructor-led, lab-based, hands-on course offered by Cisco® Learning Services. This course is part of a portfolio of security courses designed to help businesses support and maintain their Cisco Firepower™ systems.

Who should attend?

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment. Targeted roles include:

1. Security administrators
2. Security consultants
3. Network administrators
4. System engineers
5. Technical support personnel
6. Channel partners and resellers

Prerequisites

1. Technical understanding of TCP/IP networking and network architecture
2. Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS

Course Objectives

After completing this course, you should be able to:

1. Describe the key features and concepts of NGIPS and firewall security
2. Describe the Cisco Firepower system components, features, and high-level implementation steps
3. Navigate the Cisco Firepower Management Center GUI and understand the role of policies when configuring the Cisco Firepower system
4. Deploy and manage Cisco Firepower managed devices
5. Perform an initial Cisco Firepower discovery and basic event analysis to identify hosts, applications, and services
6. Identify and create the objects required as prerequisites to implementing access control policies

7. **Identify the features and functionality of access control policies and the implementation procedures**
8. **Describe the concepts and implementation procedures of security intelligence**
9. **Describe the concepts and implementation procedures of file control and advanced malware protection**
10. **Use Cisco Firepower recommendations to implement IPS policies**
11. **Explain the use of network analysis policies and the role of preprocessor technology in processing network traffic for NGIPS inspection**
12. **Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center**
13. **Describe major Cisco Firepower Management Center system administration and user account management features**

Course Content

This lab-intensive course introduces you to the basic next-generation intrusion prevention system (NGIPS) and firewall security concepts. The course then leads you through the Cisco Firepower system. Among other powerful features, you will become familiar with:

In-depth event analysis NGIPS tuning and configuration Snort® rules language

You'll also become familiar with the latest platform features: file and malware inspection, security intelligence, domain awareness, and more.

The course begins by introducing the system architecture, the latest major features, and the role of policies in implementing the solution. You learn how to manage deployed devices and perform basic Cisco Firepower discovery. You'll be able to describe how to use and configure Cisco NGIPS technology, including application control, security intelligence, firewall, and network-based malware and file controls. You'll learn how to take advantage of powerful tools so you can carry out more efficient event analysis, including the detection of file type and network-based malware. And you'll learn how to properly tune systems for better performance and greater network intelligence. The course finishes with system and user administration tasks.

This course combines lecture materials and hands-on labs that will give you practice in deploying and managing the Cisco Firepower system.