

# Check Point R81.20 – Sécurité Réseau, niveau 2

**Prix** : 2 390 € HT

**Durée** : 3 jours

**Code de Référence** : SCSR12

Cette formation Check Point vous permettra d'acquérir l'ensemble des techniques et des méthodologies nécessaires à l'installation et la gestion de Check Point niveau 2.

## 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
- Expliquer les opérations du « Kernel » et monitorer le flux de trafic interne.
- Décrire la manière dont les technologies coreXL et secureXL améliorent et optimisent les performances des passerelles de sécurité
- Gérer les déploiements VPN avancés (Route 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 »
- Gestion avancée des utilisateurs et l'outil « Identity Collector »
- Mettre en œuvre un cluster en haute disponibilité
- BONUS : Mettre en œuvre le filtrage de données

## 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, avoir suivi la formation niveau 1 ou la formation « CCSA, Check Point Certified Security Administrator R81 » ou disposer de compétences équivalentes.

## 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**

- Méthodes 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

## **Kernel operations & Traffic flow**

- Circulation des paquets à l'intérieur de la passerelle.
- Chaînes de modules
- L'outil « fw monitor »
- Management Data Plane Separation (MDPS)

## Travaux pratiques

- Utilisation de l'outil « fw monitor»

## **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)

## **VPN et Routage Avancé (Routed Based)**

- Le routage VPN
- Les modes de routage VPN
- Avantages du « Routed Based » VPN
- VTI : Virtual Tunnel Interfaces
- Protocoles supportés pour le routage dynamique VPN
- Wire Mode
- Directional VPN

## Travaux pratiques

- Mise en place de tunnels « route-based » avec du routage statique.
- Mise en place de tunnels « route based » avec du routage dynamique (OSPF)

## **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

#### **Gestion avancée des utilisateurs/Identity Collector**

- Les types d'authentification
- Problèmes de connexion AD avec AD Query
- Identity Collector
- Identity Awareness en ligne de commande

#### Travaux pratiques

- Installation et mise en œuvre d'Identity Collector
- Mise en œuvre des commandes de debug d'Identity Awareness

#### **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

#### **Filtrage de données avec la Software Blade « Content Awareness »**

- Introduction de Content Awareness
- Type d'objets utilisés pour le filtrage de données

#### Travaux pratiques

- Activation de Content Awareness
- Test de Content Awareness
- Ajout d'un message UserCheck

## 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.