Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense (SFWIPA)

Description

Master advanced threat defense techniques with Cisco Firewall

The Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA) training allows you to gain advanced expertise in configuring and managing Cisco security solutions. You will learn how to deploy complex security policies, optimize dynamic routing, and manage traffic flows and intrusion prevention rules. With this training, you will be able to implement VPNs, configure advanced NAT, and deploy identity-based policies, while automating event and threat management.

This course is designed for professionals looking to strengthen their network security skills, particularly in integrating and managing advanced Cisco Firewall systems. You will be guided through practical cases and labs to better understand the Cisco Firewall architecture and its optimal use. You will also master automation via APIs and integration with other security systems for comprehensive protection.

Reference
SFWIPA
Course Content
Module 1: Introduction to Cisco Secure Firewall Threat Defense

- Feature description
- Overview of security policies

Module 2: Advanced deployment options description

- Deployment choices
- Best deployment practices

Module 3: Configuring advanced device settings

- Interface settings
- Security zone configuration

Module 4: Configuring dynamic routing

- Advanced routing protocol
- Implementing routing rules

Module 5: Configuring advanced NAT

- Types of NAT
- Advanced NAT policies

Module 6: Deploying remote access VPN

- Basic VPN configuration
- Implementing VPN security policies

Module 7: Configuring Snort rules and analysis policies

- Creating Snort rules
- Managing NAP policies

Module 8: Advanced event management

- Configuring alerts and events
- Automating threat management

Lab / Exercises

- 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 Cisco Secure Firewall ASA configuration

Documentation

- Digital course material included

Exam

- This course prepares you for the Cisco Certified Specialist - Network Security Firepower certification with exam 300-710 Securing Networks with Cisco Firepower (SNCF). If you would like to take this exam, please contact our secretariat, who will inform you of the price and take care of all the necessary administrative procedures for you.

Participant profiles

- System and network administrators
- Security solution integrators
- Network security solution designers
- Security system installers

Prerequisites

- Mastery of TCP/IP concepts and routing protocols
- Basic knowledge of network security systems
- Experience with firewall and VPN management
- Familiarity with Cisco ASA or equivalent solutions

Objectives

- Describe advanced Cisco Firewall deployment options
- Configure dynamic routing and advanced NAT
- Deploy remote access and site-to-site VPNs
- Configure IPS and NAP rules
- Manage events and automate operations
- Troubleshoot advanced traffic flows

Description
Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense (SFWIPA) training
Niveau
Avancé
Classroom Registration Price (CHF)
4350
Virtual Classroom Registration Price (CHF)
4350
Duration (in Days)
5