FT-FGT-SEC

FortiGate Security

Overview

In this three-day course, you will learn how to use basic FortiGate features, including security profiles. In interactive labs, you will explore firewall policies, the Fortinet 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 you with a solid understanding of how to implement basic network security.

Who Should Attend

Networking and security professionals involved in the management, configuration, administration, and monitoring of FortiGate devices used to secure their organizations' networks should attend this course. You should have a thorough understanding of all the topics covered in the FortiGate Security course before attending the FortiGate Infrastructure course.

Prerequisites

- Knowledge of network protocols
- Basic understanding of firewall concepts

Objectives

After completing this course, you should be able to:

- Deploy the appropriate operation mode for your 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

Agenda

- Introduction and Initial Configuration
- Security Fabric
- Firewall Policies
- Network Address Translation (NAT)

- Firewall Authentication
- Logging and Monitoring
- Certificate Operations
- Web Filtering
- Application Control
- Antivirus
- Intrusion Prevention and Denial of Service
- SSL VPN

Certification

This course and the FortiGate Infrastructure course are intended to help you prepare for the NSE 4 certification exam.