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

Course Duration: 24 Hours **Course Code: SFWIPF**

1. Course Overview

The **Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)** course provides essential knowledge and hands-on skills to configure, manage, and troubleshoot Cisco Firepower Threat Defense (FTD) and Intrusion Prevention solutions. This course is designed to help participants understand firewall concepts, deployment modes, traffic control, and advanced threat prevention capabilities to protect enterprise networks against modern cyber threats.

2. What You'll Learn?

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

- Understand the architecture and key features of Cisco Firepower Threat Defense (FTD).
- Deploy and configure Cisco Firepower Management Center (FMC) for centralized management.
- Implement access control policies and security intelligence features.
- Configure intrusion prevention policies to detect and block threats.
- Manage and monitor firewall and intrusion prevention events.
- Perform basic troubleshooting of Cisco FTD and FMC.

3. Target Audience

This course is designed for:

- Network security engineers
- Security administrators
- Technical support personnel
- System engineers and integrators
- Anyone responsible for managing Cisco Firepower solutions

4. Pre-Requisites

Before taking this course, participants should have:

- Basic knowledge of networking protocols (TCP/IP, routing, switching)
- Understanding of network security concepts
- Familiarity with Cisco ASA or firewall technologies (recommended but not mandatory)

5. Course Content

Module 1: Introduction to Cisco Firepower Threat Defense

- Overview of Cisco Firepower System Architecture
- Firepower Threat Defense (FTD) components
- Deployment options and use cases

Module 2: Firepower Management Center (FMC)

- FMC features and functions
- System configuration and licensing
- Device registration and management

Module 3: Access Control Policies

- Access control concepts

- Configuring access control rules
- Security intelligence and reputation-based filtering

Module 4: Intrusion Prevention System (IPS)

- IPS fundamentals
- Implementing intrusion policies
- Managing signatures and tuning detection

Module 5: Advanced Threat Defense Features

- URL filtering and application control
- File and malware policies
- SSL decryption overview

Module 6: Monitoring and Troubleshooting

- Event analysis and reporting
- Connection and intrusion event logs
- Basic troubleshooting of FTD and FMC