Check Point R82, sécurité réseau, niveau 1

Cours Pratique de 4 jours - 28h
Réf : CPG - Prix 2025 : 2 920 HT

Ce cours vous fera découvrir la dernière version des produits Check Point : R82. À l'issue de cette formation, vous serez capable de mettre en place et gérer une politique de sécurité unifiée (Access Control et Threat Prevention) ainsi que des politiques de sécurité partagées (Geo Policy et HTTPS Inspection).

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Installer et configurer le produit Check Point R82

Déployer une politique de sécurité et surveiller le trafic

Déployer des sites distants et partager les politiques de sécurité

Maîtriser la visualisation des logs et le monitoring

Gérer l'authentification d'utilisateurs

Mettre en œuvre un cluster en haute disponibilité

LE PROGRAMME

dernière mise à jour : 06/2025

1) Déploiement Gaia : installation des "appliances" Check Point

- Les produits Check Point.
- Nouveautés de la versions R81.xxx et R82.
- Présentation du système Gaïa.
- Éléments 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 R82.

2) Gestion Security Management Server, 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.

3) 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.

PARTICIPANTS

Administrateurs et ingénieurs systèmes/réseaux/sécurité, techniciens.

PRÉREQUIS

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

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

- La problématique ARP et le routage.
Travaux pratiques : Mise en place de NAT automatique de type statique, hide et règles de transaction manuelle.

4) Gestion multisites
- 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).
- Gestion d'administrateurs dans la SmartConsole.
- Communication avec la Gateway distante.
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. Création d'un nouveau permission profile avec des autorisations limitées.

5) Logs et monitoring
- La politique de gestion des logs.
- Suivre les connexions avec logs et monitor (ancien SmartView Tracker).
- L'outil Monitor.
- Gestion de logs.
- Le SmartView Monitor, fonctionnalités et seuils d'alerte.
- Serveur de logs dédié.
Travaux pratiques : Monitoring : utilisation du Suspicious Activity Monitoring Protocol, visualisation du trafic, monitoring de l'état de la politique de sécurité.
Troubleshooting : accéder au mode expert, aux commandes "tcpdump" et "fw ctl zdebug drop", visualiser et manipuler les utilitaires CPView et Top.

6) 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.

7) 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.
- Politique à base d'utilisateurs.
- Récupérer l'identité des utilisateurs, les méthodes d'authentification Identity Awareness.
Travaux pratiques : Filtrage web et applications : créer et partager la politique de Filtrage Web et Applications en tant que inline layer et ordered layer.
Authentification : mise en place d'Identity Awareness, création de rôles et des accès.

8) VPN IPSec site to site et accès distant
- 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 de l'état des tunnels VPN.
- 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 : VPN-IPSec Inter-sites (Shared Secret). VPN-IPSec Intersites (certificats). Mise en place d´une connexion VPN de type remote access via le client Check Point Mobile, également pour des utilisateurs Active Directory.

9) Politique de Threat Prevention

- La politique de Threat Prevention et ses software blades.
- Gestion des règles.
- Profils de sécurité.
- Présentation des moteurs de prévention basés sur l'IA : ThreatCloud Graph, Kronos, Deep Brand Clustering.
- Introduction d'autonomous Threat Prevention.
- Automatic Zero Phishing Configuration.
- Fonctionnalité "Adaptive Hold" pour les blades Anti-Virus et Anti-Bot.

Travaux pratiques : Anti-Virus et Anti-Bot.

10) Clustering

- La redondance des firewalls.
- ClusterXL en mode High Availability.
- ClusterXL en mode load sharing.
- ClusterXL en mode Active-Active.
- VMAC et les problématiques d'ARP.

Travaux pratiques : Mise en oeuvre de ClusterXL en mode High Availability.

LES DATES

CLASSE À DISTANCE	PARIS
2025 : 25 nov.	2025 : 18 nov.