In this course, you will learn how to operate and administer some fundamental FortiGate features.

By the end of the course, you will acquire a solid understanding of how to deploy and maintain a basic network security solution. The course also covers how to enable users to remotely connect to your network in a secure way.

In interactive labs, you will learn how to use firewall policies, user authentication, routing, and SSL VPN, and how to protect your users using web filtering and application control.

Product Version
FortiOS 7.2

Course Duration
- Lecture time (estimated): 6 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated): 10 hours/2 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.

Certification
The lessons in this course are a subset of the lessons that are part of the FortiGate Security and FortiGate Infrastructure courses, which are intended to help you prepare for the NSE 4 certification exam.

If you are preparing for the NSE 4 certification, or want to learn about other FortiGate features, you should enroll in the FortiGate Security and FortiGate Infrastructure courses.
Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts

Agenda

1. Introduction and Initial Configuration
2. Firewall Policies
3. Routing
4. Firewall Authentication
5. SSL VPN
6. Web Filtering
7. Application Control

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
- Control network access to configured networks using firewall policies
- Analyze a FortiGate route
- Route packets using policy-based and static routes for multipath and load balanced deployments
- Authenticate users using firewall policies
- Offer an SSL VPN for secure access to your private network
- Configure web filtering to block inappropriate and risky websites
- Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports

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-ESS

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-FGT-ESS-LAB

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

(ISC)²

- CPE training hours: 6
- 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.