

Palo Alto Networks Firewall 11.1 : Configuration & Management

Prix : 4 015 €HT

Durée : 5 jours

Code de Référence : PAN210

Catalogue Citrix

Cette formation de cinq jours forme à la configuration, au management, et à l'exploitation des firewalls de nouvelle génération Palo Alto Networks.

Objectifs de la formation

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

- Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations
- Configurer et gérer des règles de sécurité et de NAT pour la gestion des flux autorisés
- Configurer et gérer les profils de gestion des menaces afin de bloquer les trafics provenant des adresses, domaines et URLs connues et inconnues
- Monitorer le trafic réseau en utilisant l'interfaces web et les rapports intégrés

Public

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

Prérequis

Les participants devront être familiers avec les concepts basiques de la sécurité et des réseaux, incluant routage, switching et adresses IP. Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus.

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

Palo Alto Networks portfolio et architecture

Module 2

Configuration initiale du Firewall

Module 3

Gérer les configurations sur le Firewall

Module 4

Gérer les comptes d'administration du Firewall

Module 5

Connexion du Firewall aux réseaux de production avec zones de sécurités

Module 6

Création et gestion des règles de sécurité

Module 7

Création et gestion des règles de NAT

Module 8

Contrôle des applications avec App-ID

Module 9

Blocages des menaces connues en utilisant les profils de sécurité

Module 10

Blocage du trafic web non approprié avec le filtrage des URLs

Module 11

Bloquer les menaces inconnues avec Wildfire

Module 12

Contrôler l'accès aux ressources réseaux avec la reconnaissance utilisateurs (User-ID)

Module 13

Utiliser le déchiffrement afin de bloquer les menaces sur un trafic chiffré

Module 14

Repérer les informations importantes via les logs et les rapports

Module 15

Discussion sur les autres formations et les certifications

Modules supplémentaires

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 »

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 "Next-Generation Firewall Engineer". Durée de validité : 2 ans

Il s'agit de la certification technique de 3ème niveau (Specialist) sur les produits Palo Alto Networks – Network Security, qui regroupe 4 niveaux de certifications.