mon script de pare-feu (passerelle)

- Niveau requis :
  débutant, avisé

mon-script-iptables

```
#!/bin/sh

/sbin/iptables -F
/sbin/iptables -X
/sbin/iptables -t nat -F
/sbin/iptables -t nat -X
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -t nat -P PREROUTING ACCEPT
/sbin/iptables -t nat -P POSTROUTING ACCEPT
/sbin/iptables -t nat -P INPUT ACCEPT
/sbin/iptables -t nat -P OUTPUT ACCEPT
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
##commenter / décommenter et adapter les quatre lignes suivantes pour
ne pas mettre en place / mettre en place
##un proxy transparent (squid)
/sbin/iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT -
-to 192.168.0.1:3129
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
REDIRECT --to-port 3129
/sbin/iptables -t mangle -A PREROUTING -p tcp --dport 3128 -j DROP
/sbin/iptables -t mangle -A PREROUTING -p tcp --dport 3129 -j DROP
#accepter l'interface lo
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
#accepter le sous-réseau
/sbin/iptables -A INPUT -i eth1 -j ACCEPT
/sbin/iptables -A OUTPUT -o eth1 -j ACCEPT
#permettre le passage entre les deux interfaces eternet de la
passerelle
/sbin/iptables -t filter -A FORWARD -i eth1 -o eth0 -s 192.168.1.0/24 -
d 0.0.0.0/0 -p tcp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -t filter -A FORWARD -i eth0 -o eth1 -s 0.0.0.0/0 -d
192.168.1.0/24 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -t filter -A FORWARD -p icmp -j ACCEPT
#accepter le ping entre les réseaux locaux
/sbin/iptables -t filter -A INPUT -p icmp -i eth0 -m conntrack --
ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
/sbin/iptables -t filter -A OUTPUT -p icmp -o eth0 -m conntrack --
ctstate ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -t filter -A INPUT -p icmp -i eth1 -m conntrack --
ctstate ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -t filter -A OUTPUT -p icmp -o eth1 -m conntrack --
ctstate ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 0 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 0 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 3/4 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 3/4 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 3/4 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 3/3 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 3/3 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 3/3 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 3/1 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 3/1 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 3/1 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 4 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 4 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 4 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 8 -m limit --limit 2/s -j
ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 8 -j LOG --log-prefix
"ICMP/in/8 Excessive: "
/sbin/iptables -A INPUT -p icmp --icmp-type 8 -j DROP
/sbin/iptables -A OUTPUT -p icmp --icmp-type 8 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 8 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 11 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 11 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 11 -j ACCEPT
/sbin/iptables -A INPUT -p icmp --icmp-type 12 -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp --icmp-type 12 -j ACCEPT
/sbin/iptables -A FORWARD -p icmp --icmp-type 12 -j ACCEPT
/sbin/iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.0.0/24 -p icmp -
-icmp-type echo-request -j ACCEPT
/sbin/iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -p icmp -
-icmp-type echo-reply -j DROP
/sbin/iptables -A INPUT -p icmp -m limit -j LOG --log-prefix "ICMP/IN:
"
/sbin/iptables -A OUTPUT -p icmp -m limit -j LOG --log-prefix
"ICMP/OUT: "
/sbin/iptables -N syn_flood
/sbin/iptables -I INPUT -p tcp --syn -j syn_flood
/sbin/iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j
RETURN
/sbin/iptables -A syn_flood -j LOG --log-prefix '[SYN_FLOOD] : '
/sbin/iptables -A syn_flood -j DROP
#autoriser la connexion avec les serveurs DNS
```

```
/sbin/iptables -t filter -A OUTPUT -o eth0 -p udp -m udp --dport 53 -m
state --state NEW,RELATED,ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A INPUT -i eth0 -p udp -m udp --sport 53 -m
state --state RELATED,ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A OUTPUT -o eth1 -p udp -m udp --dport 53 -m
state --state NEW,RELATED,ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A INPUT -i eth1 -p udp -m udp --sport 53 -m
state --state RELATED,ESTABLISHED -j ACCEPT
#autoriser la navigation web
/sbin/iptables -t filter -A OUTPUT -o eth0 -p tcp -m multiport --dports
80,443,8000 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A INPUT -i eth0 -p tcp -m multiport --sports
80,443,8000 -m state --state RELATED,ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -o eth1 -p tcp -m multiport --dports
80,443,8000 -j ACCEPT
/sbin/iptables -A INPUT -i eth1  -p tcp -m multiport --sports
80,443,8000 -j ACCEPT
#Si le serveur cups est branché sur un ordinateur du réseau
192.168.0.0/24, par exemple sur 192.168.0.22
# laisser décommenter les deux lignes suivantes :
/sbin/iptables -A INPUT -i eth0 -s 192.168.0.22 -d 192.168.0.1 -p tcp -
-sport 631 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -o eth0 -s 192.168.0.1 -d 192.168.0.22 -p tcp
--dport 631 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
#créer une chaîne utilisateur pour les connexion ssh, les loguer et les
accepter
/sbin/iptables -t filter -N InComingSSH
/sbin/iptables -I INPUT -i eth0 -s 192.168.0.0/24 -p tcp -m tcp --dport
22 -m conntrack --ctstate NEW,ESTABLISHED -j InComingSSH
/sbin/iptables -A InComingSSH -j LOG --log-prefix '[INCOMING_SSH] : '
/sbin/iptables -A InComingSSH -j ACCEPT
/sbin/iptables -t filter -A OUTPUT -o eth0 -p tcp -m tcp --sport 22 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A OUTPUT -o eth1 -p tcp -m tcp --dport 22 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
/sbin/iptables -t filter -A INPUT -i eth1 -s 192.168.0.0/24 -p tcp --
sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
#créer une chaîne utilisateur pour les connexions ftp, et les accepter
/sbin/iptables -N ftp_in_accept
/sbin/iptables -I INPUT -i eth0 -p tcp --sport 21 -m state --state
ESTABLISHED,RELATED -j ftp_in_accept
/sbin/iptables -I INPUT -i eth0 -p tcp --sport 20 -m state --state
ESTABLISHED,RELATED -j ftp_in_accept
/sbin/iptables -I INPUT -i eth0 -p tcp --sport 1024:65535 --dport
1024:65535 -m state --state ESTABLISHED -j ftp_in_accept
/sbin/iptables -A ftp_in_accept -p tcp -j ACCEPT
/sbin/iptables -A INPUT -i eth1 -p tcp --sport 21 -m state --state
ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A INPUT -i eth1 -p tcp --sport 20 -m state --state
ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -I INPUT -i eth1 -p tcp --sport 1024:65535 --dport
```

```
1024:65535 -m state --state ESTABLISHED -j ACCEPT
```