



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

# FortiGate® Security

**Duration: 3 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 features, including security profiles. In interactive labs, participants will also explore firewall policies, the Fortinet Security Fabric, user authentication, 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 basic network security.

## 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.

## 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:

- Deploy the appropriate operation mode for their network.
- Use the GUI and CLI for administration.
- 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).
- Collect and interpret log entries.
- Identify the characteristics of the Fortinet Security Fabric.

## Course Topics

Module 1: Introduction and Initial Configuration

Module 2: Firewall Policies

Module 3: Network Address Translation (NAT)

Module 4: Firewall Authentication

Module 5: Logging and Monitoring

Module 6: Certificate Operations

Module 7: Web Filtering

Module 8: Application Control

Module 9: Antivirus

Module 10: Intrusion Prevention and Denial of Service

Module 11: Security Fabric

## 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)

