Firewall

Julien Danjou
jdanjou@linuxenrezo.org

Le principe du firewall est de stopper les connections dont on ne veut pas ou/et d'accepter celle que l'on veut (filtrer les connections).

Dans cette exemple, un routeur a 3 cartes réseau et donc 3 adresses :

IP (eth0 = 192.168.0.1 eth1 = 192.168.0.65 eth2 = 192.168.0.129)

On veut que le sous-réseau 0 (qui est connecté à la carte eth0 du routeur), le sous-réseau 1 (qui est connecté à la carte eth1 du routeur) et le sous-réseau 2 (qui est connecté à la carte eth2 du routeur) communiquent de la fa¸con suivante (SR0 = sous réseau 0, connecté à eth0 du routeur):
SR0 SR1
SR1 SR0
SR2 SR1
SR2 SR1

Cela signifie que les sous réseau 0 et 1 pourront communiquer ensemble, mais que le sous-réseau 2 ne sera pas accessible depuis les sous réseau 0

1. En revanche, le sous réseau 2 a lui accès au sous réseau 0 et 1. Il pourrait être un sous réseau composé de PC important (comportant des données confidentielles ou critique: comptabilité, salaire...) dont on veut empecher l'accès de l'extérieur du sous réseau lui même...

Voilà un schéma récapitulatif:

Je n'ai mis ici qu'un PC par sous réseau, ce qui est possible mais un peu absurde....

Il faut donc ajouter dans un script de démarrage (par exemple /etc/rc.d/rc.local):

On efface toutes les règles
/sbin/ipchains -F

Autorise le SR0 à accéder au SR1
ipchains -A forward -s 192.168.0.0/24 -d 192.168.0.64/24 -j ACCEPT

Autorise le SR1 à accéder au SR0
ipchains -A forward -s 192.168.0.64/24 -d 192.168.0.0/24 -j ACCEPT

Autorise le SR2 à accéder à tout les SR
ipchains -A forward -s 192.168.0.128/24 -d 0.0.0.0/0 -j ACCEPT

Refuse les connections vers SR2
ipchains -A forward -s 0.0.0.0/0 -d 192.168.0.128/24 -d 0.0.0.0 -j REJECT

Oui, mais j'ai fait une erreur car il est stupide de bloquer toutes les connexions allant vers SR2, car il ne pourra recevoir aucun paquet, donc aucune réponse á ses requêtes ! C'était pour voir si vous suiviez)

Donc il faut boquer seulement les tentatives de connexions, c'est á dire les paquets SYN. Pour cela on rajoute l'option -y

Ce qui donne:

Refuse les connections vers SR2

ipchains -A forward -p tcp -s 0.0.0.0/0 -d 192.168.0.128/24 -d 0.0.0.0 -j REJECT -y

Notez toutefois que j'utilise ici les adresses IP des sous-réseaux, mais il est aussi possible d'utiliser des adresses IP de machines. On pourrait, par exemple, ne laisser qu'une machine par sous-réseau accéder aux autre sous-réseaux afin de réduire le trafic passant pas le routeur.

Si vous voulez bloquez des connections entrantes, il suffit de remplacer forward par input, ou output pour des connections sortantes.

Protection Anti-spoofing

On ma demandé plusieurs fois comment se protger de l'ip spoofing. L'ip spoofing est une méthode qui consiste à se faire passer pour un PC que l'on n'est pas. En clair, cela signifie que quelqu'un vous envoie des packets avec comme origine "thorique" une machine de votre réseau local !

Pour se protéger de cela, voilà ce qu'il faut rajouter dans votre script de firewall:

/sbin/ipchains -A input -i ! eth0 -s 192.168.0.0/24 -d 0.0.0.0/0 -j DENY

Cela signifie que si des packets arrivant de votre connection modem (ppp0) (vous pouvez le modifier par eth1 si vous avez une connexion par câble ou ADSL) ayant pour adresse une adresse de votre réseau local (changez 192.168.0.0 par l'adresse du réseau connectez à eth0 par exemple), ils seront littéralement explosé à coups de batte de base-ball sans avertissement.