FortiGate Infrastructure

Course Description

In this course, you will learn how to use the most common FortiGate networking and infrastructure features. Topics include features commonly applied in complex or larger enterprise or MSSP networks, such as advanced routing, redundant infrastructure, virtual domains (VDOMs), zero trust network access (ZTNA), SSL VPN, site-to-site IPsec VPN, single sign-on (SSO), and diagnostics.

Product Version:

- FortiOS 7.2

Course Duration:

2 days

Who should attend?.

Networking and security professionals involved in the design, implementation, and administration of a network infrastructure using FortiGate devices should attend this course. This course assumes knowledge of basic FortiGate fundamentals. You should have a thorough understanding of all the topics covered in the FortiGate Security course before attending the FortiGate Infrastructure course.

Certification:

This course, along with FortiGate Security, is intended to help you prepare for the FortiGate NSE 4 - FortiOS 7.2 exam. This exam is part of the following certification tracks:

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

Prerequisites:

- Knowledge of OSI layers
- Knowledge of firewall concepts in an IPv4 network
- Knowledge of the fundamentals of FortiGate, as presented in the FortiGate Security course

Outlines:

1. Routing
2. Virtual Domains
3. Fortinet Single Sign-On
4. ZTNA
5. SSL VPN
6. IPsec VPN
7. High Availability
8. Diagnostics

Objectives:

After completing this course, you will be able to:

- Analyze a FortiGate route table
- Route packets using policy-based and static routes for multipath and load-balanced deployments
- Divide FortiGate into two or more virtual devices, each operating as an independent FortiGate, by configuring virtual domains (VDOMs)
- Understand the fundamentals and benefits of using ZTNA
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate devices
- Implement a meshed or partially redundant VPN
- Diagnose failed IKE exchanges
- Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD)
- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance
- Diagnose and correct common problems