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.

Who Should Attend

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

Prerequisites

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

Agenda

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

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
  - HTML 5 support
  - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled in your web browser

You should use a wired Ethernet connection, *not* a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Product Versions

FortiDDoS-F 7.2

The FortiDDoS-F Series 7.2 Administrator course is applicable only to F-Series hardware and VMs.

Course Duration

- Lecture time (estimated): 5 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated): 9 hours
  - 2 full days or 3 half days

Formats

- Instructor-led (classroom and online)
- Self-paced online

ISC2

- CPE training hours: 5
- CPE lab hours: 4
- CISSP domains: Communications and Network Security

Part Number (SKU)

See Purchasing Process for more information

Certification

Datacipher Education Services | FORTINET