Objetivos

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

---

Pre-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.

Contenido

- 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

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

P á g . 1 | 2

- Next-Generation Intrusion Prevention Systems
- Network Analysis Policies
- Detailed Analysis Techniques
- Cisco Firepower Platform Integration
- Alerting and Correlation Policies
- System Administration
- Cisco Firepower Troubleshooting

Laboratorio

- 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

_____

Centro de Transferencia de Tecnología
2700215 / 591-79671047
eriveros@cttbolivia.com

Pág. 2 | 2