AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 11/10/2024

Sign up

Fortinet NSE8 Training

3 days (21 hours)

Presentation

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

In today's IT market, Fortinet NSE8 certification is an invaluable asset. As IT threats become increasingly sophisticated, companies are obliged 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'll learn how to protect data across the entire infrastructure in network, application, multicloud or device environments. You'll learn how to configure FortiGate's advanced features to deal with complex scenarios.

What's more, you'll gain a better understanding of the level and topology of the exercises present in the NSE8 exam. You'll also expand your security skills and gain real experience in network security.

Our NSE 8 training course will be based on the latest version of the tool, FortiWeb 7.6.

Objectives

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

Target audience

- Network security and cybersecurity professionals
- To all those interested in Fortinet

Prerequisites

- Have taken our NSE6 training course
- Knowledge of OSI layers and HTTP protocol
- Basic knowledge of HTML and JavaScript, as well as a dynamic server-side page language (e.g. PHP)
- Basic mastery of 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
- How Fortinet solutions work and how they are deployed
- FortiGate Cluster Protocol
- Protocol FortiGate Session Life Support
- Session-based load balancing clustering
- Secure access networks
- Web application security
- Protection against advanced threats
- FortiGate 7000 Series

Networking

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

Hardware acceleration

- Hardware acceleration overview
- Content processors
- Security processors
- Network processors
- Traffic in Fortinet products
- Unloading traffic
- Package 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

Safety 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 network and cloud)

Enhanced technologies

- FortiWeb for securing web applications
- Integrating a FortiSandbox cloud tool
- Configuring FortiAutenticator
- Protection against DDoS attacks
- FortiMail secure messaging platform
- FortiADC to balance traffic loads

Further information

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)

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning on entry to training complies with Qualiopi quality criteria. As soon as

On final registration, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

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

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.