FIREPOWER

Course Objectives

After completing this course, you should be able to:

● Describe the Cisco Firepower Threat Defense system and key concepts of NGIPS and NGFW technology

● Describe how to perform the configurations tasks required for implementing a Cisco Firepower Threat Defense device

● Describe how to implement quality of service (QoS) and Network Address Translation (NAT) by using Cisco Firepower Threat Defense

● Perform an initial network discovery using Cisco Firepower to identify hosts, applications, and services
● Identify and create the objects required as prerequisites to implementing access control policies

● Describe the behavior, usage, and implementation procedure for access control policies

● Describe the concepts and implementation procedure of security intelligence features

● Describe Cisco Advanced Malware Protection (AMP) for Networks and the implementation procedure of file control and advanced malware protection

● Implement and manage intrusion policies

● Explain the use of network analysis policies and the role of preprocessor technology in processing network traffic for NGIPS inspection

● Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center

● Describe key Cisco Firepower Management Center system administration and user account management features

● Describe the processes that can be used to troubleshoot Cisco Firepower Threat Defense systems.

Course Outline

● Module 1: Cisco Firepower Threat Defense Overview

● Module 2: Cisco Firepower System Setup

● Module 3: QoS and NAT Implementation

- Module 4: Cisco Firepower Discovery
- Module 5: Access Control Policy Prerequisites
- Module 6: Implementing Access Control Policies
- Module 7: Security Intelligence
- Module 8: AMP for Networks Malware Protection
- Module 9: Next-Generation Intrusion Prevention Systems
- Module 10: Network Analysis Policies
- Module 11: Detailed Analysis Techniques
- Module 12: System Administration
- Module 13: Cisco Firepower Threat Defense Troubleshooting

Lab Outline

- Lab 1: Connect to the Lab Environment
- Lab 2: Navigate the Cisco Firepower Management Center GUI
- Lab 3: Device Management
- Lab 4: Implementing QoS and NAT
- Lab 5: Configuring Network Discovery
- Lab 6: Implementing an Access Control Policy
- Lab 7: Implementing Security Intelligence
- Lab 8: AMP for Networks Malware Protection
- Lab 9: Implementing NGIPS
- Lab 10: Performing Detailed Analysis
- Lab 11: System Administration
- Lab 12: Cisco Firepower Troubleshooting