email : techcenter@trainocate.com.my
contact : +603-2281-1111

FT-FGT-SEC: FortiGate Security

Course Code: FT-FGT-SEC
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

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, 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.

SKILLS COVERED

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).
- Defend against data leaks by identifying files with sensitive data and block them from leaving your private network.
- Offer an SSL VPN for secure access to your private network.
- Implement a dial-up IPsec VPN tunnel between FortiGate and FortiClient.
- Collect and interpret log entries.

WHO SHOULD ATTEND?

Networking and security professionals involved in the management, configuration, administration and monitoring of FortiGate devices used to secure their organizations' networks. Participants 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

MODULES

Module 1: Introduction to FortiGate and the Security Fabric

Module 2: Firewall Policies

Module 3: Network Address Translation (NAT)

Module 4: Firewall Authentication

email : techcenter@trainocate.com.my
contact : +603-2281-1111

Module 5: Logging and Monitoring

Module 6: Certificate Operations

Module 7: Web Filtering

Module 8: Application Control

Module 9: Antivirus

Module 10: Intrusion Prevention and Denial of Service

Module 11: SSL VPN

Module 12: Dial-Up IPsec VPN

Module 13: Data Leak Prevention (DLP)

END OF PAGE