FortiGate Security - FortiGate Infrastructure

Découvrez une formation exhaustive qui vous permettra de maîtriser les compétences cruciales en matière de sécurité informatique. De la neutralisation des menaces émanant de malwares et d'applications nocives à la gestion des accès réseau, en passant par la mise en place de VPN SSL et IPsec, cette formation couvre l'ensemble du spectre de la sécurité

Objectifs pédagogiques :

Durée : 5 jours

À la fin de la formation, vous aurez les compétences suivantes :

- Décrire les fonctionnalités des UTM du FortiGate
- Neutraliser les menaces véhiculées au travers des malwares, les applications nocives et limiter les accès aux sites inappropriés
- Contrôler les accès au réseau selon les types de périphériques utilisés
- Authentifier les utilisateurs au travers du portail captif personnalisable
- Mettre en œuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Mettre en œuvre un VPN IPsec pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Appliquer de la PAT, de la source NAT et de la destination NAT
- Interpréter les logs et générer des rapports
- Mettre en œuvre la protection anti-intrusion
- Maîtriser l'utilisation des applications au sein de votre réseau
- Configurer de la SD-Wan
- Monitorer le statut de chaque lien de la SD-Wan
- Configurer de la répartition de charge au sein de la SD-Wan
- Déployer un cluster de FortiGate
- Inspecter et sécuriser le trafic réseau sans impacter le routage
- Analyser la table de routage d'un FortiGate
- Diviser un FortiGate physique en plusieurs FortiGates virtuels indépendants, via la mise en œuvre des Virtual Domains
- Étudier et choisir une architecture de VPN IPsec
- Comparer les VPN IPsec en mode Interface (route-based) ou Tunnel (Policy-based)
- Implémenter une architecture de VPN IPSec redondée
- Troubleshooter et diagnostiquer des problématiques simples sur le FortiGate
- Mettre en œuvre l'identification utilisateur ou l'authentification transparente dans les environnements Active Directory