FortiGate 7.4 Administration Course

Course Duration: 40 Hrs. **Course Code: FG-ADMIN-7.4**

Course Overview

The **FortiGate 7.4 Administration** course is designed for network and security professionals responsible for deploying, configuring, and managing FortiGate firewalls running FortiOS 7.4. This course provides in-depth knowledge of FortiGate system administration, security policy management, and monitoring. Participants will gain hands-on experience in managing firewall operations, securing network traffic, and maintaining optimal performance in enterprise environments using FortiGate 7.4.

What You'll Learn?

By completing this course, you will be able to:

- Perform initial setup and system configuration of FortiGate 7.4
- Configure interfaces, routing, and network services
- Create and manage firewall policies and NAT
- Implement user authentication and identity-based policies
- Configure security profiles such as IPS, antivirus, and web filtering
- Monitor traffic, logs, and system performance
- Troubleshoot common FortiGate operational issues

Target Audience

This course is ideal for:

- Network and Security Administrators
- Firewall and Infrastructure Engineers

- IT Operations and Support Teams
- SOC/NOC Engineers managing FortiGate environments
- Professionals administering FortiGate 7.4 firewalls

Pre-Requisites

Participants should have:

- Basic understanding of networking fundamentals (TCP/IP, routing, switching)
- Familiarity with firewall and security concepts
- Prior experience with Fortinet products is helpful but not mandatory

Course Content

Module 1: FortiGate 7.4 Overview and System Setup

- FortiGate architecture and FortiOS 7.4 features
- Deployment modes and initial configuration
- Administrative access and system settings

Module 2: Network Configuration and Routing

- Interface configuration and VLANs
- Static and dynamic routing basics
- Network services (DHCP, DNS, NTP)

Module 3: Firewall Policies and NAT

- Policy creation and management
- Address objects, services, and schedules
- Source and destination NAT

Module 4: User Authentication and Security Profiles

- User authentication methods
- Identity-based firewall policies
- Antivirus, IPS, web filtering, and application control

Module 5: Monitoring, Logging, and Reporting

- Traffic and event monitoring
- Logs, alerts, and reports
- FortiAnalyzer integration

Module 6: Maintenance, Troubleshooting, and Best Practices

- Backup and restore
- Firmware upgrades
- Troubleshooting connectivity and policy issues