Pare-feu à écran

0. Principe

1. Réalisation du réseau

a. Cablage du réseau
   ip a a 192.168.2.5/24 dev eth0
   ip r a 192.168.2.0/24 dev eth0
   ip r a default via 192.168.2.1

b. Configuration du fichier « /etc/inetd.conf »
   finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd
   inetd

c. Configuration pour les serveurs FTP/Web

d. Configuration pour le serveur Web

e. Test du fonctionnement :
   Pour le serveur Web : lynx 192.168.2.29
   Pour le serveur FTP : ncftp 192.168.2.17 (anonymous acces)
   Pour le serveur Finger : finger root@192.168.2.5

2. Policy

a. Accès aux services des serveurs : Le pare feu a accès aux services (via les commandes citées ci-dessus.)

b. Accès aux services des pare-feux : Les services du pare-feu sont accessibles.

c. Accès des clients « internet » aux services des serveurs : Les clients peuvent accéder aux services des serveurs.

d. Modification de « FORWARD » (interdit) et « INPUT/OUTPUT » (autorisé)

```
ip tables –P FORWARD DROP
ip tables –P INPUT ACCEPT
ip tables –P OUTPUT ACCEPT
```

e. Modification de « FORWARD » (autorisé) et « INPUT/OUTPUT » (interdit)

```
ip tables –P FORWARD ACCEPT
ip tables –P INPUT DROP
ip tables –P OUTPUT DROP
```

f. Modification de « FORWARD/INPUT» (interdit) et « OUTPUT » (autorisé)

```
ip tables –P FORWARD DROP
ip tables –P INPUT DROP
ip tables –P OUTPUT ACCEPT
```

g. Intérêt de cette « politique de sécurité » :
   Shell script :

```
1. # !/bin/sh
2.
3. Ip tables –F INPUT
4. Ip tables –F OUTPUT
5. Ip tables –F FORWARD
6. ip tables –P FORWARD DROP
7. ip tables –P INPUT DROP
8. ip tables –P OUTPUT ACCEPT
```

Politique de sécurité par défaut : **INPUT=DROP OUTPUT=ACCEPT FORWARD=DROP**

3. *Règles d'accès élémentaires*

a. Règle à ajouter :
iptables –A INPUT –s 192.168.2.0/24 -d 192.168.2.1 -i eth0 -j ACCEPT
b. Vérification de l'accès au serveur Web par le pare-feu : It works !!!
c. Vérification de l'accès aux services du pare-feu par les clients : Ca marche !

4. *Règles de filtrage*

a. Modification de la configuration du pare-feu
iptables –A FORWARD -s 192.168.2.29 -j ACCEPT
b. Accès aux clients de « Internet » d'accéder au « Finger » et au « FTP » Voir 6.
c. Ajout d'un filtrage ICMP : Voir 6.
d. Accès spécifique au serveur Web : Voir 6.

5. *Règles de filtrage avancé*

a. Règle de filtrage pour limitation des ping.
b. Limitation du nombre de connexion au serveur Web
c. Configuration du suivi de connexion
d. Test des adresses MAC
e. Optimisation du pare-feu

6. Script Shell final

```
# !/bin/sh

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

#       Vider les tables
iptables –F     INPUT
iptables –F     OUTPUT
iptables –F     FORWARD

#       Politique de sécurité de la table « FORWARD »
iptables –P FORWARD   DROP
iptables –P INPUT     DROP
iptables –P OUTPUT    ACCEPT
iptables –A INPUT     –s 192.168.2.0   -d 192.168.2.1   -i eth0   -j ACCEPT

# 4.1   Accès au web
iptables –A FORWARD   –p tcp   -d 192.168.2.29  -i eth1 –dport 80 -j ACCEPT
iptables –A FORWARD   –p tcp   -s 192.168.2.29  -i eth0 –sport 80 -j ACCEPT

#4.2    Accès au ftp
iptables –A FORWARD   –p tcp   -d 192.168.2.17  -i eth1 –dport 20 -j ACCEPT
iptables –A FORWARD   –p tcp   -s 192.168.2.17  -i eth0 –sport 20 -j ACCEPT
iptables –A FORWARD   –p tcp   -d 192.168.2.17  -i eth1 –dport 21 -j ACCEPT
iptables –A FORWARD   –p tcp   -s 192.168.2.17  -i eth0 –sport 21 -j ACCEPT
#       Accès au finger
iptables –A FORWARD   –p tcp   -d 192.168.2.5   -i eth1 –dport 79 -j ACCEPT
iptables –A FORWARD   –p tcp   -s 192.168.2.5   -i eth0 –sport 79 -j ACCEPT

#4.3    Filtrage ICMP
iptables  –A FORWARD  -p icmp  -s192.168.2.0/24        -I eth0   --icmp-type echo-request  -j ACCEPT
iptables  –A  FORWARD -p icmp  -d192.168.2.0/24        -I eth1   --icmp-type echo-reply    -j ACCEPT

#4.4    Accès au ftp du serveur web
iptables –A FORWARD   –p tcp   -d 192.168.2.29  -i eth1 –dport 20 -j ACCEPT
iptables –A FORWARD   –p tcp   -s 192.168.2.29  -i eth0 –sport 20 -j ACCEPT
iptables –A FORWARD   –p tcp   -d 192.168.2.29  -i eth1 –dport 21 -j ACCEPT
iptables –A FORWARD   –p tcp   -s 192.168.2.29  -i eth0 –sport 21 -j ACCEPT

#5.1    Filtrage ICMP avec limitations
iptables  –A FORWARD  -p icmp  -s192.168.2.0/24        -I eth0   --icmp-type echo-request  -j ACCEPT –m
limit --limit 20/minute
iptables  –A  FORWARD -p icmp  -d192.168.2.0/24        -I eth1   --icmp-type echo-reply    -j ACCEPT –m
limit --limit 20/minute

#5.2    Limiter les accès au web
iptables –A FORWARD   –p tcp   -d 192.168.2.29  -i eth1 –dport 80 -j ACCEPT      -m limit --limit-burst 3
iptables –A FORWARD   –p tcp   -s 192.168.2.29  -i eth0 –sport 80 -j ACCEPT      -m limit --limit-burst 3

#5.3    Ameliorations
```