Current Technologies
Computer Learning Centers

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

Cisco Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

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

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

In this Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention course provides a structured, in-depth exploration of Cisco Secure Firewall Threat Defense, guiding learners from foundational firewall concepts to advanced policy configuration, threat analysis, and troubleshooting. The curriculum begins by establishing core security principles, comparing traditional perimeter-based security models with modern, threat-centric approaches required for today's evolving workplaces, including remote users, cloud connectivity, and encrypted traffic. Students gain a clear understanding of Cisco Secure Firewall Threat Defense features, deployment models, and design recommendations for networks of all sizes, ensuring they can select and position the firewall appropriately within diverse enterprise environments.

As the course progresses, learners develop practical skills in deploying and managing Cisco Secure Firewall Threat Defense using Cisco Secure Firewall Management Center. Topics include firewall modes, interface types, transparent versus routed deployments, IPS integration, and resilience through high availability and clustering. Students configure essential network settings, interfaces, routing, NAT, and platform options, while learning how system health and failover mechanisms maintain availability. Policy-focused modules cover packet processing, objects, discovery, prefiltering, access control, security intelligence, file and malware protection, and intrusion prevention using Snort, providing a deep understanding of how traffic is evaluated and protected end to end.

The course concludes with operational and troubleshooting competencies, including threat analysis using events, dashboards, reports, Context Explorer, and the Unified Event Viewer, along with system maintenance tasks such as updates, backups, user management, and configuration rollback. Learners also gain hands-on experience troubleshooting traffic flows using both graphical tools and the Cisco Secure Firewall Threat Defense command-line interface, and are introduced to management capabilities available through Cisco Secure Firewall Threat Defense Device Manager. By the end of the course, students are equipped with the knowledge and practical skills required to deploy, manage, secure, and troubleshoot Cisco Secure Firewall Threat Defense in real-world enterprise environments.

How you'll 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

Course Duration
5 days

Course Price
$3,995.00 or 40 CLCs

Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

Why Attend with Current Technologies CLC

- Our Instructors are in 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 primary audience for this course is as follows:

- Network security engineers
- Administrators

Prerequisites

Before taking this offering, you should understand:

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

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

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

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

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
- 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

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