

Updated on 04/11/2025

Register

Fortinet NSE8 Training

3 days (21 hours)

Overview

Fortinet Network Security Expert - NSE8 is the highest and most prestigious level of Fortinet's technical certification ladder. Fortinet NSE 8 is designed to teach best practices for using Fortinet devices and advanced solutions in the network security and cybersecurity industry.

In today's information technology market, Fortinet NSE8 certification is an invaluable asset in the job market. [Increasingly sophisticated](#) IT threats are forcing companies to equip themselves with security tools that are complex to maintain, deploy, and administer.

Our 3-day Fortinet NSE 8 training course will teach you how to keep your business secure. You will learn how to protect data across the entire infrastructure in network, application, multi-cloud, and edge environments. You will learn how to configure FortiGate's advanced features in complex scenarios.

In addition, you will gain a better understanding of the level and topology of the exercises featured in the NSE8 exam. You will also expand your security skills and gain real-world experience in network security.

Our NSE 8 training will be based on the latest version of the tool, [FortiWeb 7.6](#).

Objectives

- Comprehensive and in-depth understanding of all Fortinet devices (implementation, operation, advanced features, and troubleshooting)
- Design, configure, and troubleshoot complex networks and IT security scenarios with advanced Fortinet products.
- Configure and operate advanced Fortinet products and solutions such as FortiSandbox, FortiAuthenticator, FortiADC, FortiWeb, and FortiMail.

Target audience

- Network security and cybersecurity professionals
- Anyone interested in Fortinet

Prerequisites

- Completion of our [NSE6 training](#)
- Knowledge of OSI layers and HTTP protocol
- Basic proficiency in HTML and JavaScript, as well as a server-side dynamic page language (e.g., PHP)
- Basic proficiency in FortiGate port forwarding

Fortinet NSE 8 Training Program

Fortinet NSE8 security architectures

- Fortinet cloud security solutions
- FortiGate VM Models and Licenses
- FortiGate VM deployments
- Fortinet on private/public clouds
- Advanced High Availability Features of Fortinet Solutions
- Fortinet solution operating and deployment modes
- FortiGate Cluster Protocol
- FortiGate Session Life Support Protocol
- Session-based load balancing clustering
- Secure access networks
- Web application security
- Advanced Threat Protection
- FortiGate 7000 Series

Networking

- Advanced/static/dynamic routing
- CLI in Fortinet solutions
- IPv4, IPv6 Addressing and Routing
- Secure SD-WAN
- Advanced/central NAT, NAT64, NAT46
- DNS64
- VPN technologies
- Advanced IPsec
- Advanced SSL
- Network troubleshooting
- Routing and VPN troubleshooting

Hardware Acceleration

- Hardware acceleration overview
- Content processors
- Security processors
- Network processors
- Traffic in Fortinet Products
- Traffic offloading
- Packet lifetime
- Fortinet communication ports and protocols

Content control

- Inspection modes (SSL/SSH, Certificate)
- FortiOS security profiles
- Antivirus
- Intrusion prevention systems (IPS)
- Application control
- Web filtering
- DNS Filtering
- VoIP inspection
- FortiGuard Services
- Cloud Security

Authentication

- Advanced Single Sign-On
- RADIUS
- Two-factor authentication
- 802.1x
- Certificate authentication
- Troubleshooting

Security operations

- Fortinet Solutions API
- Rest API
- Security Event Processing with Fortinet Solutions
- FortiSIEM
- FortiAnalyzer
- Log analysis
- Event management
- Fortinet centralized management solutions
- FortiManager
- FortiCloud

Integrated Solutions

- Integrate Fortinet solutions for advanced threat protection
- FortiLink
- Fortinet Wireless Solutions
- Fortinet Authentication Solutions
- Fortinet Hybrid Solutions (Traditional and Cloud Networking)

Enhanced technologies

- FortiWeb for securing web applications
- Integrate a FortiSandbox cloud tool
- FortiAuthenticator configuration
- Protection against DDoS attacks
- FortiMail email security platform
- FortiADC for traffic load balancing

To go further

Fortimanager training (EDU-NSE5)

Fortimail training (EDU-NSE6)

FortiWeb Training (NSE6)

Fortigate Infrastructure Security Training (EDU-NSE4)

Fortigate III Training (EDU-NSE7)

Fortianalyzer Training (EDU-NSE5)

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Placement at the start of training

The placement test at the start of the training course complies with Qualiopi quality criteria. Upon

final registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and discussion sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.