



Formation Check Point Security Administrator R71 [5 jours]

Durée : 5 jours

Objectifs : prendre en main l'administration au quotidien de la suite des produits de sécurité Check Point R71.

Public visé : administrateurs systèmes, architectes réseaux, responsables de la sécurité des systèmes d'informations, consultants sécurité.

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

Tarif : 3250 € 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 Aperçu des technologies Check Point

- Contrôle d'accès réseau
- Le Firewall Check Point
- Architecture d'inspection de la Security Gateway
- Composants de SmartConsole
- Gestion des utilisateurs dans Smart Dashboard
- Sécurisation des canaux de communication
- Travaux Pratiques
- Révision

2 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

3 Introduction à la politique de sécurité

- Bases de la politique de sécurité
- Gestion des objets dans Smart Dashboard
- Concepts de base des règles
- Règles implicites/explicites
- Compréhension de l'ordre des règles
- Gestion de politique et contrôle des révisions
- Implémentation du Database Revision Control
- Translation d'adresses réseau (NAT)
- NAT de type Hide
- NAT de type Static
- Configuration automatique de la NAT
- NAT en mode manuel
- Travaux Pratiques
- Révision

4 Monitoring du trafic et des connexions

- SmartView Tracker
- Types de logs
- Audit de l'administrateur
- Blockage des connexions
- SmartView Monitor
- Monitoring des règles d'activités suspectes
- Monitoring des alertes
- Travaux Pratiques
- Révision

5 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

6 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

7 Gestion des utilisateurs et authentification

- Création d'utilisateurs et de groupes dans Smart Dashboard
- Introduction aux méthodes d'authentification
- Schémas d'authentification
- Authentification de type User
- Authentification de type Session
- Authentification de type Client
- Résolution des conflits d'accès
- Gestion des utilisateurs sous LDAP avec Smart Directory
- Groupes Smart Directory
- Travaux Pratiques
- Révision

8 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

9 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

10 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