FORTINET FORTIGATE

Niveau 2 - Administration Avancée, Accès Zero Trust et Troubleshooting – 21h

OBJECTIF

L'objectif de cette formation est de permettre aux participants d'approfondir l'administration des pare-feux FortiGate et de maîtriser des architectures de sécurité réseau avancées.

Elle vise à rendre l'apprenant capable de concevoir, sécuriser, optimiser et dépanner des environnements FortiGate complexes, intégrant la haute disponibilité, l'inspection SSL avancée, les VPN site-à-site, les accès Zero Trust et les outils de supervision et d'automatisation.

À l'issue de la formation Niveau 2, les participants seront capables de :

- Concevoir et déployer des architectures FortiGate avancées, intégrant la haute disponibilité (Active/Passive, Active/Active) et des environnements multi-sites.
- Mettre en œuvre et optimiser l'inspection SSL avancée (Certificate et Deep Inspection), en tenant compte des impacts de performance, de conformité et des exceptions applicatives.
- Déployer et administrer des accès distants et inter-sites avancés, incluant VPN IPsec (site-à-site, hub-and-spoke, ADVPN) et intégration avec le SD-WAN.
- Mettre en place des accès Zero Trust (ZTNA) basés sur l'identité et la posture des postes, via FortiClient EMS et les ZTNA Tags.
- Centraliser la gestion et la supervision des équipements à l'aide de FortiManager et FortiAnalyzer (politiques, logs, rapports).
- Analyser, diagnostiquer et résoudre des incidents complexes à l'aide des outils de troubleshooting avancé (debug flow, sniffer, analyse des logs).
- Optimiser les performances et la sécurité des FortiGate, en ajustant les modes d'inspection, les profils de sécurité et les mécanismes d'accélération matérielle.

PUBLIC CIBLE

Cette formation s'adresse aux professionnels disposant déjà d'une expérience sur FortiGate et souhaitant monter en expertise :

- Administrateurs réseaux et systèmes confirmés.
- Ingénieurs sécurité, intégrateurs ou consultants Fortinet.
- Techniciens ou ingénieurs support en charge du diagnostic et de la résolution d'incidents complexes.
- Architectes réseau ou sécurité souhaitant concevoir et maintenir des infrastructures sécurisées à grande échelle.

PRE-REQUIS

Pour suivre ce cursus de niveau 2, les participants doivent :

- Avoir suivi la formation FortiGate Niveau 1 ou posséder des compétences équivalentes en administration FortiGate.
- Maîtriser les fondamentaux de la configuration d'un FortiGate : interfaces, zones, politiques de sécurité, NAT et UTM.
- Avoir une expérience pratique des environnements réseau sécurisés, incluant le SD-WAN de base et les accès VPN utilisateur.
- Être à l'aise avec l'interface CLI FortiOS pour les opérations de diagnostic.
- Disposer d'un anglais technique opérationnel, la documentation et les messages système étant en anglais.

PROGRAMME

Haute Disponibilité

- Active-Passive / Active-Active
- Session sync
- Split-brain
- Lab HA

SSL Inspection Avancée

- Certificate vs Deep Inspection
- Flow vs Proxy
- Lab Deep Inspection

ZTNA

- FortiClient EMS
- ZTNA Tags
- Posture Check
- ZTNA Proxy vs Server
- Lab accès conditionnel

VPN Expert

- IPsec IKEv2
- ADVPN Hub-and-Spoke
- VPN + SD-WAN
- Redondance tunnels

Logs & Analyse

- FortiAnalyzer
- Recherche d'incidents
- Conformité

Troubleshooting CLI

- Debug Flow
- Sniffer
- Cas réels :
    - Règle bloquée
    - VPN HS
    - Site coupé par SSL
    - Perf dégradée

Module Bonus

- FortiManager (templates)
- Automation Stitches
- API REST / Ansible
- FortiGate-VM & Cloud (Azure/AWS)

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