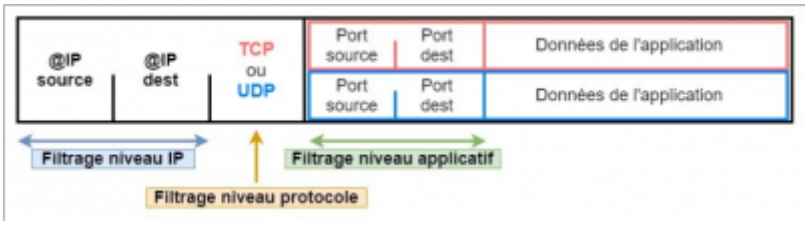
Netfilter/iptables

Netfilter : c'est le pare-feu implémenté au niveau du noyau Linux depuis la version 2.4, qui permet de faire du filtrage et la translation d'adresses.
iptables : c'est le jeu de commandes permettant de manipuler Netfilter.
Filtrage : c'est le fait d'accepter/refuser des paquets qui arrivent au niveau du pare-feu (ici netfilter)en fonction de différents paramètres (IP source, IP destination, Protocole,port source, port destination, état de la connexion, ...) définis dans les règles.

le filtrage s'effectue donc en analysant les champs (source/destination) des paquets qui transitent à travers le routeur. On peut donc filtrer les ip, les protocole, les port ...



De base, Linux permet de router les paquets IP d'une interface vers une autre et peut assurer les fonctions de routeur, si l'option "**ip_forward**" a été configurée et activée.

À partir de la version 2.4 le noyau Linux intègre **netfilter** qui permet de faire du filtrage et la translation d'adresses. **iptables** est l'outil qui permet de manipuler les filtres du noyau.

De base **netfilter/iptables** utilise trois chaînes (**INPUT, FORWARD, OUTPUT**) qui contiennent des **règles** (ou filtres) de filtrage . Ces 3 chaînes font partie de la table "**filter**" qui est la table par défaut.

- La chaîne **INPUT** est appliquée aux paquets destinés à un processus fonctionnant sur lefirewall Linux (exemple : telnet firewall).
- La chaîne **OUTPUT** est appliquée aux paquets émis par un processus du firewall Linux(exemple : telnet sortant du firewall).
- La chaîne **FORWARD** est appliquée aux paquets entrant/sortant du firewall Linux.

Pour chaque paquet, la chaîne est parcourue séquentiellement : si un filtre correspond, le traitement associé est appliqué au paquet (**ACCEPT, DROP, REJECT** pour notre étude). Sinon le filtre suivant est testé. À la fin de chaque chaîne un traitement par défaut est appliqué en dernier ressort(**ACCEPT/DROP/REJECT**)

- **ACCEPT** Les paquets sont autorisé.
- **DROP** Les paquets sont rejeté.
- **REJECT** les paquets sont rejeté avec un message à la source.

Tables & Chaînes par défaut

Filter	Nat

INPUT	Paquets qui entrent sur la machine	**PREROUTING**	NAT destination
OUTPUT	Paquets qui sont émis par la machine	**POSTROUTING**	NAT Source
FORWARD	Paquets qui transitent par la machine (qui passent d'une interface à une autre)	**OUTPUT**	NAT sur les paquets émis par la machine

Sécurisation des conteneurs

```
!/bin/bash

iptables -F
iptables -X

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#--------------------------------------------------------------------------
------------------
#--                                    STATEFULL
--
#--------------------------------------------------------------------------
------------------

iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j
ACCEPT
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j
ACCEPT

#--------------------------------------------------------------------------
------------------
#--                                       SSH
--
#--------------------------------------------------------------------------
------------------

#reseau beaup vers mon reseau
iptables -A FORWARD -p tcp -s 10.187.20.0/24 -d 10.31.80.0/20 --dport
22 -j ACCEPT

#reseau beaup vers routeur
iptables -A INPUT -p tcp -s 10.187.20.0/24 --dport 22 -j ACCEPT
```

```
#mon serveur vers routeur
iptables -A INPUT -p tcp -s 10.31.80.1 --dport 22 -j ACCEPT

#routeur vers mon reseau
iptables -A OUTPUT -p tcp -d 10.31.80.0/20 --dport 22 -j ACCEPT

#--------------------------------------------------------------------
------------------
#--                                          ICMP
--
#--------------------------------------------------------------------
------------------

# autoriser les pings
iptables -A FORWARD -p icmp -s 10.31.80.0/20 -j ACCEPT

#autoriser les pings du reseau de beaup vers mon reseau
iptables -A FORWARD -p icmp -s 10.187.20.0/24 -d 10.31.80.0/20 -j
ACCEPT

#autoriser les pings vers mon routeur
iptables -A INPUT -p icmp -s 10.187.20.0/24 -j ACCEPT

#autoriser mon routeur a ping le réseau 10.31.80.0/20
iptables -A OUTPUT -p icmp -d 10.31.80.0/20 -j ACCEPT

#--------------------------------------------------------------------
------------------
#--                                          DNS
--
#--------------------------------------------------------------------
------------------

#autoriser contact reseau beaup vers dns 1 et 2
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d 10.31.80.53
-j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d 10.31.80.54
-j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.80.53 -d 8.8.8.8 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.80.53 -d 8.8.4.4 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.80.54 -d 8.8.8.8 -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.80.54 -d 8.8.4.4 -j
ACCEPT

#autoriser le routeur a faire des request vers mes dns
iptables -A OUTPUT -p udp --dport 53 -d 10.31.80.53 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -d 10.31.80.54 -j ACCEPT
#--------------------------------------------------------------------
```

```
------------------
#--                                        HTTP
--
#-------------------------------------------------------------------------
------------------

#autoriser les request http vers mon serveur web
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d 10.31.80.80
-j ACCEPT

#autoriser mon serveur web a avoir internet
iptables -A FORWARD -p tcp --dport 80 -s 10.31.80.0/20 -j ACCEPT

iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/24 -d 10.31.81.30
-j ACCEPT

#accès internet sur mon réseau
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
#-------------------------------------------------------------------------
------------------
#--                                       HTTPS
--
#-------------------------------------------------------------------------
------------------

#autoriser les request http vers mon serveur web
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/24 -d
10.31.80.80 -j ACCEPT

#autoriser mon serveur web a avoir internet
iptables -A FORWARD -p tcp --dport 443 -s 10.31.80.0/20 -j ACCEPT

#accès internet sur mon routeur
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
#-------------------------------------------------------------------------
------------------
#--                                        FTP/S
--
#-------------------------------------------------------------------------
------------------

#autoriser les transfert ftp
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d 10.31.80.20
-j ACCEPT
iptables -A FORWARD -p tcp --dport 20 -d 10.187.20.0/24 -s 10.31.80.20
-j ACCEPT

#autoriser les transfert ftps
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d
10.31.80.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 989 -d 10.187.20.0/24 -s
```

```
10.31.80.20 -j ACCEPT

#gère le mode passif de ftp/ftps
iptables -A FORWARD -p tcp --dport 1024:65535 -m conntrack --ctstate
NEW,RELATED,ESTABLISHED -s 10.187.20.0/24 -d 10.31.80.20 -j ACCEPT
```