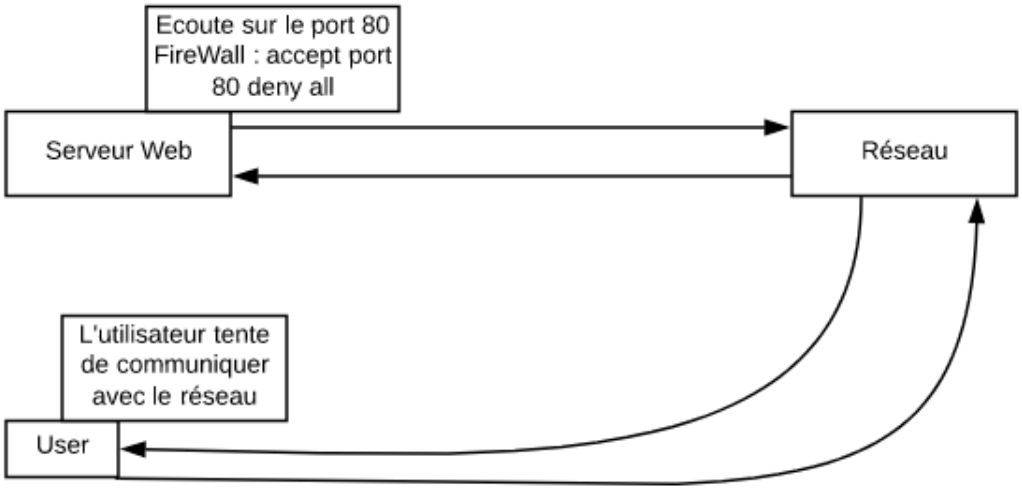
IPTABLES

Sacré Christopher

Tout d’abord il faut se rendre compte que nous laissons des traces numériques peu importe où nous allons et donc de ce fait, il existe de nombreuses traces disponibles.

Afin d’empêcher n’importe quel paquet de passer par notre réseau, nous allons utiliser les pares feux. Le pare feu unix standard est IPTABLES.

ACL



Utiliser des ACL ne fonctionne pas parfaitement bien. Un utilisateur n’arrivera pas à visualiser les données des autres sites internet. En effet il reçoit la réponse de ces derniers sur un autre port que ceux définit dans le firewall.

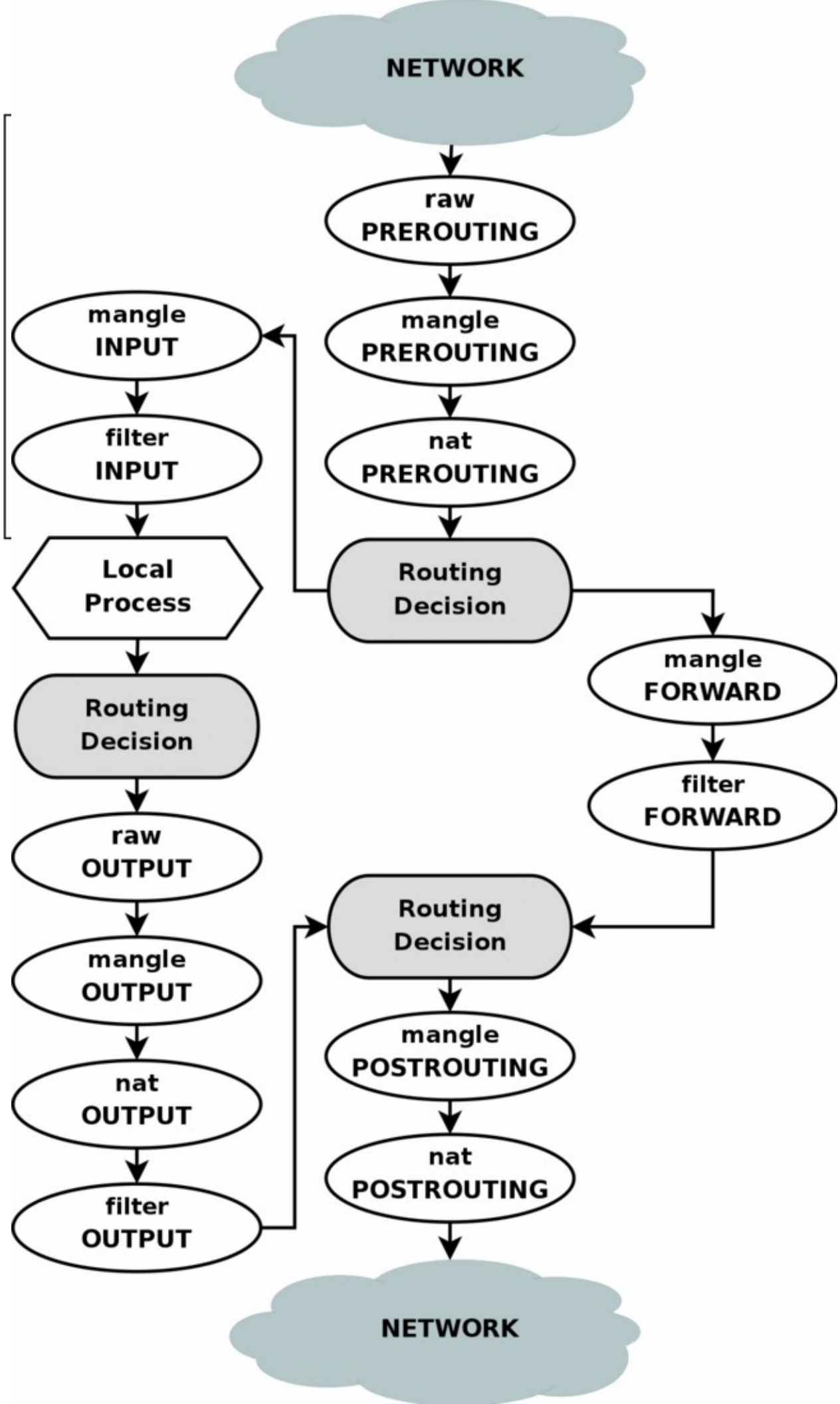
On remarquera donc plusieurs caractéristiques des ACL :
- Ils sont très peu configurables
- Le pare feu est stateless (il en retient aucune information au sujet des requêtes).
- Par contre il gérera les requêtes plus rapidemment.

Pare feu Statefull

Ces pares feux ci sont plus intelligent. Elle remarques les demandes sortantes et enregistre d’où elles proviennent, ainsi lorsque l’on obtient la réponse si celle ci correspond à l’une des requêtes sortantes (et donc qu’elle provenait à la base de notre serveur), alors celle ci sera acceptée.

Pare feu statefull : iptables.

IPTABLES


NETWORK
raw
PREROUTING
mangle
PREROUTING
nat
PREROUTING
Routing
Decision
mangle
INPUT
filter
INPUT
Local
Process
Routing
Decision
raw
OUTPUT
mangle
OUTPUT
nat
OUTPUT
filter
OUTPUT
mangle
FORWARD
filter
FORWARD
Routing
Decision
mangle
POSTROUTING
nat
POSTROUTING
NETWORK

Les 5 chaînes de IPTABLES

- PREROUTING : on a un qui entre. Requêtes d'entrées.

- POSTROUTING : on a un paquet qui sort. Requêtes de sorties.

- FORWARD : on forwarde un paquet. uniquement si le "user" est un routeur.

- INPUT : traitement du paquet juste après son entrée.

- OUTPUT : traitement du paquet avant sa sortie.

Avec le protocole IPTABLES dans la table mangle on peut régler le problème de TTL (Time To Live).

Mangle permet en soi de trafiquer le paquet IP.

Traitement des paquets

Lorsqu'un paquet arrive dans une chaîne de traitement, il peut être :

- accepté (ACCEPT) : il passera dès lors à une autre chains.

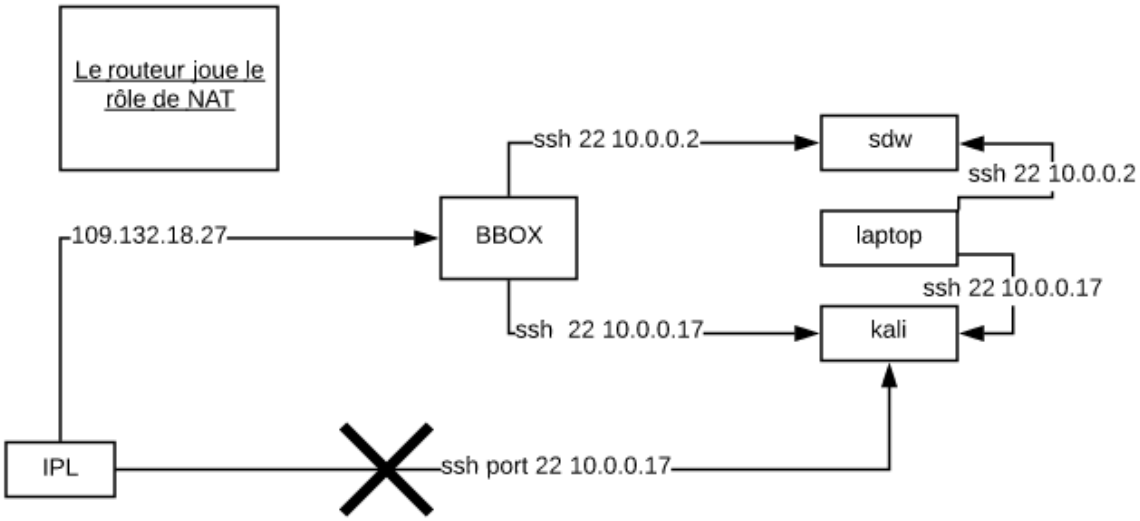
- refusé (DROP) : Le paquet n'est pas bon et doit donc être jeté (DROP ne prévient pas quand le paquet n'est pas bon).

- rejeté (REJECT) : Le paquet n'est pas bon mais on va prévenir du rejet de ce paquet. On va dès lors générer un paquet ICMP qui reviendra vers l'expéditeur.

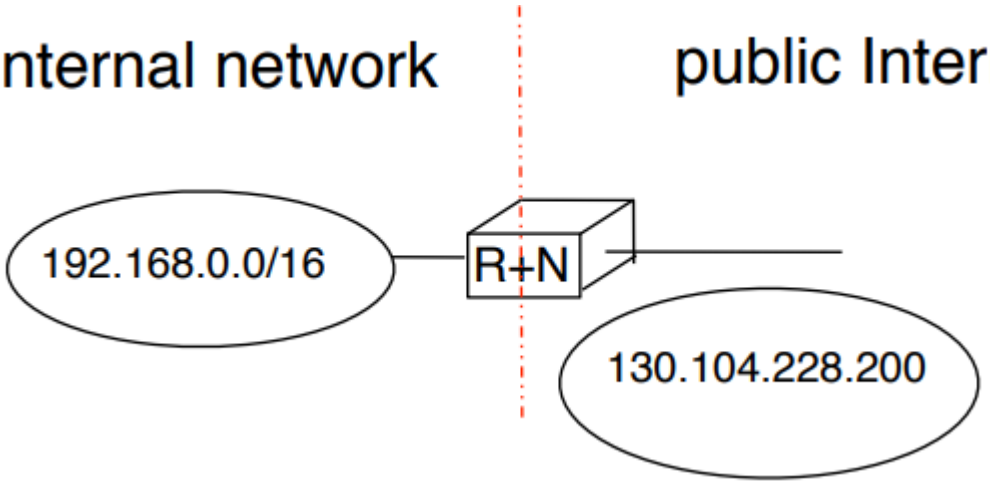
Différences entre DROP et REJECT :

DROP va permettre de cacher notre serveur ainsi que nos services, ainsi on préferera utiliser DROP dans une optique de sécurité optimale.

NAT (Network Adress Translator)



Un NAT va jouer le rôle de table de mapping. Elle va permettre de convertir des adresses internes en adresses publiques. Elle permettra de gérer à la fois les paquets provenant du réseau internes et ceux provenant du réseau public. Le NAT va traduire les adresses IP ainsi que les ports.



Private address	Protocol	Port inside	public address	Port outside
192.168.10.10	UDP	2340	130.104.228.200	4567
192.168.10.10	TCP	512	130.104.228.200	520
192.168.10.11	TCP	1024	130.104.228.200	2048

Son fichier de configuration se situe dans le fichier /etc/config

Il peut soit se faire de manière automatique soit de manière manuelle (mangle).

On laisse des traces à chaque passage au sein d’un de ces filtres (traces numériques).