



Enterprise Firewall

In this course, you will learn how to implement, troubleshoot, and centrally manage an enterprise security infrastructure composed of multiple FortiGate devices.

Product Version

- FortiGate 7.0.1
- FortiManager 7.0.1
- FortiAnalyzer 7.0.1

Course Duration

- Lecture time (estimated): 10 hours
- Lab time (estimated): 10 hours
- Total course duration (estimated): 20 hours / 3 days

Who Should Attend

Networking and security professionals involved in the design, administration, and support of an enterprise security infrastructure using FortiGate devices.

This course assumes advanced knowledge of networking, and extensive hands-on experience working with FortiGate, FortiManager, and FortiAnalyzer.

Certification

This course is intended to help you prepare for the NSE 7 Enterprise Firewall certification exam.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure

It is also recommended that you have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 5 FortiManager
- NSE 5 FortiAnalyzer

Agenda

1. Security Fabric
2. FortiOS Architecture
3. Traffic and Session Monitoring
4. Routing
5. FortiGuard
6. High Availability
7. Central Management
8. OSPF
9. Border Gateway Protocol (BGP)
10. Web Filtering
11. Intrusion Prevention System (IPS)
12. IPsec
13. Autodiscovery VPN (ADVPN)

Objectives

After completing this course, you will be able to:

- Integrate FortiManager, FortiAnalyzer, and multiple FortiGate devices using the Fortinet Security Fabric
- Centralize the management and monitoring of network security events
- Optimize FortiGate resources
- Diagnose and monitor user traffic using FortiGate debug tools
- Troubleshoot issues with conserve mode, high CPU, firewall policies, session helpers, IPsec, FortiGuard, content inspection, routing, and HA
- Harden the enterprise services
- Simultaneously deploy IPsec tunnels to multiple sites using the FortiManager VPN console
- Configure ADVPN to enable on-demand VPN tunnels between sites
- Combine OSPF and BGP to route the enterprise traffic

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-EFW

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-EFW-LAB

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

(ISC)2

- CPE training hours: 10
- CPE lab hours: 10
- 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](#).

