FortiDDoS

COURSE DETAILS

Course Code: FortiDDoS
Current Version: 4.0
Delivery Type: Instructor-led
Duration: 2 day

PREREQUISITES

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

COURSE CONTENT

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.

COURSE OBJECTIVES

After completing these courses, you will be able to:

- Train your FortiDDoS to recognize your unique network patterns
- Choose the right FortiDDoS model
- Distinguish a DDoS from a rush of Reddit traffic or a successful Thursday marketing campaign
- Defend against both volumetric and mechanistic DDoS attacks
- Mitigate SYN floods
- Handle attacks from dynamic or Tor-masked IPs by FortiGuard IP reputation and aging data
- Detect connections from proxies
- Inspect HTTP traffic on non-standard ports
- Deploy 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 vs. Prevention mode
- Create "Do Not Track" policies
- Whitelist "safe" clients or servers
- Characterize different types of attacks by using logs and statistics graphs
- Troubleshoot incorrect thresholds

FortiDDoS

COURSE OUTLINE

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

WHO SHOULD ATTEND

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