



Check Point Security Administration NGX III R65

Objectif	Connaître le fonctionnement interne des différents composants de l'offre Firewall-1/VPN-1. Savoir mettre en œuvre les outils de débogage.
Pré requis	Pour suivre ce stage, il est nécessaire d'avoir des compétences approfondies sur TCP/IP et sur le routage (statique et dynamique), des compétences systèmes (Windows / Linux) approfondies et avoir suivi les formations Check Point Security Administration I et II (ou équivalent)....
Durée	4 jours

Contenu

Module 1 : Méthodes générales de résolution des problèmes

- Objectifs
- Mots clés
- 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)
- Collecte des données

Module 2 : Gestion des fichiers

- Objectifs
- Mots clés
- cpinfo
- Objects_5_0.C et objects.C
- Fwauth.NDB
- Fichiers \$FWDIR/lib/*.def
- Fichiers de log
- Débogage des logs

Module 3 : Analyseurs de protocoles

- Objectifs
- Mots clés
- Tcpdump
- Snoop
- Fw monitor
- Ethereal

Module 4 : Outils de débogage dans NGX

- Objectifs Mots clés
- Fw ctl debug
- Débogage de fwd/fwm
- Débogage de cpd

Module 5 : Commandes fw avancées

- Objectifs
- Mots clés
- Commandes fw
- Commande fw tab
- Commandes fw ctl
- Autres commandes fw
- Commandes fw avancées
- Commandes fwm

Module 6 : Security Servers

- Objectifs.
- Mots clés
- Le « folding process »
- Résolution des problématiques du Security Server
- Débogage des Security Servers

Module 7 : Outils de débogage VPN

- Objectifs
- Mots clés
- Principes d'IKE
- Aperçu de la résolution des problèmes
- Outils de débogage VPN
- Résolution des problèmes des tables

Module 8 : Résoudre les problèmes et déboguer SecuRemote/SecureClient

- Objectifs
- Mots clés
- Ports nécessaires
- Flux des paquets
- Sélection du lien en accès distants
- Outils de débogage SecuRemote/SecureClient
- Outil de débogage avancé
- Table de résolution

Module 10 VPN Avancé

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

Module 11 ClusterXL

- Objectifs
- Mots clés
- Recommandations sur la configuration
- Gestion des problèmes sur ClusterXL
- Flags du kernel