FortiGate Security

In this three-day course, you will learn how to use basic FortiGate features, including security profiles.

In interactive labs, you will explore firewall policies, user authentication, SSL VPN, dial-up IPsec VPN, 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 basic network security.

Product Version

FortiOS 5.6.2

Formats

- Instructor-led classroom
- Instructor-led online
- Self-paced online

Agenda

1. Introduction to FortiGate and the Security Fabric
2. Firewall Policies
3. Network Address Translation (NAT)
4. Firewall Authentication
5. Logging and Monitoring
6. Certificate Operations
7. Web Filtering
8. Application Control
9. Antivirus
10. Intrusion Prevention and Denial of Service
11. SSL VPN
12. Dial-Up IPsec VPN
13. Data Leak Prevention (DLP)

Objectives

After completing this course, you should be able to:

- Deploy the appropriate operation mode for your network.
- Use the GUI and CLI for administration.
- Identify the characteristics of the Fortinet security fabric.
- Control network access to configured networks using firewall policies.
- Apply port forwarding, source NAT, and destination NAT.
- Authenticate users using firewall policies.
- 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.
- Fight hacking and denial of service (DoS).
- Defend against data leaks by identifying files with sensitive data, and block them from leaving your private network.
- Offer an SSL VPN for secure access to your private network.
- Implement a dial-up IPsec VPN tunnel between FortiGate and FortiClient.
- Collect and interpret log entries.

Who Should Attend

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

Participants should have a thorough understanding of all the topics covered in the *FortiGate Security* course before attending the *FortiGate Infrastructure* course.

Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts

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:
  - HTML5 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.

Certification

This course and the *FortiGate Infrastructure* course are intended to help participants prepare for the NSE 4 certification exam.