

CheckPoint Security Administration NGX R65 niveau 3 (Cours officiel)

Objectif :

Cette formation Check Point de 4 jours est constituée essentiellement de travaux pratiques issus de cas réels.

Les participants sont mis en situation tout au long de la formation grâce aux différents ateliers dédiés principalement à la résolution des problèmes ainsi qu'au débogage des environnements Check Point.

L'objectif à l'issue du cours est de donner aux participants une expertise de très haut niveau, une véritable méthodologie et le maximum d'autonomie à travers des outils spécifiques souvent à usage interne pour la résolution des problèmes liés notamment au firewall, au VPN, à la NAT ainsi qu'aux modules SmartDefense.

Participants :

Cette formation checkpoint administrateurs systèmes, architectes réseaux, responsables de la sécurité des systèmes d'information, consultant sécurité.

Pré-requis :

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).

Durée : 4 jours (28 heures) Référence : SCHP

Contenu de la formation :

Méthodes générales de résolution des problèmes

Mots clés Méthodologie et guide de résolution des problèmes

Que faut-il vérifier avant d'installer VPN-1 NGX

IP forwarding et sécurité au boot

Problèmes avec SIC et l'ICA

Translation d'adresses réseaux (NAT)

Gestion des fichiers

cpinfo

Objects_5_0.C et objects.C

Fwauth.NDB

Fichiers \$FWDIR/lib/*.def

Fichiers de log
Débogage des logs

TP 1 : UTILISATION DE CPINFOTP 2 : ANALYSE DE CPINFO DANS INFOVIEW TP 3 : UTILISATION DE GUIDBEDIT TP 4 : UTILISATION DE FW LOGSWITCH ET FWM LOGEXPORT

Analyseurs de protocoles

Tcpdump
Snoop
Fw monitor
Ethereal

TP 5: COMPARAISON DE LA NAT CÔTÉ CLIENT ET DE LA NAT CÔTÉ SERVEUR AVEC FW MONITOR

Outils de débogage dans NGX

Fw ctl debug
Débogage de fwd/fwm
Débogage de cpd

TP6 : MISE EN OEUVRE DU DÉBOGUAGE SUR CPD ET FWM

Commandes fw avancées

Commandes fw
Commande fw tab
Commandes fw ctl
Autres commandes fw
Commandes fw avancées
Commandes fwm

TP 7 : UTILISATION DE FW CTL PSTAT TP 8 : UTILISATION DE FW STAT, FWM LOAD, ET FW UNLOADLOCAL

Security Servers

Le « folding process »
Résolution des problématiques du Security Server
Débogage des Security Servers

Outils de débogage VPN

Principes d'IKE
Outils de débogage VPN
Résolution des problèmes des tables

TP 9 : METTRE EN PLACE LE DÉBOGUAGE SUR UN VPN SITE à SITE

Résoudre les problèmes et déboguer SecureRemote/SecureClient

Ports nécessaires
Flux des paquets
Sélection du lien en accès distants
Outils de débogage Secureremote/SecureClient

Outil de débogage avancé
Table de résolution

**TP 10 : OBSERVATION DE LA NÉGOCIATION IKE ENTRE UNE PASSERELLE ET SECURECLIENT TP 11 :
FONCTIONNEMENT DE SRFW MONITOR**

VPN Avancé

VPN Route-based
VPN Domain-based
VPN Tunnel Interface
Routage VPN dynamique
Wire Mode
Fonctionnement d'une règle VPN directionnelle
Gestion de tunnel

**TP 12 : VPN ROUTE-BASED EN UTILISANT DES ROUTES STATIQUESTP 13 : ROUTAGE VPN DYNAMIQUE EN
UTILISANT OSPF**

ClusterXL

Recommandations sur la configuration
Gestion des problèmes sur ClusterXL
Flags du kernel

**TP 14 : OBSERVATION DE LA NÉGOCIATION IKE ENTRE UNE PASSERELLE ET SECURECLIENT TP 15 :
LANCER CPHASTART -D**