# Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention

**Duration: 5 Days** **Course Code: SFWIPA** **Version: 1.0**

## Overview:

The Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention course shows you how to deploy and configure a 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 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

**This course is worth 40 Continuing Education (CE) credits towards recertification.**

## Target Audience:

Anyone involved in the deployment and maintenance of a Cisco Secure Firewall Threat Defense solution.

## Objectives:

- **After completing this course you should be able to:**
- 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

## 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 Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

## Testing and Certification

**Recommended as preparation for the following exam:**

- 300-710 - Securing Networks with Cisco Firewall Exam

Knowledge from both the SFWIPF and SWIPA course is required for this exam.

## Content:

Introducing Cisco Secure Firewall Threat Defense

- Firewall Functionality
- Cisco Secure Firewall Platform
- Use Cases
- Deployment Options
- Management Options
- Basic Network Settings
- Packet Processing
- ACP and Prefilter Policies Overview
- Cisco Secure Firewall Smart Licensing

Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense

- Cisco Secure Firewall Threat Defense Architecture
- FXOS and Secure Firewall Chassis Manager
- Multi-Instance Deployment
- Cluster Deployment
- Cluster Configuration

Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense

- QoS Implementation
- Service Policies Implementation
- FlexConfig Policies Implementation
- Traffic Bypass

Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense

- Dynamic Routing Overview
- Virtual Routing
- Dynamic Routing Configuration

Configuring Advanced NAT on Cisco Secure Firewall Threat Defense

- Network Address Translation Overview
- Advanced NT Rules Implementation

Configuring SSL Policy on Cisco Secure Firewall Threat Defense

- SSL Encryption Overview
- SSL Decryption Overview
- SSL Policy Configuration
- SSL Policy Best Practices

Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense

- Remote-Access VPN Components
- Digital Certificate Enrollment
- Remote Access VPN Configuration
- Remote Access VPN High Availability

Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense

- Identity-Based Policies
- Realm Configuration
- Identity Source Configuration
- Identity-Based Policy Configuration

Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense

- Site-to-Site VPN Components
- Policy-Based and Route-Based Site-to-Site VPNs
- Point-to-Point VPN Configuration VTIs
- Hub-and-Spoke VPN Configuration with Crypto Maps
- Site-toSite High Availability

Configuring Snort Rules and Network Analysis Policies

- Snort and Network Analysis Policy
- Snort Rules and Actions
- Secure Firewall Recommendations

Describing Advanced Event Management Cisco Secure Firewall Threat Defense

- Alerting
- Correlation Policies
- External Event Logging

Describing Integrations on Cisco Secure Firewall Threat Defense

- Integration with Cisco Identity Service Engine
- Integration with Cisco Network Analytics
- Integration with SecureX

Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense

- Traffic Flow Overview
- Troubleshooting Tools
- Troubleshooting Process
- Performance Troubleshooting

Automating Cisco Secure Firewall Threat Defense

- Network Operations Automation
- Cisco Secure Firewall Management Center API Overview
- Cisco Secure Firewall Device Manager API Overview

Migrating to Cisco Secure Firewall Threat Defense

- Migration Options
- Migration Tool
- Migration from Cisco Secure firewall ASA

Labs Outlines:

- Discovery Lab 1: Configure Multi-Instance Firewall Using Chassis Manager Interactive Activity
- Discovery Lab 2: Deploy Advanced Connection Settings
- Discovery Lab 3: Configure Dynamic Routing
- Discovery Lab 4: Configure SSL Policy
- Discovery Lab 5: Configure Remote Access VPN
- Discovery Lab 6: Configure Identity-Based Policy
- Discovery Lab 7: Configure Site-to-Site VPN
- Discovery Lab 8: Customize IPS and NAP Policies
- Discovery Lab 9: Configure Cisco Secure Firewall Threat Defense Integrations
- Discovery Lab 10: Troubleshooting Cisco Secure Firewall Threat Defense
- Discovery Lab 11: Cisco Secure Firewall Threat Defese Automation
- Discovery Lab 12: Migrate Configuration from Cisco Secure Firewall ASA

## Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar