

FortiProxy Administrator

Course Description

In this course, you will learn how to use FortiProxy features, including policy types, content analysis, and security profiles. You will also explore FortiProxy policies, deployment, user authentication, high availability, monitoring, and how to protect your web traffic using content inspection, such as DLP, antivirus, web filtering, application control, and logging.

Who Should Attend

Networking and security professionals involved in the management, configuration, administration, and monitoring of FortiProxy devices used to secure their organization's user web traffic should attend this course.

Prerequisites

- Knowledge of network protocols
- Understanding of routers, switches, firewalls, and content inspection
- Basic understanding of proxy concepts
- Understanding of authentication protocols

Agenda

1. Secure Web Gateway
2. FortiProxy Deployment
3. High Availability
4. User Authentication
5. SSL Inspection and Web Filtering
6. Security Profiles
7. Content Analysis
8. Policy and Objects
9. Security Fabric Integration
10. Monitoring and Reporting

Objectives

After completing this course, you will be able to:

- Deploy the appropriate FortiProxy configuration for your network
- Use the GUI and CLI for administration
- Control user web and application access using proxy policies
- Authenticate users for web access
- Inspect SSL/TLS-secured traffic

- Collect and interpret log entries
- Deploy FortiProxy devices as an HA cluster for fault tolerance and scalability
- Configure security profiles to neutralize threats and misuse, including the following profiles:
 - Antivirus
 - Web filtering
 - Application control
 - Content inspection
 - Data leak prevention
- Diagnose and correct common problems

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 or
 - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled on your web browser

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

Product Versions

- FortiProxy 7.6.4
- FortiAnalyzer 7.6.2
- FortiGate 7.6.0
- FortiManager 7.6.4
- FortiAuthenticator 6.6.2
- Fortisolator 2.4.8

Course Duration

- Lecture time (estimated): 7 hours
- Lab time (estimated): 5 hours
- Total course duration (estimated): 12 hours
 - 2 full days or 4 half days

Formats

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

ISC2

- CPE training hours: 7
- CPE lab hours: 5
- CISSP domains: Security Operations

Part Number (SKU)

See Purchasing Process for more information

Certification

This course does not have a certification exam.