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

Objetivo

After taking this course, you should be able to: â□¢ 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; â□¢ 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; â□¢ 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; â□¢ Integrate the Cisco Firepower Management Center with an external logging destination; â□¢ Describe and demonstrate the external alerting options available to Cisco Firepower Management Center and configure a correlation policy; â□¢ Describe key Cisco Firepower Management Center software update and user account management features; â□¢ 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.

PrÃ©-Requisitos

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

Carga HorÃiria

40 horas (5 dias).

ConteÃºdo ProgramÃitico

Course Introduction
Course Outline
Course Goals

Cisco Firepower Threat Defense Overview
Examining Firewall & IPS Technologyu
Cisco FTD Features & Components

Examining Firepower Platforms
Examining Cisco FTD Licensing
Cisco Firepower Implementation Use Cases

Cisco Firepower NGFW Device Configuration
Firepower FTD Registration
FXOS & Firepower Device Manager (FDM)
Managing NGFW Devices
Examining Firepower Management Center (FMC)
Examining System Configuration & Health Monitoring

Cisco Firepower NGFW Traffic Control
Cisco FTD Packet Processing
Bypassing Traffic

Cisco Firepower Discovery
Configuring Firepower Network Discovery
Interpreting Host Profile Information
Examining User Identity Information

Implementing Access Control Policies
Examining Access Control Policies (ACP)
Examining ACP Rules & Default Action
Introducing Further Inspection
Examing Connection Events
ACP (Access Control Policy) Advanced Settings
ACP (Access Control Policy) Considerations

Security Intelligence
Examining Security Intelligence
Examing Security Intelligence Objects
Security Intelligence Deployment & Logging

File Control and Advanced Malware Protection
Examining Malware & File Policy
Examining Advanced Malware Protection

Next-Generation Intrusion Prevention Systems
Examining Variables & Variables Sets
Examining Intrusion Policies
Creating Intrusion Policies
Managing Intrusion Policies

Network Analysis Policies
Examining Preprocessor Technologies
Examining Netowrk Analysis Policies
Examining Adaptive Profiles

Detailed Analysis Techniques
Examining Events Analysis
Examining Event Types
Examining Contextual Data
Examining Analysis Tools
Tuning IPS Using Intrusion Events

Cisco Firepower Platform Integration
Examining Cisco Threat Intelligence Director
Examining Integration with ISE (Identity Services Engine)
Configuring Firepower Integration with Splunk

Alerting and Correlation Policies
Examining External Auditing Alerting
Configuring Correlation Policies

System Administration
Manual Updates
Examining User Account Management Features
Configuring User Accounts

Cisco Firepower Troubleshooting
Examining Common Misconfigurations
Examining Troubleshooting Commands
Examining Packet Capture

Lab Outline
Lab 1: Initial Device Setup
Lab 2: Device Management
Lab 3: Configuring Network Discovery
Lab 4: Implementing and Access Control Policy
Lab 5: Implementing Security Intelligence
Lab 6: File Control and Advanced Malware Protection
Lab 7: Implementing NGIPS
Lab 8: Customizing a Network Analysis Policy
Lab 9: Detailed Analysis
Lan 11: Configuring Cisco Firepower Platform Integration with Splunk
Lab 12: Configuring Alerting and Event Correlation
Lab 13: System Administration
Lab 14: Cisco Firepower Troubleshooting