Palo Alto Networks Firewall 10.0 Essentials : Configuration & Management

Description

Palo Alto Networks est un visionnaire dans le domaine de la sécurité réseau. Il propose des Firewalls nouvelle génération qui permettent :

Identifier les applications, d'identifier les utilisateurs, d'inspecter le contenu en temps réel, de simplifier la gestion des stratégies, d'activer un périmètre logique mais aussi de fournir un débit multi-gigabits.

Profil du consultant

Consultant formateur expert Palo Alto

Objectifs

A l'issue des cinq jours de formation, les stagiaires seront capables de :

- Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations
- Configurer et gérer des règles de sécurités 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

Ingénieurs sécurité, les administrateurs sécurité, les analystes en sécurité, les ingénieurs réseaux et membres d'une équipe de support.

Durée

5 jours

Prérequis

Les participants devront être familiers avec les concepts basics 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.

Méthode pédagogique de cette formation

La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions. Remise d'une documentation pédagogique papier ou numérique pendant le stage 6 à 8 personnes maximum par cours, éventuellement 1 poste de travail par stagiaire.

Méthode d’évaluation des acquis de la formation

Auto évaluation des acquis par le stagiaire via une questionnaire. Attestation de fin de stage signée remise au stagiaire en fin de formation

Programme de cette formation

Module 1 : Offre et architecture des produits Palo Alto Networks

Module 2 : Connexion et administration de la solution

Module 3 : Gestion des configurations

Module 4 : Gestion des comptes d’administrations sur la solution

Module 5 : Mise en place de la solution dans le réseau

Module 6 : Cycle de vie des attaques

Module 7 : Bloquer les menaces en utilisant les règles de sécurités et de NATs

Module 8 : Bloquer les attaques basées sur les paquets et les protocoles

Module 9 : Bloquer les menaces venant de sources connues

Module 10 : Bloquer les menaces par l’identification des applications

Module 11 : Maintenir les règles de sécurité basées sur les applications

Module 12 : Bloquer les menaces en utilisant les signatures applicatives personnalisées

Module 13 : Bloquer les menaces par l’identification des utilisateurs

Module 14 : Bloquer les menaces en identifiant les appareils

Module 15 : Bloquer les menaces inconnues

Module 16 : Bloquer les menaces dans le trafic chiffré

Module 17 : Prévenir le vol d’identifiant

Module 18 : Bloquer les menaces en utilisant les profils de sécurités

Module 19 : Observation du trafic et des menaces

Module 20 : Pour aller plus loin …