# Check Point Certified Security Expert CCSE R81 – Préparation à la certification

**Prix** : 2 390 €HT

**Durée** : 3 jours

**Code de Référence** : SCCSE81

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 CCSE R81.

## Objectifs de la formation

- Utiliser les APIs pour créer des objets et règles de base.
- Effectuer les mises à niveau.
- Expliquer les principaux processus sur les serveurs de gestion de la sécurité et les passerelles de sécurité.
- Comprendre le flux d'installation de la politique, les fichiers utilisés et l'installation de la politique accélérée.
- Décrire la manière dont les technologies coreXL et secureXL améliorent et optimisent les performances des passerelles de sécurité.
- Gérer les déploiements VPN avec le routage « Domain Based ».
- Gérer les accès distants VPN avec les options proposées par le blade « Mobile Access » : IPSec et SSL
- Décrire les composants de SmartEvent et leurs options de déploiement . configurer une « Event Policy »
- Mettre en œuvre le déchiffrement HTTPS.
- Gérer l'authentification d'utilisateurs.
- Mettre en œuvre un cluster en haute disponibilité.
- Préparer l'examen officiel menant à la certification CCSE

## Public

Cette formation s'adresse aux techniciens, administrateurs et ingénieurs système, réseau et sécurité avec un niveau CCSA requis.

## Prérequis

Bonnes connaissances de TCP/IP, de la sécurité des SI et des principales fonctions de Check Point ou avoir suivi le stage « CCSA, Check Point Certified Security Administrator R81 »

## Programme de la formation

**Gaia avancée & API**

- Gaia en ligne de commandes
- Présentation de l'API
- Créer des objets et règles via l'API

Travaux pratiques

- Installation du SMS et des GWs en R80.40
- Utilisation de l'API pour créer des objets et règles de base

**Mise à niveau de Gaia**

- Methodes de mise à niveau de Gaia
- Mise à jour/niveau centralisé des passerelles

Travaux pratiques

- Mise à niveau avancée du Management de R80.40 vers R81.20
- Clish
- Mise à niveau centralisée de la passerelle principale.

**Les processus Check Point**

- Principaux processus Check Point
- Commandes pour visualiser les processus Check Point
- Les scripts et les « SmartTasks »

Travaux pratiques

- Configure SmartTasks

**Installation de la politique de sécurité**

- Processus d'installation de la politique de sécurité
- Installation Accélérée
- Policy Packages & Layers
- Objets Dynamiques
- Updatable Objects

Travaux pratiques

- Vérification des fichiers d'installation
- Création des objets dynamiques

**SecureXL & CoreXL**

- L'accélération SecureXL et ses templates
- Commandes de SecureXL
- CoreXL et SND (Secure Network Distributor)
- CoreXL Affinity
- Dynamic Balancing

- Multi-Queue
- Le CoreXL Dynamic Dispatcher
- Priority Queues (PrioQ)

**Routage VPN (Domain Based)**

- Domain Based & Routed Based VPN
- Configuration du domaine VPN
- Les communautés VPN
- Configuration du routage VPN (« Domain-based »)
- Wire Mode
- Méthodes d’authentification

Travaux pratiques

- Mise en place du Routage VPN (Domain-Based)

**Accès Distant**

- Le VPN SSL et le VPN IPSec
- Le Blade Mobile Access
- Mobile Access du type : « Remote Access »
- Mobile Access SSL : Clientless Applications & Native Applications. SSL Network Extender (SNX). Portail « Check Point Mobile »
- Les clients VPN couche 3

Travaux pratiques

- Mise en place d´une connexion VPN de type « Remote Access » via le client « Check Point Mobile »
- Mise en place d´une connexion VPN de type « Remote Access » via le client « Check Point Mobile » pour des utilisateurs « Active Directory »
- Mise en place d´une connexion VPN de type « Mobile Access SSL »

**Logs, monitor et reporting avancés**

- Présentation de l’onglet Logs & Monitor
- SmartEvent
- Compliance
- SmartEvent GUI Client
- Suspicious Activity Monitoring (SAM)

Travaux pratiques

- Configuration de SmartEvent

**Déchiffrement-HTTPS**

- Création des règles
- Gestion de certificats
- Server Name Indications (SNI)

Travaux pratiques

- Mise en œuvre de l’inspection HTTPS

**Politique à base d’utilisateurs**

- Besoin de récupérer l’identité des utilisateurs
- Les méthodes d’authentification Identity Awareness R81.20
- Les objets de type « Access Role »

Travaux pratiques

- Authentification : mise en place d’Identity Awareness, création de rôles et des accès.

**Custom-Threat-Prevention**

- La politique de Threat Prevention et ses « Software Blades »
- Gestion des règles
- Profils de sécurité

Travaux pratiques

- Anti-Virus et Anti-Bot

**Clustering**

- La redondance des firewalls
- Le ClusterXL High Availability (Actif/Passif)
- Le ClusterXL Load Sharing
- Load Sharing Multicast
- Le ClusterXL High Availability (Actif/Actif)
- VMAC et les problématiques d’ARP
- La haute disponibilité du Management Server

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.