

Check Point R77, sécurité réseaux, niveau 1



PL-66 4 Jours (28 Heures)

Description

Cette formation vous fera découvrir les nouveautés apportées par la dernière mouture des produits Check Point, la version R77. A l'issue, vous serez capable de mettre en place et gérer une politique de sécurité, la translation d'adresses (NAT) ou encore le module Intrusion Prevention System (IPS).

À qui s'adresse cette formation ?

Pour qui

Technicien, administrateur et ingénieur systèmes/réseaux/sécurité.

Prérequis

Aucune

Les objectifs de la formation

- Installer et configurer Check Point R77
- Mettre en oeuvre une politique de sécurité
- Bloquer les intrusions avec SAM (Suspicious Activity Monitor)
- Mettre en oeuvre Check Point Mobile

Programme de la formation

Introduction

- Les produits Check Point.
- Les composants.
- Nouveautés de la version R77.

Fonctionnement et installation

- L'architecture en mode distribué et en standalone.
- Le serveur de management.
- Le protocole SIC.
- Présentation du système Gaia.
- L'interface en ligne de commandes (CLI).
- Les commandes de sauvegarde et de restauration.
- Travaux pratiques Installation de Check Point sous Gaia en version R77.

Mise en place d'une politique de sécurité

- Prise en main de SmartConsole.
- Démarrer et utiliser SmartDashboard.
- Gestion des administrateurs et des profils.
- Politique de sécurité.
- Gestion des règles.
- Travaux pratiques Installer SmartConsole.
- Créer des objets et une politique de sécurité.
- Activer l'anti-spoofing.

La translation d'adresses (NAT)

- Les règles de translation d'adresses.
- Le NAT "static" et le NAT "hide".
- Gestion de l'ARP.
- Travaux pratiques Mise en place de NAT automatique de type "hide", "static" et de règles de transaction manuelle.

Le monitoring et la gestion des logs

- La politique de gestion des logs.
- Suivre les connexions avec SmartView Tracker.
- Le SmartView Monitor, fonctionnalités et seuils d'alerte.
- Travaux pratiques Mise en place de NAT automatique de type "hide", "static" et de règles de transaction manuelle.

Authentification client R77

- Les anciens modes d'authentification.
- Identity Awareness.
- Application Control.
- Authentification : portail captif, Identity Agent, intégration Active Directory.
- Travaux pratiques Mise en place d'Identity Awareness.

Le VPN site à site et le VPN nomade

- L'architecture du VPN.
- Bases du chiffrement.
- Introduction IPSec, l'autorité de certification.
- L'autorité de certification (CA).
- Le Domain-Based VPN, le mode client lourd.
- Les modes d'authentification en Mobile Access : Check Point Mobile, SSL/SNX, .
- Travaux pratiques Mise en place d'un tunnel IPSec site à site.
- Configuration de l'accès distant en VPN IPSec.
- Activation et mise en place de Check Point Mobile.

Le module IPS

- Présentation.
- Vulnérabilités et failles de sécurité.
- Mise en application d'un profil de sécurité.
- Geo-Protection, inspection HTTPS.
- Autres modules : Data Leakage Prevention, QoS, .
- Travaux pratiques Exemple de protection contre les vulnérabilités avec le module IPS.