interface
We teach. You do.

Cisco Security

SSNGFW: Securing Networks with Cisco Firepower Next Generation Firewall

$4,300.00

- 5 Days

Upcoming Dates

Course Description

The Securing Networks with Cisco Firepower Next-Generation Firewall (SSNGFW) v1.0 is a 5-day instructor-led course that introduces learners to 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.

This course will show students 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.

Students 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.

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.

Course Outline

The course contains these components:

- Cisco Firepower Threat Defense Overview
- Firepower NGFW Device Configuration
- Firepower NGFW Traffic Control
- Firepower NGFW Address Translation
- Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- 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
- Firepower Troubleshooting

Lab outline:

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Firepower Threat Defense
- Implementing QoS

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.

Targeted roles include:

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

Prerequisites

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

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

What You Will Learn

Upon completion of 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 Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense
- 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 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