FORTINET FORTIGATE : BASES FORTIGATE & SÉCURITÉ ESSENTIELLE – DURÉE 21h

OBJECTIF

L'objectif de cette formation est de permettre aux participants de prendre en main un pare-feu FortiGate et de le rendre opérationnel dans une architecture réseau standard.

À l'issue de la formation, les apprenants seront capables de déployer un FortiGate, configurer la connectivité réseau et Internet, appliquer des politiques de sécurité de base, activer les services UTM essentiels et fournir un accès distant sécur À l'issue de la formation, les participants seront capables de :

- ❍ Installer et initialiser un FortiGate, accéder à l'interface graphique et CLI, et comprendre son positionnement dans la Security Fabric (vue globale).
- ❍ Configurer les interfaces, VLANs, zones de sécurité et le routage statique, afin d'assurer la connectivité LAN/WAN et l'accès Internet.
- ❍ Mettre en œuvre des règles de pare-feu et des mécanismes de NAT, incluant la publication de services via VIP.
- ❍ Déployer les profils de sécurité UTM essentiels : Filtrage Web, Antivirus, Contrôle d'Applications et IPS.
- ❍ Mettre en place un SD-WAN de base, permettant la résilience et le partage de charge entre plusieurs liens Internet.
- ❍ Configurer un accès distant utilisateur via VPN SSL, avec gestion des groupes et des profils d'accès.

PUBLIC CIBLE

Cette formation s'adresse aux professionnels de l'informatique souhaitant acquérir les **fondamentaux de l'administration et de la sécurité réseau avec FortiGate** :

- ❍ Administrateurs réseaux et systèmes débutants ou intermédiaires.
- ❍ Techniciens ou ingénieurs support amenés à exploiter des pare-feux FortiGate.
- ❍ Intégrateurs ou consultants IT débutant sur les solutions Fortinet.
- ❍ Responsables informatiques souhaitant comprendre le fonctionnement et les capacités de base d'un FortiGate.

PRE-REQUIS

Pour suivre ce cursus de niveau 1, les participants doivent posséder :

- ❍ Des **connaissances réseaux fondamentales** : modèle OSI, TCP/IP, notions de LAN, WAN et VLAN, principes de routage statique.
- ❍ Des **notions de sécurité réseau** : règles de pare-feu et principes de NAT.
- ❍ Une **compréhension de l'anglais technique**, l'interface FortiOS et la documentation étant majoritairement en anglais.

PROGRAMME

Bases FortiGate & Réseau

- **Écosystème Fortinet**
  - Security Fabric (vue globale)
  - FortiGate dans la gamme
  - Accès GUI / CLI
  - Licences, FortiCare, firmware
  - Modes NAT / Transparent
- **Interfaces, Zones & Routage**
  - Interfaces, VLANs, LACP
  - Zones et segmentation
  - Routage statique
  - OSPF (intro uniquement)
  - Lab : LAN / WAN / DMZ

Politiques & Sécurité Essentielle

- **Politiques & NAT**
  - Règles firewall
  - Objets & groupes
  - VIP / Port forwarding
  - Central NAT (intro)
  - Lab : publication serveur
- **Profils UTM**
  - Web Filter
  - Application Control
  - Antivirus
  - IPS
  - Lab : politique Internet sécurisée

SD-WAN & VPN Utilisateur

- **SD-WAN Essentiel**
  - Membres SD-WAN
  - Health-check
  - Load balancing
  - Lab : 2 liens WAN
- **VPN SSL**
  - Tunnel vs Web
  - Groupes utilisateurs
  - MFA (présentation)
  - Lab : accès distant utilisateur

MOYENS TECHNIQUES ET HUMAINS

Moyens Humains :

- **Formateur EXPERNET**
- **Accompagnement :** Un ratio de 3 à 6 stagiaires maximum par formateur pour garantir un suivi personnalisé.

Moyens Techniques :

- **Environnement de Lab :** Un accès individuel par stagiaire à une instance **FortiGate-VM** (version 7.4+) et une machine cliente (Windows ou Linux).
- **Support de cours :** Support numérique complet incluant les slides et les guides de travaux pratiques (Lab Guide).
- **Infrastructure :** Accès Internet haut débit pour les mises à jour FortiGuard et une plateforme de virtualisation (EVE-NG, PNETLab ou simulateur Fortinet).

MODALITÉS D'ÉVALUATION

L'évaluation se fait en deux étapes pour valider les compétences théoriques et pratiques :

1. **Évaluation formative (en continu) :** Exercices pratiques après chaque module pour valider la configuration technique (ex : réussir à monter un tunnel VPN fonctionnel).
2. **Évaluation sommative (final) :** * **Quiz de validation :** Questionnaire à choix multiples (QCM) de 20 questions portant sur les concepts clés.
3. **Attestation de suivi de formation**