In this course, you will be assigned a series of do-it-yourself (DIY) configuration tasks in a virtual lab environment.

The configuration tasks cover some of the topics in the NSE 4 certification exam and include the use of the most common FortiGate features, such as firewall policies, the Fortinet Security Fabric, user authentication, SSL and IPsec VPNs, equal-cost multi-path (ECMP) routing, IPS, high availability (HA), and content inspection.

This course is not a replacement for the FortiGate Security and FortiGate Infrastructure courses.

Product Version
FortiOS 7.2

Course Duration
- Lab time (estimated): 7 hours
- Total course duration (estimated): 7 hours/1 day

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.

The NSE 4 Immersion course is intended for students who have some experience operating FortiGate devices and want to refresh their skills. This course is ideal for students who have already taken the NSE 4 FortiGate Security and FortiGate Infrastructure courses, or have equivalent working experience, and want to get more hands-on lab practice before taking the NSE 4 certification exam.

Certification
The NSE 4 Immersion course helps students to reinforce the knowledge they learned during the FortiGate Security and FortiGate Infrastructure courses.

The labs in this course cover a subset of the topics that are part of the NSE 4 certification. If you are preparing for the NSE 4 certification, or want to learn about other FortiGate features, Fortinet recommends that you enroll in the FortiGate Security and FortiGate Infrastructure courses first, before enrolling in the NSE4 Immersion course.
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

Agenda

1. Firewall Policy, DNAT, and Authentication
2. SSL and Content Inspection
3. IPS
4. SSL VPN and IPsec VPN
5. ECMP Routing
6. Security Fabric
7. HA

Objectives

After completing this course, you will be able to:

- Use the GUI and CLI for administration
- Control access to network resources using firewall policies
- Authenticate users using firewall policies
- Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
- Apply web filter and application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports
- Protect your network against known attacks using IPS signatures
- Mitigate and block DoS attacks
- Configure SSL VPN and IPsec VPN for remote access
- Route packets using ECMP routing
- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance
- Configure the Fortinet Security Fabric

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-NSE4-IMM

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-NSE4-IMM-LAB

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

(ISC)²

- CPE training hours: 0
- 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.