

FortiGate Infrastructure

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

Topics include features commonly applied in complex or larger enterprise or MSSP networks, such as advanced routing, redundant infrastructure, virtual domains (VDOMs), zero trust network access (ZTNA), SSL VPN, site-to-site IPsec VPN, single sign-on (SSO), and diagnostics.

Product Version

FortiOS 7.2

Course Duration

- Lecture time (estimated): 6 hours
- Lab time (estimated): 5 hours
- Total course duration (estimated): 11 hours/2 days

Who Should Attend

Networking and security professionals involved in the design, implementation, and administration of a network infrastructure using FortiGate devices should attend this course.

This course assumes knowledge of basic FortiGate fundamentals. 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 Security* course are intended to help you prepare for the NSE 4 certification exam.

Prerequisites

- Knowledge of OSI layers
- Knowledge of firewall concepts in an IPv4 network
- Knowledge of the fundamentals of FortiGate, as presented in the *FortiGate Security* course

Agenda

1. Routing
2. Virtual Domains
3. Fortinet Single Sign-On
4. ZTNA
5. SSL VPN
6. IPsec VPN
7. High Availability
8. Diagnostics

Objectives

After completing this course, you will be able to:

- Analyze a FortiGate route table
- Route packets using policy-based and static routes for multipath and load-balanced deployments
- Divide FortiGate into two or more virtual devices, each operating as an independent FortiGate, by configuring virtual domains (VDOMs)
- Understand the fundamentals and benefits of using ZTNA
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate devices
- Implement a meshed or partially redundant VPN
- Diagnose failed IKE exchanges
- Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD)
- 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).

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

FT-FGT-INF

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-INF-LAB

See [Purchasing Process](#) for more information about purchasing Fortinet training products.

(ISC)²

- CPE training hours: 6
- CPE lab hours: 5
- 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](#).

