
FortiGate Infrastructure

Durée : 2 Jours

Public visé

Networking and security professionals involved in the design, implementation, and administration of a network infrastructure using FortiGate appliances. This course assumes knowledge of basic FortiGate fundamentals. 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:

- Analyze a FortiGate's route table.
- Route packets using policy-based and static routes for multi-path 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 appliances.
- 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.
- 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.

Pré-requis

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

Contenu

Le plan de la formation est comme suit :

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