FCP FortiGate Administrator

Duration: 4 Days **Course Code: ENFCPFGAD** **Delivery Method: Virtual Learning**

Overview:

English - Please note this course is only available in English.
Nederlands - Let op: deze training is alleen in het Engels beschikbaar.
Franais - Veuillez noter que ce cours est uniquement disponible en anglais. In this course, you will learn how to use the most common FortiGate features. In interactive labs, you will explore firewall policies, user authentication, high availability, SSL VPN, site-to-site IPsec VPN, Fortinet Security Fabric, and how to protect your network using security profiles, such as IPS, antivirus, web filtering, application control, and more. These administration fundamentals will provide you with a solid understanding of how to implement the most common FortiGate features.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Objectives:

- **After completing this course, you will be able to:**
- · Configure FortiGate basic networking from factory default settings
- · Configure and control administrator access to FortiGate
- · Use the GUI and CLI for administration
- · Control network access to configured networks using firewall policies
- · Apply port forwarding, source NAT, and destination NAT
- · Analyze a FortiGate route table
- · Route packets using policy-based and static routes for multi-path and load-balanced deployments
- · Authenticate users using firewall policies
- · Monitor firewall users from the FortiGate GUI
- · Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD)
- · 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
- · Offer an SSL VPN for secure access to your private network
- · Establish an IPsec VPN tunnel between two FortiGate devices
- · Configure static routing
- · Configure SD-WAN underlay, overlay, and local breakout
- · Identify the characteristics of the Fortinet Security Fabric
- · Deploy FortiGate devices as an HA cluster for fault tolerance and high performance
- · Diagnose and correct common problems

Testing and Certification

- · Fortinet Certified Professional - Network Security
- · Fortinet Certified Professional - Public Cloud Security

- Fortinet Certified Professional - Security Operations

Content:

Agenda:

1. System and Network Settings
2. Firewall Policies and NAT
3. Routing
4. Firewall Authentication
5. Fortinet Single Sign-On (FSSO)
6. Certificate Operations
7. Antivirus
8. Web Filtering
9. Intrusion Prevention and Application Control
10. SSL VPN
11. IPsec VPN
12. SD-WAN Configuration and Monitoring
13. Security Fabric
14. High Availability
15. Diagnostics and Troubleshooting

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/