Check Point R81, installation et configuration

Cours Pratique de 2 jours - 14h
Réf : CPI - Prix 2024 : 1 650CHF HT

Cette formation vous permettra d'acquérir les connaissances nécessaires pour installer et configurer une solution de sécurité basée sur le firewall Check Point version R80. Vous verrez également comment mettre en place et gérer une politique de sécurité.

OBJECTIFS PÉDAGOGIQUES

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

Installer et configurer Check Point R80

Mettre en œuvre une politique de sécurité

LE PROGRAMME

dernière mise à jour : 02/2021

1) Introduction

- La gamme de produits Check Point.
- Quels sont les différents composants d'un produit Check Point ?
- Quels sont les nouveautés apportées par la version R80 ?

2) Architecture et installation

- L'architecture en mode distribué et en standalone.
- Qu'est ce que le serveur de management ? Présentation du protocole SIC (Secure Internal Communications).
- Le système d'exploitation Check Point Gaïa.
- L'interface en ligne de commandes (CLI). Quels sont les avantages et les inconvénients d'utiliser cette interface ?
- Comment effectuer la sauvegarde et la restauration. Quelles sont les commandes pour effectuer ces opérations ?

Travaux pratiques : Installation de Check Point sous Gaïa en version R80.

3) Mettre en place une politique de sécurité

- Découverte de la SmartConsole. Prise en main de SmartConsole.
- Qu'est ce que le SmartDashboard ? Comment démarrer et utiliser le SmartDashboard ?
- Mettre en place une gestion des administrateurs et des profils.
- Quelle politique de sécurité mettre en place. Comment gérer l'ensemble des règles de sécurité qui ont été définies ?

Travaux pratiques : Installer SmartConsole. Créer des objets et une politique de sécurité. Activer l'anti-spoofing.

4) La translation d'adresses (NAT)

- Rappels sur la translation d'adresses (NAT).
- Quelles sont les règles de la translation d'adresses ? Est-il obligatoire de l'utiliser systématiquement ?
- Les différents types de NAT : le NAT "static" et le NAT "hide". Comment effectuer la gestion de l'ARP ?

Travaux pratiques : Mise en place de NAT automatique de type "hide", "static" et de règles de transaction manuelle.

PARTICIPANTS

TechnicienS/Administrateurs réseaux ou 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.

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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5) Le VPN site à site

- L'architecture du VPN. Bases du chiffrement.
- Introduction IPSec, l'autorité de certification.
- L'autorité de certification (CA).
- Le Domain-Based VPN, le mode client lourd.
- Les modes d'authentification en Mobile Access : Check Point Mobile, SSL/SNX...

Travaux pratiques : Mise en place d'un tunnel IPSec site à site. Configuration de l'accès distant en VPN IPSec.

LES DATES

CLASSE À DISTANCE
2024 : 11 juil., 14 oct.