

CheckPoint Security Administration NGX R71 niveau 2 (Cours officiel)

Objectif :

les produits de Check Point Software sont parmi les plus utilisés dans le monde de la sécurité. Ce cours de niveau deux constitue un cours complet sur Firewall-1 incluant de nombreuses options de configuration avancées (Routage Avancé, QoS, Redondance et Haute Disponibilité des liens, VPN SSL?). Il 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.

Cette formation Check Point vous permettra de configurer et administrer des solutions avancées de la suite des produits de sécurité Check Point R71

Participants :

Cette formation Check Point s'adresse aux administrateurs systèmes, architectes réseaux, responsables de la sécurité des systèmes d'informations, consultants sécurité.

Pré-requis :

compétences sur TCP/IP et sur le routage statique. Connaissances des environnements Windows et Unix (Linux). Avoir suivi le cours RCPF, avoir la certification ou disposer d'un niveau équivalent.

Durée : 5 jours (35 heures) **Référence : SCPS**

Contenu de la formation :

Check Point Security Expert R71

- Plan du cours
- Mise en place recommandée pour les labs
- Formation et certification Check Point
- CCMA

Management Portal

- Administration Web
- Déploiement sur un serveur dédié
- Déploiement sur un Security Management Server
- Les commandes et la configuration du Management Portal
- Pré-requis côté client
- Travaux Pratiques

Révision

SmartWorkflow

- Introduction à SmartWorkflow
- L'environnement SmartWorkflow
- Task Flow
- La barre d'outils SmartWorkflow
- La fenêtre de gestion des sessions
- Information sur les sessions
- Assigner des permissions
- Activer SmartWorkflow
- Configurer SmartWorkflow
- Travailler avec des sessions
- Comparer les politiques de sécurité
- Approuver les sessions
- Auditer les changements
- Travaux Pratiques
- Révision

SmartProvisioning

- Tour d'horizon de SmartProvisioning
- La gestion de SmartProvisioning
- La console SmartProvisioning
- La gestion des profils
- L'administration des gateways
- Action temps-réel et édition des Gateways
- Gestion des SmartLSM Security Gateways
- UTM-1 Edge Portal
- Comprendre les objets dynamiques
- Travaux Pratiques
- Révision

Accès VPN SSL via portail Web

- Introduction à La blade VPN SSL
- Déploiement de la blade VPN SSL
- Installation et configuration
- Connexion à l'interface d'Administration
- Gestion des contrôles d'accès
- Vérification des configurations
- Déploiement de Cluster
- Travaux Pratiques
- Révision

Accélération

- Accélération
- Secure XL : Accélération de la sécurité
- CoreXL : Accélération Multi-Coeurs

Configuration par défaut de CoreXL
Allocation de cœurs de processeurs
Travaux Pratiques
Révision

Haute Disponibilité

Gestion de la Haute Disponibilité
Actif vs. passif
Les modes de synchronisation
Les statuts de synchronisation
Travaux Pratiques
Révision

Clustering

ClusterXL et l'équilibrage de charge
Installation de Cluster XL
La synchronisation de clusters
Les connexions « sticky »
La configuration de ClusterXL
Tour d'horizon de VRRP
Travaux Pratiques
Révision

Réseau et Routage Avancés

La lame logicielle « Réseau Avancé »
La CLI (Command Line Interface)
Commandes Multicast
Border Gateway Protocol (BGP)
Internet Control Message Protocol (ICMP)
Découverte de routeurs
Multiplexing SNMP (SMUX)
Distance Vector Multicast Routing Protocol (DVMRP)
Internet Group Management Protocol (IGMP)
Listes d'Accès
Agrégation de routes
Contrôle d'Accès Multicast
Travaux Pratiques
Révision

Réseau avancé - L'Equilibrage de Charges

Equilibrage de charges
Les différentes méthodes de « Load Balancing »
Disponibilité des serveurs
Mesure de charge
Révision

Réseau avancé - Qualité de Service (QoS)

- Qualité de Service et « Stateful Inspection »
- Architecture QoS
- QoS Gateway
- QoS Security Management Server
- La configuration de la Qualité de Service
- La gestion des règles et de l'allocation de ressources
- Déploiement de la QoS
- Exemples d'allocation de bande passante
- Travaux Pratiques
- Révision

Check Point IPS

- Introduction
- Nouveau moteur et nouvelle architecture IPS
- Flexibilité de la politique de Sécurité IPS
- IPS Event Manager
- Configurer et gérer l'IPS
- Les profils et les protections IPS
- Les critères de performance, de criticité et de confiance
- Activation manuelle et automatique des protections
- Bypass Under Load
- Troubleshooting
- Téléchargement des mises à jour
- Travaux Pratiques
- Révision

Data Loss Prevention

- La passerelle Data Loss Prevention
- Les options de déploiement
- Les plateformes DLP et performances
- DLP UserCheck
- Installer, connecter et vérifier les clients
- Le portail DLP
- Les politiques de sécurité DLP
- Politique DLP vs. Politique de sécurité
- Types de données, protection des fichiers
- Protection par pattern et par CPcode
- Travaux Pratiques
- Révisions

SmartEvent

- L'architecture Smart Event
- Les requêtes sur les événements
- Requêtes prédéfinies
- Les log d'évènements

- Rechercher, trier, grouper et exporter les évènements
- Le panneau de statistiques d'évènements
- Les permissions administrateur
- Vérifier la vulnérabilité client
- Travaux Pratiques
- Révisions

SmartReporter

- Introduction à Smart Reporter
- La consolidation des logs
- Rapports standards, express et prédéfinis
- Haute disponibilité
- Les filtres
- La génération de rapports
- Modification et customisation de la base de données
- Planifier la création de rapports
- Révisions