Formation **Check Point Certified Security Expert R81**

Réussir l'examen de certification CCSE

A l'issue de cette formation avancée CCSE, les stagiaires ont acquis une compréhension approfondie de la technologie Check Point ainsi que les compétences nécessaires pour concevoir, maintenir, optimiser et protéger efficacement leur réseau d'entreprise contre les cybermenaces. Le passage de l'examen de certification CCSE est inclus dans le prix de la formation.

Durée

3 jours

Objectifs pédagogiques

- Sauvegarder le R81 Security Gateway and Management Server
- Construire, tester et dépanner une Security Gateway en cluster
- Mettre à niveau et dépanner le Management Server
- Configurer et maintenir les solutions d'accélération de la sécurité
- Gérer, tester et optimiser des tunnels VPN d'entreprise
- Se préparer efficacement au passage de la certification officielle CCSE

Public

Ingénieurs, techniciens et administrateurs systèmes et réseaux, RSSI.

Prérequis

Avoir suivi notre formation CCSA et être titulaire de la certification CCSA. Bonnes connaissances sur les systèmes Windows Server, UNIX ainsi que sur les technologies réseaux et Internet.

Programme de formation

Introduction à la formation CCSE

Présentation générale de la formation CCSE
Le cursus de certifications Check Point

Thèmes abordés

Le service de mise à niveau et les options disponibles
Mise à niveau et migration du serveur de gestion
Les fonctionnalités CPUSE
L'intérêt de Management High Availability
Primary vs Secondary, Active vs Standby et la synchronisation
Les étapes de la reprise après sinistre en cas d'indisponibilité du serveur primaire
Vue d'ensemble de Central Deployment dans la SmartConsole
Les méthodes de mise à niveau du cluster Security Gateway
Les mises à niveau de Multi Version Cluster (MVC)
Les commandes Gaia et leur utilisation

Les scripts et SmartTasks pour configurer des actions automatiques
Management Data Plane Separation (MDPS)
Opérations kernel et flux de trafic
Les objets Dynamic et Updatable dans les Security Gateways
Flux et fichiers pour l'installation de la politique de sécurité
Utilisation de l'historique d'installation de la politique
La politique d'installation simultanée et accélérée
Vue d'ensemble des APIs et moyens d'utilisation et d'authentification
Changements dans Gaia et dans la configuration de la gestion
Installation d'une politique avec l'API
Comment les technologies d'accélération SecureXL et CoreXL améliorent et optimisent les performances de Security Gateway
Utilisation de plusieurs files d'attente pour rendre le traitement du trafic plus efficace
Les bases d'un VPN site-to-site, déploiement et communautés
Analyse et interprétation du trafic des tunnels VPN
Les options Link Selection et ISP Redundancy
Les fonctionnalités de gestion des tunnels
Les différentes solutions Check Point Remote Access
Comment la sécurité du client peut être assurée par Remote Access
Les méthodes d'authentification
Multiple Entry Point (MEP)
La Mobile Access Software Blade et comment elle sécurise la communication et l'échange de données pendant les connexions distantes
Les options de déploiement de Mobile Access
Les fonctionnalités de Mobile Access : Portal, Link Translation, exécution d'applications natives, Reverse Proxy...
Concepts de base de Clustering et ClusterXL
Cluster Control Protocol (CCP) et synchronisation
Fonctions et modes avancés de ClusterXL : Load Sharing, Active-Active, mode VMAC...
La Cluster Correction Layer (CCL)
Logs et monitoring
Comment déterminer si la configuration est conforme aux meilleures pratiques
Comment définir les actions à entreprendre pour respecter la conformité
Identification des problèmes de sécurité critiques avec les fonctions SmartEvent
Les composants de SmartEvent et leurs options de déploiement
Comment SmartEvent peut aider à signaler les menaces de sécurité
Personnalisation des définitions d'évènements et définition d'une Event Policy

Exercices pratiques réalisés pendant la formation

Préparer la mise à niveau du Security Management Server
Mettre à niveau le Security Management Server
Déployer un Security Management Server secondaire
Configurer un serveur de logs distribué
Mettre à niveau une Security Gateway depuis la SmartConsole
Travailler avec la ligne de commande
Utiliser les scripts et SmartTasks
Configurer les objets dynamiques
Surveiller le trafic
Vérifier l'installation et le statut de la politique
Travailler avec Gaia et les APIs de management
Utiliser les fonctions d'accélération
Configurer un VPN site à site en local
Configurer un VPN site à site avec un Interoperable Device
Configurer un VPN Remote Access
Configurer un VPN Mobile Access
Configurer un cluster de haute disponibilité
Travailler avec ClusterXL
Configurer la conformité aux politiques
Déployer SmartEvent

Modalités d’évaluation

Nombre de questions : 90
Type de questions : QCM, basées sur des scénarios de situations réelles
Score requis : 70% de bonnes réponses