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!

+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)

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.

+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)

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

Prerequisites

Before taking this offering, you should understand:

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

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

- Introduce firewall concepts and Technologies with examples of each type
- Describe traditional network security and how it does not keep up with today's modern reality
- Provide an overview of the traditional security workplace and how it has changed to an evolving workplace
- Provide an overview of Cisco Secure Firewall Threat Defense features
- Describe the different Cisco Secure Firewall deployments and recommendations for any size network and deployment type

MODULE 2: Describing Cisco Secure Firewall Threat Defense Deployment Options

- Describe the deployment options of Cisco Secure Firewall, including firewall modes, IPS interface modes, and redundancy options
- Describe transparent and routed firewall modes for Cisco Secure Firewall
- Describe the Cisco Secure Firewall supported types of interfaces for management and network traffic
- Describe the role of IPS in the network and how IPS-only interfaces augment IPS deployments
- Overview of resilience using Cisco high availability and clustering configuration options of Cisco Secure Firewall and high availability for the Cisco Secure Management Center

MODULE 3: Describing Cisco Secure Firewall Threat Defense Management Options

- Cisco Firewall Threat Defense Management Overview
- Describe basic functionalities of Cisco Secure Firewall Management Center

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

Course Outline

MODULE 4: Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense

- Perform basic Cisco Secure Firewall setup by using setup wizard
- Perform basic network settings on Cisco Secure Firewall Management Center
- Perform registration of Cisco Firewall Threat Defense device with Cisco Secure Firewall
- Describe how to edit basic Cisco Secure Firewall Threat Defense device settings
- Configure basic interface properties and assign interface to security zone
- Configure static routing on Cisco Secure Firewall Threat Defense
- Configure platform settings on Cisco Secure Firewall Threat Defense
- Explain how to monitor system health using health policy

MODULE 5: Configuring High Availability on Cisco Secure Firewall Threat Defense

- Provide an overview of active/standby high availability feature on Cisco Firewall Threat Defense
- Explain difference between stateless and stateful failover configuration
- Explain how Cisco Secure Firewall Threat Defense monitors overall health and interface health to trigger failover in high availability pair
- Configure and verify Active/Standby failover on Cisco Secure Firewall Threat Defense
- Monitor and troubleshoot Active/Standby failover on Cisco Secure Firewall Threat Defense

MODULE 6: Configuring Auto NAT on Cisco Secure Firewall Threat Defense

- Explain the drivers for network address translation and explain types of network translation
- Describe the configuration steps for basic auto network address translation

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

Course Outline

MODULE 7: Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense

- Describe objects and explain usage of objects in policies
- Describe Cisco Secure Firewall Threat Defense policies
- Describe how an ingress packet is processed by Cisco Secure Firewall Threat Defense

MODULE 8: Configuring Discovery Policy on Cisco Secure Firewall Threat Defense

- Provide an overview of discovery policy
- Configure network discovery policy
- Perform discovery events and host profile analysis

MODULE 9: Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense

- Provide an overview of prefilter policy and reasons for using it
- Configure tunnel and prefilter policy components
- Analyze events that are produced by prefilter rules

MODULE 10: Configuring Access Control Policy on Cisco Secure Firewall Threat Defense

- Provide an overview of access control policy
- Configure access control policy
- Deploy access control policy configuration changes
- Explain best practices for configuring access control policy on Cisco Secure Firewall Threat Defense

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

Course Outline

MODULE 11: Configuring Security Intelligence on Cisco Secure Firewall Threat Defense

- Provide an overview of security intelligence
- Configure and explain the purpose of security intelligence objects
- Describe IP and URL Security Intelligence configuration
- Describe DNS Security Intelligence configuration

MODULE 12: Configuring File Policy on Cisco Secure Firewall Threat Defense

- Provide an overview of file policy
- Provide an overview of network malware protection and file type detection architectures
- Configure file policy
- Perform Malware and file event analysis

MODULE 13: Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense

- Describe intrusion prevention and Snort
- Describe intrusion rules
- Describe Intrusion policies
- Explain how to create a custom IPS policy
- Describe intrusion events

MODULE 14: Performing Basic Threat Analysis on Cisco Secure Firewall Management Center

- Provide an overview of different types of events on Cisco Secure Firewall Threat Defense
- Show how indications of compromise (IoC) events can help with threat analysis
- Provide an overview of Context Explorer analysis tool

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

Course Outline

CONT. MODULE 14:

- Provide an overview of Firewall Management Center dashboards and how to create custom dashboards
- Generate pre-defined and custom reports on the Firewall Management Center
- Describe the operation of the Unified Event Viewer
- Perform threat analysis for a highly infected host

MODULE 15: Managing Cisco Secure Firewall Threat Defense System

- Explain how to implement Cisco Secure Firewall Threat Defense system updates
- Describe the user management options and explain how to configure local user accounts
- Explain how to perform backup of the Cisco Secure Firewall Threat Defense and Cisco Secure Firewall
- Explain how to copy configuration between different appliances
- Explain the Cisco Secure Firewall Management Center configuration rollback feature

MODULE 16: Troubleshooting Basic Traffic Flow

- Explain basics of Cisco Secure Firewall Threat Defense command line interface
- Provide an overview of traffic flow troubleshooting process and tools that can be used during this process
- Provide a complete traffic flow troubleshooting process on a sample traffic

MODULE 17: Cisco Secure Firewall Threat Defense Device Manager

- Configure initial network settings using Cisco Secure Firewall Threat Defense Manager
- Provide an overview of policies available on Cisco Secure Firewall Threat Defense Device Manager