Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0 (SFWIPF)

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0 (SFWIPF)

Course Duration

5 Days

Course Price

$3,995.00
40 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

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 CCNP Security certification, which requires passing the 350-701 Implementing and Operating Cisco Security Core Technologies (SCOR) core exam and one concentration exam such as the 300-710 Securing Networks with Cisco Firepower (SNCF) concentration exam. This training also earns you 40 Continuing Education (CE) credits towards recertification.

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0 (SFWIPF)

How you will benefit

This class 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

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Network Security Engineers
- Administrators

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0 (SFWIPF)

Objectives

After taking this course, you should be able to:

- 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

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0 (SFWIPF)

Course Outline

Module 1: Introducing Cisco Secure Firewall Threat Defense
Module 2: Describing Cisco Secure Firewall Threat Defense Deployment Options
Module 3: Describing Cisco Secure Firewall Threat Defense Management Options
Module 4: Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense
Module 5: Configuring High Availability on Cisco Secure Firewall Threat Defense
Module 6: Configuring Auto NAT on Cisco Secure Firewall Threat Defense
Module 7: Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense
Module 8: Configuring Discovery Policy on Cisco Secure Firewall Threat Defense
Module 9: Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense
Module 10: Configuring Access Control Policy on Cisco Secure Firewall Threat Defense
Module 11: Configuring Security Intelligence on Cisco Secure Firewall Threat Defense
Module 12: Configuring File Policy on Cisco Secure Firewall Threat Defense
Module 13: Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense
Module 14: Performing Basic Threat Analysis on Cisco Secure Firewall Management Center
Module 15: Managing Cisco Secure Firewall Threat Defense System
Module 16: Troubleshooting Basic Traffic Flow
Module 17: Cisco Secure Firewall Threat Defense Device Manager

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention 1.0 (SFWIPF)

Lab Outline

- **Lab 1: Perform Initial Device Setup**
- **Lab 2: Configure High Availability**
- **Lab 3: Configure Network Address Translation**
- **Lab 4: Configure Network Discovery**
- **Lab 5: Configure Prefilter and Access Control Policy**
- **Lab 6: Configure Security Intelligence**
- **Lab 7: Implement File Control and Advanced Malware Protection**
- **Lab 8: Configure Cisco Secure IPS**
- **Lab 9: Detailed Analysis Using the Firewall Management Center**
- **Lab 10: Manage Cisco Secure Firewall Threat Defense System**
- **Lab 11: Secure Firewall Troubleshooting Fundamentals**
- **Lab 12: Configure Managed Devices Using Cisco Secure Firewall Device Manager**