

Fortinet, sécurité réseaux

-Référence: **PL-68**

-Durée: **4 Jours (28 Heures)**

Les objectifs de la formation

- Décrire les fonctionnalités du FortiGateMettre en oeuvre un VPN SSL et IPSEC
- Installer et configurer le firewall
- Mettre en oeuvre une stratégie de filtrage réseau et applicative
- Mettre en oeuvre la haute disponibilité des FortiGate

A qui s'adresse cette formation ?

POUR QUI :

- Technicien, administrateur et ingénieur systèmes/réseaux/sécurité.

Programme

- **Introduction**
 - Technologies et caractéristiques des firewalls.
 - L'architecture.
 - La famille des produits FORTINET.
 - Les composants de l'Appliance.
- **Configuration et administration**
 - Les tâches d'administration.
 - Les modes CLI/GUI et FortiManager.
 - La procédure d'installation.
 - Prise en main de l'interface.
 - Travaux pratiques Installer et configurer le firewall.
- **Le filtrage réseau et le filtrage applicatif**
 - La politique de contrôle d'accès du firewall.
 - Le filtrage des adresses et des ports.

- Définir une politique de filtrage.
 - Gestion des règles.
 - Le filtrage de contenu et détection de pattern.
 - Le filtrage URL.
 - Les options avancées.
 - Les filtres anti-spam.
 - Le contrôle du protocole SMTP.
 - Les fichiers attachés.
 - Les profils de protection.
 - L'antivirus.
 - Le blocage par extension de fichiers.
 - Travaux pratiques Mise en place d'une stratégie de filtrage réseau et applicative.
- **Le NAT et le routage**
 - Les modes d'utilisation NAT/Route/Transparent.
 - Le routage statique et le routage dynamique.
 - Quelle politique de routage mettre en place ? Travaux pratiques Mise en place d'une politique de routage.
 - L'authentification avec l'AD ou Radius.
- **Les VLAN et le Virtual Domains (VDM)**
 - Rappels sur le concept de VLAN.
 - Quand l'utiliser ? Administration et supervision.
 - Le routage InterVDM.
 - Travaux pratiques Installation et configuration de VLAN et VDM.
- **Le VPN avec IPSEC**
 - Rappels d'IPSEC.
 - Le VPN IPSEC site à site.
 - Le mode interface et le mode tunnel.
 - Le VPN IPSEC client à site.
 - Le client "FortiClient".
 - L'authentification Xauth.
 - Les tunnels avec la clé prépartagée.

- Travaux pratiques Configurer un tunnel IPSEC.
- **Le VPN avec SSL**
 - Rappels sur le protocole SSL.
 - Le mode Tunnel et le mode Portail.
 - Choisir le mode approprié.
 - Travaux pratiques Configuration de tunnel SSL mode portail et tunnel.
- **Haute disponibilité**
 - Les concepts de haute disponibilité.
 - Le mode actif-passif/actif-actif.
 - Répondre au besoin de l'entreprise.
 - Travaux pratiques Mise en place de la haute disponibilité FGCP actif/passif.



(+212) 5 22 27 99 01



(+212) 6 60 10 42 56



Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7ème étage N° 30
Casablanca 20340, Maroc