

# Check Point Certified Security Administrator CCSA R81- Préparation à la certification

**Prix** : 2 990 € HT

**Durée** : 4 jours

**Code de Référence** : SCCSA81

Cette formation Check Point vous permettra d'acquérir l'ensemble des techniques et des méthodologies nécessaires au passage de l'examen pour l'obtention de la certification CCSA R81.

## Objectifs de la formation

- Installer et configurer le produit Check Point R81.20
- Déployer une politique de sécurité et surveiller le trafic
- Mettre en œuvre la translation d'adresse (NAT)
- Maîtriser la gestion de licences
- Déployer des sites distants et partager les politiques de sécurité
- Maîtriser la gestion d'administrateurs
- Maîtriser la visualisation des logs et le monitoring
- Mettre en œuvre le déchiffrement HTTPS
- Maîtriser la visualisation des logs et le monitoring
- Mettre en œuvre le déchiffrement HTTPS
- Mettre en œuvre le contrôle applicatif et le filtrage URL
- Connaître les différentes méthodes de sauvegarde et de mise à niveau
- Gérer les déploiements VPN site à site
- Comprendre la politique d'Autonomous Threat Prevention
- BONUS : Mettre en œuvre un cluster en haute disponibilité
- Préparer l'examen officiel menant à la certification CCSA

## Public

Cette formation s'adresse aux techniciens, administrateurs et ingénieurs système, réseau et sécurité.

## Prérequis

Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.

## Programme de la formation

## **Présentation de l'architecture Check Point R81.20**

- Les produits Check Point
- Nouveautés de la version R81, R81.10 et R81.20

## **Déploiement Gaia : Installation des « appliances » Check Point**

- Présentation du système Gaia
- Eléments de l'architecture trois-tiers
- Architecture modulaire des "Software Blades"
- Check Point Infinity
- L'architecture en mode distribué et en mode standalone
- Le serveur de management. Le protocole SIC

### Travaux pratiques

- Installation de Check Point R81.20

## **Gestion du Security Management Server avec l'outil de gestion unifié « Smart Console » : communication avec le protocole SIC et Gestion des objets**

- Prise en main de SmartConsole R81.20
- Politique de sécurité. Gestion des règles
- Politiques Unifiées
- Inspection des paquets
- « Inline » Polices (sous règles)

### Travaux pratiques

- Installation de SmartConsole. Créer des objets. Réaliser une politique de sécurité. Activer l'anti-spoofing

## **Translation d'adresses (NAT)**

- Les règles de translation d'adresses avec IPv4 et IPv6
- Le NAT statique (One To One NAT) et le NAT dynamique (.Many To One NAT)/PAT
- Le NAT Manuel
- La problématique ARP et le routage.

### Travaux pratiques

- Mise en place de NAT automatique de type statique, Hide et règles de transaction manuelle

## **Gestion des licences**

- Structure de licences
- Gestion de licences dans SmartUpdate et SmartConsole
- Types de licences
- Gestion de contrats et services
- Monitoring le statut de licences

## **Gestion Multi-Sites**

- Définition de Policy Packages
- Gestion de Policy Packages
- Définition et types de “Layers”
- Inspection des packets dans une « Ordered Layer »
- Partage de « Layers » (Policy Layers Sharing)

### **Gestion Multi-Sites**

- Définition de Policy Packages
- Gestion de Policy Packages
- Définition et types de “Layers”
- Inspection des packets dans une « Ordered Layer »
- Partage de « Layers » (Policy Layers Sharing)

### Travaux pratiques

- 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 »

### **Gestion d’administrateurs**

- « Permission Profiles »
- Limiter la portée d’action des administrateurs
- Gestion des utilisateurs concurrents
- Gestion des sessions

### Travaux pratiques

- Création d’un nouveau « Permission Profile » avec des autorisations limitées

### **Logs & monitoring**

- La politique de gestion des logs.
- Suivre les connexions avec LOGS & MONITOR (ancien SmartView Tracker).
- l’outil « Monitor »
- Gestion de Logs
- Le SmartView Monitor, fonctionnalités et seuils d’alerte.
- Serveur de logs dédié

### Travaux pratiques

- Activation du monitoring, utilisation du Suspicious Activity Monitoring Protocol, visualisation du trafic, monitoring de l’état de la politique de sécurité.
- Introduction à Troubleshooting : Accéder au mode « expert », utilisation des commandes « tcpdump » et « fw ctl zdebug drop », visualiser et manipuler les utilitaires « CPView » et « Top »
- Ajout d’un serveur de logs dédié

### **Déchiffrement-HTTPS**

- Création des règles
- Gestion de certificats

- Server Name Indications (SNI)

### Travaux pratiques

- Mise en œuvre de l'inspection HTTPS

### **Contrôle Applicatif / Filtrage URL**

- Les limites d'un firewall classique par IP et par port
- Le contrôle d'accès
- Le « AppWiki ». L'URL Filtering
- Le "User Check"

### Travaux pratiques

- Filtrage Web et Applications : créer et partager la politique de « Filtrage Web et Applications » en tant que « Inline Layer » et « Ordered Layer »

### **Sauvegardes et Maintenance**

- Méthodes de Sauvegarde
- Présentation de CPUSE
- Mise à jour/niveau centralisé des passerelles
- La commande **cpconfig**

### Travaux pratiques

- Restauration de la configuration d'une passerelle.

### **VPN IPSEC site to site**

- L'architecture du VPN. Les bases du chiffrement
- Introduction à IKE et IPSec
- L'autorité de certification (CA). Le Domain-Based VPN
- Mode Simplifié. Configuration des communautés VPN
- Routage VPN

### Travaux pratiques

- VPN-IPSec Inter-sites (Shared Secret)
- VPN-IPSec Inter-sites (Certificats)

### **Autonomous « Threat Prevention »**

- La politique de Threat Prevention et ses « Software Blades »
- Custom et Autonomous Threat Prevention
- Profils de sécurité
- Technologies utilisées par Autonomous Threat Prevention

### Travaux pratiques

- Mis en place d'Autonomous Threat Prevention

## **BONUS : HA avec ClusterXL**

- La redondance des firewalls
- Le ClusterXL High Availability (Actif/Passif)
- VMAC et les problématiques d'ARP

### Travaux pratiques

- Mise en œuvre de ClusterXL en mode High Availability

## **Méthodes pédagogiques**

Des exercices pratiques et des démonstrations vous permettront de mettre en pratique les notions théoriques présentées.

## **Méthodes d'évaluation des acquis**

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.