Palo Alto Networks Firewall 11.1 : Troubleshooting

Prix : 2 915 €HT

Durée : 3 jours

Code de Référence : PAN330

Catalogue Palo Alto Networks

L’achèvement des 3 jours de formation permet aux stagiaires de comprendre comment troubleshooter la ligne complète des produits Palo Alto Networks next-generation firewalls.

Les participants auront reçu une expérience pratique pour troubleshooter les problèmes courants liés à la configuration et à l’administration des fonctionnalités des firewall Palo Alto Networks.

Cette formation va améliorer les connaissances du stagiaire en matière de troubleshooting, de visibilité et de contrôle des applications, utilisateurs et contenus.

Objectifs de la formation

A l’issue de cette formation Palo Alto Networks, vous serez capable de :

- Investiguer les problèmes de connexion réseau en utilisant les outils et la CLI
- Suivre des procédures de troubleshooting éprouvées
- Analyser les logs de façon avancée pour résoudre des scénarios variés du quotidien
- Mettre en pratique ces méthodes dans des labs (exercices pratiques de lab basés sur des scenarios)

Public

Cette formation Palo Alto s’adresse aux ingénieurs sécurité, ingénieurs réseaux, administrateurs de sécurité, spécialistes en opération de sécurité, analystes en sécurité et membres d’une équipe de support.

Prérequis

Les participants devront avoir suivi la formation PAN210 – Palo Alto Networks Firewall – Configuration & Management ou avoir une expérience pratique correspondante.

Les stagiaires devront être familiers avec les fondamentaux des concepts réseaux (routage, switching et adressage IP. Ils devront également avoir au moins 6 mois d’expérience professionnelle sur les firewalls Palo Alto Networks.

Vous souhaitez faire vérifier vos prérequis ? Contactez-nous pour l’organisation d’un entretien téléphonique avec un de nos consultants formateurs.

Programme de la formation

Module 1

Outils et ressources

Module 2

Gestion des sessions

Module 3

Capture de Paquets

Module 4

Analyse bas niveau – Paquet

Module 5

Gestion des sessions à destination du Firewall

Module 6

Gestion des sessions traversant le Firewall

Module 7

Services internes

Module 8

Gestion des certificats et déchiffrement SSL

Module 9

Identification des Users User-ID

Module 10

VPN Nomade, GlobalProtect

Module 11

Ouverture des tickets, escalade et RMA

Module 12

Et après …

Annexe

Introduction aux lignes de commandes

Méthodes pédagogiques

Cette formation Palo Alto est rythmée par une alternance d’exposés et de travaux pratiques. Les exercices réalisés lors des travaux pratiques permettent la mise en œuvre des connaissances acquises.

Méthodes d’évaluation des acquis

L’évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques (des labs de formation fournis par l’éditeur)
- Et, en fin de formation, par un questionnaire d’auto-évaluation

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.

Certification préparée

Certification Palo Alto Networks “Certified Network Security Engineer (PCNSE)” :

Durée de validité : 2 ans A ce jour, cette certification est toujours valide. Elle est amenée à disparaitre au profit de nouvelles certifications. Nous ne manquerons pas de vous tenir informés dès lors que nous en saurons plus.