Securing Networks with Cisco Firepower Threat Defense NGFW (Firepower200)

Course ID #: 1575-994-ZZ-W

Hours: 35

Course Content

Course Description:

The Securing Networks with Cisco Firepower Threat Defense NGFW(FIREPOWER200) v2.0 course shows you how to deploy and use Cisco®Firepower®Threat Defense system. This hands-on course gives you the knowledge and skills to use and configure Cisco Firepower Threat Defense technology, beginning with initial device setupand configuration and including routing, high availability, Cisco Adaptive Security Appliance (ASA) to Cisco Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting.

Course Objectives:

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 ThreatDefense
- 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

Securing Networks with Cisco Firepower Threat Defense NGFW (Firepower200)

Course ID #: 1575-994-ZZ-W

Hours: 35

Target Audience:

The primary audience for this course is technical professionals who need to know how to deploy and manage a Cisco Firepower Threat Defense NGFW in their network environments. This class would be suitable for anyone who is replacing Cisco ASA devices with Cisco Firepower Threat Defense.

- System administrators
- Network administrators
- Solution designers
- System installers
- Cisco integrators and partners

Prerequisites:

To fully benefit from this course, you should have the following knowledge:

- Knowledge of TCP/IP and basic routing protocols, and familiarity with firewall, VPN, and IntrusionPrevention System (IPS) concepts

Topics:

- **Cisco Firepower Threat Defense Overview**
- **Cisco Firepower NGFW Device Configuration**
- **Cisco Firepower NGFW Traffic Control**
- **Cisco Firepower NGFW Address Translation**
- **Cisco Firepower Discovery**
- **Implementing Access Control Policies**
- **Security Intelligence**
- **Learning@CiscoCourse overviewPage3of 3**
- **File Control and Advanced Malware Protection**
- **Next-Generation Intrusion Prevention Systems**
- **Site-to-Site VPN**
- **Remote-Access VPN**
- **SSL Decryption**
- **Detailed Analysis Techniques**
- **System Administration**
- **Cisco Firepower Troubleshooting**