



**REAL WORLD**  
TECHNOLOGY TRAINING & SOLUTIONS  
"Training You Can Really Use"

# FortiGate® Administrator

**Duration: 4 Days**

**Method: Instructor-Led Training (ILT) | Live Online Training**

---

**Certification:** Fortinet Certified Professional (FCP) — **Exam:**  
FCP - FortiGate 7.4 Administrator

---

## Course Description

In this course, participants will learn how to use the most common FortiGate features. In interactive labs, participants 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 participants with a solid understanding of how to implement the most common FortiGate features.

## Target Audience

This course is intended for:

- Networking and security professionals involved in the management, configuration, administration, and monitoring of FortiGate devices used to secure their organizations' networks.

## Prerequisites

To attend this course, candidates must have:

- Knowledge of network protocols.
- Basic understanding of firewall concepts.
- Completed the *FortiGate Operator* course, attained the *Fortinet Certified Associate Cybersecurity* certification or have equivalent knowledge.

## 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*.



**Microsoft** Partner

**Tel:** 876-978-1107 / 876-978-1486

**WhatsApp:** 876-978-9353

**E-Mail:** [training@RWTTTS.com](mailto:training@RWTTTS.com) | **Website:** [www.RWTTTS.com](http://www.RWTTTS.com)





**REAL WORLD**  
TECHNOLOGY TRAINING & SOLUTIONS  
*"Training You Can Really Use"*

## Course Objectives

Upon successful completion of this course, attendees 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.
- Analyse 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.



**Microsoft** Partner

**Tel:** 876-978-1107 / 876-978-1486

**WhatsApp:** 876-978-9353

**E-Mail:** [training@RWTTTS.com](mailto:training@RWTTTS.com) | **Website:** [www.RWTTTS.com](http://www.RWTTTS.com)





**REAL WORLD**  
TECHNOLOGY TRAINING & SOLUTIONS  
*"Training You Can Really Use"*

## Course Topics

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

## LABS INCLUDED



**Microsoft** Partner

**Tel:** 876-978-1107 / 876-978-1486

**WhatsApp:** 876-978-9353

**E-Mail:** [training@RWTTTS.com](mailto:training@RWTTTS.com) | **Website:** [www.RWTTTS.com](http://www.RWTTTS.com)

