

Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention

DURATION: 5 DAYS **COURSE CODE:** SFWIPA **FORMAT:** Kit & Lab

Course Description

The Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense training shows you how to deploy and configure Cisco Secure Firewall Threat Defense system and its features as a data center network firewall or as an Internet Edge firewall with Virtual Private Network (VPN) support. You will learn how to configure identity-based policies, Secure Sockets Layer (SSL) decryption, remote-access VPN, and site-to-site VPN before moving on to advanced Intrusion Prevention System (IPS) configuration and event management, integrations with other systems, and advanced troubleshooting. You will also learn how to automate configuration and operations of Cisco Secure Firewall Threat Defense system using programmability and Application Programming Interfaces (APIs) and how to migrate configuration from Cisco Secure Firewall Adaptive Security Appliances (ASA).

CERTIFICATION

This training prepares you for the 300-710 Securing Networks with Cisco Firepower (SNCF) exam. If passed, you earn the Cisco Certified Specialist – Network Security Firepower certification and satisfy the concentration exam requirement for the Cisco Certified Networking Professional (CCNP) Security certification. **This training also earns you 40 Continuing Education (CE) credits toward recertification.**

Who Should Enroll

- System Installers
- System Integrators
- System Administrators
- Network Administrators
- Solutions Designers

Course Prerequisites

- Knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP)
- Basic knowledge of routing protocols
- Familiarity with the content explained in the Securing Internet Edge with Cisco Secure Firewall Threat Defense training

These skills can be found in the following Cisco Learning Offerings:

- Implementing and Administering Cisco Solutions 2.0
- Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0

Course Outline

- Introducing Cisco Secure Firewall Threat Defense
- Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense
- Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense
- Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense
- Configuring Advanced NAT on Cisco Secure Firewall Threat Defense
- Configuring SSL Policy on Cisco Secure Firewall Threat Defense
- Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense
- Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense
- Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense
- Configuring Snort Rules and Network Analysis Policies
- Describing Advanced Event Management Cisco Secure Firewall Threat Defense
- Describing Integrations on Cisco Secure Firewall Threat Defense
- Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense
- Automating Cisco Secure Firewall Threat Defense
- Migrating to Cisco Secure Firewall Threat Defense

Lab Outline

- Deploy Advanced Connection Settings
- Configure Dynamic Routing
- Configure SSL Policy
- Configure Remote Access VPN
- Configure Site-to-Site VPN
- Customize IPS and NAP Policies
- Configure Cisco Secure Firewall Threat Defense Integrations
- Troubleshoot Cisco Secure Firewall Threat Defense
- Migrate Configuration from Cisco Secure Firewall ASA