



Check Point Security Administration NGX I R65

Objectif	Cette formation permet d'obtenir le premier niveau de certification (CCSA) avec la toute dernière version du produit phare de Check Point : Firewall-1/VPN-1 NGX R65
Pré requis	Expérience dans l'utilisation de Windows NT/2000 et/ou Unix/Linux. Connaissances de base des réseaux informatiques en environnement Ethernet. Expérience dans l'utilisation de TCP/IP et d'Internet.
Durée	3 jours

Contenu

Module 1 Aperçu de VPN-1

- Principes fondamentaux de VPN-1
- Module de sécurité de Check Point
- Mode "bridge"
- Mode "bridge" et STP
- Architecture de filtrage de la passerelle VPN-1
- Gestion de la politique de sécurité
- Composants de la SmartConsole
- Serveur SmartCenter de VPN-1
- Concepts de base et terminologie
- Utilisation des plug-ins de management
- Sécurisation des canaux de communication
- Login d'administration avec SIC
- SmartUpdate et la gestion des licences
- Fonctionnement de SmartUpdate
- Aperçu de la gestion des licences
- Contrats/Services
- Contrats de service
- Fonctionnement des fichiers de contrats

Module 2 Introduction à SecurePlatform

- Introduction
- Prérequis matériels de SecurePlatform et mise en place
- Outil de test de compatibilité matérielle
- Usage de la ligne de commande
- Commandes de base sous Linux
- Sauvegarde et restauration
- Visualisation du statut des travaux en cours dans l'interface Web
- Restauration de la sauvegarde en ligne de commande
- Restauration des versions anciennes de SecurePlatform
- Planifier une sauvegarde avec l'interface Web
- Visualiser les logs de backup dans l'interface Web
- Création du fichier CPInfo
- Répertoires Check Point importants
- Fichiers de log
- Fichiers objects.C et objects_5_0.C
- Fichier rulebases_5_0.fws
- Fichier fwauth.NDB
- Export de la base de données des utilisateurs
- Sauvegarde à l'aide de upgrade_export

- Gestion de votre système SecurePlatform
- Connexion au système SecurePlatform en utilisant SSH
- Gestion des utilisateurs
- SecurePlatform en ligne de commande
- Commandes administratives
- Commandes de documentation
- Commandes systèmes
- Gestion des images systèmes
- Commandes de diagnostic système
- Commandes Check Point
- Commandes de diagnostic réseau
- Commandes de configuration réseau
- Commandes utilisateurs et administrateurs

Module 3 Introduction à la politique de sécurité

- Bases de la politique de sécurité
- La base des règles
 - Gestion des objets dans SmartDashboard
 - SmartDashboard et les objets
 - Gestion des objets
 - Changement de la vue dans l'arbre des objets
 - Création de la base des règles
 - Concepts fondamentaux de la base des règles
 - Règle par défaut
 - Règles de base
 - Règles implicites/explicites
 - Connexions de contrôle
 - Compléter la base de règles
 - Compréhension de l'ordre des règles
 - Gestion de la base des règles
 - Révision
 - Astuces
 - Gestion de la politique et contrôle de révision
 - Aperçu de la politique de gestion
 - Packages de politique .
 - Cibles d'installation
 - Recherche et classification des règles et des objets
 - Database Revision Control
 - Mise en oeuvre du Database Revision Control
 - Lab 4: configuration de la politique de sécurité
 - Translation d'adresses réseaux (NAT)
 - Adressage IP NAT dynamique (Hide)
 - NATstatique
 - Comparaison des NAT Hide et Static



- Choix de l'adresse dans la NAT de type Hide..
- Configuration de la NAT
- Configuration de l'objet NAT en dynamique
- NAT manuelle
- Autorisation du trafic en VoIP
- Protocoles supportés
- Session Initiation Protocol
- H.323
- Détection du spoofing IP .
- Configuration de l'anti-spoofing
- Multicast
- Configuration du contrôle d'accès au multicast

Module 4 Monitoring du trafic et des connexions

- SmartView Tracker
- Login sur le SmartView Tracker
- Types de Log
- Onglets du SmartView Tracker
- Icones d'action
- Gestion des fichiers de Log
- Audit des administrateurs
- Gestion globale des logs et des alertes
- Paramètres de temps
- Bloquer les connexions
- Mettre fin et terminer les connexions actives
- SmartView Monitor
- Login sur le SmartView Monitor
- Personnaliser les vues
- Monitoring des règles d'activité suspectes
- Monitoring les alertes
- SmartView Tracker par rapport au SmartView Monitor
- Eventia Reporter
- Types de rapports
- Rapports prédéfinis
- Personnaliser les rapports prédéfinis
- Considérations du Eventia Reporter
- Licences du Eventia Reporter

Module 5 gestion des utilisateurs et authentification

- Création des utilisateurs et des groupes dans SmartDashboard
- Introduction à l'authentification VPN-1
- Introduction aux méthodes d'authentification
- Schémas d'authentification
- Méthodes d'authentification
- Authentification utilisateur
- Configuration de l'authentification utilisateur
- Authentification de type Session
- Configuration de l'Authentification de type Session
- Authentification de type Client
- Configuration de l'Authentification de type Client
- Résolution des conflits d'accès
- Configuration du suivi de l'authentification
- Gestion des utilisateurs sous LDAP avec SmartDirectory
- Fonctionnalités LDAP
- Serveurs LDAP multiples
- Utilisation d'un serveur LDAP existant
- Configuration d'entités pour fonctionner avec VPN-1
- Gestion des utilisateurs
- Groupes Smart Directory

Module 6 Check Point QoS

- Aperçu de la QoS sous Check Point
- Stateful Inspection
- Moteur d'Intelligent Queuing
- Algorithme « Weighted Flow Random Early Drop »
- Algorithme «Retransmission Detection Early Drop»
- Architecture de QoS de Check Point
- Architecture de base
- SmartCenter pour la QoS
- SmartConsole pour la QoS
- La passerelle de sécurité
- Déploiement de la QoS.
- Restrictions de topologie QoS sous Check Point
- Base de règles QoS sous Check Point
- Allocation et règles de bande passante
- Modes traditionnels et express
- Propriétés d'action de la QoS
- Allocation et sous-règles de la gestion de bande passante
- Implémentation de la base de règles
- Considération de la base de règles QoS
- Services DiffServ.
- Marquages DiffServ pour les paquets IPSEC
- Interaction entre les règles DiffServ et les autres
- Queues à faible latence (LLQ)
- Classes à faible latence
- Priorités des classes à faible latence
- Quand utiliser les queues à faible latence
- QoS authentifiée
- Monitoring de la politique de QoS
- SmartView Tracker
- SmartView Monitor
- Eventia Reporter
- Optimisation de la QoS Check Point

Module 7 Principe de SmartDefense et de l'inspection de contenu

- Introduction à SmartDefense
- Intelligence réseaux et applicative
- Intelligence Web
- Mises à jour en ligne
- Mode de monitoring uniquement
- Sécurité réseau
- Déni de service
- IP et ICMP
- TCP
- Modification des empreintes
- Evenements successifs
- DShield Storm Center
- Scan de ports
- Application Intelligence
- Messagerie
- FTP
- Réseaux Microsoft
- Peer-to-Peer
- Messagerie instantanée
- DNS
- VoIP
- SNMP
- Web Intelligence
- Protections via Web Intelligence
- Mise en oeuvre de la licence dans Web Intelligence
- Services SmartDefense
- Onglet des téléchargements



- Onglet des conseils
- Onglet des recommandations en matière de sécurité
- Inspection du contenu
- Introduction aux technologies antivirales et de filtrage Web intégrées
- Mises à jour des bases de données
- Paramètres de scan antiviral
- Filtrage Web