Objetivos

After taking this course, you should be able to:

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenarios
- Perform initial Cisco Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services
- Describe the behavior, usage, and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security intelligence features
- Describe Cisco Advanced Malware Protection (AMP) for Networks and the procedures for implementing file control and advanced malware protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect®
- Describe SSL decryption capabilities and usage

Pre-requisitos

To fully benefit from this course, you should have:

- Knowledge of TCP/IP and basic routing protocols
- Familiarity with firewall, VPN, and Intrusion Prevention System (IPS) concepts

---

Contenido

- Cisco Firepower Threat Defense Overview
  - Examining Firewall and IPS Technology
  - Firepower Threat Defense Features and Components
  - Examining Firepower Platforms
  - Examining Firepower Threat Defense Licensing
  - Cisco Firepower Implementation Use Cases
- Cisco Firepower NGFW Device Configuration
  - Firepower Threat Defense Device Registration
  - FXOS and Firepower Device Manager

  - Initial Device Setup
  - Managing NGFW Devices
  - Examining Firepower Management Center Policies
  - Examining Objects
  - Examining System Configuration and Health Monitoring
  - Device Management
  - Examining Firepower High Availability
  - Configuring High Availability
  - Cisco ASA to Firepower Migration
  - Migrating from Cisco ASA to Firepower Threat Defense
- Cisco Firepower NGFW Traffic Control
  - Firepower Threat Defense Packet Processing
  - Implementing QoS
  - Bypassing Traffic
- Cisco Firepower NGFW Address Translation
  - NAT Basics
  - Implementing NAT
  - NAT Rule Examples
  - Implementing NAT
- Cisco Firepower Discovery
  - Examining Network Discovery
  - Configuring Network Discovery
- Implementing Access Control Policies
  - Examining Access Control Policies
  - Examining Access Control Policy Rules and Default Action
  - Implementing Further Inspection
  - Examining Connection Events
  - Access Control Policy Advanced Settings
  - Access Control Policy Considerations
  - Implementing an Access Control Policy
- Security Intelligence
  - Examining Security Intelligence
  - Examining Security Intelligence Objects
  - Security Intelligence Deployment and Logging

  - Implementing Security Intelligence
- File Control and Advanced Malware Protection
  - Examining Malware and File Policy
  - Examining Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
  - Examining Intrusion Prevention and Snort Rules
  - Examining Variables and Variable Sets
  - Examining Intrusion Policies
- Site-to-Site VPN
  - Examining IPsec
  - Site-to-Site VPN Configuration
  - Site-to-Site VPN Troubleshooting
  - Implementing Site-to-Site VPN
- Remote-Access VPN
  - Examining Remote-Access VPN
  - Examining Public-Key Cryptography and Certificates
  - Examining Certificate Enrollment
  - Remote-Access VPN Configuration
  - Implementing Remote-Access VPN
- SSL Decryption
  - Examining SSL Decryption
  - Configuring SSL Policies
  - SSL Decryption Best Practices and Monitoring
- Detailed Analysis Techniques
  - Examining Event Analysis
  - Examining Event Types
  - Examining Contextual Data
  - Examining Analysis Tools
  - Threat Analysis
- System Administration
  - Managing Updates
  - Examining User Account Management Features
  - Configuring User Accounts
  - System Administration

- Cisco Firepower Troubleshooting
    - Examining Common Misconfigurations
    - Examining Troubleshooting Commands
    - Firepower Troubleshooting

Laboratorio

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting
