

## INSTALLER ET ADMINISTRER UN FIREWALL PALO ALTO

### Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Configurer et gérer les fonctionnalités essentielles des firewalls de nouvelle génération Palo Alto Networks
- Configurer et gérer des politiques de sécurité et de NAT pour la gestion des flux autorisés
- Configurer et gérer les profils de gestion des menaces afin de bloquer le trafic provenant d'adresses, domaines et URL connus et inconnus
- Monitorer le trafic réseau en utilisant l'interface Web et les rapports intégrés.

### Prérequis

Avoir des connaissances de base sur les concepts de sécurité et de réseau, incluant le routage, le switching et l'adressage IP. Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus.

L'apprenant s'engage à respecter les prérequis nécessaires via un questionnaire qui lui sera transmis en amont de la formation.

### Support pédagogique

Le support de cours et les labs

### Public concerné

Ingénieurs et administrateurs sécurité, analystes en sécurité, ingénieurs réseaux et membres d'une équipe de support.

**Durée de la Formation** : 4 Jours

**Prix de la Formation** : 3850 euros TTC

## INSTALLER ET ADMINISTRER UN FIREWALL PALO ALTO

### Programme

- ❖ Palo Alto Networks portfolio et architecture
- ❖ Configuration initiale du firewall
- ❖ Gérer les configurations sur le firewall
- ❖ Gérer les comptes d'administration du firewall
- ❖ Connexion du firewall aux réseaux de production avec zones de sécurité
- ❖ Création et gestion des règles de sécurité
- ❖ Création et gestion des règles de NAT
- ❖ Contrôle des applications avec App-ID
- ❖ Blocages des menaces connues en utilisant les profils de sécurité
- ❖ Blocage du trafic Web non approprié avec le filtrage des URL
- ❖ Bloquer les menaces inconnues avec Wildfire
- ❖ Contrôler l'accès aux ressources réseaux avec la reconnaissance utilisateurs (User-ID)
- ❖ Utiliser le déchiffrement afin de bloquer les menaces sur un trafic chiffré
- ❖ Repérer les informations importantes via les logs et les rapports

Modules supplémentaires abordés :

- ✚ Sécuriser les postes de travail avec Global Protect
- ✚ Apporter de la redondance au firewall avec la haute disponibilité
- ✚ Connecter des sites distants via des VPN site à site
- ✚ Se protéger des attaques courantes en utilisant la "zone protection"

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

### Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou

Le formateur alterne entre méthode

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne

## INSTALLER ET ADMINISTRER UN FIREWALL PALO ALTO

- Supports de cours et exercices

### **Modalités d'évaluation des acquis**

- En cours de formation, par des études de cas concrets, des quiz en salle, des mises en situation et/ou des questions orales ou écrites (QCM)
- Et, en fin de formation, par un questionnaire d'auto-évaluation

### **Accessibilité de la formation**

Mafttechnologies s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page [Accueil PSH](#).