Current Technologies
Computer Learning Centers

CISCO
Partner

Platinum Learning

Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense v1.0 (SFWIPA)

WHERE GREAT TRAINING HAPPENS EVERYDAY!

+1 (219) 764-3800

6210 Central Ave, Portage IN

sales@ctclc.com

www.ctclc.com

CISCO Partner

Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense v1.0 (SFWIPA)

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 Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense training shows you how to deploy and configure Cisco Secure Firewall Threat Defense system and its features as a data center network firewall or as an Internet Edge firewall with Virtual Private Network (VPN) support. You will learn how to configure identity-based policies, Secure Sockets Layer (SSL) decryption, remote-access VPN, and site-to-site VPN before moving on to advanced Intrusion Prevention System (IPS) configuration and event management, integrations with other systems, and advanced troubleshooting. You will also learn how to automate configuration and operations of Cisco Secure Firewall Threat Defense system using programmability and Application Programming Interfaces (APIs) and how to migrate configuration from Cisco Secure Firewall Adaptive Security Appliances (ASA).

This training prepares you for the 300-710 Securing Networks with Cisco Firepower (SNCF) exam. If passed, you earn the Cisco Certified Specialist – Network Security Firepower certification and satisfy the concentration exam requirement for the Cisco Certified Networking Professional (CCNP) Security certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

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!

Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense v1.0 (SFWIPA)

How you will benefit

This class will help you:

- Attain advanced knowledge of Cisco Secure Firewall Threat Defense technology
- Gain competency and skills required to implement and manage a Cisco Secure Firewall Threat Defense system regardless of platform
- Learn detailed information on policy management, traffic flow through the system, and the system architecture
- Deploy and manage many of the advanced features available in the Cisco Secure Firewall Threat Defense system
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level data center roles
- Earn 40 CE credits toward recertification

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:

- System Installers
- System Integrators
- System Administrators
- Network Administrators
- Solutions Designers

Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense v1.0 (SFWIPA)

Objectives

After taking this course, you should be able to:

- Describe Cisco Secure Firewall Threat Defense
- Describe advanced deployment options on Cisco Secure Firewall Threat Defense
- Describe advanced device settings for Cisco Secure Firewall Threat Defense device
- Configure dynamic routing on Cisco Secure Firewall Threat Defense
- Configure advanced network address translation on Cisco Secure Firewall Threat Defense
- Configure SSL decryption policy on Cisco Secure Firewall Threat Defense
- Deploy Remote Access VPN on Cisco Secure Firewall Threat Defense
- Deploy identity-based policies on Cisco Secure Firewall Threat Defense
- Deploy site-to-site IPsec-based VPN on Cisco Secure Firewall Threat Defense
- Deploy advanced access control settings on Cisco Secure Firewall Threat Defense
- Describe advanced event management on Cisco Secure Firewall Threat Defense
- Describe available integrations with Cisco Secure Firewall Threat Defense
- Troubleshoot traffic flow using advanced options on Cisco Secure Firewall Threat Defense
- Describe benefits of automating configuration and operations of Cisco Secure Firewall Threat Defense
- Describe configuration migration to Cisco Secure Firewall Threat Defense

Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense v1.0 (SFWIPA)

Course Outline

- **Module 1:** Introducing Cisco Secure Firewall Threat Defense
- **Module 2:** Describing Advanced Deployment Options on Cisco Secure Firewall Threat Defense
- **Module 3:** Configuring Advanced Device Settings on Cisco Secure Firewall Threat Defense
- **Module 4:** Configuring Dynamic Routing on Cisco Secure Firewall Threat Defense
- **Module 5:** Configuring Advanced NAT on Cisco Secure Firewall Threat Defense
- **Module 6:** Configuring SSL Policy on Cisco Secure Firewall Threat Defense
- **Module 7:** Deploying Remote Access VPN on Cisco Secure Firewall Threat Defense
- **Module 8:** Deploying Identity-Based Policies on Cisco Secure Firewall Threat Defense
- **Module 9:** Deploying Site-to-Site VPN on Cisco Secure Firewall Threat Defense
- **Module 10:** Configuring Snort Rules and Network Analysis Policies
- **Module 11:** Describing Advanced Event Management Cisco Secure Firewall Threat Defense
- **Module 12:** Describing Integrations on Cisco Secure Firewall Threat Defense
- **Module 13:** Troubleshooting Advanced Traffic Flow on Cisco Secure Firewall Threat Defense
- **Module 14:** Automating Cisco Secure Firewall Threat Defense
- **Module 15:** Migrating to Cisco Secure Firewall Threat Defense

Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense v1.0 (SFWIPA)

Lab Outline

Lab 1: Deploy Advanced Connection Settings

Lab 2: Configure Dynamic Routing

Lab 3: Configure SSL Policy

Lab 4: Configure Remote Access VPN

Lab 5: Configure Site-to-Site VPN

Lab 6: Customize IPS and NAP Policies

Lab 7: Configure Cisco Secure Firewall Threat Defense Integrations

Lab 8: Troubleshoot Cisco Secure Firewall Threat Defense

Lab 9: Migrate Configuration from Cisco Secure Firewall ASA