Formation : Check Point R82, Sécurité Réseau, niveau 2

Cours pratique - 4j - 28h00 - Réf. CPJ
Prix : 3030 CHF H.T.

NEW

Cette formation apporte toutes les connaissances nécessaires à l'optimisation de l'application et à la mise en place des mécanismes de clustering et de haute disponibilité. Elle détaille l'utilisation de nombreuses options de configuration avancée comme la qualité de service (QoS), la redondance...

Objectifs pédagogiques

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

- Comprendre les principaux processus sur les serveurs de gestion de la sécurité et les passerelles de sécurité
- Utiliser « Dynamic Layer » afin d'ajouter des objets et règles directement sur la passerelle à l'aide de l'API Gaia
- Décrire les technologies coreXL et secureXL améliorent et optimisent les performances des passerelles de sécurité
- Gérer les accès distants VPN avec les options proposées par le blade "Mobile Access" : IPSec et SSL
- Mettre en oeuvre un cluster ElasticXL pour garantir une haute disponibilité et un équilibrage de charge

Public concerné

Administrateurs et ingénieurs systèmes/réseaux/sécurité, techniciens.

Prérequis

Bonnes connaissances de TCP/IP, de la sécurité des SI et des principales fonctions de Check Point ou connaissances équivalentes à celles apportées par le cours réf. CPG. Expérience souhaitable.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

PARTICIPANTS

Administrateurs et ingénieurs systèmes/réseaux/sécurité, techniciens.

PRÉREQUIS

Bonnes connaissances de TCP/IP, de la sécurité des SI et des principales fonctions de Check Point ou connaissances équivalentes à celles apportées par le cours réf. CPG. Expérience souhaitable.

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.

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 Gaia avancée & API

- Gaia en ligne de commandes.
- Présentation de l'API.
- Créer des objets et règles via l'API.
- Methodes de mise à niveau de Gaia.
- Mise à jour/niveau centralisé des passerelles.

Travaux pratiques

Installation du SMS et des GWs en R81.20. Utilisation de l'API pour créer des objets et règles de base. Mise à niveau avancée du Management de R81.20 vers R82. Mise à niveau centralisée de la passerelle principale et distante.

2 Les processus Check Point

- Principaux processus Check Point.
- Commandes pour visualiser les processus Check Point.
- Les scripts et les « SmartTasks ».

Travaux pratiques

Configure SmartTasks.

3 Installation de la politique de sécurité

- Processus d'installation de la politique de sécurité.
- Installation Accélérée.
- Policy Packages & Layers.
- Objets Dynamiques.
- Updatable Objects.
- Présentation du concept de « Dynamic Layer ».
- Communication avec la passerelle en utilisant l'API Rest.
- Utilisation du Gaia API « call », « set-dynamic-content ».

Travaux pratiques

Vérification des fichiers d'installation. Création des objets dynamiques. Utilisation du « Dynamic Layer » pour créer des objets et règles directement dans le firewall principal.

4 Kernel operations & Traffic flow

- Circulation des paquets à l'intérieur de la passerelle.
- Chaînes de modules.
- L'outil « fw monitor ».
- Management Data Plane Separation (MDPS).

Travaux pratiques

Utilisation de l'outil « fw monitor ».

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.

5 SecureXL & CoreXL

- L'accélération SecureXL et ses templates.
- Commandes de SecureXL.
- CoreXL et SND (Secure Network Distributor).
- CoreXL Affinity.
- Dynamic Balancing.
- Multi-Queue.
- Le CoreXL Dynamic Dispatcher.
- Priority Queues (PrioQ).
- Acceleration Hyperflow pour les connections SMB/CIFS/QUIC.

6 VPN et Routage Avancé (Routed Based)

- Le routage VPN.
- Les modes de routage VPN.
- Avantages du « Routed Based » VPN.
- VTI : Virtual Tunnel Interfaces.
- Protocoles supportés pour le routage dynamique VPN.
- Wire Mode.
- Directional VPN.

Travaux pratiques

Mise en place de tunnels « route-based » avec du routage statique. Mise en place de tunnels « route based » avec du routage dynamique (OSPF).

7 Accès Distant

- Le VPN SSL et le VPN IPSec.
- Le Blade Mobile Access.
- Mobile Access du type : « Remote Access ».
- Mobile Access SSL : Clientless Applications et Native Applications.
- SSL Network Extender (SNX). Portail « Check Point Mobile ».
- Les clients VPN couche 3.
- Support de l'authentification SAML.

Travaux pratiques

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

8 Logs, monitor et reporting avancés

- Présentation de l'onglet Logs & Monitor.
- SmartEvent.
- Compliance.
- SmartEvent GUI Client.
- Suspicious Activity Monitoring (SAM).
- Introduction du nouvel outil "ConnView".

Travaux pratiques

Configuration de SmartEvent.

9 Gestion avancée des utilisateurs/Identity Collector

- Les types d'authentification.
- Fournisseurs d'identité externes.
- Problèmes de connexion AD avec AD Query.
- Nouveau « Identity Cache Mode ».
- Identity Collector.
- Identity Awareness en ligne de commande.

Travaux pratiques
Installation et mise en oeuvre d'Identity Collector. Mise en oeuvre des commandes de debug d'Identity Awareness.

10 Clustering

- La redondance des firewalls.
- Le ClusterXL High Availability (Actif/Passif).
- Le ClusterXL Load Sharing.
- Load Sharing Multicast.
- Le ClusterXL High Availability (Actif/Actif).
- VMAC et les problématiques d'ARP.
- La haute disponibilité du Management Server.
- Cluster ElasticXL.

Travaux pratiques
Mise en oeuvre de « Load Sharing » via ElasticXL (installation, configuration et tests).

Dates et lieux

CLASSE À DISTANCE
2026 : 9 juin, 22 sep., 1 déc.