Check Point R81.20 – Sécurité Réseau, niveau 1

Prix : 2 990 € HT

Durée : 4 jours

Code de Référence : SCSR10

Cette formation Check Point vous permettra d'acquérir l'ensemble des techniques et des méthodologies pour installer et gérer Check Point R81.

Objectifs de la formation

- Installer et configurer le produit Check Point R81.20
- Déployer une politique de sécurité et surveiller le trafic
- Mettre en oeuvre la translation d'adresse (NAT)
- Déployer des sites distants et partager les politiques de sécurité
- Maîtriser la visualisation des logs et le monitoring
- Mettre en œuvre le déchiffrement HTTPS
- Mettre en œuvre le contrôle applicatif et le filtrage URL
- Gérer l'authentification d'utilisateurs
- Gérer les déploiements VPN site à site
- Gérer les accès distants VPN avec les options proposées par le blade « Mobile Access » : IPSec et SSL
- Comprendre la politique de Threat Prevention
- Mettre en œuvre un cluster en haute disponibilité

Public

Cette formation s'adresse aux techniciens, administrateurs et ingénieurs système, réseau et sécurité.

Prérequis

Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.

Programme de la formation

Présentation de l'architecture Check Point R81.20

- Les produits Check Point
- Nouveautés de la version R81, R81.10 et R81.20

Déploiement Gaia : Installation des « appliances » Check Point

- Présentation du système Gaïa
- Eléments de l'architecture trois-tiers
- Architecture modulaire des "Software Blades"
- Check Point Infinity
- L'architecture en mode distribué et en mode standalone
- Le serveur de management. Le protocole SIC

Travaux pratiques

- Installation de Check Point R81.20

Gestion du Security Management Server avec l'outil de gestion unifié « Smart Console » : communication avec le protocole SIC et Gestion des objets

- Prise en main de SmartConsole R81.20
- Politique de sécurité. Gestion des règles
- Politiques Unifiées
- Inspection des paquets
- « Inline » Policies (sous règles)

Travaux pratiques

- Installation de SmartConsole. Créer des objets. Réaliser une politique de sécurité. Activer l'anti-spoofing

Translation d'adresses (NAT)

- Les règles de translation d'adresses avec IPv4 et IPv6
- Le NAT statique (One To One NAT) et le NAT dynamique (.Many To One NAT)/PAT
- Le NAT Manuel
- La problématique ARP et le routage.

Travaux pratiques

- Mise en place de NAT automatique de type statique, Hide et règles de transaction manuelle

Gestion Multi-Sites

- Définition de Policy Packages
- Gestion de Policy Packages
- Definition et types de "Layers"
- Inspection des packets dans une « Ordered Layer »
- Partage de « Layers » (Policy Layers Sharing)

Travaux pratiques

- Installation d'une passerelle distante, création d'une politique de sécurité (Policy Pack), et de règles de base pour le site distant.
- Création et partage d'une « Ordered Layer »

Logs & monitoring

- La politique de gestion des logs.
- Suivre les connexions avec LOGS & MONITOR (ancien SmartView Tracker).
- l'outil « Monitor »
- Gestion de Logs
- Le SmartView Monitor, fonctionnalités et seuils d'alerte.
- Serveur de logs dédié

Travaux pratiques

- Activation du monitoring, utilisation du Suspicious Activity Monitoring Protocol, visualisation du trafic, monitoring de l'état de la politique de sécurité.
- Introduction à Troubleshooting : Accéder au mode « expert », utilisation des commandes « tcpdump » et « fw ctl zdebug drop », visualizer et manipuler les utilitaires « CPView » et « Top »
- Ajout d'un serveur de logs dédié

Déchiffrement-HTTPS

- Création des règles
- Gestion de certificats
- Server Name Indications (SNI)

Travaux pratiques

- Mise en œuvre de l'inspection HTTPS

Contrôle Applicatif / Filtrage URL

- Les limites d'un firewall classique par IP et par port
- Le contrôle d'accès
- Le « AppWiki ». L'URL Filtering
- Le "User Check"

Travaux pratiques

- Filtrage Web et Applications : créer et partager la politique de « Filtrage Web et Applications » en tant que « Inline Layer » et « Ordered Layer »

Politique à base d'utilisateurs

- Besoin de récupérer l'identité des utilisateurs
- Les méthodes d'authentification Identity Awareness R81
- Les objets de type « Access Role »

Travaux pratiques

- Authentification : mise en place d'Identity Awareness, création de rôles et des accès.

VPN IPSEC site to site

- L'architecture du VPN. Les bases du chiffrement
- Introduction à IKE et IPSec
- L'autorité de certification (CA). Le Domain-Based VPN
- Mode Simplifié. Configuration des communautés VPN

- Routage VPN

Travaux pratiques

- VPN-IPSec Inter-sites (Shared Secret)
- VPN-IPSec Inter-sites (Certificats)

Accès Distant

- Le VPN SSL et le VPN IPSec
- Le Blade Mobile Access
- Mobile Access du type : « Remote Access »
- Endpoint Security VPN
- NAT-Traversal, Visitor Mode, Hub Mode et Office Mode

Travaux pratiques

- Mise en place d´une connexion VPN de type « Remote Access » via le client « Check Point Mobile »
- Mise en place d´une connexion VPN de type « Remote Access » via le client « Check Point Mobile » pour des utilisateurs « Active Directory »

Politique de « Threat Prevention »

- La politique de Threat Prevention et ses « Software Blades »
- Gestion des règles
- Profils de sécurité
- Autonomous Threat Prevention

Travaux pratiques

- Anti-Virus et Anti-Bot

HA avec ClusterXL

- La redondance des firewalls
- Le ClusterXL High Availability (Actif/Passif)
- VMAC et les problématiques d'ARP

Travaux pratiques

- Mise en œuvre de ClusterXL en mode High Availability

Méthodes pédagogiques

Des exercices pratiques et des démonstrations vous permettront de mettre en pratique les notions théoriques présentées.

Méthodes d'évaluation des acquis

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.