Formation Palo Alto Networks Firewall 9.0 Essentiels : Configuration et Management

★★★★★

SII-422 **5 Jours (35 Heures)**

Description

Cette formation officielle Palo Alto Networks "Firewalls 9.0 Essentials" vous apprend à configurer, manager et exploiter les firewalls Palo Alto Networks de nouvelle génération, ainsi que les étapes de configuration pour les fonctionnalités de sécurité, réseau, prévention des menaces, journalisation et génération des rapports dans l'environnement Pan-OS. Cette formation se déroule sur la version Pan-OS 9.0. La formation se déroule dans un centre de formation ATC officiel de l'éditeur.

À qui s'adresse cette formation ?

Pour qui

Ce cours s'adresse aux ingénieurs et administrateurs réseau et sécurité, aux analystes sécurité, administrateurs systèmes, ainsi qu'aux personnes en charge du support technique.

Prérequis

Connaissances basiques en administration réseau et sécurité réseau.

Les objectifs de la formation

- Configurer et manager les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelle génération
- Configurer et gérer GlobalProtect pour protéger des postes clients situés à l'extérieur du réseau de l'entreprise
- Configurer et manager la haute disponibilité des pare-feux Palo Alto Networks
- Monitorer le trafic réseau en utilisant les interfaces web interactives et les rapports intégrés

Programme de la formation

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