



Check Point Security Administration NGX II R65

Objectif	Cette formation permet d'obtenir le niveau avancé de certification (CCSE) avec la toute dernière version du produit phare de Check Point : Firewall-1/VPN-1 NGX R65.
Pré requis	Avoir suivi la formation VPN-1 / Firewall-1 Management I NGX R65 ou disposer d'un niveau équivalent.
Durée	2 jours

Contenu

Module 1 : SmartUpdate

- Introduction à SmartUpdate
- Architecture de SmartUpdate
- Mise à niveau des packages
- Prérequis pour les packages distants
- Récupération des données depuis les passerelles VPN-1
- Ajout de nouveaux packages au container de packages
- Vérification de la viabilité d'une distribution
- Transfert des fichiers à des boîtiers distants
- Mise à niveau des firmware Edge avec SmartUpdate
- Reboot de la passerelle VPN-1
- Réparer une mise à jour ayant échoué
- Supprimer des packages du container de packages
- Gestion des licences
- Mise à niveau des licences .
- Récupération des données de licence des passerelles VPN-1
- CPInfo
- Ligne de commande SmartUpdate

Module 2 : Mise à niveau de VPN-1

- Configuration de la pré-installation
- Installation en mode distribué
- Mise à niveau vers VPN-1 NGX R65
- Guide de mise à niveau
- Ordre de mise à niveau
- Upgrade Export/Import
- Mise à niveau à travers SmartUpdate
- Compatibilité descendante de VPN-1
- Versions supportées
- Licences VPN-1 .
- Récupération des licences
- Chemins de mise à niveau supportés
- Vérification du contrat
- Effectuer la mise à jour de la licence.
- Considérations de pré-mise à niveau
- Outil de vérification en pré-mise à niveau
- Mise en place de la licence pour Web Intelligence
- Mise à niveau sur SecurePlatform
- Mise à niveau du SmartCenter Server
- Utilisation de l'outil de vérification de pré-mise à niveau
- Mise à niveau de la passerelle .
- Mise à niveau de la passerelle avec Smart Update

Module 3 : Chiffrement et VPNs

- Sécurisation des communications
- Confidentialité
- Chiffrement symétrique
- Désavantages du chiffrement symétrique
- Chiffrement asymétrique
- Diffie-Hellman.
- Intégrité
- Authentification
- Deux phases du chiffrement
- Algorithmes de chiffrement
- IKE
- ISAKMP
- Oakley .
- ISAKMP/Oakley
- Phase 1
- Phase 2
- Exemple IKE
- Chiffrement en mode Tunnel
- Autorités de certification
- Certificats
- Autorités de certification multiples
- Hiérarchie des autorités de certification
- Autorité de certification locale
- Service d'AC à travers Internet
- Autorité de Certification Interne (ICA)
- Clés publiques de CA .
- Créer des certificats

Module 4 : Introduction aux VPNs .

- Le VPN Check Point
- Comment fonctionne un VPN
- Spécifier le chiffrement
- Déploiements VPNs
- VPNs en site à site
- VPNs en accès distant
- Implémentation VPN
- Trois composants critiques des VPNs
- Mise en place d'un VPN .
- Fonctionnement d'un VPN
- Communautés VPNs
- Topologies d'un VPN
- Choix d'une topologie
- Authentification entre les membres de la communauté
- Passerelles avec des adresses IP dynamiques
- Routage du trafic à l'intérieur d'une communauté VPN
- Control d'accès et communautés VPN
- Services exclus



- Considérations spécifiques pour la mise en place d'une topologie VPN
- Autorisation du contrôle des connexions dans les communautés VPN
- Intégration des VPNs à la base de règles

Module 5 : VPNs site à site

- VPN site à site
- VPN basé sur le domaine
- VPN basé sur le routage
- Processus de routage VPN pour les VTIs
- Routage des paquets multicast à travers les tunnels VPN
- Gestion des tunnels VPNs
- Tunnels permanents
- Partage de tunnel VPN
- Wire Mode
- Wire Mode dans une configuration de type MEP
- Wire Mode avec des VPNs basés sur le routage
- Wire Mode entre deux communautés VPNs
- Mise en place d'un VPN directionnel
- VPN directionnel entre les communautés
- VPNs à points d'entrée multiples
- Haute disponibilité du VPN avec MEP
- VPNs en mode traditionnel

Module 6 : VPNs en accès distant

- VPN en accès distant
- Etendre SecuRemote avec SecureClient
- Connect Mode
- Etablissement de l'accès distant - Processus .
- Office Mode
- Fonctionnement de l'Office Mode
- Planification de l'Office Mode.
- IP Pool contre DHCP
- Modifications de la table de routage
- Interfaces externes multiples
- Avant de configurer l'Office Mode
- Politique de sécurité au niveau Poste de travail
- Expiration et renouvellement de la politique
- Haute disponibilité (HA) du Policy Server
- Enregistrement Wifi sur les points d'accès/hotels
- Logging SecureClient Mobile
- Routage VPN – Accès distant
- Hub Mode
- SSL Network Extender
- Fonctionnement du SSL Network Extender
- Prérequis
- VPN sans clients
- Considérations particulières pour le VPN sans client
- Configuration du VPN sans client
- Création des règles appropriées dans la politique de sécurité

Module 7 : Haute disponibilité et ClusterXL

- Haute disponibilité du management
- Environnement de la haute disponibilité du management
- Statut de synchronisation
- ClusterXL .
- Partage de charge .
- Modes de ClusterXL
- Haute disponibilité en Legacy Mode
- Haute disponibilité en New Mode
- Load Sharing en Mode Multicast

- Load Sharing en Mode Unicast (Pivot)
- Cluster Control Protocol
- Synchronisation des Clusters
- Le réseau de synchronisation
- Comment fonctionne la synchronisation d'état
- Restrictions des clusters synchronisés
- Connexions persistantes
- Le processus décisionnel de la persistance
- Commandes CPHA
- cphastart.
- cphastop
- cphaprob
- cphaprob Example
- fw hastat
- Débogage des problématiques ClusterXL
- Résultat de la commande « fw ctl pstat Sync »
- Problématiques de configuration de ClusterXL
- Modes de ClusterXL supportant SecureXL
- Support des cables croisés