Check Point Certified Security Administrator CCSA R82- Préparation à la certification

Prix : 2 850 € HT

Durée : 4 jours

Code de Référence : SCCSA82

Cette formation Check Point vous permettra d'acquérir l'ensemble des techniques et des méthodologies nécessaires au passage de l'examen pour l'obtention de la certification CCSA R82.

Objectifs de la formation

- Installer et configurer le produit Check Point R82
- 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 gestion d'administrateurs
- Maîtriser la visualisation des logs et le monitoring
- Gérer l'authentification d'utilisateurs.
- Mettre en oeuvre le déchiffrement HTTPS. Comprendre le protocole HTTP/3 et sa prise en charge du décryptage HTTPS
- Mettre en oeuvre le contrôle applicatif et le filtrage URL.
- Gérer les déploiements VPN site à site.
- Comprendre la politique d'Autonomous Threat Prevention.
- BONUS : Mettre en oeuvre un cluster en haute disponibilité.
- Préparer l'examen officiel menant à la certification CCSA

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 R82

- Les produits Check Point
- Nouveautés de la version R81.xxx, et R82

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
- CLI : interface en mode ligne de commandes

Travaux pratiques

- *Installation de Check Point R82*

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 R82
- Politique de sécurité. Gestion des règles
- Politiques Unifiées
- Inspection des paquets
- « Inline » Policies (sous règles)
- La SmartConsole Web

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
- Définition 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 »*

Gestion d'administrateurs

- « Permission Profiles »
- Limiter la portée d'action des administrateurs
- Gestion des utilisateurs concurrents
- Gestion des sessions

Travaux pratiques

- *Création d'un nouveau « Permission Profile » avec des autorisations limitées*

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*

Politique à base d'utilisateurs (Identity Awareness)

- Besoin de récupérer l'identité des utilisateurs
- Les méthodes d'authentification Identity Awareness R82
- Fournisseurs d'identité externes
- Les objets de type « Access Role »
- Nouveau « Identity Cache Mode »
- PDP-Only mode

Travaux pratiques

- *Installation et mise en oeuvre d'Identity Collector*

Déchiffrement-HTTPS

- Création des règles « Outbond » et « Inbound »
- Gestion de certificats
- Server Name Indications (SNI)
- Gestion des outils avancés dans la SmartConsole
- Présentation du « Learning mode » et des prédictions de performance
- Présentation de la fonctionnalité « Client Side Fail mode »
- Présentation de la fonctionnalité « Bypass under load”
- Prise en charge des flux HTTP/3 avec le protocole de transport QUIC (UDP)

Travaux pratiques

- *Mise en œuvre de l’inspection HTTPS*

Contrôle Applicatif / Filtrage URL

- Les limites d’un firewall classique par IP et par port
- La reconnaissance applicative
- Le contrôle d’accès
- Le « AppWiki ». L’URL Filtering
- Le “User Check”
- Le filtrage du DNS avec la blade « Advanced DNS »

Travaux pratiques

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

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
- Utilisation du nouvel objet « Network Probe » afin de surveiller l’état des tunnels VPN.

Travaux pratiques

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

Autonomous « Threat Prevention »

- La politique de Threat Prevention et ses « Software Blades »
- Custom et Autonomous Threat Prevention
- Profils de sécurité
- Technologies utilisées par Autonomous Threat Prevention
- Présentation des moteurs de prévention basés sur l’IA : ThreatCloud Graph, Kronos, Deep Brand Clustering
- Automatic Zero Phishing Configuration

- Fonctionnalité « Adaptive Hold » pour les blades Anti-Virus et Anti-Bot

Travaux pratiques

- *Mis en place d'Autonomous Threat Prevention*

BONUS : HA avec ClusterXL

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

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.