Cisco® Securing Networks with Cisco Firepower® Next Generation Firewall v1.0 (SSNGFW)

Register Online

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

Overview

This course gives you knowledge and skills to use and configure Cisco® Firepower Threat Defense technology, beginning with initial device setup and 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 Secure Sockets Layer (SSL) decryption before moving on to detailed analysis, system administration, and troubleshooting.

Prerequisite Comments

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 Intrusion Prevention System (IPS) concepts

Target Audience

Security administrators
Security consultants
Network administrators
System engineers
Technical support personnel
Cisco integrators and partners

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 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

Course Outline

1 - Cisco Firepower Threat Defense Overview

Examining Firewall and IPS Technology
Firepower Threat Defense Features and Components
Examining Firepower Platforms
Examining Firepower Threat Defense Licensing
Cisco Firepower Implementation Use Cases

2 - Cisco Firepower NGFW Device Configuration

Firepower Threat Defense Device Registration
FXOS and Firepower Device Manager
Initial Device Setup
Managing NGFW Devices
Examining Firepower Management Center Policies
Examining Objects
Examining System Configuration and Health Monitoring
Device Management
Examining Firepower High Availability
Configuring High Availability
Cisco ASA to Firepower Migration
Migrating from Cisco ASA to Firepower Threat Defense

3 - Cisco Firepower NGFW Traffic Control

Firepower Threat Defense Packet Processing
Implementing QoS
Bypassing Traffic

4 - Cisco Firepower NGFW Address Translation

NAT Basics
Implementing NAT
NAT Rule Examples
Implementing NAT

5 - Cisco Firepower Discovery

Examining Network Discovery
Configuring Network Discovery
Implementing Access Control Policies
Examining Access Control Policies
Examining Access Control Policy Rules and Default Action
Implementing Further Inspection
Examining Connection Events
Access Control Policy Advanced Settings
Access Control Policy Considerations
Implementing an Access Control Policy

6 - Security Intelligence

Examining Security Intelligence
Examining Security Intelligence Objects
Security Intelligence Deployment and Logging
Implementing Security Intelligence

7 - File Control and Advanced Malware Protection

Examining Malware and File Policy
Examining Advanced Malware Protection

8 - Next-Generation Intrusion Prevention Systems

Examining Intrusion Prevention and Snort Rules
Examining Variables and Variable Sets
Examining Intrusion Policies

9 - Site-to-Site VPN

Examining IPsec
Site-to-Site VPN Configuration
Site-to-Site VPN Troubleshooting
Implementing Site-to-Site VPN

10 - Remote-Access VPN

Examining Remote-Access VPN
Examining Public-Key Cryptography and Certificates
Examining Certificate Enrollment
Remote-Access VPN Configuration
Implementing Remote-Access VPN

11 - SSL Decryption

Examining SSL Decryption
Configuring SSL Policies
SSL Decryption Best Practices and Monitoring

12 - Detailed Analysis Techniques

Examining Event Analysis
Examining Event Types
Examining Contextual Data
Examining Analysis Tools
Threat Analysis

13 - System Administration

Managing Updates
Examining User Account Management Features
Configuring User Accounts
System Administration

14 - Cisco Firepower Troubleshooting

Examining Common Misconfigurations
Examining Troubleshooting Commands
Firepower Troubleshooting