Annex 3

Exemples de configuracions de tallafocs

1. Política general d'acceptació per el tallafocs

```
#!/bin/sh
## Exemple configuració IPTABLES LAN-INTERNET
## Serveis oberts als ports: 22, 25, 80, 110, 443, 10000 cap a l'exterior.
## Fem Neteja
iptables −F
iptables −X
iptables −Z
iptables −t nat −F
## Política per defecte d'acceptació a TOT (perillós!!)
iptables −P INPUT ACCEPT
iptables −P OUTPUT ACCEPT
iptables −P FORWARD ACCEPT
iptables −t nat −P PREROUTING ACCEPT
iptables −t nat −P POSTROUTING ACCEPT
## FILTRE des de l'exterior
iptables −A INPUT −i lo −j ACCEPT
iptables −A INPUT −s 192.168.1.0/24 −i eth1 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 22 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 25 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 80 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 110 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 443 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −p tcp −−dport 10000 −j ACCEPT
## FILTRE de la xarxa local
iptables −A FORWARD −s 192.168.1.0/24 −i eth1 −p tcp −−dport 80 −j ACCEPT
iptables −A FORWARD −s 192.168.1.0/24 −i eth1 −p tcp −−dport 443 −j ACCEPT
iptables −A FORWARD −s 192.168.1.0/24 −i eth1 −p tcp −−dport 53 −j ACCEPT
iptables −A FORWARD −s 192.168.1.0/24 −i eth1 −p udp −−dport 53 −j ACCEPT
iptables −A FORWARD −s 192.168.1.0/24 −i eth1 −j DROP
# MASQUERADING i FORWARDING
iptables −t nat −A POSTROUTING −s 192.168.1.0/24 −o eth0 −j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables −A INPUT −s 0.0.0.0/0 −i eth0 −p tcp −dport 1:1024 −j DROP
iptables −A INPUT −s 0.0.0.0/0 −i eth0 −p udp −dport 1:1024 −j DROP
```

2. Política general de denegació per el tallafocs

```
#!/bin/sh
## DROP per defecte
## Fem neteja
iptables −F
iptables −X
iptables −Z
iptables −t nat −F
## Política per defecte de denegació total
iptables −P INPUT DROP
iptables −P OUTPUT DROP
iptables −P FORWARD DROP
## FILTRE
iptables −A INPUT −s 127.0.0.1 −j ACCEPT
iptables −A OUTPUT −d 127.0.0.1 −j ACCEPT
iptables −A INPUT −s 0.0.0.0/0 −j DROP
# Donem accés a diferents ports
iptables −A FORWARD −d 0.0.0.0 −p tcp −−dport 22 −j ACCEPT
iptables −A FORWARD −s 0.0.0.0 −p tcp −−sport 22 −j ACCEPT
iptables −A FORWARD −d 0.0.0.0 −p tcp −−dport 80 −j ACCEPT
iptables −A FORWARD −s 0.0.0.0 −p tcp −−sport 80 −j ACCEPT
iptables −A FORWARD −d 0.0.0.0  −p tcp −−dport 25 −j ACCEPT
iptables −A FORWARD −s 0.0.0.0  −p tcp −−sport 25 −j ACCEPT
iptables −A FORWARD −d 0.0.0.0  −p tcp −−dport 110 −j ACCEPT
iptables −A FORWARD −s 0.0.0.0  −p tcp −−sport 110 −j ACCEPT
iptables −A FORWARD −d 0.0.0.0  −p tcp −−dport 143 −j ACCEPT
iptables −A FORWARD −s 0.0.0.0 −p tcp −−sport 143 −j ACCEPT
iptables −A FORWARD −d 0.0.0.0 −p tcp −−dport 443 −j ACCEPT
iptables −A FORWARD −s 0.0.0.0 −p tcp −−sport 443 −j ACCEPT
# I seguirem afegint fins i tot redireccions
```