

Enterprise Firewall

Duration: 3 Days**Product Version: FortiGate 6.4**

Description

The Enterprise Firewall course combines instructor-led training and interactive labs to build a working knowledge of how to isolate and fix the most common issues in networks with FortiGate.

Topics that are covered include resolving FortiGate misconfigurations, monitoring traffic passing through FortiGate, optimising FortiGate memory usage, FortiGate diagnostic tools, troubleshooting FortiGate issues, scaling out FortiGate deployments, configuring BGP, OSPF, and Autodiscovery VPN (ADVPN).

Target Audience

The Enterprise Firewall course is intended for networking and security professionals who are involved in the administration and support of a security infrastructure using FortiGate appliances. This includes network managers, administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals.

Anyone planning to taking Enterprise Firewall course is strongly recommended to complete the Fortigate Security, Fortigate Infrastructure and FortiManager courses before this course

Prerequisite Requirements

- Advanced knowledge of all topics presented in the Fortigate Security and Infrastructure courses
- Knowledge of network protocols
- Knowledge of network security concepts

Certification

The Enterprise Firewall course is the recommended training to prepare for the NSE 7 certification exam to achieve **Network Security Expert** status.

Course Outline

Day 1

- Security Fabric
- FortiOS Architecture
- Traffic and Session Monitoring
- Routing

Day 2

- FortiGuard
- High Availability
- Central Management
- OSPF
- BGP
- Web Filtering

Day 3

- Intrusion Prevention System
- IPSec
- Autodiscovery VPN (ADVPN)

+ Course details are subject to change