FortiGate Immersion

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 Fortinet NSE 4 - FortiOS 7.2 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 *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure* courses.

Product Version

FortiOS 7.2

Course Duration

- Lab time (estimated): 7 hours
- Total course duration (estimated): 7 hours
  - 1 full day or 2 half 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.

This course is ideal for students who have already taken the *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure* courses, or have equivalent working experience, and want to get more hands-on lab practice before taking the *Fortinet NSE 4 - FortiOS 7.2* certification exam.

Certification

The *FortiGate Immersion* course helps you to reinforce the knowledge you learned during the *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure* courses, and covers a subset of the topics that are part of the *Fortinet - NSE 4 FortiOS 7.2* certification exam. That exam is part of the following certification tracks:

- Fortinet Certified Professional - Network Security
- Fortinet Certified Professional - Public Cloud Security
- Fortinet Certified Professional - Security Operations

Prerequisites

You must have an understanding of the topics covered in *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure* (or have equivalent experience).

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.