Date de publication : 17/05/2024

Formation : Check Point R81, sécurité réseaux, niveau 2

Cours pratique - 3j - 21h00 - Réf. CPN
Prix : 2470 CHF H.T.

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 :

- Maîtriser l'Identity Awareness
- Mettre en œuvre un cluster en High Availability et Load Sharing
- Vérifier la qualité de service (QoS)

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. CPB. Expérience souhaitable.

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

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

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. CPB. 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.

1 Identity Awareness et Application Control

- Fonctionnalités avancées.
- Commandes CLI utiles.
- Création d'un certificat à la volée pour l'inspection HTTPS.

Travaux pratiques
Mise en œuvre d'Identity Awareness sous différentes formes.

2 Modules d'accélération

- Présentation de CoreXL.
- Accélération des connexions avec SecureXL.
- Module SecureX et l'accélération des sessions, d'HTTP.
- Présentation des Optimized Drops, des NAT Templates.
- SecureXL Dynamic Dispatcher.
- Fonctionnement de SecureXL et CoreXL simultanément.

3 Clustering Check Point

- Haute disponibilité du Management Server (Smartcenter HA).
- Redondance des firewalls.
- ClusterXL High Availability (Actif/Passif).
- ClusterXL Load Sharing (Actif/Actif).
- VMAC et problématiques d'ARP.
- Comparaison SecureXL vs VRRP.

Travaux pratiques
Mise en place d'un cluster en High Availability et Load Sharing.

4 VPN et routage avancé

- Debug, routage et route-based VPN.
- Routage dynamique avec les protocoles de routage RIP, OSPF et BGP.
- Modes de fonctionnement du Wire Mode.
- VTI (Virtual Tunnel Interface).
- Directional VPN Route Match.
- Link Selection et redondance VPN.
- VPN traditionnel/simplifié, Tunnel Management.

Travaux pratiques
Mise en place de VPN de type Route-Based.

5 Firewall avancé

- Les outils (Dbedit, guiDBedit).
- Les fichiers système, la gestion des logs.
- Mise en œuvre de CPInfo, Solr.
- Exemple d'utilisation de InfoView et Confwiz.
- SIC, ICA et les certificats.
- Fonctionnement de fw monitor et analyse sous Wireshark. Mise en œuvre de tcpdump.
- Présentation de CPsizeme, de CPView.

Travaux pratiques
Utilisation des outils de debug.

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.

6 Software Blade Compliance

- Présentation de la Software Blade Compliance.
- Meilleures pratiques en termes de sécurité.

7 Content Awareness et DLP

- Présentation des Objets Data Type.
- Mise en place d'une Software Blade DLP.
- Choix d'actions d'une politique DLP.
- Gestion du Watermark.

Travaux pratiques

Utilisation de la Software Blade Content Awareness. Création d'un objet Data Type.

8 QoS

- Présentation de la Software Blade QoSAwareness.
- Mise en œuvre de DiffServ et des classes à faible latence (LLQ).

Travaux pratiques

Contrôle de la bande passante à l'aide de la Software Blade QoS.