NSE 6 FortiDDoS Course

Course Duration: 8 Hrs. **Course Code: NSE6-FDDOS-7.x**

Course Overview

The **NSE 6 FortiDDoS** course is designed for network and security professionals responsible for protecting enterprise networks against Distributed Denial of Service (DDoS) attacks. This course focuses on deploying, configuring, and managing FortiDDoS appliances and solutions to detect, mitigate, and respond to DDoS threats. Participants will gain hands-on experience in traffic analysis, attack mitigation, and system optimization while preparing for the NSE 6 FortiDDoS certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiDDoS appliances in enterprise networks
- Monitor network traffic and detect potential DDoS attacks
- Implement automated mitigation strategies to protect critical resources
- Configure thresholds, policies, and alerts for DDoS protection
- Integrate FortiDDoS with FortiGate and other Fortinet security solutions
- Analyze DDoS attack patterns and optimize system performance
- Troubleshoot and maintain FortiDDoS deployments

Target Audience

This course is ideal for:

- Network Security Engineers and Administrators

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

- SOC Analysts and Incident Response Teams
- IT Infrastructure Teams managing enterprise networks
- Professionals preparing for the NSE 6 FortiDDoS certification

Pre-Requisites

Participants should have:

- Basic understanding of networking fundamentals (TCP/IP, LAN/WAN)
- Knowledge of DDoS attacks and network security concepts
- Experience with Fortinet products or NSE 4-level knowledge is recommended

Course Content

Module 1: FortiDDoS Architecture and Deployment

- FortiDDoS system components and models
- Deployment scenarios and network integration
- Initial configuration and system setup

Module 2: Traffic Monitoring and Analysis

- Understanding traffic patterns and anomalies
- Monitoring dashboards and metrics
- Logging and reporting

Module 3: DDoS Threat Detection and Mitigation

- Identifying volumetric and protocol-based attacks
- Configuring mitigation policies and thresholds
- Real-time response and automated protection

Module 4: Integration with Security Fabric

- FortiDDoS integration with FortiGate and other Fortinet solutions
- Coordinated threat response
- Event correlation and alerting

Module 5: Troubleshooting and Best Practices

- Common deployment and configuration issues
- Performance optimization and tuning
- Operational best practices for enterprise DDoS protection