SSFIPS (SECURING NETWORKS WITH CISCO FIREPOWER NEXT-GENERATION IPS) 4.0

Objetivo

After taking this course, you should be able to: Describe the components of Cisco Firepower Threat Defense and the managed device registration process Detail Next-Generation Firewalls (NGFW) traffic control and configure the Cisco Firepower system for network discovery Implement access control policies and describe access control policy advanced features Configure security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection Implement and manage intrusion and network analysis policies for NGIPS inspection Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center Integrate the Cisco Firepower Management Center with an external logging destination Describe and demonstrate the external alerting options available to Cisco Firepower Management Center and configure a correlation policy Describe key Cisco Firepower Management Center software update and user account management features Identify commonly misconfigured settings within the Cisco Firepower Management Center and use basic commands to troubleshoot a Cisco Firepower Threat Defense device

PÃºblico Alvo

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment. Security administrators Security consultants Network administrators System engineers Technical support personnel Channel partners and resellers

PrÃ©-Requisitos

To fully benefit from this course, you should have the following knowledge and skills: Technical understanding of TCP/IP networking and network architecture. Basic familiarity with the concepts of Intrusion Detection Systems (IDS) and IPS.

Carga HorÃ¡ria

40 horas (5 dias).

ConteÃºdo ProgramÃ¡tico

Cisco Firepower Threat Defense Overview

Cisco Firepower NGFW Device Configuration

Cisco Firepower NGFW Traffic Control

Cisco Firepower Discovery

Implementing Access Control Policies

Security Intelligence

File Control and Advanced Malware Protection

Next-Generation Intrusion Prevention Systems

Network Analysis Policies

Detailed Analysis Techniques

Cisco Firepower Platform Integration

Alerting and Correlation Policies

System Administration

Cisco Firepower Troubleshooting

Lab Outline
Initial Device Setup
Device Management
Configuring Network Discovery
Implementing and Access Control Policy
Implementing Security Intelligence
File Control and Advanced Malware Protection
Implementing NGIPS
Customizing a Network Analysis Policy
Detailed Analysis
Configuring Cisco Firepower Platform Integration with Splunk
Configuring Alerting and Event Correlation
System Administration
Cisco Firepower Troubleshooting