Fiche Technique

Firewall sous Linux avec IPCHAINS

Les anciennes versions du noyau Linux incluaient en natif un logiciel de filtrage de paquets, ainsi qu'une fonction de masquerading. Il fallait juste employer un module appelé ipfwadm permettant de configurer ces fonctions dans le noyau. Ipfwadm était disponible jusqu'aux versions 2.1 du noyau Linux. IPChains le remplace dans les versions 2.2.x.

rappel : pour activer le routage sur une machine Linux :

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

tester le support des chaînes firewall :

```
# ls /proc/net/ip_fwchains
```

si le fichier est absent, le noyau est mal configuré

masquage avec 3 comandes :

```
# ipchains –P forward DENY
```

; forward interdit sauf pour ce qui précisé dans la suite

```
# ipchains –A forward –s 192.168.1.0/24 –j MASQ
```

; pour les paquets dont l'adresse source provient du réseau interne, forward avec masquage

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

; active le forward, le routage IP

commande ipchains :

3 règles : input, output, forward
Le paquet qui arrive est d'abord traité par la règle input,
s'il est destiné à un autre réseau, il est traité par la règle forward,
quand il va sortir, il est traité par la règle output.

-F	flush	supprime toutes les règles d'une chaîne, pas la policy
-A	add	ajoute une règle à une chaîne
-P	policy	fixe la policy (action par défaut) d'une chaîne
-L	list	liste les règles d'une chaîne spécifiée, sinon de toutes
-D	delete	efface une règle dans une chaîne
-N	new	crée une chaîne
-X		suppression d'une chaîne

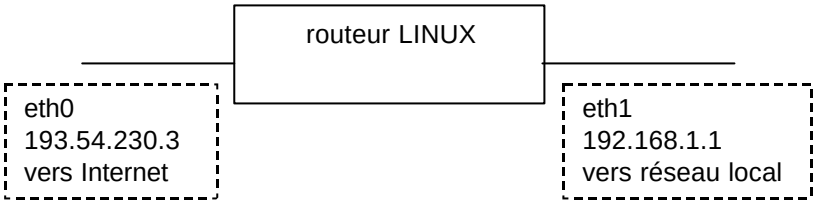
spécifications :

-s	source	adresse IP source
-d	dest	adresse IP destination
-i	interface	carte réseau ou modem...
-p	protocole	tcp, udp, icmp
-y	syn	paquet TCP SYN=1 (ouverture de connexion)
-j	jump (action)	ACCEPT : accepter DENY : détruire le paquet REJECT : détruire et générer un message de réponse ICMP MASQ : masquer le paquet (uniquement dans forward) REDIR : rediriger le paquet vers un port local RETURN : revenir à la chaîne appelante, sinon exécuter l'action définie par –P chaîne
-l	log	écrit les évènements dans un journal de logs
!	not	négation de l'argument suivant ex: -i ! eth0 ...signifie toute interface sauf eth0

exemples:

```
ipchains –F input          ; supprime toutes les règles de la chaîne input
ipchains –P forward DENY   ; interdit par défaut le forward
ipchains –A input –s localhost –p icmp –j DENY
; interdit en entrée tout paquet ICMP ayant comme adresse source 127.0.0.1
; donc ping localhost ne marche plus
```

exemple complet :




```
ipchains –P input DENY
ipchains –P output DENY
ipchains –P forward DENY
```
; policy (politique par défaut) pour input, output et forward

```
ipchains –F input
ipchains –F output
ipchains –F forward
```
; vide les règles pour input, output et forward

```
ipchains –A input –j ACCEPT –i lo
```
; accepte tout paquet entrant sur interface locale

```
ipchains –A input –j ACCEPT –i eth1 –s 192.168.1.1/255.255.255.0
```
; accepte tout paquet entrant sur eth1 ayant une adresse source 192.168.1.1 à 192.168.1.255, c'est à dire du réseau local

```
ipchains –A input –j ACCEPT –i eth0 –d 193.54.230.3/32
```
; accepte tout paquet entrant sur eth0 destiné à 193.54.230.1, c'est à dire vers l'Internet

```
ipchains –A input –j DENY –i eth0 –s 192.168.1.1/255.255.255.0 –l
```
; rejette tout paquet entrant sur eth0 ayant une adresse source du réseau interne, et on écrit dans le log (un paquet venant le l'Internet en se faisant passer pour un paquet du réseau local)

```
ipchains –A forward –j MASQ –i eth0 –s 192.168.1.1/255.255.255.0
```
; on masque tout paquet allant sur eth0 et ayant une adresse source du réseau interne

```
ipchains –A output –j ACCEPT –i lo
```
; on accepte tout ce qui sort par l'interface locale

```
ipchains –A output –j ACCEPT –i eth1 –d 192.168.1.1/255.255.255.0
```
; on accepte tout ce qui sort par eth1 et ayant une adresse destination du réseau interne

```
ipchains –A output –j ACCEPT –i eth0 –s 193.54.230.3/255.255.255.0
```
; on accepte tout ce qui sort par eth0 et ayant une adresse source du routeur Linux

```
ipchains –A output –j DENY –i eth0 –d 192.168.1.1/255.255.255.0 –l
```
; on rejette tout ce qui sort par eth0 et ayant une adresse destination du réseau interne et on écrit dans le log les infractions (paquets voulant sortir avec une adresse destination du réseau interne)

autre exemple :

```
ipchains –A input –p tcp ! –y –s 130.79.200.3 smtp –j ACCEPT
```
; autorise les paquets entrants ayant l'adresse source 130.79.200.3, port SMTP, protocole TCP mais pas SYN (refuse qu'il se connecte par TCP sur le port SMTP de notre machine).
L'option –y désigne les paquets TCP avec SYN=1 (ouverture de connexion TCP).
La chaîne " ! –y " signifie "pas avec SYN=1".

-p TCP -d 0.0.0.0/0 ! www	tout paquet TCP adr dest quelconque, sauf port www
-p TCP -d ! 192.168.1.1 www	tout paquet TCP sauf adr dest 192.168.1.1 avec port www
-p TCP -d 192.168.1.1 ! www	tout paquet TCP adr dest 192.168.1.1 sauf port www
-p TCP -d ! 192.168.1.1 ! www	tout paquet TCP sauf adr dest 192.168.1.1 et sauf port www