Training overview
Cisco public

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

Description

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.

This training prepares you for the Securing Networks with Cisco Firepower (300-710 SNCF) v1.1 exam. If passed, you earn the Cisco Certified Specialist – Network Security Firepower certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training will help you:

- Configure settings and policies on Cisco Secure Firewall Threat Defense
- Gain an understanding of Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device
- Perform basic threat analysis and administration tasks using Cisco Secure Firewall Management Center
- Prepare for the 300-710 SNCF v1.1 exam
- Earn 40 CE credits toward recertification

Who should enroll

- Network Security Engineers
- Administrators

Technology areas

- Security

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

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 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 Offering:

- Implementing and Administering Cisco Solutions (CCNA)

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

- 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 Manager

What to expect on the exam

Securing Networks with Cisco Firepower (300-710 SNCF) v1.1 is a 90-minute exam associated with the Cisco Certified Specialist – Network Security Firepower certification and satisfies the concentration exam requirement for the CCNP Security certification.

The multiple-choice format tests your knowledge of Cisco Firepower Threat Defense and Firepower 7000 and 8000 Series virtual appliances, including:

- Policy configurations
- Integrations
- Deployments
- Management and troubleshooting

Links

- Cisco U. Learning Path
- Cisco Learning Network Store
- Cisco Learning Locator