FortiGate Security

Durée : 3 Jours

Public visé

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.

Objectifs

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 dialup IPsec VPN tunnel between FortiGate and FortiClient.
- Collect and interpret log entries.

Pré-requis

Knowledge of network protocols Basic understanding of firewall concepts

---

Contenu

Le plan de la formation est comme suit :

- Introduction to FortiGate and the Security Fabric
- Firewall Policies
- Network Address Translation (NAT)
- Firewall Authentication
- Logging and Monitoring
- Certificate Operations
- Web Filtering
- Application Control
- Antivirus
- Intrusion Prevention and Denial of Service
- SSL VPN
- Dialup IPsec VPN
- Data Leak Prevention (DLP)