



FortiDDoS

In this 1-day class, you will learn how to form network baseline data, and how to recognize and mitigate individual and distributed denial of service (DDoS) attacks while preserving service and network performance.

In interactive labs, you will deploy FortiDDoS to learn about normal network traffic patterns. Then you will simulate attacks, observe the defense, and adjust the automatically estimated behavior.

With a focus on core feature skills, topics also include network behavior analysis and ASIC chips.

Product Version

FortiDDoS 4.5

Formats

- Instructor-led classroom
- Self-paced online (without lab access)*

*Only provides the self-paced videos. If you are interested in lab access, we recommend you sign up for a classroom session. The lab session is highly recommended before attempting the specialist exam at a PearsonVUE testing center.

Agenda

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

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
- Mitigate SYN floods
- Detect connections from proxies
- Inspect HTTP traffic on non-standard ports
- Deploy FortiDDoS to protect both network appliances and servers
- Describe how the blocking periods and penalty factors intelligently determine which packets will be dropped after an attack has been detected
- Implement bypass or a high availability FortiDDoS cluster for maximum service uptime

- Understand when to use detection and prevention modes
- Whitelist safe clients or servers
- Characterize different types of attacks by using logs and statistics graphs
- Troubleshoot incorrect threshold levels

Who Should Attend

Anyone who is responsible for day-to-day management of a FortiDDoS appliance.

Prerequisites

- Knowledge of TCP, UDP, ICMP, and HTTP protocols
- Knowledge of network security

System Requirements

To attend the instructor-led classroom training, you must have a computer with:

- Wired Ethernet connection
- Up-to-date web browser
- PDF viewer
- SSH client, such as PuTTY
- Up-to-date Java run-time environment (JRE) with Java plug-in enabled in your web browser

Certification

This course prepares you for the FortiDDoS 4.5 Specialist exam.

The FortiDDoS 4.5 Specialist exam counts toward one of the four NSE 6 specializations required to get the NSE 6 certification.