Formation Palo Alto Networks Firewall 10.1 - Configuration et Management

Mettre en oeuvre les firewalls de nouvelle génération

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Palo Alto Networks, le spécialiste américain de la sécurité informatique et des firewalls, a lancé mi 2020 une nouvelle version de son système d'exploitation PAN OS. Avec PAN OS 10.1, le constructeur propose le tout premier pare-feu de dernière génération basé sur le Machine Learning. Avec cette avancée technologique majeure Palo Alto bouscule le monde de la prévention en fournissant une solution capable de se prémunir des attaques inconnues tout en améliorant ses fonctionnalités précédentes. Bien au-delà de la seule prise en main des dernières fonctionnalités les participants à cette formation apprendront à installer, configurer et manager les firewalls de nouvelle génération de Palo Alto. Cette formation prépare au test PCNSA. Cette formation entre en jeu dans le cursus de certification Palo Alto Networks Certified Network Security Administrator (PCNSA).

Référence	SEC52
Durée	5 jours (35h)
Tarif	4 015 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 27 au 31 mai 2024
du 17 au 21 juin 2024
du 1er au 5 juillet 2024
du 26 au 30 août 2024
du 16 au 20 septembre 2024
du 7 au 11 octobre 2024
du 4 au 8 novembre 2024
du 2 au 6 décembre 2024

VOIR TOUTES LES DATES

Objectifs

| Être capable de configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations
| Identifier comment configurer et gérer les règles de sécurité et de NAT pour la gestion des flux autorisés vers et depuis les zones
| Savoir configurer et gérer les stratégies de prévention des menaces pour bloquer le trafic provenant d'adresses IP, de domaines et d'URL connus et inconnus
| Pouvoir monitorer le trafic réseau en utilisant les interfaces web interactives et les rapports intégrés

Public

| Ingénieurs sécurité, administrateurs sécurité, spécialistes des opérations de sécurité, analystes sécurité et personnel de support

Prérequis

| Connaissance de base des concepts de réseau, y compris le routage, la commutation et l'adressage IP
| Être familiarisé avec les concepts de base de la sécurité
| Une expérience avec d'autres technologies de sécurité (IPS, proxy et filtrage de contenu) est un plus

Programme de la formation

1 - Portfolio et architecture de Palo Alto Networks
2 - Configuration initiale des paramètres du pare-feu
3 - Gestion des configurations du pare-feu
4 - Gérer les comptes d'administrateur du pare-feu
5 - Connexion du pare-feu aux réseaux de production avec des zones de sécurité
6 - Créer et gérer des règles de stratégie de sécurité
7 - Créer et gérer des règles de stratégie NAT
8 - Contrôler l'utilisation des applications avec App-ID
9 - Blocage des menaces connues à l'aide de profils de sécurité
10 - Blocage du trafic Web inapproprié avec le filtrage d'URL

11 - Blocage des menaces inconnues avec Wildfire
12 - Contrôle de l'accès aux ressources réseau avec l'ID utilisateur
13 - Utilisation du déchiffrement pour bloquer les menaces dans le trafic chiffré
14 - Localisation des informations importantes à l'aide de journaux et de rapports

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.