BOOST
THE LEADING TRAINING PROVIDER

Information Technology

FortiGate Security and FortiGate Infrastructure

Course Introduction

This training course is designed to provide participants with the basic functions of the FortiGate Firewall, including security profiles. These administration fundamentals will provide participants with a solid understanding of how to implement basic network security.

This course will discuss topics such as firewall policies, the Fortinet Security Fabric, user authentication, SSL VPN, and how to protect your network using security profiles, such as IPS, antivirus, web filtering, application control, and more. how to use the basic functions of the FortiGate Firewall, including security profiles. Participants will also review the operation of firewall policies, Security Fabric, user authentication, SSL VPN, and how to protect a network using security profiles such as IPS, antivirus, web filtering, application control, and more.

The training course is designed to be interactive and participatory, and includes various learning tools to enable the participants to operate effectively and efficiently in a multifunctional environment. The course will use lectures and presentations, exercises, experiential and exposure to real world problems and policy choices confronting delegates

Target Audience

- Cloud Computing Engineer
- Computer Network Specialist
- Computer Support Specialist
- Database Administrator
- Information Technology Analyst
- Information Technology Leadership
- Information Security Specialist
- Software/Application Developer
- Web Developer
- Technology sales consultant

Learning Objectives

Effectively deploy the appropriate operation mode for your network
• Utilize the GUI and CLI for administration
• Discuss the characteristics of the Fortinet Security Fabric
• Control network access to configured networks using firewall policies
• Apply port forwarding, source NAT, and destination NAT
• Authenticate users using firewall policies
• Understand encryption functions and certificates
• Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
• Configure security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites
• Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports
• Fight hacking and denial of service (DoS)
• Offer an SSL VPN for secure access to your private network
• Collect and interpret log entries.

Course Outline

- **Day 01**

  NSE 4 FortiGate Security

  - Module 1: Introduction and Initial Configuration
  - Module 2: Security Fabric
  - Module 3: Firewall Policies
  - Module 4: Network Address Translation (NAT)
  - Module 5: Firewall Authentication
  - Module 6: Logging and Monitoring

- **Day 02**

  Module 7: Certificate Operations

  - Module 8: Web Filtering

- Module 9: Application Control
- Module 10: Antivirus
- Module 11: Intrusion Prevention and Denial of Service
- Module 12: SSL VPN

• **Day 03**

NSE 4 FortiGate Infrastructure

- Module 1: NSE4 FortiGate Infrastructure Course Introduction
- Module 2: FortiGate Routing
- Module 3: Software-Defined WAN
- Module 4: Virtual Domains (VDOMs)
- Module 5: Layer 2 Switching

• **Day 04**

Module 6: IPSEC VPN

- Module 7: Fortinet Single Sign-On (FSSO
- Module 8: High Availability (HA)
- Module 9: Web Proxy
- Module 10: Diagnostics
- Module 11: NSE 4 FortiGate Infrastructure Labs

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
Dec. 8, 2025	Dec. 12, 2025	5 days	4250.00 $	UAE - Dubai