

# FortiGate Administrator

***In this course, you will learn how to use the most common FortiGate features.***

***In interactive labs, you will explore firewall policies, user authentication, high availability, SSL VPN, site-to-site IPsec VPN, Fortinet Security Fabric, and how to protect your network using security profiles, such as IPS, antivirus, web filtering, application control, and more. These administration fundamentals will provide you with a solid understanding of how to implement the most common FortiGate features.***

## Product Version

FortiOS 7.6.0

## Course Duration

- Lecture time (estimated): 12 hours
- Lab time (estimated): 10 hours
- Total course duration (estimated): 22 hours
  - 4 full days or 5 half days

## Who Should Attend

Networking and security professionals involved in the management, configuration, administration, and monitoring of FortiGate devices used to secure their organizations' networks should attend this course.

You should have a thorough understanding of all the topics covered in the *FortiGate Operator* course before attending the *FortiGate Administrator* course.

## Certification

This course is intended to help you prepare for the FCP - *FortiGate 7.6 Administrator* exam. This exam is part of the following certification tracks:

- Fortinet Certified Professional - Network Security
- Fortinet Certified Professional - Public Cloud Security
- Fortinet Certified Professional - Security Operations

## Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts

## Agenda

1. System and Network Settings
2. Firewall Policies and NAT
3. Routing
4. Firewall Authentication
5. Fortinet Single Sign-On (FSSO)
6. Certificate Operations
7. Antivirus
8. Web Filtering
9. Intrusion Prevention and Application Control
10. SSL VPN
11. IPsec VPN
12. SD-WAN Configuration and Monitoring
13. Security Fabric
14. High Availability
15. Diagnostics and Troubleshooting

## Objectives

After completing this course, you will be able to:

- Configure FortiGate basic networking from factory default settings
- Configure and control administrator access to FortiGate
- Use the GUI and CLI for administration
- Control network access to configured networks using firewall policies
- Apply port forwarding, source NAT, and destination NAT
- Analyze a FortiGate route table
- Configure static routing
- Route packets using static routes for multi-path and load-balanced deployments
- Authenticate users using LDAP and RADIUS
- Monitor firewall users from the FortiGate GUI
- Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD)
- Understand encryption functions and certificates
- Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
- Configure security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites

- Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate devices
- Configure SD-WAN and verify traffic distribution
- Identify the characteristics of the Fortinet Security Fabric
- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance
- Diagnose and correct common problems

## 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).

Contact your [Fortinet Resellers](#) or [Authorized Training Partners](#) to purchase this course.

### 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.

For training and lab SKUs, or additional purchasing information, refer to [Purchasing Process](#).

## ISC2

- CPE training hours: 12
- CPE lab hours: 10
- 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](#).

