Document Generated: 09/12/2026

Learning Style: Virtual Classroom

Technology: Cisco

Difficulty: Advanced

Course Duration: 5 Days

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)

About This Course:

The Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) training shows you how to implement and configure Cisco Secure Firewall Threat Defense for deployment as a next generation firewall at the internet edge. You'll gain an understanding of Cisco Secure Firewall architecture and deployment, base configuration, packet processing and advanced options, and

conducting Secure Firewall administration troubleshooting.

Course Objectives:

- Describe Cisco Secure Firewall Threat Defense
- Describe Cisco Secure Firewall Threat Defense Deployment Options
- Describe management options for Cisco Secure Firewall Threat Defense
- Configure basic initial settings on Cisco Secure Firewall Threat Defense
- Configure high availability on Cisco Secure Firewall Threat Defense
- Configure basic Network Address Translation on Cisco Secure Firewall Threat Defense
- Describe Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device
- Configure Discovery Policy on Cisco Secure Firewall Threat Defense
- Configure and explain prefilter and tunnel rules in prefilter policy
- Configure an access control policy on Cisco Secure Firewall Threat Defense
- Configure security intelligence on Cisco Secure Firewall Threat Defense
- Configure file policy on Cisco Secure Firewall Threat Defense
- Configure Intrusion Policy on Cisco Secure Firewall Threat Defense
- Perform basic threat analysis using Cisco Secure Firewall Management Center
- Perform basic management and system administration tasks on Cisco Secure Firewall Threat Defense
- Perform basic traffic flow troubleshooting on Cisco Secure Firewall Threat Defense
- Manage Cisco Secure Firewall Threat Defense with Cisco Secure Firewall Threat Defense Manager

Audience:

The primary audience for this course is as follows:

- Network security engineers
- Administrators

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- TCP/IP
- Basic routing protocols
- Firewall, VPN, and IPS concepts

Course Outline:

- Introducing Cisco Secure Firewall Threat Defense
- Describing Cisco Secure Firewall Threat Defense Deployment Options
- Describing Cisco Secure Firewall Threat Defense Management Options

- Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense
- Configuring High Availability on Cisco Secure Firewall Threat Defense
- Configuring Auto NAT on Cisco Secure Firewall Threat Defense
- Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense
- Configuring Discovery Policy on Cisco Secure Firewall Threat Defense
- Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense
- Configuring Access Control Policy on Cisco Secure Firewall Threat Defense
- Configuring Security Intelligence on Cisco Secure Firewall Threat Defense
- Configuring File Policy on Cisco Secure Firewall Threat Defense
- Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense
- Performing Basic Threat Analysis on Cisco Secure Firewall Management Center
- Managing Cisco Secure Firewall Threat Defense System
- Troubleshooting Basic Traffic Flow
- Cisco Secure Firewall Threat Defense Device Manager

Lab Outline:

Labs are designed to assure learners a whole practical experience, through the following practical activities:

- Perform Initial Device Setup
- Configure High Availability
- Configure Network Address Translation
- Configure Network Discovery
- Configure Prefilter and Access Control Policy
- Configure Security Intelligence
- Implement File Control and Advanced Malware Protection
- Configure Cisco Secure IPS
- Detailed Analysis Using the Firewall Management Center
- Manage Cisco Secure Firewall Threat Defense System
- Secure Firewall Troubleshooting Fundamentals
- Configure Managed Devices Using Cisco Secure Firewall Device Manage

Difference between SFWIPF and SSNGFW

New Topics in SFWIPF

- Configuring Access Control Policy on Cisco Secure Firewall Threat Defense

Labs

- Implement File Control and Advanced Malware Protection
- Configure Cisco Secure IPS
- Detailed Analysis Using the Firewall Management Center
- Manage Cisco Secure Firewall Threat Defense System
- Configure Managed Devices Using Cisco Secure Firewall Device Manager

Topics (from SSNGFW) which are no longer covered in SFWIPF

- Site-to-Site VPN
- Remote-Access VPN
- SSL Decryption

Labs:

- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Device Management
- Implementing QoS
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- System Administration

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges