FORTINET

Fortinet® NSE 4 - FortiGate Network Security Professional

5 jours (35h00) | NSE4 | Num form : form-73 | Initiation / Fondamentaux

INFORMATIQUE / SÉCURITÉ IT / FORTINET

À l'issue de ce stage vous serez capable de :

- 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
- Utiliser la GUI et la CLI
- 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.

Niveau requis :

- Notions TCP/IP et concepts firewall.
- connaissance des couches du modèle OSI et des concepts de firewall est nécessaire

Public concerné :

- Ceux qui administrent régulièrement un firewall FortiGate
- Ceux qui participent au design des architectures réseau et sécurité reposant sur des matériels FortiGate
- Toutes les personnes souhaitant passer la certification NSE 4 - FortiGate Network Security Professional.

Programme :

FORTIGATE : NOTIONS DE BASE

- Introduction sur Fortigate et les UTM
- Gestion des logs et supervision
- Les règles firewall
- Les règles firewall avec authentification des utilisateurs : Authentifier les utilisateurs au travers des règles firewalls
- Le VPN SSL : Mettre en œuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Introduction au VPN IPSEC
- L'antivirus
- Le proxy explicit
- Le filtrage d'URL : Mettre en œuvre le proxy explicit, le cache et l'authentification des utilisateurs
- Le contrôle applicatif : Maîtriser l'utilisation des applications au sein de votre réseau

FORTIGATE : NOTIONS AVANÇÉES

- Le routage : Analyser la table de routage d'un Fortigate
- La virtualisation
- Le mode transparent
- La haute disponibilité : Réaliser du load balancing de trafic sur plusieurs opérateurs
- Le VPN IPSec avancé : Implémenter une architecture de VPN IPSec redondée
- L'IPS
- Le FSSO : Mettre en œuvre le FSSO
- Les certificats, la cryptographie : Déchiffrer les flux chiffrés

- Le DLP : Déployer des profils de DLP
- Le s diagnostics
- L’accélération matérielle : Comprendre le fonctionnement de l’accélération matérielle
- IPv6