PALO ALTO NETWORKS

Niveau 1 - Administration des NGFW Palo Alto (PAN-OS) – 21h

OBJECTIF

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

À l'issue de la formation, les apprenants seront capables de déployer un NGFW Palo Alto, configurer la connectivité réseau et Internet, appliquer des politiques de sécurité basées sur les applications et les utilisateurs, activer les services de sécurité essentiels et fournir un accès distant sécurisé aux utilisateurs.

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

- Installer et initialiser un pare-feu Palo Alto Networks, accéder à l'interface Web (PAN-OS) et comprendre son positionnement dans une architecture de sécurité moderne.
- Configurer les interfaces, zones de sécurité, VLANs et le routage statique, afin d'assurer la connectivité LAN/WAN et l'accès Internet.
- Mettre en œuvre des politiques de sécurité basées sur les applications (App-ID), les utilisateurs (User-ID) et les services.
- Configurer les mécanismes de NAT, incluant le Source NAT et le Destination NAT pour la publication de services.
- Activer et appliquer les profils de sécurité essentiels : Antivirus, Anti-Spyware, Vulnerability Protection et URL Filtering.
- Mettre en place un accès distant utilisateur via GlobalProtect (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 Palo Alto Networks :

- Administrateurs réseaux et systèmes débutants ou intermédiaires.
- Techniciens ou ingénieurs support amenés à exploiter des pare-feux Palo Alto Networks.
- Intégrateurs ou consultants IT débutant sur les solutions Palo Alto Networks.
- Responsables informatiques souhaitant comprendre les capacités techniques de base des NGFW Palo Alto.

PRE-REQUIS

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

- Des connaissances réseaux fondamentales : modèle OSI, TCP/IP, LAN, WAN, VLAN et routage statique.
- Des notions de sécurité réseau : règles de pare-feu, principes de NAT et bases du chiffrement SSL/TLS.
- Une compréhension de l'anglais technique, l'interface PAN-OS et la documentation étant en anglais.

PROGRAMME

Découverte de l'écosystème Palo Alto Networks

- Positionnement des NGFW Palo Alto
- Concepts clés : App-ID, User-ID, Content-ID
- Accès à l'interface Web PAN-OS
- Licences et abonnements (Threat Prevention, URL Filtering)
- Modes de déploiement : Layer 3, Layer 2, Virtual Wire

Interfaces, Zones & Routage

- Interfaces physiques et logiques
- Zones de sécurité
- VLANs (notions)
- Routage statique
- Introduction au routage dynamique (OSPF – notions)
- Lab : architecture LAN / WAN / DMZ

Politiques de Sécurité & NAT

- Structure d'une règle de sécurité
- App-ID, Service et Action
- Ordre d'évaluation des règles
- Source NAT / Destination NAT
- Publication de services
- Lab : accès Internet et publication serveur

Profils de Sécurité

- Antivirus
- Anti-Spyware
- Vulnerability Protection
- URL Filtering
- Application des profils aux règles
- Lab : politique Internet sécurisée

VPN Utilisateur avec GlobalProtect

- Principe du VPN SSL GlobalProtect
- Portail vs Gateway
- Groupes utilisateurs (LDAP/Local – notions)
- Lab : accès distant utilisateur sécurisé

Supervision et Exploitation

- Logs : Traffic, Threat, URL
- Filtres et analyse des événements
- Monitor et dashboards
- Sauvegarde et restauration de configuration
- Bonnes pratiques d'exploitation

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 Palo Alto Networks NGFW (VM-Series, PAN-OS 10.x ou 11.x) et une machine cliente (Windows ou Linux).

Support de cours **:** Support numérique complet incluant les supports de présentation et les guides de travaux pratiques (Lab Guides) couvrant chaque module de la formation.

Infrastructure **:** Accès Internet haut débit pour les mises à jour de contenus de sécurité Palo Alto Networks (Threat Prevention, URL Filtering) et une plateforme de virtualisation telle que EVE-NG, PNETLab ou un environnement équivalent compatible VM-Series.

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.