FortiProxy

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 IPS, antivirus, web filtering, application control, and logging.

Product Version

- FortiProxy 7.0.1
- FortiAnalyzer 7.0.2
- FortiGate 7.0.2
- FortiManager 7.0.2
- FortiIsolator 2.3.4
- FortiAuthenticator 6.4.1

Course Duration

- Lecture time (estimated): 8 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated): 12 hours/2 days

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.

Certification

There is no certification exam associated with this course.

Prerequisites

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

Agenda

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

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-FPX

Self-Paced Training

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

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- 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-FPX-LAB

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

(ISC)2

- CPE training hours: 8
- CPE lab hours: 4
- CISSP domains: Security Operations

Program Policies and FAQs

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