Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)

Modality: Virtual Classroom

Duration: 5 Days

CLC: 43 Units

About this course:

This lab-intensive 5-day course introduces the student to the basic next-generation intrusion prevention system (NGIPS) and next-generation firewall (NGFW) security concepts. The course then leads you through the Cisco Firepower system. Among other powerful features, you become familiar with:

- Firepower Threat Defense configuration
- In-depth event analysis
- NGIPS tuning and configuration

You also become familiar with the latest platform features: file and malware inspection, security intelligence, domain awareness, and more.

The course begins by introducing the system architecture, the latest major features, and the role of policies in implementing the solution. You learn how to deploy and manage Cisco Firepower Threat Defense devices and perform basic Cisco Firepower discovery. You learn how to use and configure Threat Defense technology, including application control, security intelligence, NGFW, NGIPS, and network-based malware and file controls. Also, you learn how to take advantage of powerful tools, so you can perform more efficient event analysis, including the detection of file types and network-based malware. And you'll learn how to properly tune systems for better performance and greater network intelligence. The course concludes with system and user administration tasks and Threat Defense system troubleshooting. This course combines lecture materials and hands-on labs that give you practice in deploying and managing the Cisco Firepower system.

Course Objective:

Upon completing this course, the learner will be able to meet these overall objectives:

- 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

Audience:

The primary audience for this course is as follows:

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

Prerequisite:

The knowledge and skills that a learner should have before attending this course are as follows:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with firewall and IPS concepts

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