

Offre éditeurs

## Palo Alto Networks - Firewall 10.x - Essentials - Configuration et management

5 jours (35h00) | ★★★★★ 4,6/5 | PAN-EDU210 | Certification PCNSA (incluse) |  
Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel <sup>(1)</sup>

Formations Informatique › Cybersécurité › Offre éditeurs



### À l'issue de ce stage vous serez capable de :

- Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelle génération
- Paramétrer et gérer des politiques de sécurité et de NAT pour activer le trafic autorisé en provenance et à destination de zones
- Configurer et gérer des stratégies de prévention des menaces afin de bloquer le trafic provenant d'adresses IP, domaines et URL connus et inconnus
- Monitorer le trafic réseau en utilisant l'interface Web interactive et les rapports du firewall.

### Niveau requis

Avoir des connaissances de base sur les concepts de sécurité et de mise en 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.

### Public concerné

Ingénieurs et administrateurs sécurité, spécialistes des opérations de sécurité, analystes en sécurité et membres d'une équipe de support.

### Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

#### (1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel \* (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes \*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les 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. Supports de cours et exercices.

\* Nous consulter pour la faisabilité en distanciel. \*\* Ratio variable selon le cours suivi.

# Programme

**Présentation et architecture de Palo Alto Networks**

**Configuration des paramètres initiaux du firewall**

**Gestion des configurations du firewall**

**Gestion des comptes administrateurs du firewall**

**Connexion du firewall aux réseaux de production avec des zones de sécurité**

**Création et gestion des règles de politique de sécurité**

**Création et gestion des règles de politique NAT**

**Contrôle de l'utilisation des applications avec App-ID**

**Blocage des menaces connues à l'aide des profils de sécurité**

**Blocage du trafic Web inapproprié avec le filtrage d'URL**

**Blocage des menaces inconnues avec Wildfire**

**Contrôle de l'accès aux ressources du réseau avec User-ID**

**Utilisation du décryptage pour bloquer les menaces dans le trafic crypté**

**Trouver des informations précieuses à l'aide des logs et des rapports**

**Passage de la certification**

- Le prix de la certification est inclus dans la formation, mais le passage devra se faire ultérieurement, dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectue en ligne et durera en moyenne 1h30

**Modalités d'évaluation des acquis**

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

**Les + de la formation**

Le support de cours et les labs sont en anglais.