Exemple de configuració de iptables

Fitxer de configuració simple de iptables.

El podem posar a /etc/init.d perquè s'executi quan engega l'ordinador

```
#!/bin/bash
#-----------------Script a executar quant es connecta-----------------
IPTABLES="/sbin/iptables"
#----------------------Fi configuracio-----------------------

$IPTABLES -F
$IPTABLES -t nat -F
$IPTABLES -t mangle -F
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P FORWARD DROP
$IPTABLES -P OUTPUT ACCEPT

#prioritat ssh
iptables -A PREROUTING -t mangle -p tcp --sport ssh \
        -j TOS --set-tos Minimize-Delay

#spoofing
$IPTABLES -A INPUT -s ! 192.168.0.0/24 -i eth1 -j REJECT
$IPTABLES -A INPUT -s ! 192.168.1.0/24 -i eth0 -j REJECT

$IPTABLES -A FORWARD -s ! 192.168.0.0/24 -i eth1 -j REJECT
$IPTABLES -A FORWARD -s ! 192.168.1.0/24 -i eth0 -j REJECT

$IPTABLES -A INPUT -s 127.0.0.1/255.0.0.0 -i ! lo -j REJECT

$IPTABLES -A INPUT -p tcp --destination-port 1024 -j REJECT


#activar masquerading des de dins (per 2 xarxes)
$IPTABLES -A FORWARD -s 192.168.0.0/24 -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED \
        -d 192.168.0.0/24 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -o eth2 -s 192.168.0.0/24 -j MASQUERADE


$IPTABLES -A FORWARD -s 192.168.1.0/24 -j ACCEPT
```

```
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED \
        -d 192.168.1.0/24 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -o eth2 -s 192.168.1.0/24 -j MASQUERADE

#tallem tot lo de fora i obrim uns ports només
$IPTABLES -I INPUT -p tcp -i eth2 -j REJECT
$IPTABLES -I INPUT -p tcp -i eth2 -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 25 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 80 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 110 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 22 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 21 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 443 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 995 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 5222 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 5223 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --destination-port 5269 -j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --source 213.97.34.169 --destination-port 873
-j ACCEPT
$IPTABLES -I INPUT -p tcp -i eth2 --source 80.33.45.115 --destination-port 873
-j ACCEPT

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

Carles Pina i Estany
cpina@salleurl.edu
Juny 2004