



Formation Check Point Security Administration NGX III (R65) [4 jours]

Durée : 4 jours

Objectifs : connaître le fonctionnement interne des différents composants de l'offre Firewall-1/VPN-1. Savoir mettre en œuvre les outils de débogage.

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

Prérequis : compétences approfondies sur TCP/IP et sur le routage (statique et dynamique).
Compétences systèmes (Windows / Linux) approfondies.
Avoir suivi les formations Check Point Security Administration I et II (ou équivalent).

Tarif : 2440 € H.T.

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

Objectifs du cours	xiii
1 Check Point Security Administration NGX III	1
Objectifs du cours	1
Plan du cours	3
Prérequis	3
Mise en place recommandée pour les Labs	4
2 Méthodes générales de résolution des problèmes	11
Objectifs	11
Mots clés	12

Guide de résolution des problèmes	13
Que faut-il vérifier avant d'installer VPN-1 NGX	16
IP forwarding et sécurité au boot	19
Problèmes avec SIC et l'ICA	20
Translation d'adresses réseaux (NAT)	32
Collecte des données	36
Révision du chapitre	43
Questions de révision.....	44
Réponses aux questions	45
3 Gestion des fichiers	47
Objectifs	47
Mots clés	48
cpinfo.....	49
Objects_5_0.C et objects.C	61
Fwauth.NDB.....	72
Fichiers \$FWDIR/lib/*.def	73
Fichiers de log.....	75
Déboguage des logs	81
Lab 1 : utilisation de cpinfo.....	83
Lab 2 : analyse de cpinfo dans InfoView	89
Lab 3 : utilisation de GuiDBedit	93
Lab 4 : utilisation de fw logswitch et fwm logexport	101
Révision	107
Questions de révision.....	108
Réponses aux questions	109
4 Analyseurs de protocoles	111
Objectifs	111
Mots clés	112
Tcpdump	113
Snoop	119
Fw monitor	124
Ethereal	140
Lab 5: comparaison de la NAT côté client et de la NAT côté serveur avec fw monitor	149
Révision	155
Questions de révision.....	156
Réponses aux questions	157
5 Outils de déboguage dans NGX	159
Objectifs	159
Mots clés	160
Fw ctl debug	161
Déboguage de fwd/fwm	169
Déboguage de cpd	174
Lab 6 : mise en œuvre du déboguage sur cpd et fwm	177
Révision	181
Questions de révision	181

Réponses aux questions	183
6 Commandes fw avancées	185
Objectifs	185
Mots clés.....	186
Commandes fw	187
Commande fw tab	188
Commandes fw ctl	197
Autres commandes fw	207
Commandes fw avancées	214
Commandes fwm	222
Lab 7 : utilisation de fw ctl pstat	229
Lab 8 : utilisation de fw stat, fwm load, et fw unloadlocal	231
Révisions	233
Questions de révision	233
Réponses aux questions	235
7 Security Servers	237
Objectifs	237
Mots clés	238
Le « folding process ».....	239
Résolution des problématiques du Security Server	244
Débogage des Security Servers	249
Révision	253
Questions de révision.....	254
Réponses aux questions	256
8 Outils de débogage VPN	257
Objectifs	257
Mots clés	258
Principes d'IKE	259
Aperçu de la résolution des problèmes	270
Outils de débogage VPN	271
Résolution des problèmes des tables.....	276
Lab 9 : mettre en place le débogage sur un VPN site à site	281
Révision	289
Questions de révision	289
Réponses aux questions	291
9 Résoudre les problèmes et déboguer SecuRemote/SecureClient	293
Objectifs	293
Mots clés	294
Ports nécessaires	295
Flux des paquets	297
Sélection du lien en accès distants	299
Outils de débogage Secureremote/SecureClient	306
Outil de débogage avancé.....	311

Table de résolution.....	313
Lab 10 : observation de la négociation IKE entre une passerelle et SecureClient	319
Lab 11 : fonctionnement de srfw monitor	325
Révision	329
Questions de révision	330
Réponses aux questions	331
10 VPN Avancé.....	333
Objectifs	333
Mots clés	334
VPN Route-based	335
VPN Domain-based	337
VPN Tunnel Interface	338
Routage VPN dynamique	345
Wire Mode	350
Fonctionnement d'une règle VPN directionnelle	355
Gestion de tunnel	358
Lab 12 : VPN route-based en utilisant des routes statiques.....	367
Lab 13 : Routage VPN dynamique en utilisant OSPF	385
Révision	401
Questions de révision	403
Réponses aux questions	405
11 ClusterXL	407
Objectifs	407
Mots clés	408
Recommandations sur la configuration	409
Gestion des problèmes sur ClusterXL	412
Flags du kernel	424
Lab 14 : observation de la négociation IKE entre une passerelle et SecureClient	431
Lab 15 : lancer cphastart -d	437
Révision	439
Questions de révision	440
Réponses aux questions	441
Appendice A : Utilisation de DbEdit	443