



Formation Upgrade Check Point Security Administrator R71 [3 jours]

Durée : 3 jours

Objectifs : Ce cours vise un public ayant déjà de l'expérience sur les produits Check Point (idéalement R65), souhaitant se mettre à jour sur la dernière version de la suite Check Point R71. Il met l'accent sur les nouveautés des versions R70 et R71 en ne revenant pas sur les chapitres fondamentaux.

Public visé : administrateurs systèmes, architectes réseaux, responsables de la sécurité des systèmes d'informations, consultants sécurité. Expérience sur d'anciennes versions de Check Point.

Prérequis : compétences sur TCP/IP et sur le routage statique. Connaissances des environnements Windows et Unix (Linux).

Tarif : 2100 € H.T.

Certification : ce cours prépare à la certification CCSA R71 (Check Point Certified Security Administrator).

Avis d'expert : les produits de Check Point Software sont parmi les plus utilisés dans le monde de la sécurité. Cette introduction constitue un cours complet sur le Firewall Check Point, incluant la gestion de la politique de sécurité, la translation d'adresses (NAT), la mise à jour des systèmes, la mise en place des tunnels VPNs ou encore la sécurité de messagerie et de contenu.

Objectifs du cours

Préface : Check Point Security Administration R71

Plan du cours
Mise en place recommandée pour les labs
Formation et certification Check Point
CCMA

1 Plateformes de déploiement

- Boitiers UTM-1 Edge
- Boitiers Power-1
- Boitiers IP
- IP Network Voyager
- IPSO
- Système de fichiers et structure des répertoires dans IPSO
- Commandes de premier niveau
- Secure Platform
- Sauvegarde et restauration
- Fichiers de logs
- Objects.C et Objects_5_0.C
- Shell de commande sous Secure Platform
- Commandes Check Point
- Commandes de diagnostic réseau
- Travaux Pratiques
- Révision

2 Utilisation de Smart Update

- Smart Update et la gestion des licences
- Processus d'attachement des licences
- Contrats de service
- Obtention d'une clé de licence
- Packages d'installation logicielle
- Mise à jour de la passerelle
- Smart Update en ligne de commande
- Travaux Pratiques
- Révision

3 Mise à jour vers R71

- Compatibilité de pré-installation
- Compatibilité descendante pour les passerelles
- Mise à jour du Security Management Server
- Mise à jour de la Security Gateway
- Mise à jour d'un cluster
- Travaux Pratiques
- Révision

4 Chiffrement et Réseaux Privés Virtuels

- Sécurisation des communications
- Chiffrement symétrique
- Chiffrement asymétrique
- Diffie-Hellman
- Intégrité
- Authentification

IKE

Phase 1

Phase 2

Chiffrement en mode tunneling

Autorités de certification

Internal Certificate Authority

Travaux Pratiques

Révision

5 Introduction aux Réseaux Privés Virtuels

Le VPN selon Check Point

VPN en site à site

VPN en accès distant

Communautés VPNs

Authentification entre les membres de la communauté

VPNs basés sur le domaine et sur la route

Services exclus

Intégration des VPNs à la base de règles

VPNs en mode simplifié vs mode traditionnel

Tunnels VPN permanents

Partage des tunnels VPN

Etablissement d'une connexion entre un utilisateur distant et une passerelle

Travaux Pratiques

Révision

6 Sécurité de contenu et de la messagerie

Protection antivirale

Scan de sécurité de contenu en pratique

Reconnaissance du type de fichier

Limitations de taille de fichier et scan

Filtrage d'URLs de base

Antispam et messagerie

Rapport des faux positifs à Check Point

Travaux Pratiques

Révision