Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense (SFWIPA) 1.0

Course Duration: 40 Hours **Course Code: SFWIPA 1.0**

1. Course Overview

The *Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense (SFWIPA) 1.0* course provides in-depth knowledge and hands-on skills to design, implement, and manage secure data center networks using Cisco Secure Firewall Threat Defense. Participants will learn how to configure VPNs, secure critical workloads, and enforce advanced security policies to protect against evolving threats. This course blends theoretical concepts with practical lab exercises to ensure learners are fully prepared to secure enterprise-level data centers.

2. What You'll Learn?

By the end of this course, you will be able to:

- Understand Cisco Secure Firewall Threat Defense architecture and features.
- Secure data center environments with Cisco Secure Firewall policies.
- Configure and manage secure site-to-site and remote-access VPNs.
- Protect workloads in hybrid and multi-cloud environments.
- Implement advanced intrusion prevention, threat intelligence, and high availability.
- Troubleshoot and optimize firewall and VPN configurations.

3. Target Audience

This course is designed for:

- Network Security Engineers
- Data Center Network Engineers
- Security Administrators
- System Engineers
- IT Professionals responsible for securing enterprise networks and VPNs

4. Pre-Requisites

Participants are expected to have:

- Basic understanding of networking and TCP/IP concepts
- Knowledge of Cisco ASA or Firepower technologies (recommended)
- Familiarity with VPN concepts and security fundamentals
- Completion of **Cisco CCNA or equivalent knowledge**

5. Course Content

Module 1: Introduction to Cisco Secure Firewall Threat Defense

- Overview of Cisco Secure Firewall
- Deployment modes and architecture
- Management with Cisco Secure Firewall Management Center (FMC)

Module 2: Securing Data Center Networks

- Data center architecture and security challenges
- Implementing segmentation and access control policies
- Securing east-west and north-south traffic

Module 3: Virtual Private Networks (VPNs) with Cisco Secure Firewall

- Fundamentals of VPNs (IPsec, SSL, FlexVPN)
- Configuring site-to-site VPNs
- Configuring remote access VPNs
- Monitoring and troubleshooting VPNs

Module 4: Advanced Security Policies

- Intrusion Prevention System (IPS) configuration
- Threat intelligence integration
- High availability and clustering

Module 5: Securing Hybrid and Multi-Cloud Data Centers

- Cloud security integration with Cisco Secure Firewall
- Securing workloads in public and private clouds
- Policy consistency across environments

Module 6: Monitoring, Troubleshooting, and Best Practices

- Log collection and analysis
- Troubleshooting firewall and VPN issues
- Best practices for securing data center networks