Check Point
SOFTWARE TECHNOLOGIES LTD.

Le firewall contrôle l'accès au réseau, c'est la première barrière de sécurité.

Le VPN permet des connexions site à site chiffrées et sécurisées.

Détection et prévention d'activités anormales sur le réseau:

exploitation de failles logicielles ou navigateurs connues, scans de ports,…

Convivialité de l'interface de Management ?

Capacité d'analyse des logs et des remontées d'information de la part des passerelles de sécurité ?

=> outils de SIEM, alerting en cas d'incidents,…

bot : robot logiciel installé sur le plus de machines possible afin de former un réseau (botnet). Les bots se connectent sur des serveurs au travers desquels ils reçoivent des instructions (envoi de spams, vol d'information, participation à des attaques Ddos...).

Les politiques de sécurité sont-elles construites sur des adresses IP ou directement en fonction des utilisateurs / groupes d'utilisateurs?

Synchronisation avec l'annuaire?

Attaque 0 day : infection par un virus non connu ou une variante de virus connu. Peut être lié au délai de mise à jour des bases antivirales.

Quelle est la politique d'encadrement des accès web (surf et applications):

Blocage des URL compromises et applications dangereuses

Responsabilité légale

Contrôle de la productivité

Utilisation de la bande passante

Comment se fait la connexion des terminaux distants?

L'accès aux ressources est-il protégé?

Quelle protection sur le poste?

Quelle mesure en cas de perte ou de vol?

Quelle sécurité pour les terminaux mobiles se connectant via des hotspots et wifi non maîtrisés?

Quelle sécurité pour l'accès et les données stockées sur des smartphones et tablettes (BYOD)?

Comment contrôler la confidentialité d'un document dans le cadre d'échange hors de l'entreprise?

Management Global :

Blade Network Policy Management : permet aux administrateurs de se connecter au serveur d'administration centralisé et de définir des politiques de sécurité, de VPN de QoS, de filtrage de contenu (IPS, URL, Antivirus, Antispam).

Blade Logging & Status : permet de consulter les logs et sessions actives afin de contrôler la sécurité et suivre l'activité réseau.

Blade SmartEvent /Smartreporter: outil de corrélation d'évènements et de logs en temps réels remontés par les passerelles Check Point et par d'autres équipements de sécurité et de réseau. Fournit également des rapports graphiques complets et intuitifs.

Blade Firewall : produit historique CHKP, intégre les techno Stateful Inspection & Application Intelligence. Les fonctionnalités majeures sont le contrôle d'accès, le NAT, l'authentification et le mode « bridge ».

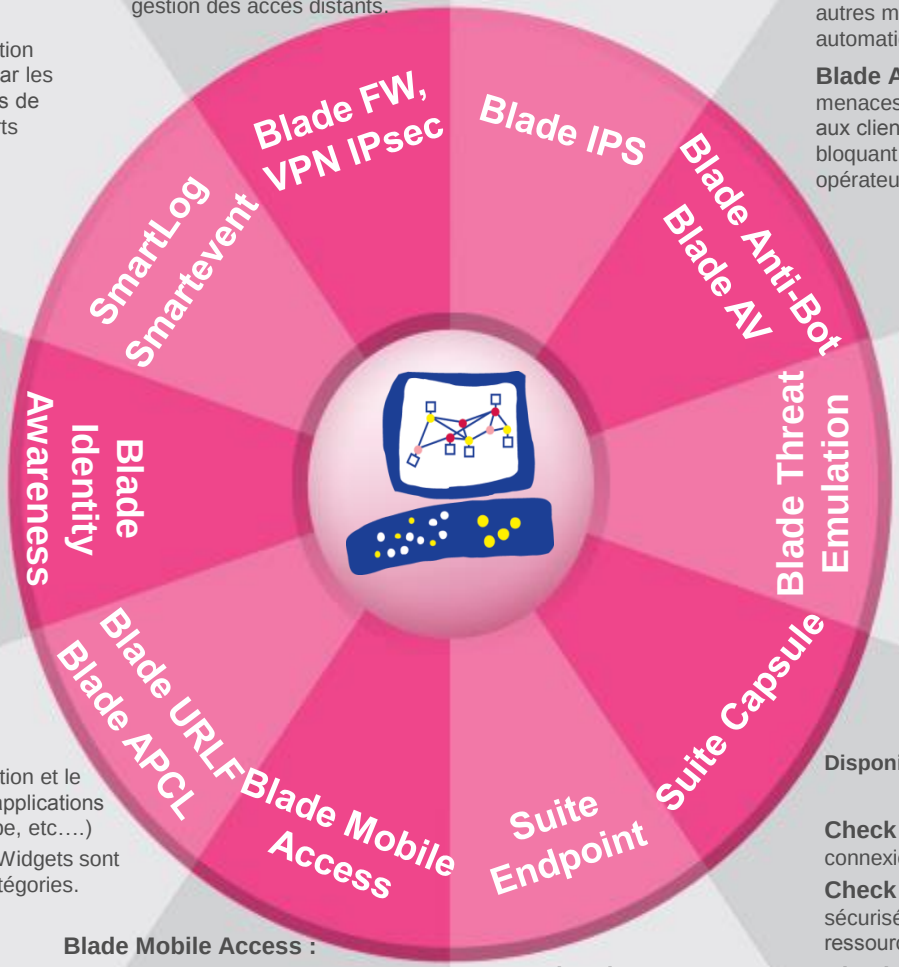
Blade VPN IPSEC : passerelle de chiffrement pour l'interconnexion site à site et la gestion des accès distants.

Blade IPS : intègre les fonctions de détection d'intrusions et de contrôle applicatifs tels que la messagerie instantanée et le Peer-to-Peer.

Check Point SOFTWARE TECHNOLOGIES LTD.

Blade Antivirus & Anti-Malware : protection AV/AM incluant un moteur heuristique propre à stopper virus, vers et autres malwares. Les bases de signatures sont mises à jour automatiquement.

Blade Anti-bot: offre une protection contre les bots et les menaces persistantes avancées (APT). Cette Blade permet aux clients de détecter les bots et d'éviter les dommages en bloquant la communication entre les hôtes contaminés et les opérateurs à distance.



Blade Threat Emulation : cette Blade introduite avec la version R77 offre une solution innovante permettant l'inspection rapide des fichiers et les exécutions dans un bac à sable virtuel afin de découvrir tout comportement malveillant. Les logiciels malveillants découverts sont stoppés avant qu'ils ne puissent pénétrer dans les réseaux

Blade Identity Awareness : Avec cette Blade, l'administrateur peut construire sa politique de sécurité sur l'identité des utilisateurs et des machines. Peut se faire selon 3 méthodes distinctes:

- Clientless (synchronisation avec l'annuaire)
- Via Agent
- Browser based

Blade Application Control : détection et le contrôle en temps réel de l'accès aux applications (Facebook, Twitter, Tor, Skype, Youtube, etc….)

Plus de 4.500 applications et 100.000 Widgets sont ainsi répertoriés et réparties en 150 catégories.

Blade URL Filtering : référence plus de 21 millions d'URLs au travers de 40 catégories pour garantir un usage professionnel et optimisé du surf Internet. La liste des URLs est mise à jour en temps réel avec plus de 100000 nouveaux sites par semaine

Blade Mobile Access :

Accès distant via un portail Web offrant une connexion sécurisée (VPN SSL) et une protection complètes des postes utilisateurs, des données manipulées durant une session et des ressources applicatives à disposition.

Protection du poste :

FW et AV de poste

Remote Acces (VPN)

Cryptage du disque dur et des ports

Suite complète : AB, URLF, Forensics

Disponible sur PC/MAC, IOS/Android

Check Point Capsule Cloud : filtrage des connexions sortantes des terminaux depuis le Cloud.

Check Point Capsule Workspace : container sécurisé sur les terminaux mobile pour accéder aux ressources de l'entreprise.

Check Point Capsule Docs : protège les documents en mettant un niveau de classification permettant le contrôle de leurs diffusions.

softwareblades™