Training Course

FortiGate Security

Duration: 3 Days **Product Version:** FortiGate 6.4

Description

The FortiGate Security course combines instructor-led training and interactive labs to build a working knowledge of basic configuration and administration of FortiGate appliances' most commonly used features.

Administrative fundamentals such as the Fortinet Security Fabric, firewall policies, NAT, user authentication, logging, certificates, SSL inspection, SSL VPNs, and FortiGate's security profiles will provide a solid understanding of how to integrate and maintain basic network security using FortiGate appliances.

Target Audience

The FortiGate Security course is intended for anyone who is responsible for the day-to-day management of the security of a FortiGate appliance. This includes network managers, administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals.

Anyone planning on taking the FortiGate Infrastructure course is strongly recommended to complete the FortiGate Security course first.

Prerequisite Requirements

- TCP/IP network experience
- Basic understanding of firewall concepts

Certification

The FortiGate Security course combined with the FortiGate Infrastructure course is highly recommended to prepare for the NSE 4 exam to achieve Network Security Expert status.

Course Outline

Day 1

- Introduction to FortiGate
- Security Fabric
- Firewall Policies
- Network Access Translation

Day 2

- Logging and Monitoring
- Certificate Operations
- Web Filtering
- Firewall Authentication

Day 3

- Antivirus
- Intrusion Prevention and Denial of Service
- SSL-VPN
- Application Control

+ Course details are subject to change