

# Course Outline

## Fortinet NSE 4 Bundle Course F-NSE4B: 5 days Instructor Led

*All Fortinet courses are delivered by a Fortinet Authorized Learning Partner*

### About this course

The Fortinet NSE 4 Bundle class is a 5-day program including basic configuration and administration of the most commonly used features of FortiGate appliances and a selection of advanced FortiGate networking and security features. The NSE 4 exam topics are based on the content of these recommended instructor led training courses:

FortiGate I  
FortiGate II

In interactive labs, you will explore firewall policies, user authentication, basic VPNs, explicit proxy, virus detection, web filtering, application control and more. These administrative fundamentals will provide you with a solid understanding of how to integrate and maintain basic network security. In the last three days you will review topics including features commonly used in complex or larger enterprise/MSSP networks, such as advanced routing, transparent mode, redundant infrastructure, security-as-a-service (SaaS), advanced IPsec VPN, IPS, SSO, certificates, data leak prevention, diagnostics, and fine-tuning performance.

### At course completion

After completing this course, students will be able to:

- Describe capabilities of FortiGate UTM
- Neutralize threats / misuse: viruses, phishing, spam, torrents, and inappropriate web sites
- Control network access based on device type
- Authenticate users via firewall policies
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate appliances
- Compare policy- vs. tunnel-based IPsec VPN
- Apply port forwarding, source NAT, and destination NAT
- Interpret log entries
- Generate reports
- Use the web UI and CLI for administration
- Deploy the right operation mode
- Simplify protocol handling with application control
- Deploy FortiGate devices as an HA cluster for fault-tolerance & high performance
- Inspect traffic transparently, forwarding as a Layer 2 device
- Manage FortiGate device's route table
- Route packets using policy-based and static routes for multi-path and load-balance deployments
- Connect virtual domains (VDOMs) without packets leaving FortiGate
- Implement a meshed / partially redundant VPN
- Diagnose failed IKE exchanges
- Fight hacking & denial of service (DoS)
- Diagnose IPS engine performance issues
- Offer Fortinet Single Sign On (FSSO) access to network services, integrated with Microsoft Active Directory
- Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
- Understand encryption functions and certificates

## Course Outline

- Defend against data leaks by identifying files with sensitive data, and blocking them from leaving your private network
- Diagnose and correct common problems
- Optimize performance by configuring to leverage ASIC acceleration chips, such as CP or NPs, instead of only the CPU resources
- Implement IPv6 and hybrid IPv4-IPv6 networks

### Course Outline

Module 1 Introduction to Fortinet UTM

Module 2 Logging and Monitoring

Module 3 Firewall Policies

Module 4 Firewall Authentication

Module 5 SSL VPN

Module 6 Basic IPsec VPN

Module 7 Antivirus

Module 8 Explicit Proxy

Module 9 Web Filtering

Module 10 Application Control

Module 11 Routing

Module 12 Virtual Networking

Module 13 Transparent Mode

Module 14 High Availability

Module 15 Advanced IPsec VPN

Module 16 IPS

Module 17 FSSO

Module 18 Certificate Operations

Module 19 DLP

Module 20 Diagnostics

Module 21 Hardware Acceleration

Module 22 IPv6