Forum: Aide - Recherche de logiciels

Topic: Comodo Firewall ou Internet Suite, telle est ma question

Subject: Re: Comodo Firewall : règle finale pour bloquer tout sauf autorisé ?

Publié par: Popeye23

Contribution le : 08/03/2011 23:52:58

Il faut d'abord mettre le firewall en niveau de sécurité "personnalisé (Clic droit sur l'icône du systray)
Ensuite utiliser les applis qui ont le droit de sortir, et répondre de façon adéquate aux messages de Comodo.
Pour chaque appli, Comodo demandera d'abord l'autorisation de sortie en UDP sur le port 53, puis dans un deuxième temps l'autorisation pour aller sur le net.
Cela donnera des règles plus ou moins nombreuses pour un même programme, c'est pourquoi je suggère de définir soi-même des règles prédéfinies, cela évite d'avoir plusieurs règles pour une même appli. J'en ai défini pour DNS, clients mails, navigateurs etc. Une règle prédéfinie peut être utilisée au sein d'une autre. C'est le cas de la règle DNS qui est obligatoire pour la résolution de noms (sortie en UDP port de destination 53), et aussi le loopback (IP sortant, destination "zone réseau", choisir "loopback zone")
Également, à moins que vous ayez défini une ip précise pour votre carte réseau, il faut une règle pour le DHCP : autoriser svchost.exe avec une règle prédéfinie nommée DHCP : autoriser UDP sortant port source 68, port de destination 67.
Svchost.exe a besoin aussi de pouvoir sortir en TCP sur les ports 80 et 443 pour Windows Update.
J'ai pour ma part crée une règle spéciale pour ça que je valide quand c'est nécessaire, car il faut savoir que si on autorise cela de façon permanente, le risque d'un malware utilisant svchost pour sortir existe.

Pour la dernière règle qui bloque tout :
Il suffit d'ajouter dans "Règles de programmes":

- Programme-> Choisir -> Groupe de fichiers -> All applications
- Stratégie prédéfinie : Blocked application

En bas de liste bien sur, et en veillant bien à la repositionner si vous autorisez une autre application à sortir après.
Comme avec Kerio, cette règle empêchera Comodo de signaler une tentative de sortie
Dans cette stratégie la journalisation est activée.
On peut l'enlever en modifiant la stratégie "Blocked application" via "Stratégie de sécurité réseau" -> Règles Prédéfinies

Et aussi dans "gérer mes configurations", faire une sauvegarde.

Bon courage.