Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS)

Objectives

After completing this course, you should be able to:

- Describe the key features and concepts of NGIPS and firewall security
- Describe the Cisco Firepower system components, features, and high-level implementation steps
- Navigate the Cisco Firepower Management Center GUI and understand the role of policies when configuring the Cisco Firepower system
- Deploy and manage Cisco Firepower managed devices
- Perform an initial Cisco Firepower discovery and basic event analysis to identify hosts, applications and services
- Identify and create the objects required as prerequisites to implementing access control policies
- Identify the features and functionality of access control policies and the implementation procedures
- Describe the concepts and implementation procedures of security intelligence
- Describe the concepts and implementation procedures of file control and advanced malware protection
- Use Cisco Firepower recommendations to implement IPS policies
- Explain the use of network analysis policies and the role of preprocessor technology in processing network traffic for NGIPS inspection
- Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center
- Describe major Cisco Firepower Management Center system administration and user account management features

Target Audience

Technical professionals who need to know how to deploy and manage a Cisco FirePower NGIPS in their network environment.

Content

Security Technology Overview

Cisco Firepower System Components and Features

Introducing the Cisco Firepower Management Center

Deploying Cisco Firepower Managed Devices

Cisco Firepower Discovery

Access Control Policy Prerequisites

Implementing Access Control Policies

Security Intelligence

File Control and Advanced Malware Protection

Next-Generation Intrusion Prevention Systems

Network Analysis Policies

Detailed Analysis Techniques

System Administration

Labs

- Lab 1: Connect to the Lab Environment
- Lab 2: Navigate the Cisco Firepower Management Center GUI
- Lab 3: Device Management
- Lab 4: Cisco Firepower Discovery
- Lab 5: Access Control Policy Prerequisites
- Lab 6: Implementing an Access Control Policy
- Lab 7: Security Intelligence
- Lab 8: File Control and Advanced Malware Protection
- Lab 9: Implementing NGIPS
- Lab 10: Detailed Analysis
- Lab 11: System Administration