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

FortiGate® Security & Infrastructure

Duration: 5 Days

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

Certification: *Fortinet® NSE 4 Network Security Professional —*
Exam*: Fortinet NSE (Network Security Engineer) 4 FortiOS® 6.2*

Course Description

This course is a two part course series that covers the skills needed to prepare for the certification exam:

Part 1: FortiGate® Security

In this course, participants will learn how to use basic FortiGate features, including security profiles. In interactive labs, participants will explore firewall policies, security fabric, user authentication, SSL VPN, 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.

Part 2: FortiGate® Infrastructure

In this course, participants will learn how to use advanced FortiGate networking and security. They will cover topics such as the features commonly applied in a complex or larger enterprise or MSSP networks. These features are: advanced routing, transparent mode, redundant infrastructure, site-to-site ipsec VPN, Single Sign-On (SSO), web proxy, and diagnostics.

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.

AND

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

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

Prerequisites

To attend this course, candidates must have:

- Knowledge of network protocols
- Basic understanding of firewall concepts
- Knowledge of OSI layers.
- Firewall concepts in an IPv4 network.

Exam Details

Exam Code:	• NSE4_FGT-6.4
Length of Exam:	• 2 Hours
Number of Questions:	• 70
Passing Score:	• 60%
Question Format:	• Multiple Choice

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.
- Identify the characteristics of the Fortinet Security Fabric.
- 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).
- Offer an SSL VPN for secure access to your private network.

Course Objectives *Continued*

- Implement a dialup IPsec VPN tunnel between FortiGate and FortiClient®.
- Collect and interpret log entries
- Analyse a FortiGate's route table.
- Route packets using policy-based and static routes for multi-path and load-balanced deployments.
- Configure SD-WAN to load balance traffic between multiple WAN links effectively.
- Inspect traffic transparently, forwarding as a Layer 2 device.
- Divide FortiGate into two or more virtual devices, each operating as an independent
- FortiGate, by configuring virtual domains (VDOMs).
- Establish an IPsec VPN tunnel between two FortiGate appliances.
- Compare policy-based to route-based IPsec VPN.
- 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®.
- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance.
- Deploy implicit and explicit proxy with firewall policies, authentication, and caching.
- Diagnose and correct common problems.

Course Topics

Introduction and Initial Configuration

Security Fabric

Firewall Policies

Network Address Translation (NAT)

Firewall Authentication

Logging and Monitoring

Certificate Operations

Web Filtering

Application Control

Course Topics *Continued*

Antivirus

Intrusion Prevention and Denial of Service

SSL VPN

Dialup IPsec VPN

Routing

Software-Defined WAN (SD-WAN)

Layer 2 Switching

Virtual Domains

Site-to-Site IPsec VPN

Fortinet Single Sign-On (FSSO)

High Availability (HA)

Web Proxy

Diagnostics

LABS INCLUDED