FORTINET
Premier Authorized
Training Center

fast lane

FortiDDoS-F Series (FT-FDD)

Course Description

In this course, you will learn how to form network baseline data, and how to recognize and mitigate individual and distributed denial of service attacks while preserving service and network performance.

Product Version:

- FortiDDoS-F 6.3
- The FortiDDoS-F Series 6.3 course is applicable only for F-series hardware and VMs.

Course Duration:

2 days

Certification:

This course is not included in the certification program.

Prerequisites:

You should have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure

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 right FortiDDoS model
- Defend against both volumetric and mechanistic DDoS attacks
- Deploy FortiDDoS to protect both network appliances and servers
- Understand 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
- Understand the main characteristics of protection policies
- Characterize different types of attacks by using logs and statistics graphs
- Troubleshoot incorrect threshold levels

Who should attend

Cybersecurity professionals responsible for the day-to-day administration, management, and troubleshooting of a FortiDDoS F-Series device should attend this course.