NSE 4 FortiGate Training

Duration: 5 days

The NSE 4 training bundle covers **FortiGate Security** and **FortiGate Infrastructure**. In this five-day course, you will learn:

FortiGate Security (3 days)

• How to use basic FortiGate features, including security profiles. In interactive labs, you will explore firewall policies, security fabric, user authentication, SSL VPN, dial-up IPsec 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.

FortiGate Infrastructure (2 days)

• How to use advanced FortiGate networking and security. Topics include features commonly applied in complex or larger enterprise or MSSP networks, such as advanced routing, transparent mode, redundant infrastructure, site-to-site IPsec VPN, single sign-on (SSO), web proxy, and diagnostics.

This course is intended to help you prepare for the NSE 4 certification exam.

Product Versions

• FortiOS 6.0
• FortiOS 6.2 (soon)

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

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
• Implement a dialup IPsec VPN tunnel between FortiGate and FortiClient
• Collect and interpret log entries

• Analyze a FortiGate route table
• Route packets using policy-based and static routes for multipath 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 devices
• 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 (AD)
• 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

Target Audience

Networking and security professionals involved in the management, configuration, design, implementation, administration, and monitoring of FortiGate devices used to secure their organizations' networks should attend this course.

Participants should have a thorough understanding of all the topics covered in the FortiGate Security course before attending the FortiGate Infrastructure course.

Outline

FortiGate Security

1. Introduction and Initial Configuration
2. Security Fabric
3. Firewall Policies
4. Network Address Translation (NAT)
5. Firewall Authentication
6. Logging and Monitoring
7. Certificate Operations
8. Web Filtering
9. Application Control
10. Antivirus
11. Intrusion Prevention & Denial of Service
12. SSL VPN
13. Dialup IPsec VPN

FortiGate Infrastructure

1. Routing
2. Software-Defined WAN (SD-WAN)
3. Virtual Domains
4. Layer 2 Switching
5. Site-to-Site IPsec VPN
6. Fortinet Single Sign-On (FSSO)
7. High Availability (HA)
8. Web Proxy
9. Diagnostics

Prerequisites

FortiGate Security

- Knowledge of network protocols
- Basic understanding of firewall concepts

FortiGate Infrastructure

- Knowledge of OSI layers
- Knowledge of firewall concepts in an IPv4 network
- Knowledge of the fundamentals of FortiGate, as presented in the FortiGate Security course

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- A PDF viewer
- An up-to-date web browser
- Speakers or headphones

One of the following:

- HTML 5 support
- An up-to-date Java Runtime Environment (JRE with Java plugin enabled in your web browser

You should use a wired Ethernet connection, not a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.