IO4 2005 - Exemples de règles de filtrage

```
#!/bin/sh

#
# Protection d'une machine avec adresse publique
# reliée à internet
#
INT=eth0

# 1. Chargement des modules utiles

modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe iptable_nat
modprobe ipt_multiport
modprobe ipt_MASQUERADE

# 2. Effacement des tables prédéfinies, et politiques par défaut

# on autorise toutes les communications sortantes
iptables -F OUTPUT  ; iptables -P OUTPUT  ACCEPT

# par défaut, rien ne doit rentrer (sauf ce qui sera
# explicitement autorisé)
iptables -F INPUT   ; iptables -P INPUT   DROP

# rien ne traverse cette machine (ce n'est pas un routeur)
iptables -F FORWARD ; iptables -P FORWARD DROP

# 3. Le filtrage des entrées

# les paquets entrants liés à une connexion déjà établie sont acceptés
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# ce qui vient de l'interface locale aussi.
iptables -A INPUT -i lo -j ACCEPT

# et quelques ports bien connus

iptables -A INPUT --protocol udp --destination-port domain -j ACCEPT
iptables -A INPUT --protocol tcp --destination-port domain -j ACCEPT
iptables -A INPUT --protocol tcp --destination-port 80     -j ACCEPT
iptables -A INPUT --protocol tcp --destination-port 20:23  -j ACCEPT
iptables -A INPUT --protocol tcp --destination-port 25     -j ACCEPT
iptables -A INPUT --protocol tcp --destination-port pop3   -j ACCEPT
iptables -A INPUT --protocol tcp --destination-port imap2  -j ACCEPT
```

```
#!/bin/sh

#
# Firewall pour une machine qui sert aussi de routeur
# pour un réseau privé.

# les interfaces, et le réseau local
EXTERIEUR=eth0
INTERIEUR=eth1
LAN="192.168.1.0/24"

# chargement des modules
for m in ip_conntrack  ip_conntrack_ftp iptable_nat \
      ipt_multiport ipt_MASQUERADE
do
   modprobe $m
done

# vidage des tables (flush), politiques par défaut
iptables -F INPUT    ; iptables -P INPUT DROP
iptables -F OUTPUT   ; iptables -P OUTPUT ACCEPT
iptables -F FORWARD  ; iptables -P FORWARD DROP
iptables -F POSTROUTING -t nat

# nouvelle table
iptables -N controle  ; iptables -F controle

#### paquets destinés au routeur

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i $INTERIEUR                        -j ACCEPT
iptables -A INPUT -i lo                                -j ACCEPT
iptables -A INPUT -i $EXTERIEUR                        -j controle

#### paquets traversant le routeur

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD --source $LAN                         -j ACCEPT


#### « masquerading » des paquets qui partent vers l'extérieur ########

iptables -t nat -A POSTROUTING \
    --source $LAN --dest \! $LAN -j MASQUERADE

echo 1 > /proc/sys/net/ipv4/ip_forward

#####  Contrôle des entrées ############################################

iptables -A controle --protocol udp --destination-port domain -j ACCEPT
iptables -A controle --protocol tcp --destination-port domain -j ACCEPT

iptables -A controle --protocol tcp --destination-port 80     -j ACCEPT
iptables -A controle --protocol tcp --destination-port 25     -j ACCEPT

iptables -A controle                                           -j DROP
```