Enterprise Firewall

In this three-day class, students will learn how to implement, troubleshoot, and centrally manage an enterprise security infrastructure composed of multiple FortiGate devices.

Product Version

FortiGate 5.4.1

Formats

- Instructor-led classroom
- Instructor-led online*****
- Self-paced videos with instructor-led lab over the web

* Private class only. Please contact your Fortinet sales representative.

Agenda

1   Enterprise Firewall
2   FortiOS Architecture
3   System Troubleshooting
4   Traffic and Session Monitoring
5   Routing
6   FortiGuard
7   Central Management
8   OSPF
9   Web Filtering
10 IPS
11 BGP
12 IPsec
13 ADVPN

Objectives

After completing this course, you will be able to:
- Integrate FortiManager, FortiAnalyzer, and multiple FortiGate devices using Fortinet's security fabric
- Centralize the management and monitoring of network security events
- Optimize FortiGate resources
- Diagnose and monitor user traffic using FortiGate debug tools
- Troubleshoot issues with conserve mode, high CPU, firewall policies, session helpers, IPsec, FortiGuard, content inspection, routing, and HA
- Harden the enterprise services
- Simultaneously deploy IPsec tunnels to multiple sites using the FortiManager VPN console
- Configure ADVPN to enable on-demand VPN tunnels between sites
- Combine OSPF and BGP to route the enterprise traffic

Who Should Attend

Networking and security professionals involved in the design, administration, and support of an enterprise security infrastructure using FortiGate devices.

This course assumes advanced knowledge of networking, and extensive hand-on experience working with FortiGate, FortiManager, and FortiAnalyzer.

Prerequisites

- Knowledge of network protocols
- Knowledge of network security concepts
- FortiGate I and FortiGate II

- FortiAnalyzer
- FortiManager

System Requirements

If you take an online format of this class, you must have a computer that has:

- High-speed Internet connection
- Up-to-date web browser
- PDF viewer
- Speakers or headphones
- SSH client (such as PuTTY) is recommended
- RDP client is recommended

Wired Ethernet connection (*not* Wi-Fi) recommended. *Firewalls, including Windows Firewall or FortiClient, must allow connections with the online labs.*

Certification

This course prepares you for the NSE 7 Enterprise Firewall certification exam.