SECURING NETWORKS WITH FIREPOWER THREAT DEFENSE NGFW

DURATION: 5 DAYS

COURSE OVERVIEW

The Securing Networks with Cisco Firepower Threat Defense NGFW (FIREPOWER200) course demonstrates the powerful features of Cisco Firepower Threat Defense, including VPN configuration, traffic control, NAT configuration, SSL decryption, advanced NGFW and NGIPS tuning and configuration, analysis and troubleshooting. Students will learn how to use and configure Cisco Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco ASA to Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). The course will then explore 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. Configuration of site-to-site VPN, remote-access VPN, and SSL decryption are also covered before moving on to detailed analysis, system administration, and troubleshooting. This course combines lecture materials and hands-on labs throughout to make sure that students are able to successfully deploy and manage the Cisco Firepower system.

TARGET AUDIENCE

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS and NGFW in their network environments.

COURSE OBJECTIVES

After completing this course, you should be able to:

1. Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system and identify deployment scenarios
2. Perform initial Firepower Threat Defense device configuration and setup tasks
3. Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense
4. Describe how to implement NAT by using Cisco Firepower Threat Defense
5. Perform an initial network discovery, using Cisco Firepower to identify hosts, applications and services
6. Describe the behavior, usage and implementation procedure for access control policies

7. Describe the concepts and procedures for implementing security Intelligence features
8. Describe Cisco AMP for Networks and the procedures for implementing file control and Advanced Malware Protection
9. Implement and manage intrusion policies
10. Describe the components and configuration of site-to-site VPN
11. Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect
12. Describe SSL decryption capabilities and usage

COURSE CONTENT

Module 1: Cisco Firepower Threat Defense Overview

Module 2: Firepower NGFW Device Configuration

Module 3: Firepower NGFW Traffic Control

Module 4: Firepower NGFW Address Translation

Module 5: Firepower Discovery

Module 6: Implementing Access Control Policies

Module 7: Security Intelligence

Module 8: File Control and Advanced Malware Protection

Module 9: Next-Generation Intrusion Prevention Systems

Module 10: Site-to-Site VPN

Labs

Lab 1: Initial Device Setup

Lab 2: Device Management

Lab 3: Configuring High Availability

Lab 4: Migrating from Cisco ASA to Firepower Threat Defense

Lab 5: Implementing QoS

Lab 6: Implementing NAT

Lab 7: Configuring Network Discovery

Lab 8: Implementing an Access Control Policy

Lab 9: Implementing Security Intelligence

Lab 10: Implementing Site-to-Site VPN

Lab 11: Implementing Remote Access VPN

Lab 12: Threat Analysis

Lab 13: System Administration

Lab 14: Firepower Troubleshooting

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

Knowledge of TCP/IP and basic routing protocols

Familiarity with firewall, vpn and IPS concepts

TEST CERTIFICATION

Recommended as preparation for the following exams:

There are no exams current aligned to this course