Atelier 8:NETFILTER | IPTABLES

0. Entrée en Matière

Afin de mener à bien notre mission , nous allons particulièrement avoir besoin et utiliser :

- Un routeur
- Un serveur
- Tous les conteneurs aussi nous seront utiles

1. IPtables, The Firewall of Linux

Gérer le trafic réseau est certainement la partie la plus difficile du métier d'administrateur système. Il faut impérativement configurer les pare-feu sur l'ensemble des éléments actifs du réseau, serveurs inclus, en prenant en compte les besoins des utilisateurs et des systèmes à la fois pour le trafic entrant et sortant, sans laisser des systèmes vulnérables à des attaques.

C'est le rôle du pare-feu IPTables, entièrement administrable en ligne de commandes. IPtables utilise un jeu de tables qui contiennent des chaînes comprenant les règles du firewall. Il existe 3 types de chaines :

- INPUT : Messages ou paquets à destination du parefeu ou routeur
- OUTPUT : Messages émis par le parefeu ou routeur
- FORWARD : Filtre tous les flux qui ne font que traverser le routeur (ex: tout ce qui concerne le serveur , serveur web ,ftp ect)

I) APPLICATION

Le but de ce TP est de mettre un pare-feu local sur le serveur ainsi qu'un pare-feu local et réseau sur le routeur.

1. Sécurisation des conteneurs par des règles iptables sur le routeur

✔ INPUT et OUTUP : ACCEPT (Le but du TP est de protéger le réseau 10.31.80.0/20 et non le routeur lui-même)
✔ FORWARD : DROP

II) CREATION DE NOTRE FICHIER(SCRIPT) SUR LE ROUTEUR

Nous devons créer un script dans lequel nous allons mettre toutes nos règles de **parefeu** avec la commande :

```
root@rtr-g5:/home# nano parefeu.sh
```

III)CONTENU DE NOTRE SCRIPT

2) Qu'est ce que notre script devrait réellement contenir et pourquoi

Premièrement nous devons rejeter (DROP) toutes les chaines afin de tout interdire , puis mettre des règles appropriées afin d'effectuer tout ce dont on a besoin de faire sur notre ou depuis notre réseau .

On devra établir des règles pour le routeur , le serveur et tous les conteneurs :

- Permettre l'accès en ssh pour les serveur et routeur
- Permettre au réseau Beaupeyrat de Ping toutes les machines
- Autoriser l'accès à Internet en **HTTP** et **HTTPS** à toutes les machines
- Autoriser le réseau Beaup à joindre le serveur **FTP** ect s'il y en a d'autres

IV) SCRIPT PAREFEU

3) Premières Lignes du SCRIPT

```
#!/bin/sh -e

#On passe la politique par défaut des toutes les chaines à DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# On vide les chaînes prédéfinie et les règles
iptables -F
iptables -X

# STATEFUL : On autorise tous les retours sur les 3 chaines
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

4) Pour le Routeur

```
################## LE FIREWALL EN PERSONNE
# On autorise la connexion SSH depuis le réseau de beaupeyrat vers le
parefeu
iptables -A INPUT -p tcp -s 10.187.20.0/24 --dport 22 -j ACCEPT

# On autorise toutes les machines du réseau beaupeyrat à effectuer des ping
vers le parefeu
iptables -A INPUT -p icmp -s 10.187.20.0/24  -j ACCEPT

# On autorise le parefeu à avoir accès Internet (HTTP et HTTPS)
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
# On autorise le parefeu à accéder au DNS de google
```

```
iptables -A OUTPUT -p udp -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp -d 8.8.4.4 --dport 53 -j ACCEPT
```

5) Pour Le Serveur

```
################## LE SERVEUR (.1)
# On autorise la connexion SSH depuis le réseau de beaupeyrat vers le
serveur
iptables -A FORWARD -p tcp -s 10.187.20.0/24 -d 10.31.80.1/32 --dport 22 -j
ACCEPT

#on autorise les machines du réseau de beaupeyrat à effectuer des ping au
serveur
iptables -A FORWARD -p icmp -s  10.187.20.0/24 -d 10.31.80.1/32 -j  ACCEPT


# On autorise le  serveur à avoir accès Internet (HTTP et HTTPS)
iptables -A FORWARD  -p tcp -s  10.31.80.1/20  --dport 80  -j ACCEPT
iptables -A FORWARD  -p tcp -s  10.31.80.1/20  --dport 443 -j ACCEPT
```

6) Pour les Serveurs DNS

```
# On autorise le réseau beaupeyrat à avoir accès au serveur DNS
iptables -A FORWARD -p udp -s 10.187.20.0/24 -d 10.31.80.53/32 --dport 53 -j
ACCEPT
iptables -A FORWARD -p udp -s 10.187.20.0/24 -d 10.31.80.54/32 --dport 53 -j
ACCEPT

iptables -A FORWARD -p udp -s 10.187.20.0/24 -d 10.31.80.63/32 --dport 53 -j
ACCEPT
iptables -A FORWARD -p udp -s 10.187.20.0/24 -d 10.31.80.64/32 --dport 53 -j
ACCEPT

# On autorise le serveur DNS à acceder au seveur DNS de Google (faire des
requetes)
iptables -A FORWARD -p udp -s 10.31.80.53/20 -d 8.8.4.4 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.63/20 -d 8.8.4.4 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.54/20 -d 8.8.4.4 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.64/20 -d 8.8.4.4 --dport 53 -j ACCEPT

iptables -A FORWARD -p udp -s 10.31.80.53/20 -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.63/20 -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.54/20 -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.64/20 -d 8.8.8.8 --dport 53 -j ACCEPT

# on autorise nos serveurs DNS à avoir accès à internet  en HTTP et HTTPS
iptables -A FORWARD -p tcp -s 10.31.80.53/20 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.54/20 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.63/20 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.64/20 --dport 80 -j ACCEPT
```

```
iptables -A FORWARD -p tcp -s 10.31.80.53/20 --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.54/20 --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.63/20 --dport 443 -j ACCEPT

#on autorise le réseau Beaupeyrat à ping nos DNS
iptables -A FORWARD -p icmp -s 10.187.20.0/24 -d 10.31.80.53/32 -j ACCEPT
iptables -A FORWARD -p icmp -s 10.187.20.0/24 -d 10.31.80.54/32 -j ACCEPT

iptables -A FORWARD -p icmp -s 10.187.20.0/24 -d 10.31.80.63/32 -j ACCEPT
iptables -A FORWARD -p icmp -s 10.187.20.0/24 -d 10.31.80.64/32 -j ACCEPT
```

7) Pour Les Serveurs Web 1 & 2

```
############### LES SEVEURS WEB 1 & 2
#on autorise uniquement les machines du réseau beaupeyrat  à accéder au
serveur web 1
iptables -A FORWARD -p  tcp -s  10.187.20.0/24 -d 10.31.80.80/32 --dport 80
-j ACCEPT
iptables -A FORWARD -p  tcp -s  10.187.20.0/24 -d 10.31.80.80/32 --dport 443
-j ACCEPT

#on autorise uniquement les machines du réseau beaupeyrat  à accéder au
serveur web 2
iptables -A FORWARD -p  tcp -s  10.187.20.0/24 -d 10.31.80.81/32 --dport 80
-j ACCEPT
iptables -A FORWARD -p  tcp -s  10.187.20.0/24 -d 10.31.80.81/32 --dport 443
-j ACCEPT

#on autorise les machines du réseau de beaupeyrat à effectuer des ping au
serveur web 1
iptables -A FORWARD -p icmp -s  10.187.20.0/24 -d 10.31.80.80/32 -j  ACCEPT

#on autorise les machines du réseau de beaupeyrat à effectuer des ping au
serveur web 2
iptables -A FORWARD -p icmp -s  10.187.20.0/24 -d 10.31.80.81/32 -j  ACCEPT

#autorise le  serveur web 1  à avoir accès à Internet
iptables -A FORWARD -p  tcp -s 10.31.80.80 --dport 80 -j ACCEPT
iptables -A FORWARD -p  tcp -s 10.31.80.80 --dport 443 -j ACCEPT

#autoriser le serveur web 2 à avoir accès à Internet
iptables -A FORWARD -p  tcp -s 10.31.80.81 --dport 80 -j ACCEPT
iptables -A FORWARD -p  tcp -s 10.31.80.81 --dport 443 -j ACCEPT
```

8) Pour les Serveurs FTP 1 & 2

8.1Modification dans le fichier de conf de FTP : /etc/proftpd/proftpd.conf

En ce qui concerne le serveur FTP, nous devons aussi modifier les configurations dans son fichier de conf pour le mode **PASSIF** , en décommentant la ligne suivante et en mettant une intervalle de numéros de ports sur lequel il pourrait répondre :

```
/etc/proftpd/proftpd.conf
```

```
PassivePorts 40000 45000
```

```
######## LES SERVEURS FTP 1 & 2

#on autorise le serveur FTP 1 à avoir accès à Internet  en HTTP et HTTPS
iptables -A FORWARD  -p tcp -s  10.31.80.20/20  --dport 80  -j ACCEPT
iptables -A FORWARD  -p tcp -s  10.31.80.20/20  --dport 443 -j ACCEPT

#on autorise le serveur FTP 2 à avoir accès à Internet  en HTTP et HTTPS
iptables -A FORWARD  -p tcp -s  10.31.80.21/20  --dport 80  -j ACCEPT
iptables -A FORWARD  -p tcp -s  10.31.80.21/20  --dport 443 -j ACCEPT

#autoriser les clients FTP du réseau Beaupeyrat  à pouvoir effectuer des
requêtes FTP au serveur FTP 1 et 2
iptables -A FORWARD  -p tcp -s 10.187.20.0/24   -d 10.31.80.20/32 --dport
40000:45000  -j ACCEPT
iptables -A FORWARD  -p tcp -s 10.187.20.0/24   -d 10.31.80.21/32 --dport
40000:45000   -j ACCEPT

iptables -A FORWARD  -p tcp -s 10.187.20.0/24   -d 10.31.80.20/32 --dport 21
-j ACCEPT
iptables -A FORWARD  -p tcp -s 10.187.20.0/24   -d 10.31.80.21/32 --dport 21
-j ACCEPT

#on autorise les serveur FTP 1 à communiquer avec les serveurs  DNS de
Google
iptables -A FORWARD -p udp -s 10.31.80.20/20 -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.20/20 -d 8.8.4.4 --dport 53 -j ACCEPT

iptables -A FORWARD -p udp -s 10.31.80.21/20 -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.80.21/20 -d 8.8.4.4 --dport 53 -j ACCEPT
```

9) Pour Les serveurs Supervision 1 & 2

```
######## LES SERVEURS SUPERVISION 1 et 2 à avoir accès à Internet
iptables -A FORWARD  -p tcp -s  10.31.80.90/20  --dport 80  -j ACCEPT
iptables -A FORWARD  -p tcp -s  10.31.80.90/20  --dport 443 -j ACCEPT

iptables -A FORWARD  -p tcp -s  10.31.80.91/20  --dport 80  -j ACCEPT
iptables -A FORWARD  -p tcp -s  10.31.80.91/20  --dport 443  -j ACCEPT

#autoriser le réseau Beaupeyrat à accéder à nos serveurs Supervions
iptables -A FORWARD -p  tcp -s 10.187.20.0/24 -d 10.31.80.90/32  --dport 80
-j ACCEPT
iptables -A FORWARD -p  tcp -s 10.187.20.0/24 -d 10.31.80.91/32   --dport 80
-j ACCEPT

#les machines du réseau beaupeyrat doivent ping vers le serveur supervision1
```

```
et 2
iptables -A FORWARD -p icmp  -s 10.187.20.0/24 -d 10.31.80.90/32  -j ACCEPT
iptables -A FORWARD  -p icmp -s  10.187.20.0/24 -d 10.31.80.91/32 -j ACCEPT
```

10) Pour Les BACKUP 1 & 2

```
######  LES BACKUP 1 et 2
iptables -A FORWARD -p tcp -s 10.31.80.98/20 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.98/20 --dport 443 -j ACCEPT

iptables -A FORWARD -p tcp -s 10.31.80.99/20 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.80.98/20 --dport 443 -j ACCEPT
```

V) EXECUTION DU SCRIPT

Nous pouvons éxecuter notre scrip de 2 façons : en tapant une commande après modification de Script ou le mettre dans le fichier de configuration du Routeur **etc/rc.local** . La commande à taper est :

```
bash /home/parefeu.sh
```

Modification appliquée sur le fichier de Conf du Routeur

```
#!/bin/sh -e

ifconfig enp2s0 172.31.80.254/16 up
ifconfig enp4s0 10.31.95.254/20 up


route add default gw 172.31.0.1
echo "nameserver 10.31.80.54" > /etc/resolv.conf
echo "nameserver 10.31.80.64" > /etc/resolv.conf


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

/home/parefeu.sh # ligne qui a été ajoutée

iptables -t nat -A POSTROUTING -j MASQUERADE
```