FortiGate® Infrastructure

Duration: 2 Days
Method: Instructor-Led Training (ILT) | Live Online Training

Certification: *Fortinet Certified Professional (FCP)* — **Exam:** *Fortinet NSE 4 - FortiOS 7.2*

Course Description

In this course, participants 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.

NOTE: *This course is the second part of a two-course series that covers the skills needed to prepare for the certification exam:*

- *FortiGate Security*
- *FortiGate Infrastructure (This course)*

Target Audience

This course is intended for:

- Networking and security professionals involved in the design, implementation, and administration of a network infrastructure using FortiGate appliances.

Prerequisites

To attend this course, candidates must have:

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

Certification

This course is intended to help participants prepare for the course exam. This exam is part of the following *FCP* certification tracks:

- *Network Security*
- *Public Cloud Security*
- *Security Operations.*

Tel: 876-978-1107 / 876-978-1486
WhatsApp: 876-978-9353
E-Mail: training@RWTTS.com | **Website:** www.RWTTS.com

Microsoft Partner

Accredited Training Center
EC-Council

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Analyse 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.

Course Topics

Module 1: Routing

Module 2: Virtual Domains

Module 3: Fortinet Single Sign-On

Module 4: ZTNA

Module 5: SSL VPN

Module 6: IPsec VPN

Module 7: High Availability

Module 8: Diagnostics

LABS INCLUDED