NSE 4 FortiGate Security 7.0 Course

Course Duration: 24 Hrs. **Course Code: NSE4-FG-7.0**

Course Overview

The **NSE 4 FortiGate Security 7.0 course** is designed to provide network and security professionals with in-depth knowledge of configuring, managing, and securing networks using FortiGate firewalls running FortiOS 7.0. This course focuses on essential security features such as firewall policies, NAT, VPNs, user authentication, and security profiles. Participants will gain practical skills to deploy and manage FortiGate devices effectively in enterprise environments and prepare for the NSE 4 certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Understand FortiGate architecture and FortiOS 7.0 features
- Configure firewall policies and network address translation (NAT)
- Implement user authentication and role-based access
- Configure security profiles including antivirus and web filtering
- Set up and manage IPsec and SSL VPNs
- Monitor, troubleshoot, and optimize FortiGate security deployments

Target Audience

This course is ideal for:

- Network and Security Engineers
- System and Infrastructure Administrators
- SOC and IT Support Professionals

- Network Consultants and Integrators
- Professionals preparing for the Fortinet NSE 4 certification

Pre-Requisites

Participants should have:

- Basic understanding of networking concepts (TCP/IP, routing, switching)
- Familiarity with firewalls and security fundamentals
- Experience with FortiGate is helpful but not mandatory

Course Content

Module 1: Introduction to FortiGate and FortiOS 7.0

- Fortinet Security Fabric overview
- FortiGate hardware and virtual platforms
- FortiOS 7.0 features and interface

Module 2: Firewall Policies and NAT

- Policy-based firewall concepts
- Address objects and services
- Source and destination NAT configuration

Module 3: User Authentication and Access Control

- User and device authentication methods
- Firewall policies with identity-based rules
- Two-factor authentication

Module 4: Security Profiles and Threat Protection

- Antivirus and intrusion prevention (IPS)
- Web filtering and application control
- SSL inspection

Module 5: VPN Configuration and Secure Connectivity

- IPsec VPN fundamentals
- SSL VPN for remote access
- Site-to-site VPN deployment

Module 6: Monitoring, Troubleshooting, and Management

- Logging and reporting
- Diagnostics and troubleshooting tools
- Performance optimization and best practices

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com