iptables : logiciel permettant le filtrage de paquets et le NAT

YuGiOhJCJ

8 septembre 2007

Table des matières

1 Avant propos...

Cette documentation a été rédigée par YuGiOhJCJ. Vous lisez actuellement la version 20070908 qui est gratuite. Si vous souhaitez utiliser une partie de cette documentation pour vos créations, veuillez d'abord me contacter à yugiohjcj@free.fr. La version la plus récente de ce document est disponible à l'adresse http ://yugiohjcj.free.fr/. Cette publication peut contenir certaines erreurs. N'hésitez pas à me les rapporter pour que j'effectue une correction.

2 Les cibles

- ACCEPT
- DROP
- QUEUE
- RETURN

3 Les tables

- filter qui contient les châines INPUT FORWARD et OUTPUT
- nat qui contient les chaînes PREROUTING OUPUT et POSTROUTING
- mangle qui contient les chaînes PREROUTING OUTPUT INPUT FORWARD POSTROUTING
- raw qui contient les chaînes PREROUTING OUTPUT

4 Les chaînes

- INPUT
- OUTPUT
- FORWARD
- POSTROUTING
- PREROUTING

D'autres spécifiques à la table nat

- DNAT
- MASQUERADE
- SNAT
- LOG

5 Les commandes

- -A chaîne règle Ajoute une règle à la fin de la chaîne.
- -D chaîne règle Supprime une règle à la fin de la chaîne.
- -L [chaîne] Affiche les règles des chaînes.
- -F [chaîne] Supprime toutes les règles des chaînes.

– -P chaîne cible Configure la politique pour la chaîne.

6 Les paramètres

– -p protocole si le protocole est tcp ou udp, on a accès aux options suivantes :
  – –sport port[:port]
  – –dport port[:port]
– -s adresse
– -d adresse
– -j cible

7 Exemple

```
#!/bin/sh

echo "Configration du routeur/pare-feu..."

#On vide les tables
iptables -t filter -F
iptables -t filter -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X

#On fixe la politique par défaut
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT
iptables -t mangle -P PREROUTING ACCEPT
iptables -t mangle -P OUTPUT ACCEPT

#On accepte en local
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT

#On fait du NAT
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
#On redirige des ports
iptables -t nat -A PREROUTING -p tcp --dport 2048 -j DNAT --to-destination 192.168.0.9:2048
iptables -t nat -A PREROUTING -p udp --dport 2049 -j DNAT --to-destination 192.168.0.9:2049

#On ouvre certains ports
iptables -t filter -A INPUT -p tcp --dport 9999 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 5555 -j ACCEPT
```