FortiDDoS-F Series

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

- Lecture time (estimated): 6 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated): 10 hours/2 days

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.

Certification

This course does not have a certification exam.

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*

Agenda

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

Objectives

After completing these courses, 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

Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FDD

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- Purchase order (PO), through Fortinet Resellers or Authorized Training Partners

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-FDD-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)^2

- CPE training hours: 6
- CPE lab hours: 4
- CISSP domains: Communication and Network Security

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.