FORTINET NSE4 – Fortigate security & infrastructure

Référence : **SEC-FOR3** Durée : **5 jours** Certification : **NSE4**

CONNAISSANCES PREALABLES

• 1-Des notions TCP/IP et des concepts firewall. • 2-Connaissance des couches du modèle OSI.

PROFIL DES STAGIAIRES

• 1-Administrateurs régulier d'un firewall. • 2-Toutes les personnes participent au design des architectures réseaux et sécurité reposant sur des matériels FortiGate.

OBJECTIFS

• Prendre en main les fonctions UTM du FortiGate.. • Configurer pare-feu, des tunnels VPN IPSEC, des accès VPN SSL, la protection contre les malwares, des profils de filtrage d'URL, l'authentification au travers d'un portail captif, la prévention de fuites de données, le déchiffrement… . • Prendre en main les fonctions d'architectures avancées du FortiGate. • Confugrer de la SD-Wan, du routage avancé, la mise en haute disponibilité des FortiGate, le mode transparent, des tunnels IPsec redondés, les VDOMS, le Single Sign On, ….

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Fortinet

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Partie 1 : FortiGate Security

- Introduction sur FortiGate et les UTMs
- La « Security Fabric »
- Les règles firewall
- La NAT
- Les règles firewall avec authentification des utilisateurs
- Gestion des logs et supervision
- Les Certificats
- Le filtrage d'URL
- Le contrôle applicatif
- L'antivirus
- Le contrôle anti-intrusion
- Le VPN SSL
- Le VPN IPSEC en mode dial-up

Partie 2 : FortiGate Infrastructure

- Le routage
- La SD-Wan

La virtualisation

L’analyse L2

Le VPN IPSec en mode site à site

Le FSSO

La haute disponibilité

Le Proxy Explicite

Les diagnostics