EduGroupe
Accompagner pour réussir

CheckPoint Security Administration R82

Référence : **CHS-CCSAR82** Durée : **4 heures** Certification : **CCSA**

Connaissances préalables

- Avoir de bonnes connaissances de TCP/IP
- Avoir des connaissances de base en sécurité informatique.

Profil des stagiaires

- Techniciens, administrateurs et ingénieurs système/réseaux/sécurité

Objectifs

- Installer et configurer Check Point R82
- Déployer et gérer des politiques de sécurité
- Mettre en œuvre la translation d'adresses (NAT)
- Gérer les licences et les contrats
- Administrer des environnements multi-sites
- Contrôler les accès administratifs
- Superviser les logs et le trafic réseau
- Configurer l'inspection HTTPS et le support HTTP/3
- Appliquer le contrôle applicatif et le filtrage URL
- Mettre en œuvre des VPN et la prévention des menaces

Certification préparée

La certification est délivrée par Check Point Software Technologies. Elle valide les compétences fondamentales nécessaires pour administrer les solutions de sécurité Check Point. La durée est de 90 minutes et repose sur un QCM de 90 questions, en anglais.

Le coût de la certification n'est pas inclus dans le tarif de la formation, cette option à demander lors de votre inscription. Un voucher vous sera remis pour vous permettre de planifier votre passage.

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-formateur expert CheckPoint

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Introduction à l'architecture Check Point R82 : Configuration initiale

- Produits Check Point et nouveautés R82
- Présentation de Gaia OS
- Architecture trois-tiers, des Software Blades et Check Point Infinity
- Modes standalone vs distribué
- Présentation du protocole SIC
- CLI : interface en mode ligne de commandes
- La SmartConsole Web
- 💡 *Exercice : Installation de Gaia en R82 dans le serveur de management et la passerelle principale*

2. Gestion des politiques de sécurité

- Prise en main de SmartConsole R82
- Inspection des paquets
- Création d'objets et règles
- Politiques « Inline layers » (sous règles)
- 💡 *Exercice : Installation de SmartConsole. Créer des objets. Réaliser une politique de sécurité*

3. Translation d'adresses (NAT)

- NAT statique, dynamique, manuel
- Problématiques ARP et routage
- Mise en œuvre de règles NAT
- 💡 *Exercice : Mise en place de NAT automatique de type statique, Hide et règles de transaction manuelle*

4. Gestion des licences et des sites distants

- Types de licences et gestion via SmartUpdate
- Déploiement multi-sites et Policy Packages
- Ordered Layers et partage de politiques
- 💡 *Exercice : Installation d'une passerelle distante, création d'une politique de sécurité (Policy Pack), et de règles de base pour le site distant. Création et partage d'une « Ordered Layer »*

5. Gestion d'administrateurs

- Profils de permissions
- Sessions concurrentes et gestion des administrateurs
- 💡 *Exercice : Création d'un nouveau « Permission Profile » avec des autorisations limitées*

6. Logs, monitoring et dépannage

- Suivi des connexions et alertes
- Outils de monitoring (CPView, SmartView Monitor)
- Introduction au troubleshooting (tcpdump, zdebug)

7. Inspection HTTPS. Contrôle applicatif, filtrage URL et maintenance

- Règles Outbound/Inbound
- Gestion des certificats et SNI
- Fonctionnalités avancées de l'inspection HTTPS
- App Control, URL Filtering, DNS Filtering. Le « User Check »
- Sauvegardes (locales et cloud), CPUSE, mises à jour. La commande cpconfig
- 💡 *Exercice : Mise en oeuvre de l'inspection HTTPS.Filtrage Web et Applications : créer et partager la politique de « Filtrage Web et Applications » en tant que « Inline Layer » et « Ordered Layer ». Restauration de la configuration d'une passerelle*

8. VPN site-à-site, prévention des menaces et haute disponibilité

- Architecture VPN, IKE/IPSec, routage VPN
- ClusterXL et redondance (bonus)
- 💡 *Exercice : Utilisation de VPN-IPSec Inter-sites (Shared Secret) et VPN-IPSec Inter-sites (Certificats)*

9. Prévention des menaces

- Autonomous Threat Prevention (IA, ThreatCloud)
- 💡 *Exercice : Mise en place d'Autonomous Threat Prevention*

10. Clustering

- ClusterXL et redondance
- 💡 *Exercice : Mise en œuvre de ClusterXL en mode HA*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.