Formation **Palo Alto Networks Firewall Essentials : Configuration et Management**

Cette formation prépare également au passage de la certification PCNSA (coût de l'examen non-inclus)

Mené par un instructeur certifié, ce cours officiel de 5 jours permettra aux stagiaires d'apprendre à configurer et gérer les principales fonctionnalités des pare-feux de nouvelle génération Palo Alto Networks. Ils découvriront notamment comment configurer GlobalProtect pour sécuriser des machines situées à l'extérieur du réseau interne de leur entreprise, sauront mettre en œuvre la haute-disponibilité des pare-feux, et réaliser une surveillance efficace du trafic réseau en utilisant les rapports intégrés ou directement depuis l'interface web. A l'issue de la formation, les participants sont en mesure de passer l'examen de certification PCNSA (coût de l'examen non inclus dans le tarif de la formation).

Durée

[durée]

Objectifs pédagogiques

- Configurer et gérer les fonctionnalités essentielles des firewalls Next Gen Palo Alto Networks
- Configurer et gérer des règles de sécurités et de NAT pour la gestion des flux autorisés
- Configurer et gérer les profils de sécurité avancés afin de bloquer les trafics provenant des sources connues ou inconnues (adresses, domaines et URLs)
- Contrôler les accès aux ressources réseaux par l'identification des utilisateurs (User-ID)
- Monitorer le trafic réseau en utilisant l'interfaces web et les rapports intégrés
- Préparation à la certification PCNSA

Public

Administrateurs systèmes et réseaux, ingénieurs télécoms et réseaux...

Prérequis

Connaissances basiques en administration réseau et sécurité réseau.

Programme de formation

Chapitres du programme de formation Palo Alto

Portefeuille et architecture de Palo Alto Networks
Se connecter au réseau de Management
Gérer les configurations de pare-feu
Gérer les comptes d'administrateurs de pare-feu
Se connecter aux réseaux de production
Le cycle de vie de la cyberattaque
Bloquer les menaces à l'aide de politiques de sécurité et NAT
Bloquer les attaques basées sur les paquets et les protocoles
Bloquer les menaces provenant de sources malveillantes
connues
Bloquer les menaces en identifiant les applications
Maintenir les politiques basées sur les applications
Bloquer les menaces à l'aide d'applications personnalisées
Bloquer les menaces en identifiant les utilisateurs
Bloquer les menaces en identifiant les Devices
Bloquer les menaces inconnues
Bloquer les menaces dans le trafic chiffré
Empêcher l'utilisation d'informations d'identification volées
Bloquer les menaces à l'aide de profils de sécurité
Afficher les informations sur les menaces et le trafic
Étapes suivantes

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.