Check Point Security Administration R76 CCSA

Déscription :

Les produits de Check Point Software sont parmi les plus utilisés dans le monde de la sécurité. Cette introduction constitue un cours complet sur le Firewall Check Point, incluant la gestion de la politique de sécurité, la translation d'adresses (NAT), la mise à jour des systèmes, la mise en place des tunnels VPNs ou encore la sécurité de messagerie et de contenu.

Cette formation CheckPoint vous permettra de prendre en main l'administration au quotidien de la suite des produits de sécurité CheckPoint

Objectifs

- Ce cours fournit une compréhension des concepts de base et les compétences nécessaires pour configurer Check
- Point Software Blades : Filtrage IP, VPN IPSec, gestion des politiques, supervision, authentification, filtrage URL,
- antivirus & anti-malware, anti-spam & sécurité email, et IPS

Publics

Administrateur système et réseau, responsable sécurité

Durée

3 jours

Pré-requis

compétences sur TCP/IP et sur le routage statique. Connaissances des environnements Windows et Unix (Linux).

Programme de cette formation

Décrire l'approche unifiée de Check Point à la gestion du réseau, et les éléments clés de celui-ci

- Concevoir un environnement distribué
- Installez la gateway de sécurité dans un environnement distribué
- Depuis la ligne de commande, effectué un backup et restaurer l'installation
- Identifier les fichiers critiques nécessaires pour purger ou sauvegarder, importer et d'exporter les utilisateurs et les groupes et d'ajouter ou supprimer des administrateurs depuis la ligne de commande
- Déployer une gateway à l'aide de l'interface Web Gaia

Créer et configurer des réseaux, des hôtes et une gateway

- Vérifiez l'établissement de la SIC entre le Security Management Server et la gateway à l'aide SmartDashboard
- Créer les premières règles de base à partir de SmartDashboard qui inclut des autorisations pour les utilisateurs, les services externes et le réseau sortant
- Configurer des règles NAT sur le Web et les serveurs Gateway

Évaluer les politiques existantes et d'optimiser les règles en fonction des exigences actuelles de l'entreprise •

- Maintenir la Security Management Server avec les sauvegardes planifiées et les versions de règles de base en assurant la mise à jour sans interruption de service
- Utilisez des requêtes dans SmartView Tracker pour surveiller l'IPS, le trafic réseau et dépanner à l'aide de données collectées
- Utiliser les données collectées pour générer des rapports, dépanner les problèmes de sécurité et système et d'assurer le bon fonctionnement du réseau
- Utilisation SmartView Monitor, configurer des alertes et des compteurs de trafic, voir le statut d'un Gateway, contrôler les Suspicious Activity Rules, analyser l'activité des tunnels et contrôler l'accès des utilisateurs distants
- Surveillez les Gateways distants à l'aide SmartUpdate pour évaluer la nécessité de mises à jour, les nouvelles installations et les modifications de licence
- Utilisez SmartUpdate pour appliquer les packages de mise à niveau pour une ou plusieurs VPN-1 Gateways

Mettre à jour des licences des produits utilisant SmartUpdate

- Réaliser la gestion centralisée des utilisateurs afin de s'assurer que les personnes authentifiés accéder en toute sécurité au réseau d'entreprise localement ou à distance
- Gérer les accès des utilisateurs au réseau de l'entreprise à l'aide de bases de données externes
- Utilisez Identity Awareness pour fournir un accès de niveau granulaire aux ressources réseau
- Connaitre les informations utilisateur utilisés par le contrôleur d'accès Security Gateway
- Définir les rôles d'accès pour une utilisation dans une règle Identity Awareness
- Mettre en œuvre l'Identity Awareness dans les règles du Firewall
- Configurer un VPN de site à site avec une clé partagée
- Configurer les tunnels permanents pour l'accès distant aux ressources d'entreprise
- Configurer le partage du tunnel VPN, et donner les différences entre les tunnels host-based, subunit-based et gateway-based