FortiOS Administrator (OS-ADM)

Days: 4

Prerequisites: Knowledge of network protocols and a basic understanding of firewall concepts. Students should thoroughly understand the topics covered in the FortiGate Operator course before attending.

Audience: Networking and security professionals responsible for managing, configuring, administering, and monitoring FortiGate devices that secure their organizations' networks.

Description: Learn to configure, administer, and monitor the most common FortiGate features. Through interactive labs, explore firewall policies, user authentication, logging and monitoring, high availability, and site-to-site IPsec VPNs. Use security profiles such as intrusion prevention, antivirus, web filtering, and application control to protect your network. The course also introduces FortiGate in the cloud and FortiSASE. This course supports preparation for the Fortinet NSE 4 FortiOS Administrator exam and replaces FortiGate Administrator.

Course Objectives: Upon successful completion of this course, students will be able to:

- Configure basic networking from factory defaults, control administrator access, use the GUI and CLI, and describe device registration methods.
- View and search logs on FortiGate and FortiAnalyzer.
- Configure IPv4 firewall policies, port forwarding, source NAT, and destination NAT.
- Analyze route tables, configure static routing, and implement route redundancy and load balancing.
- Configure remote LDAP and RADIUS authentication, monitor firewall users, and deploy Fortinet Single Sign-On integrated with Microsoft Active Directory.
- Describe encryption, certificates, and SSL inspection on FortiGate.
- Configure antivirus, web filtering, intrusion prevention, and application control to address threats and misuse across standard and nonstandard protocols and ports.
- Configure IPsec VPNs using the wizard and manual configuration methods.
- Configure SD-WAN and verify traffic distribution.
- Identify primary and secondary device tasks and operation modes in FortiGate Clustering Protocol high availability clusters.
- Diagnose and correct common problems.
- Identify FortiGate virtual machines and devices in AWS and Microsoft Azure, and describe FortiSASE use cases.

OUTLINE:

MODULE 1: SYSTEM AND NETWORK SETTINGS
MODULE 2: LOGGING AND MONITORING
MODULE 3: FIREWALL POLICIES AND NAT
MODULE 4: ROUTING
MODULE 5: FIREWALL AUTHENTICATION
MODULE 6: FORTINET SINGLE SIGN-ON
MODULE 7: CERTIFICATE OPERATIONS
MODULE 8: ANTIVIRUS
MODULE 9: WEB FILTERING
MODULE 10: INTRUSION PREVENTION AND APPLICATION CONTROL
MODULE 11: IPSEC VPN
MODULE 12: SD-WAN CONFIGURATION AND MONITORING
MODULE 13: HIGH AVAILABILITY
MODULE 14: DIAGNOSTICS AND TROUBLESHOOTING
MODULE 15: FORTIGATE IN THE CLOUD
MODULE 16: FORTISASE