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

Description

The Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) training offers an in-depth understanding of modern threat protection techniques through Cisco Secure Firewall. This course will guide you in configuring and deploying this next-generation firewall, essential for securing enterprise networks.

This program is designed to provide practical skills, enabling you to efficiently configure security policies, manage packet handling, and perform real-time threat analysis. You will also learn to implement advanced features such as high availability, network address translation (NAT), and intrusion prevention.

Niveau
Intermédiaire
Course Content
Module 1: Introduction to Cisco Secure Firewall Threat Defense

- Understand the main functions of Cisco Secure Firewall Threat Defense
- Identify the key components of the solution
- Describe the deployment options of Cisco Secure Firewall Threat Defense

Module 2: Configuring Basic Network Settings

- Configure network interfaces on Cisco Secure Firewall Threat Defense
- Implement network address translation (NAT)
- Set up high availability (HA)

Module 3: Managing Security Policies

- Configure access control policies (ACL)
- Set up pre-filter and VPN tunnel policies
- Manage security rules with Cisco Secure Firewall Threat Defense

Module 4: Advanced Security with Cisco Secure Firewall

- Configure security intelligence (Security Intelligence)

- Set up intrusion policies with Cisco IPS
- Manage events and threats using Cisco Secure Firewall Management Center

Module 5: Threat Analysis and Advanced Management

- Perform basic threat analysis on network threats
- Implement security and event reporting
- Troubleshoot traffic flow issues

Module 6: System Management and Troubleshooting

- Manage Cisco Secure Firewall Threat Defense with Cisco Firewall Device Manager
- Perform system maintenance with Cisco tools
- Troubleshoot network and security incidents

Lab / Exercises

- Perform initial device setup
- Configure high availability
- Set up network address translation (NAT)
- Configure network discovery
- Set up pre-filter and access control policies
- Configure security intelligence
- Implement file control and advanced malware protection
- Configure Cisco Secure IPS
- Analyze in detail using Firewall Management Center
- Manage Cisco Secure Firewall Threat Defense system
- Basic troubleshooting of secure firewall traffic
- Manage devices using Cisco Secure Firewall Device Manager

Documentation

- Digital course materials included

Exam

- This course prepares you for CCNP Security certification.

Participant profiles

- Network security engineers
- Network administrators
- Network architects
- IT security consultants

Prerequisites

- Mastery of TCP/IP concepts
- Understanding of basic routing protocols
- Firewall and VPN concepts
- Knowledge of intrusion prevention systems (IPS)

Objectives

- Deploy Cisco Secure Firewall Threat Defense

- Configure high availability
- Implement network address translation (NAT)
- Set up security and discovery policies
- Manage Cisco Secure Firewall Management Center
- Troubleshoot and resolve network issues

Description
Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) training
Classroom Registration Price (CHF)
4350
Virtual Classroom Registration Price (CHF)
4350
Duration (in Days)
5
Reference
SFWIPF