Technicien Supérieur Gestionnaire
de Ressources Informatiques
et Réseaux

Configuration Express

Netfilter IPtable

Behind the wall

netfilter
firewalling, NAT, and packet mangling for linux

O RLY?

L.Marchal

Table des matières

Filtrage de paquets avec Netfilter....1
Fichier interfaces....2
Regles iptables....2
pre-up iptables-restore < /etc/iptables.up.rules....2
pre-up ip6tables-restore < /etc/ip6tables.up.rules....2
Iptables.up.rules suite....3
Suite....4
Modifier le fichier : /etc/sysctl.conf....4
NAT....5

Filtrage de paquets avec Netfilter

Trouver les interfaces

Il peut être utile de savoir qui est qui.

A cette occasion j'utilise :

ip a

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 08:00:27:e6:65:a3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.102/24 brd 192.168.8.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee6:65a3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen
1000
    link/ether 08:00:27:e3:37:85 brd ff:ff:ff:ff:ff:ff
```

Qui voit les 2 carte contrairement à :

ifconfig

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:e6:65:a3
          inet adr:192.168.8.102  Bcast:192.168.8.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fee6:65a3/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:823 errors:0 dropped:0 overruns:0 frame:0
          TX packets:492 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:73856 (72.1 KiB)  TX bytes:69128 (67.5 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Toutefois ifconfig donne des informations importantes.

Fichier interfaces

La carte regardant dehors, le WAN sur la eth0 en DHCP, le LAN sur l'autre carte eth1, en fixe faisant donc office de passerelle.

On indique quel fichiers charger au lancement du service ici les règles de routages que nous nous apprêtons à éditer.

```
# Carte WAN eth0
# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

# Carte LAN eth1 Reseau grp3
allow-hotplug eth1
iface eth1 inet static
        address 172.25.3.254
        netmask 255.255.255.0
        Broadcast 172.25.3.255

      pre-up iptables-restore < /etc/iptables.up.rules
      pre-up ip6tables-restore < /etc/ip6tables.up.rules
```

Regles iptables

Le fichier est commenté, et vous disposez du même fichier.

```
# /etc/iptables.up.rules
# Script qui démarre les règles de filtrage IPv4
# Formation Debian GNU/Linux par Alexis de Lattre
# http://formation-debian.via.ecp.fr/

# iptables-restore(8) remet implicitement à zéro toutes les règles

# Les instructions qui suivent concernent la table « filter »,
# c'est-à-dire… le filtrage.
*filter

#########################
# Politiques par défaut #
#########################
# Les politiques par défaut déterminent le devenir d'un paquet auquel
# aucune règle spécifique ne s'applique.

# Les connexions entrantes sont bloquées par défaut
-P INPUT DROP                                   #c'est mieux
# Les connexions destinées à être routées sont acceptées par défaut
-P FORWARD ACCEPT
# Les connexions sortantes sont acceptées par défaut
-P OUTPUT ACCEPT                                #ça peut servir

######################
# Règles de filtrage #
######################
# Nous précisons ici des règles spécifiques pour les paquets vérifiant
# certaines conditions.

# Pas de filtrage sur l'interface de "loopback"
-A INPUT -i lo -j ACCEPT                        #Evidement

# Accepter le protocole ICMP (notamment le ping)
-A INPUT -p icmp -j ACCEPT                      #ça peut servir
```

Iptables.up.rules suite

```
# Accepter le protocole IGMP (pour le multicast)
-A INPUT -p igmp -j ACCEPT                                  #Dans une SI ça sert
# Accepter les packets entrants relatifs à des connexions déjà
# établies : cela va plus vite que de devoir réexaminer toutes
# les règles pour chaque paquet.
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT      #Maintient de la connexion

# Décommentez la ligne suivante pour que le serveur SSH éventuel
# soit joignable de l'extérieur
#-A INPUT -p tcp --dport ssh -j ACCEPT                      #C'est selon, prévoir Fail2Ban

# Décommentez la ligne suivante pour que le serveur de courrier éventuel soit
# joignable de l'extérieur. Laissez bien smtps et submission si vous avez
# activé les services SMTPS et soumission de messages… L'option --dports
# permet de traiter plusieurs ports en une fois.
#-A INPUT -p tcp --dports smtp,smtps,submission -j ACCEPT

# Décommentez les deux lignes suivantes pour que le serveur de noms
# éventuel soit joignable de l'extérieur.
#-A INPUT -p tcp --dport domain -j ACCEPT
#-A INPUT -p udp --dport domain -j ACCEPT

# Décommentez la ligne suivante pour que le serveur Web éventuel
# soit joignable de l'extérieur.
#-A INPUT -p tcp --dport http -j ACCEPT
# Si vous avez activé le HTTPS…
#-A INPUT -p tcp --dport https -j ACCEPT

# Décommentez les deux lignes suivantes pour que le serveur d'impression
# éventuel soit joignable de l'extérieur.
#-A INPUT -p tcp --dport ipp -j ACCEPT
#-A INPUT -p udp --dport ipp -j ACCEPT


# Décommentez les deux lignes suivantes pour que le serveur Samba
# éventuel soit joignable de l'extérieur.
#-A INPUT -p tcp --dport netbios-ssn -j ACCEPT
#-A INPUT -p udp --dport netbios-ssn -j ACCEPT

# Décommentez la ligne suivante pour que des clients puissent se connecter
# à l'ordinateur par XDMCP.
#-A INPUT -p udp --dport xdmcp -j ACCEPT

# Décommentez la ligne suivante pour que l'ordinateur puisse se connecter
# par XDMCP à une machine distante).
#-A INPUT -p tcp --dport x11-1 -j ACCEPT

# Décommentez la ligne suivante pour pouvoir recevoir des flux VideoLAN.
#-A INPUT -p udp --dport 1234 -j ACCEPT

# Décommentez la ligne suivante pour pouvoir recevoir des annonces SAP
# (ce sont des annonces de session multicast).
#-A INPUT -p udp -d 224.2.127.254 --dport 9875 -j ACCEPT

# Décommentez les 3 lignes suivantes pour pouvoir utiliser GnomeMeeting
#-A INPUT -p tcp --dport 30000:33000 -j ACCEPT
#-A INPUT -p tcp --dport 1720 -j ACCEPT
#-A INPUT -p udp --dport 5000:5006 -j ACCEPT

# Décommentez la ligne suivante pour pouvoir partager de la musique par
# DAAP.
#-A INPUT -p tcp --dport daap -j ACCEPT

# Décommentez la ligne suivante pour que votre ordinateur
# annonce son nom et ses services par mDNS sur le réseau local (cela
# permet de le contacter sous « son nom d'hôte ».local).
#-A INPUT -p udp -d 224.0.0.251 --dport mdns -j ACCEPT
```

Suite

```
# La règle par défaut pour la chaine INPUT devient REJECT (contrairement
# à DROP qui ignore les paquets, avec REJECT, l'expéditeur est averti
# du refus). Il n'est pas possible de mettre REJECT comme politique par
# défaut. Au passage, on note les paquets qui vont être jetés, ça peut
# toujours servir.
-A INPUT -j LOG --log-prefix "paquet IPv4 inattendu "
-A INPUT -j REJECT

COMMIT



# Les instructions qui suivent concernent la table « nat ».
*nat

########################
# Partage de connexion #
########################

# Décommentez la ligne suivante pour que le système fasse office de
# routeur NAT et remplacez « eth0 » par le nom de l'interface
# connectée à Internet.
-A POSTROUTING -o eth0 -j MASQUERADE


########################
# Redirections de port #
########################

# Décommentez la ligne suivante pour que les requêtes TCP reçues sur
# le port 80 de l'interface eth0 soient redirigées à la machine dont
# l'adresse IPv4 est 192.168.0.3 sur son port 80 (la réponse à la
# requête sera transférée au client)Vous pouvez tout à fait indiquer un autre port.
#-A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.3:80

COMMIT

####################
# Problème de MTU… #
####################

# Les instructions qui suivent concernent la table « mangle », c'est
# à dire l'altération des paquets
*mangle

# Si la connexion que vous partagez est une connexion ADSL directement gérée
# par votre ordinateur, vous serez probablement confronté au fameux problème du
# MTU. En résumé, le problème vient du fait que le MTU de la liaison entre
# votre fournisseur d'accès et le serveur NAT est un petit peu inférieur au MTU
# de la liaison Ethernet qui relie le serveur NAT aux machines qui sont
# derrière le NAT. Pour résoudre ce problème, décommentez la ligne suivante et
# remplacez « eth0 » par le nom de l'interface connectée à Internet.
#-A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS -o eth0 --clamp-mss-to-pmtu

COMMIT
```

Modifier le fichier : /etc/sysctl.conf

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1
```

NAT

Network Address Translation.

Cette méthode permet de « dissimuler » ; « cammoufler » les adresse IP Privé derrière un routeur .

Le routeur organise et enregistre les requêtes des clients (le socket) afin de ne présenter que l'IP public.

Cela se met en place très facilement comme ceci :

```
########################
# Partage de connexion #
########################

# Décommentez la ligne suivante pour que le système fasse office de
# routeur NAT et remplacez « eth0 » par le nom de l'interface
# connectée à Internet.
-A POSTROUTING -o eth0 -j MASQUERADE
```