Check Point Certified Security Expert CCSE R82 – Préparation à la certification

Prix : 2 850 €HT

Durée : 4 jours

Code de Référence : SCCSE82

Catalogue Check Point

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 R82.

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.
- Utilisation de « **Dynamic Layer** » afin d'ajouter des objets et règles directement sur la passerelle à l'aide de l'appel de l'API Gaia : « **set-dynamic-content** ».
- Gérer les déploiements VPN avec le routage « Domain Based ».
- Décrire les composants de SmartEvent et leurs options de déploiement . configurer une « Event Policy »
- Mettre en œuvre un cluster ElasticXL pour garantir une haute disponibilité et un équilibrage de charge.
- 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 R82 »

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 R81.20*
- *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 R81.20 vers R82*
- *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
- NAT Statique pour le Serveur de Management (SMS behind the NAT)
- Nouvelles fonctionnalités du NAT Statique pour le SMS et passerelles
- Objets Dynamiques
- Updatable Objects
- Présentation du concept de « **Dynamic Layer** »
- Communication avec la passerelle en utilisant l'API Rest.
- Utilisation du Gaia API « call », « **set-dynamic-content** »

Travaux pratiques

- *Vérification des fichiers d'installation*
- *Création des objets dynamiques*
- *Utilisation du « **Dynamic Layer** » pour créer des objets et règles directement dans le firewall principal.*

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)
- Acceleration Hyperflow pour les connections SMB/CIFS/QUIC

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
- Sélection de multiples liens (Enhanced Link Selection)
- Utilisation du nouvel objet « Network Probe » afin de surveiller l’état des tunnels VPN.

Travaux pratiques

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

Logs, monitor et reporting avancés

- Présentation de l’onglet Logs & Monitor
- SmartEvent
- Compliance
- SmartEvent GUI Client
- Suspicious Activity Monitoring (SAM)
- Introduction du nouvel outil “ConnView”

Travaux pratiques

- *Configuration de SmartEvent*

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
- Cluster ElasticXL

Travaux pratiques

- *Mise en oeuvre de « Load Sharing » au travers d’ElasticXL*

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.