Date de publication : 28/05/2025

Formation : CCSA, Check Point Certified Security Administrator R82, certification

Formation pratique - 4j - 28h00 - Réf. CPH
Prix : 2460 € H.T.

NEW

La formation vise à vous apprendre à installer et configurer Check Point R82, déployer des politiques de sécurité, gérer les licences et administrateurs, surveiller les logs et le trafic, mettre en œuvre le déchiffrement HTTPS, contrôler les applications et filtrer les URL, effectuer des sauvegardes et mises à niveau, gérer les VPN site à site, et comprendre la prévention des menaces autonomes. Elle inclut également la préparation à l'examen de certification CCSA et la mise en œuvre d'un cluster en haute disponibilité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Installer et configurer Check Point R82
- Déployer et gérer des politiques de sécurité
- Mettre en œuvre la translation d'adresses (NAT)
- Gérer les licences et les contrats
- Administrer des environnements multi-sites
- Contrôler les accès administratifs
- Superviser les logs et le trafic réseau
- Configurer l'inspection HTTPS et le support HTTP/3
- Appliquer le contrôle applicatif et le filtrage URL
- Mettre en œuvre des VPN et la prévention des menaces

Public concerné

Techniciens, administrateurs et ingénieurs système/réseaux/sécurité.

Prérequis

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

PARTICIPANTS

Techniciens, administrateurs et ingénieurs système/réseaux/sécurité.

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.

Méthodes et moyens pédagogiques

Travaux pratiques

Exercices pratiques: Installation de Check Point R82. Installation de SmartConsole. Créer des objets. Réaliser une politique de Sécurité.

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.

Programme de la formation

1 Introduction à l'architecture Check Point R82: Configuration initiale

- Produits Check Point et nouveautés R82.
- Présentation de Gaia OS.
- Architecture trois-tiers, des Software Blades et Check Point Infinity.
- Modes standalone vs distribué.
- Présentation du protocole SIC.
- CLI : interface en mode ligne de commandes.
- La SmartConsole Web.

Exercice

Installation de Gaia en R82 dans le serveur de management et la passerelle principale.

2 Gestion des politiques de sécurité

- Prise en main de SmartConsole R82.
- Inspection des paquets.
- Création d'objets et règles.
- Politiques « Inline layers » (sous règles).

Exercice

Installation de SmartConsole. Créer des objets. Réaliser une politique de sécurité.

3 Translation d'adresses (NAT)

- NAT statique, dynamique, manuel.
- Problématiques ARP et routage.
- Mise en œuvre de règles NAT.

Exercice

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

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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.

4 Gestion des licences et des sites distants

- Types de licences et gestion via SmartUpdate.
- Déploiement multi-sites et Policy Packages.
- Ordered Layers et partage de politiques.

Exercice
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 ».

5 Gestion d'administrateurs

- Profils de permissions.
- Sessions concurrentes et gestion des administrateurs.

Exercice
Création d'un nouveau « Permission Profile » avec des autorisations limitées.

6 Logs, monitoring et dépannage

- Suivi des connexions et alertes.
- Outils de monitoring (CPView, SmartView Monitor).
- Introduction au troubleshooting (tcpdump, zdebug).

7 Inspection HTTPS. Contrôle applicatif, filtrage URL et maintenance

- Règles Outbound/Inbound.
- Gestion des certificats et SNI.
- Fonctionnalités avancées de l'inspection HTTPS.
- App Control, URL Filtering, DNS Filtering. Le « User Check ».
- Sauvegardes (locales et cloud), CPUSE, mises à jour. La commande cpconfig.

Exercice
Mise en oeuvre de l'inspection HTTPS.Filtrage Web et Applications : créer et partager la politique de « Filtrage Web et Applications » en tant que « Inline Layer » et « Ordered Layer ». Restauration de la configuration d'une passerelle.

8 VPN site-à-site, prévention des menaces et haute disponibilité

- Architecture VPN, IKE/IPSec, routage VPN.
- ClusterXL et redondance (bonus).

Exercice
Utilisation de VPN-IPSec Inter-sites (Shared Secret) et VPN-IPSec Inter-sites (Certificats).

9 Prévention des menaces

- Autonomous Threat Prevention (IA, ThreatCloud).

Exercice
Mise en place d'Autonomous Threat Prevention.

10 Clustering

- ClusterXL et redondance.

Exercice
Mise en œuvre de ClusterXL en mode HA.

Options

Certification : 300 € HT

La certification est délivrée par Check Point Software Technologies. Elle valide les compétences fondamentales nécessaires pour administrer les solutions de sécurité Check Point. La durée est de 90 minutes et repose sur un QCM de 90 questions, en anglais.

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

CLASSE À DISTANCE
2026 : 16 juin, 29 sep., 8 déc.

PARIS LA DÉFENSE
2026 : 16 juin, 29 sep., 8 déc.