FORTINET
Premier Authorized Training Center

NSE 6 CERTIFIED
CLOUD SECURITY
FORTINET

fast lane

FortiDDoS Administrator

Course Description

In this course, you will learn how to establish network baseline data and identify, analyze, and mitigate both individual and distributed DDoS attacks while maintaining service availability and network performance. This course covers the fundamental administration and operational concepts of FortiDDoS, providing a solid understanding of how to deploy, configure, and manage FortiDDoS solutions in your network environment.

Course Duration:

2 Days

Prerequisites:

You should have a basic understanding of DDoS attacks and common DDoS mitigation solutions.

Outlines:

1. Introduction and Deployment
2. Initial Configuration
3. Monitoring and Reporting
4. Global Settings
5. Service Protection

Objectives:

After completing this course, you will be able to:

- Train your FortiDDoS to recognize your unique network patterns
- Choose the correct FortiDDoS model
- Defend against both volumetric and mechanistic DDoS attacks
- Deploy FortiDDoS to protect both network appliances and servers
- Identify when to use detection and prevention modes
- Implement bypass or a high availability FortiDDoS cluster for maximum service uptime
- Detect connections from proxies
- Describe how the blocking periods and penalty factors intelligently determine which packets are dropped after an attack is detected
- Configure access control lists and blocklists
- Mitigate anomalies and SYN floods
- Describe the main characteristics of protection policies
- Characterize different types of attacks by using logs and statistics graphs
- Troubleshoot incorrect threshold levels

Who should attend

Security professionals involved in the day-to-day administration, management, and troubleshooting of FortiDDoS-F Series devices should attend this course. .