



# Check Point EndPoint Security Secure Access R70

---

<b>Objectif</b>	Endpoint Security de Check Point est une approche unifiée permettant de protéger les postes de travail des accès non autorisés et illicites. Le module Secure Access permet de protéger contre les usages non autorisés des postes ainsi que les menaces telles que les spywares et les attaques virales en utilisant le contrôle des programmes, le firewall personnel, et l'usage de réseaux privés virtuels. Ce cours vous apprend à configurer et gérer un client Endpoint Security en utilisant la console d'administration
<b>Pré requis</b>	Pour suivre ce stage, il est nécessaire d'avoir des compétences sur TCP/IP et sur le routage statique. Connaissances des environnements Windows Server et d'Internet...
<b>Durée</b>	2 jours

## Contenu

---

### Module 1 : introduction à Endpoint Security

- Aperçu d' Endpoint Security
- Architecture système
- Principales fonctionnalités de sécurité
- Communications, modes et vues
- Ports
- Modes et vues
- Changement des vues
- Activer les politiques
- Gestion des catalogues et des groupes
- Authentification des utilisateurs
- Catalogues d'utilisateurs
- Planification
- Pré requis
- Choix du type de client
- Choix des types de politique d'entreprise
- Choix du modèle de sécurité
- Modèle d'administration générale

### Module 2 : l'infrastructure de sécurité

- Introduction aux politiques de sécurité
- Politiques connectées
- Politiques déconnectées
- Arbitrage entre les politiques
- Packages de politiques
- Assignation de politiques
- Aperçu du composant de politique de sécurité
- Gestion des politiques de sécurité
- Diagramme de la politique
- Introduction aux packages d'installation du client
- Diagramme du package client
- Planification de la distribution client
- Options de déploiement
- Types de client
- Nouvelles versions du client
- Politiques
- Assignation des politiques
- Options d'installation
- Configuration du réseau du client
- Configurer une nouvelle connexion réseau

### Chapitre 3 : fonctionnalités avancées d' Endpoint Security

- Program Control
- Permissions des programmes.
- Groupes de programmes
- Ordre de priorité des permissions
- Permissions globales et de politiques..
- Diagramme du Program Control
- Astuces de planification du contrôle de programme
- Protection contre les spywares
- Disques cibles du scan et exclusions
- Options de traitement
- Diagramme de l'anti-spyware
- Protection contre les virus
- Méthodes de scan
- Disques cibles du scan et exclusions
- Options de traitement
- Monitoring de l'activité antivirus et antispyware
- Monitoring de l'activité infectieuse sur les postes de travail connectés
- Monitoring de l'historique des spywares et virus
- Monitoring du statut d'infection et des mises à jour DAT
- Mise en œuvre des critères de sécurité de poste
- Types de règles mise en œuvre
- Processus des règles mises en œuvre
- Diagramme des règles mises en œuvre
- Règles du fournisseur antiviral
- Règles de mise en œuvre sur le poste client
- Grouper les règles de mise en oeuvre et les règles du fournisseur antiviral
- Ressources de remédiation
- Utiliser des règles qui observent ou avertissent
- Tracer la concordance des règles de mise en oeuvre
- Visualiser le statut de compliance
- Violations par règle et politique
- Visualiser les versions d'antivirus
- Haute disponibilité
- Architecture
- Configuration de la haute disponibilité
- Forcer la réplication



#### **Module 4 : mise en œuvre coopérative et VPN**

- Passerelles et mise en œuvre coopérative
- Bases des réseaux privés virtuels
- Configuration de la connexion au réseau privé virtuel
- Configuration des profils et des sites
- Options VPN et diagramme
- Gestion des profils de connexion
- Gestion des sites VPN
- Gestion des certificats
- Configuration des options de connexion