

Updated on 04/02/2026

Sign up

# Fortinet Network Security Support Engineer Training

3 days (21 hours)

## Overview

In this course, you will learn how to diagnose and resolve the most common network and security issues within a Fortinet-protected security solution.

Through hands-on troubleshooting workshops, you will use tools, diagnostics, and debug commands to detect, isolate, and resolve issues related to the most commonly used FortiGate features, such as IPsec, routing, web filtering, high availability (HA), intrusion prevention (IPS), and more. These skills and knowledge will enable you to master the support of a network security solution based on FortiGate devices.

## Objectives

- Set up a basic configuration on the FortiGate and analyze the initial steps of troubleshooting.
- Monitor process activity, diagnose retention mode, and resolve unexpected reboots and device freezes
- Analyze session table information and the output of the debug flow command.
- Resolve issues related to session helpers.
- Resolve common issues with local authentication, LDAP, RADIUS, and SAML.
- Resolve common FSSO issues.
- Troubleshoot FortiGuard and web filtering issues.
- Monitor an HA cluster and troubleshoot common HA issues.
- Diagnose and resolve IPsec VPN issues using debug and traffic analysis commands.
- Troubleshoot routing issues using debug commands.
- Monitor OSPF status and troubleshoot common OSPF issues using debug commands.\*
- Monitor and verify BGP status using commands and troubleshoot common BGP issues.

## Target Audience

- This course is intended for network and security professionals responsible for diagnosing, troubleshooting, and supporting an enterprise security infrastructure using FortiGate devices.

## Prerequisites

- You must have a solid understanding of the topics covered in the following course, or have equivalent experience:
  - FCP – FortiOS Administrator
- It is also recommended that you have a good understanding of the topics covered in the following course, or have equivalent experience:
  - FCSS – Enterprise Firewall

## Fortinet Network Security Support Engineer Training Program

### NSE-7 Preparation

1. Troubleshooting Concepts2. System Resources3. Sessions, Traffic Flow, and Networking4. Security Fabric5. Firewall Authentication6. FSSO7. Security Profiles8. High Availability9. IPsec10. IPsec/IKEv211. Routing12. BGP13. OSPF

FortiManager Training (EDU-NSE5)

FortiMail Training (EDU-NSE6)

FortiWeb Training (NSE6)

## Target Audience

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

## Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also enables us to anticipate certain connection issues or

internal security issues within the company (intra-company or virtual classroom) that could pose challenges for the monitoring and smooth running of the training session.

## Teaching Methods

Practical Course: 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 reflection sessions, and group work.

## Assessment

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

## Certification

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