FortiWeb

In this course, you will learn how to deploy, configure, and troubleshoot FortiWeb. You will learn key concepts of web application security, and explore protection and performance features. You will experience traffic and attack simulations that use real web applications. You will learn how to distribute the load from virtual servers to real servers, while enforcing logical parameters, inspecting flow, and securing HTTP session cookies.

Product Version

FortiWeb 6.4

Course Duration

- Lecture time (estimated): 10 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 17 hours/3 days

Who Should Attend

Networking and security professionals involved in the administration and support of FortiWeb should attend this course.

Certification

This course is intended to help you prepare for the *NSE 6 FortiWeb* certification exam.

Prerequisites

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

- *NSE 4 FortiGate Security*
- *NSE 4 FortiGate Infrastructure*

It is also recommended that you have an understanding of the following topics:

- HTTP protocol
- Basic knowledge of HTML, JavaScript, and server-side dynamic page languages, such as PHP

Agenda

1. Introduction
2. Basic Setup
3. Compliance
4. Authentication and Access Control
5. Web Application Security
6. DoS and Defacement
7. Machine Learning and Bot Detection
8. SSL/TLS
9. Application Delivery
10. API Protection and Bot Mitigation
11. Additional Configuration
12. Troubleshooting

Objectives

After completing this course, you will be able to:

- Define web application firewall and describe its role in the network
- Perform basic configuration and initial deployment
- Configure FortiWeb for deployment in a load balanced network environment
- Implement FortiWeb machine learning capabilities
- Configure and customize FortiWeb signatures
- Configure FortiWeb to protect against DoS and defacement attacks
- Implement SSL/TLS encryption, including inspection and offloading
- Configure user authentication and access control features
- Configure FortiWeb to ensure PCI DSS compliance of your web applications
- Configure FortiWeb to perform caching and compression tasks
- Configure FortiWeb to perform HTTP content based routing, rewriting, and redirection
- Perform basic troubleshooting of FortiWeb

Training 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-FWB

Self-Paced Training

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

You can purchase on-demand lab access with interactive, hands-on activities using a 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-FWB-LAB

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

(ISC)^2

- CPE training hours: 10
- CPE lab hours: 7
- CISSP domains: Communications and Network Security

Program Policies and FAQs

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