

# FORTIGATE ADMINISTRATOR 7.6

## 4 DAYS

### Description

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.

### Target Audience

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.

### Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts

### Agenda

- System and Network Settings
- Firewall Policies and NAT

- Routing
- Firewall Authentication
- Fortinet Single Sign-On (FSSO)
- Certificate Operations
- Antivirus
- Web Filtering
- Intrusion Prevention and Application Control
- SSL VPN
- IPsec VPN
- SD-WAN Configuration and Monitoring
- Security Fabric
- High Availability
- 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
- Route packets using policy-based and static routes for multi-path and load-balanced deployments
- Configure static routing
- Route packets using static routes for multi-path and loadbalanced 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

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

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