



## Formation Check Point Security Administrator Accelerated R70 [ 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 R70. Il met l'accent sur les nouveautés de la R70 en ne revenant pas sur les chapitres fondamentaux (colorés en rouge).

**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 R70 (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. Ce cours d'upgrade vous familiarisera par exemple avec le nouveau module d'IPS, ou avec la création de Virtual Private Networks (VPN). Vous interviendrez dans une nouvelle architecture de labs totalement virtualisée, et aurez à gérer votre propre réseau de bout en bout. Ce cours vous offrira également un descriptif complet du nouveau schéma de commercialisation basée sur des lames logicielles (« software blades ») qui permettent de construire une solution de sécurité à la carte.

<b>Objectifs du cours</b> .....	<b>xiii</b>
<b>Préface : Check Point Security Administration R70</b> .....	<b>1</b>
Plan du cours .....	2
Mise en place recommandée pour les labs .....	3
Formation et certification Check Point.....	6
CCMA.....	6
<b>1 Aperçu des technologies Check Point</b> .....	<b>7</b>
Contrôle d'accès réseau.....	9
Le Firewall Check Point.....	11
Architecture d'inspection de la Security Gateway .....	17
Composants de SmartConsole .....	25
Gestion des utilisateurs dans Smart Dashboard .....	39
Sécurisation des canaux de communication .....	43
Révision .....	51
<b>2 Architecture des Software Blades</b> .....	<b>53</b>
Architecture des Software Blades de Check Point .....	54
Sélection de votre Software Blade .....	57
Les conteneurs de Software Blades.....	62
Security Gateway R70.....	75
Révision .....	84
<b>3 Plateformes de déploiement</b> .....	<b>85</b>
Boîtiers UTM-1 Edge .....	85
Boîtiers Power-1 .....	87
Boîtiers IP.....	91
IP Network Voyager .....	94
IPSO.....	94
Système de fichiers et structure des répertoires dans IPSO .....	101
Commandes de premier niveau .....	113
Secure Platform .....	120
Sauvegarde et restauration .....	126
Génération d'un CPInfo.....	132
Fichiers de logs .....	133
Objects.C et Objects_5_0.C.....	134
Shell de commande sous Secure Platform .....	139
Commandes Check Point.....	145
Commandes de diagnostic réseau .....	148
Révision .....	153

<b>4 Introduction à la politique de sécurité .....</b>	<b>155</b>
Bases de la politique de sécurité.....	158
Gestion des objets dans Smart Dashboard.....	159
Concepts de base des règles.....	166
Règles implicites/explicites.....	170
Compréhension de l'ordre des règles.....	179
Gestion de politique et contrôle des révisions .....	182
Implémentation du Database Revision Control .....	192
Translation d'adresses réseau (NAT).....	195
NAT de type Hide.....	197
NAT de type Static .....	199
Configuration automatique de la NAT .....	201
NAT en mode manuel .....	208
Révision .....	339
<b>5 Monitoring du trafic et des connexions .....</b>	<b>217</b>
SmartView Tracker.....	219
Types de logs.....	220
Audit de l'administrateur.....	228
Blockage des connexions.....	233
SmartView Monitor.....	235
Monitoring des règles d'activités suspectes .....	244
Monitoring des alertes.....	244
Eventia Reporter .....	250
Considérations liées à Eventia Reporter .....	257
Licence de l'Eventia Reporter .....	260
Révision .....	261
<b>6 Utilisation de Smart Update .....</b>	<b>263</b>
Smart Update et la gestion des licences .....	265
Processus d'attachement des licences .....	269
Contrats de service .....	278
Obtention d'une clé de licence .....	284
Packages d'installation logicielle .....	286
Mise à jour de la passerelle.....	287
Smart Update en ligne de commande .....	289
Révision .....	291
<b>7 Mise à jour vers R70.....</b>	<b>293</b>
Compatibilité de préinstallation .....	295
Compatibilité descendante pour les passerelles .....	297

Notes importantes de mises à jour pour R70 .....	298
Installation en mode distribué.....	302
Mise à jour du Security Management Server .....	304
Mise à jour de la Security Gateway.....	306
Mise à jour d'un cluster .....	306
Révision .....	307

## **8 Gestion des utilisateurs et authentification ..... 309**

Création d'utilisateurs et de groupes dans Smart Dashboard .....	311
Introduction aux méthodes d'authentification .....	313
Schémas d'authentification .....	315
Authentification de type User .....	319
Authentification de type Session .....	326
Authentification de type Client.....	328
Résolution des conflits d'accès .....	335
Gestion des utilisateurs sous LDAP avec Smart Directory.....	337
Groupes Smart Directory.....	347
Révision .....	349

## **9 Chiffrement et Réseaux Privés Virtuels ..... 351**

Sécurisation des communications.....	353
Chiffrement symétrique .....	354
Chiffrement asymétrique .....	356
Diffie-Hellman.....	356
Intégrité .....	358
Authentification.....	359
IKE .....	363
Phase 1 .....	364
Phase 2.....	365
Chiffrement en mode tunneling .....	369
Autorités de certification .....	371
Internal Certificate Authority .....	375
Révision .....	377

## **10 Introduction aux Réseaux Privés Virtuels ..... 379**

Le VPN selon Check Point .....	381
VPN en site à site.....	383
VPN en accès distant.....	383
Communautés VPNs.....	387
Authentification entre les membres de la communauté.....	395
VPNs basés sur le domaine et sur la route .....	396
Services exclus .....	400
Intégration des VPNs à la base de règles .....	401

VPNs en mode simplifié vs mode traditionnel .....	403
Tunnels VPN permanents .....	404
Partage des tunnels VPN .....	407
Etablissement d'une connexion entre un utilisateur distant et une passerelle.....	410
Révision .....	415
<b>11 Sécurité de contenu et de la messagerie .....</b>	<b>417</b>
Protection antivirus.....	419
Scan de sécurité de contenu en pratique .....	423
Reconnaissance du type de fichier .....	429
Limitations de taille de fichier et scan.....	432
Filtrage d'URLs de base.....	435
Antispam et messagerie.....	437
Rapport des faux positifs à Check Point.....	442
Révision .....	446
<b>12 L'IPS Check Point .....</b>	<b>447</b>
Principes généraux de l'IPS .....	449
Gestionnaire d'évènements de l'IPS .....	455
Protection IPS .....	460
Profils IPS .....	462
Export de la liste des protections .....	468
Activation automatique des protections.....	473
Activation manuelle des protections .....	476
Exceptions réseaux.....	478
Optimisations de l'IPS .....	482
Gestion des souscriptions IPS .....	489
Révision .....	492
<b>Appendice A : shell de commande Secure Platform .....</b>	<b>493</b>
Commandes de gestion .....	494
Commandes de documentation .....	495
Commandes systèmes.....	496
Commandes de diagnostic système.....	497
Commandes Check Point.....	498
Commandes de configuration réseau.....	502
Révision .....	505
<b>Appendice B : sécurité de contenu intégrée avec OPSEC .....</b>	<b>507</b>
Security Servers.....	508
Configuration de la sécurité de contenu.....	519

Création et utilisation d'une Resource.....	520
Configuration du CVP pour la performance Web .....	523
Configuration du filtrage URL – UFP Server .....	524
Inspection UFP/CVP sur n'importe quel service TCP.....	528