PALO ALTO NETWORKS

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 Palo Alto Networks et de maîtriser des architectures de sécurité réseau avancées.

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

- Concevoir et déployer des architectures Palo Alto avancées, incluant HA et multi-sites
- Mettre en œuvre et optimiser l'inspection SSL avancée (Certificate & Full Decryption)
- Déployer et administrer des VPN site-to-site IPsec et des accès distants GlobalProtect avancés
- Mettre en place des politiques d'accès conditionnel Zero Trust
- Centraliser la gestion et la supervision via Panorama et analyser les logs avancés
- Diagnostiquer et résoudre des incidents complexes à l'aide des outils CLI et des logs
- Optimiser les performances et sécuriser les firewalls en production

PUBLIC CIBLE

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

- Administrateurs réseaux et systèmes confirmés
- Ingénieurs sécurité, intégrateurs ou consultants Palo Alto
- 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 Palo Alto Niveau 1 ou posséder des compétences équivalentes en administration PAN OS
- Maîtriser les fondamentaux de la configuration d'un NGFW Palo Alto : interfaces, zones, politiques de sécurité, NAT et profils UTM de base
- Avoir une expérience pratique des environnements réseau sécurisés, incluant SD-WAN de base et accès VPN utilisateur
- Être à l'aise avec l'interface CLI PAN-OS pour les opérations de diagnostic
- Disposer d'un anglais technique opérationnel, la documentation et les messages système étant en anglais

PROGRAMME

Haute Disponibilité (HA) et Redondance

- Concepts Active/Passive et Active/Active
- Session sync et failover
- Scénarios multi-sites et VPN redondant
- Lab : Mise en place HA Active/Passive entre deux VM

Inspection SSL Avancée

- Certificate Inspection vs Full Decryption
- Gestion des exceptions (banques, RGPD…)
- Impact sur la performance et tuning
- Lab : Déchiffrement SSL avec exceptions configurées

Accès Zero Trust et GlobalProtect avancé

- Architecture ZTNA / Posture check
- FortiClient équivalent : GlobalProtect / Endpoint Management
- Politiques d'accès conditionnel selon utilisateur, groupe et posture
- Lab : Accès conditionnel utilisateur ZTNA

VPN site-to-site et IPsec avancé

- IPsec IKEv2 et phase 1/2
- Hub-and-Spoke et ADVPN
- Redondance tunnels + SD-WAN
- Lab : VPN site-to-site multi-tunnel avec failover

Panorama et gestion centralisée

- Templates et policies globales
- Gestion multi-firewalls
- Logs centralisés, reporting et conformité
- Lab : Gestion de plusieurs NGFW via Panorama

Analyse avancée et Troubleshooting

- Commandes CLI essentielles et debug flow
- Packet capture et traffic log analysis
- Résolution de problèmes complexes (règles bloquantes, VPN qui ne monte pas, perf dégradée)
- Lab : Cas pratiques de troubleshooting avancé

Optimisation et automatisation

- Tuning de performance : App-ID, User-ID, SSL Proxy
- Scripts d'automatisation simples (Panorama, API REST)
- Réponses automatisées aux incidents
- Lab : Automatisation d'une action de blocage IP suite à alerte

Sauvegarde et maintenance avancée

- Backup / restore configuration
- Mise à jour PAN-OS sécurisée
- Documentation et runbooks
- Lab : Mise à jour et restauration de configuration

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 **:** Instances Palo Alto NGFW VM-Series avec HA, VPN multi-site et postes clients (Windows/Linux)
- Support de cours complet **:** support de présentation + Lab Guide avancé
- Infrastructure **:** Internet haut débit pour mises à jour de sécurité + plateforme virtualisation (EVE-NG, PNETLab, ou équivalent)
- Outils complémentaires **:** Panorama, dashboards de monitoring, scripts et templates pour automatisation

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.