CheckPoint Security Expert

Référence : **CHS-CCSE** Durée : **3 jours** Certification : **CCSE**

CONNAISSANCES PREALABLES

• Avoir suivi le cours CHS-CCSA et/ou avoir la certification CCSA ou disposer d'un niveau équivalent. • La réussite de ce cours dépend de la connaissance de plusieurs disciplines liées aux activités, les systèmes UNIX et d'exploitation Windows, la gestion de certificat, l'administration système, le réseau securisé (TCP / IP).

PROFIL DES STAGIAIRES

• Administrateurs système. • Ingénieurs réseau. • Supports analystes. • Toute personne souhaitant obtenir la certification CCSE.

OBJECTIFS

• Apporte également un descriptif complet de toutes les nouvelles applications et solutions apparues avec les versions R70 et R71 du produit et ses fameuses lames logicielles (« software blades ») qui permettent de construire une solution de sécurité à la carte. • Cours complet sur Firewall-1 incluant de nombreuses options de configuration avancées (Routage Avancé, QoS, Redondance et Haute Disponibilité des liens, VPN SSL…).

CERTIFICATION PREPAREE

Check Point Certified Security Expert

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert CheckPoint

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Effectuer une sauvegarde d'une Security Gateway et de Management Server à l'aide de votre compréhension des différences entre les sauvegardes, photos, et update-exports

Mettre à jour et diagnostiquer un Management Server en utilisant une migration de base de données

Mettre à jour et diagnostiquer un déploiement d'un cluster Security Gateway

Utiliser les connaissances des infrastructures d'uneSecurity Gateway, les chaines de modules, les paquets de flux et des tables de noyau pour effectuer des debugs sur les processus de firewall

Construire, tester et diagnostiquer le déploiement d'un ClusterXL Load Sharing sur un réseau d'entreprise

Construire, tester et diagnostiquer le déploiement d'un ClusterXL High Availability sur un réseau d'entreprise

Construire, tester et diagnostiquer le déploiement d'un Management HA sur un réseau d'entreprise

Configurer, maintenir et diagnostiquer les solutions d'accélération SecureXL et CoreXL sur le trafic réseau de l'entreprise afin d'assurer l'amélioration des performances

Utiliser une base de données d'utilisateurs externes tels que LDAP, configurer le User Directory en intégrant les informations utilisateur pour les services d'authentification sur le réseau

Gérer l'accès des utilisateurs internes et externes à des ressources pour l'accès à distance ou à travers un VPN

Diagnostiquer les problèmes d'accès utilisateur trouvés grâce à l'application Identity Awareness

Diagnostiquer un site à site ou un certificat VPN sur une gateway d'entreprise en utilisant IKE View, les fichiers de connexion VPN et les outils de débogage de ligne de commande

Optimiser les performances et la disponibilité d'un VPN en utilisant un Link Selection et la solution Multiple Entry Point

Gérer et tester des tunnels VPN d'entreprise pour permettre une meilleure surveillance et la possibilité d'évolution avec d'autres tunnels définis dans une communauté, y compris d'autres fournisseurs

Créer des événements ou utiliser des définitions d'événements existants pour générer des rapports sur le trafic réseau spécifique à l'aide SmartReporter et SmartEvent et de fournir des informations de conformité de gestion

Diagnostiquer une génération de rapport des outils de ligne de commande et les informations de débogage fichier