



Formation Check Point Security Expert R70 [5 jours]

Durée : 5 jours

Objectifs : Configurer et administrer des solutions avancées de la suite des produits de sécurité Check Point R70.

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). Avoir suivi le cours CCSA R70, avoir la certification ou disposer d'un niveau équivalent.

Tarif : 3100 € H.T.

Certification : ce cours prépare à la certification CCSE R70 (Check Point Certified Security Expert).

Avis d'expert : les produits de Check Point Software sont parmi les plus utilisés dans le monde de la sécurité. Ce cours de niveau deux constitue un cours complet sur Firewall-1 incluant de nombreuses options de configuration avancées (Routage Avancé, QoS, Redondance et Haute Disponibilité des liens, VPN SSL...). Il apporte également un descriptif complet de toutes les nouvelles applications et solutions apparues avec la version R70 du produit et ses fameuses lames logicielles (« software blades ») qui permettent de construire une solution de sécurité à la carte.

Préface : Check Point Security Expert R70.....	1
Plan du cours	2
Mise en place recommandée pour les labs	3
Formation et certification Check Point.....	10
CCMA.....	10

1 Management Portal	11
Administration Web	12
Déploiement sur un serveur dédié.....	12
Déploiement sur un Security Management Server.....	13
Les commandes et la configuration du Management Portal.....	13
Pré-requis côté client.....	14
Révision	17
2 SmartWorkflow	19
Introduction à SmartWorkflow	20
L'environnement SmartWorkflow	20
Task Flow.....	21
La barre d'outils SmartWorkflow	24
La fenêtre de gestion des sessions.....	25
Information sur les sessions.....	28
Assigner des permissions	30
Activer SmartWorkflow	31
Configurer SmartWorkflow	31
Travailler avec des sessions	33
Comparer les politiques de sécurité	37
Approuver les sessions	39
Auditer les changements.....	41
Révision	43
3 SmartProvisioning	45
Tour d'horizon de SmartProvisioning	46
La gestion de SmartProvisioning.....	47
La console SmartProvisioning.....	52
La gestion des profils	59
L'administration des gateways	63
Action temps-réel et édition des Gateways	69
Gestion des SmartLSM Security Gateways	71
UTM-1 Edge Portal.....	88
Comprendre les objets dynamiques.....	92
Révision	97
4 Accès VPN SSL via portail Web	99
Introduction à Connectra	100
Déploiement de Connectra.....	102
Installation et configuration.....	109
Connexion à l'interface d'Administration	112
Gestion des contrôles d'accès	114

Vérification des configurations	115
Déploiement de Cluster	116
Révision	119
5 Accélération	121
Accélération	122
Secure XL : Accélération de la sécurité.....	122
CoreXL : Accélération Multi-Coeurs	133
Configuration par défaut de CoreXL.....	134
Allocation de cœurs de processeurs	136
Révision	139
6 Haute Disponibilité	141
Gestion de la Haute Disponibilité	142
Actif vs. passif	144
Les modes de synchronisation.....	145
Les statuts de synchronisation	146
Révision	149
7 Clustering	151
ClusterXL et l'équilibrage de charge.....	152
Installation de Cluster XL	154
La synchronisation de clusters	161
Les connexions « sticky »	164
La configuration de ClusterXL	166
Tour d'horizon de VRRP	167
Révision	173
8 Réseau et Routage Avancés	175
La lame logicielle « Réseau Avancé ».....	176
La CLI (Command Line Interface)	181
Commandes Multicast.....	186
Border Gateway Protocol (BGP)	187
Internet Control Message Protocol (ICMP).....	191
Découverte de routeurs.....	195
Multiplexing SNMP (SMUX)	197
Distance Vector Multicast Routing Protocol (DVMRP)	198
Internet Group Management Protocol (IGMP).....	199
Listes d'Accès	201
Agrégation de routes	204
Contrôle d'Accès Multicast	206
Révision	211

9 Réseau avancé – L'Équilibrage de Charges	213
Équilibrage de charges.....	214
Les différentes méthodes de « Load Balancing »	215
Disponibilité des serveurs	222
Mesure de charge	222
Révision	225
10 Réseau avancé – Qualité de Service (QoS)	227
Qualité de Service et « Stateful Inspection »	229
Architecture QoS	232
QoS Gateway	232
QoS Security Management Server.....	233
La configuration de la Qualité de Service	235
La gestion des règles et de l'allocation de ressources	241
Déploiement de la QoS	247
Exemples d'allocation de bande passante	249
Révision	253
11 Reporting	255
Introduction	256
Rapports pré-définis	260
Eventia Reporter	265
Haute Disponibilité	266
Rapports programmés.....	267
Filtrage de rapports	267
Reporter Database Management	271
Politique de consolidation pré-définie.....	272
Révision	275
12 IPS Event Analysis	277
Introduction à IPS Event Analysis	278
Configuration Initiale.....	284
Analyse d'évènements	288
Gestion d'évènements.....	295
Investiguer sur les évènements.....	301
Configurer la politique d'évènements	303
Révision	307