FortiGate Security

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

In interactive labs, you will explore firewall policies, the Fortinet Security Fabric, user authentication, SSL 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 7.0

Course Duration

- Lecture time (estimated): 10 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 17 hours / 3 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 Security* course before attending the *FortiGate Infrastructure* course.

Certification

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

Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts

Agenda

1. Introduction and Initial Configuration
2. Security Fabric
3. Firewall Policies
4. Network Address Translation (NAT)
5. Firewall Authentication
6. Logging and Monitoring
7. Certificate Operations
8. Web Filtering
9. Application Control
10. Antivirus
11. Intrusion Prevention and Denial of Service
12. SSL VPN

Objectives

After completing this course, you will 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)
- Offer an SSL VPN for secure access to your private network
- Collect and interpret log entries

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).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FGT-SEC

Self-Paced Training

Includes online training videos and resources through the NSE 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 NSE 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-FGT-SEC-LAB

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

(ISC)²

- CPE training hours: 10
- CPE lab hours: 7
- 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.