SFWIPA - ADVANCED TECHNIQUES FOR CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION V1.0

Course Code: 860015

The Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense training shows you how to deploy Cisco Secure Firewall Threat Defense system and its features as a data center network firewall or as an Internet Edge firewall with VPN support.

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).

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.

Course Objectives

- Describe Cisco Secure Firewall Threat Defense
- Describe advanced deployment options on Cisco Secure Firewall Threat Defense
- Describe advanced device settings for Cisco Secure Firewall Threat Defense device
- Configure dynamic routing on Cisco Secure Firewall Threat Defense
- Configure advanced network address translation on Cisco Secure Firewall Threat Defense

- Configure SSL decryption policy on Cisco Secure Firewall Threat Defense
- Deploy Remote Access VPN on Cisco Secure Firewall Threat Defense
- Deploy identity-based policies on Cisco Secure Firewall Threat Defense
- Deploy site-to-site IPsec-based VPN on Cisco Secure Firewall Threat Defense
- Deploy advanced access control settings on Cisco Secure Firewall Threat Defense
- Describe advanced event management on Cisco Secure Firewall Threat Defense
- Describe available integrations with Cisco Secure Firewall Threat Defense
- Troubleshoot traffic flow using advanced options on Cisco Secure Firewall Threat Defense
- Describe benefits of automating configuration and operations of Cisco Secure Firewall Threat Defense
- Describe configuration migration to Cisco Secure Firewall Threat Defense

What You'll Learn

This training will help you:

- Attain advanced knowledge of Cisco Secure Firewall Threat Defense technology
- Gain competency and skills required to implement and manage a Cisco Secure Firewall Threat Defense system regardless of platform
- Learn detailed information on policy management, traffic flow through the system, and the system architecture
- Deploy and manage many of the advanced features available in the Cisco Secure Firewall Threat Defense system
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level data center roles
- Earn 40 CE credits toward recertification

Who Needs to Attend

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

Prerequisites

Attendees should meet the following 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 Courses:
  - Implementing and Administering Cisco Solutions v2.0
  - Securing Internet Edge with Cisco Secure Firewall Threat Defense 1.0

SFWIPA - ADVANCED TECHNIQUES FOR CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION V1.0

Course Code: 860015

VIRTUAL CLASSROOM LIVE	$3,995 USD	5 Day

Virtual Classroom Live Outline

1. Introducing Cisco Secure Firewall Threat Defense
2. Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense
3. Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense
4. Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense
5. Configuring Advanced NAT on Cisco Secure Firewall Threat Defense
6. Configuring SSL Policy on Cisco Secure Firewall Threat Defense
7. Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense
8. Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense
9. Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense
10. Configuring Snort Rules and Network Analysis Policies
11. Describing Advanced Event Management Cisco Secure Firewall Threat Defense
12. Describing Integrations on Cisco Secure Firewall Threat Defense
13. Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense
14. Automating Cisco Secure Firewall Threat Defense
15. Migrating to Cisco Secure Firewall Threat Defense

Virtual Classroom Live Labs

1. Deploy Advanced Connection Settings
2. Configure Dynamic Routing
3. Configure SSL Policy
4. Configure Remote Access VPN

5. Configure Site-to-Site VPN
6. Customize IPS and NAP Policies
7. Configure Cisco Secure Firewall Threat Defense Integrations
8. Troubleshoot Cisco Secure Firewall Threat Defense
9. Migrate Configuration from Cisco Secure Firewall ASA

Mar 23 - 27, 2026 | 8:30 AM - 4:30 PM EDT

May 18 - 22, 2026 | 8:30 AM - 4:30 PM EDT

Jul 6 - 10, 2026 | 8:30 AM - 4:30 PM EDT

Sep 14 - 18, 2026 | 8:30 AM - 4:30 PM EDT

Nov 9 - 13, 2026 | 8:30 AM - 4:30 PM EST

SFWIPA - ADVANCED TECHNIQUES FOR CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION V1.0

Course Code: 860015

ON-DEMAND	$900 USD

On-Demand Outline

1. Introducing Cisco Secure Firewall Threat Defense
2. Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense
3. Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense
4. Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense
5. Configuring Advanced NAT on Cisco Secure Firewall Threat Defense
6. Configuring SSL Policy on Cisco Secure Firewall Threat Defense
7. Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense
8. Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense
9. Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense
10. Configuring Snort Rules and Network Analysis Policies
11. Describing Advanced Event Management Cisco Secure Firewall Threat Defense
12. Describing Integrations on Cisco Secure Firewall Threat Defense
13. Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense
14. Automating Cisco Secure Firewall Threat Defense
15. Migrating to Cisco Secure Firewall Threat Defense

On-Demand Labs

1. Deploy Advanced Connection Settings
2. Configure Dynamic Routing
3. Configure SSL Policy
4. Configure Remote Access VPN

5. Configure Site-to-Site VPN
6. Customize IPS and NAP Policies
7. Configure Cisco Secure Firewall Threat Defense Integrations
8. Troubleshoot Cisco Secure Firewall Threat Defense
9. Migrate Configuration from Cisco Secure Firewall ASA

SFWIPA - ADVANCED TECHNIQUES FOR CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION V1.0

Course Code: 860015

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 2/1/2026 6:01:07 PM