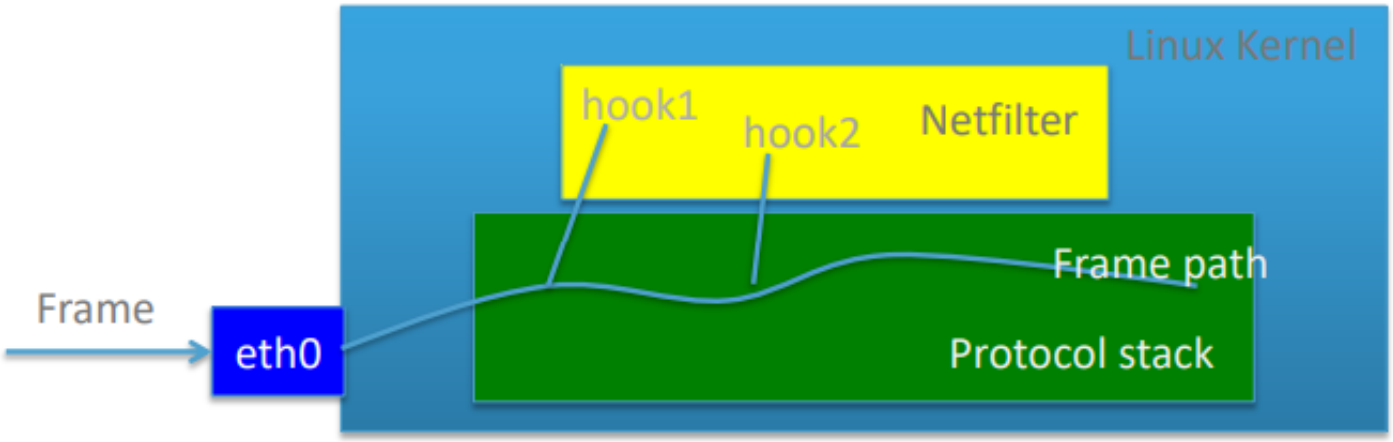
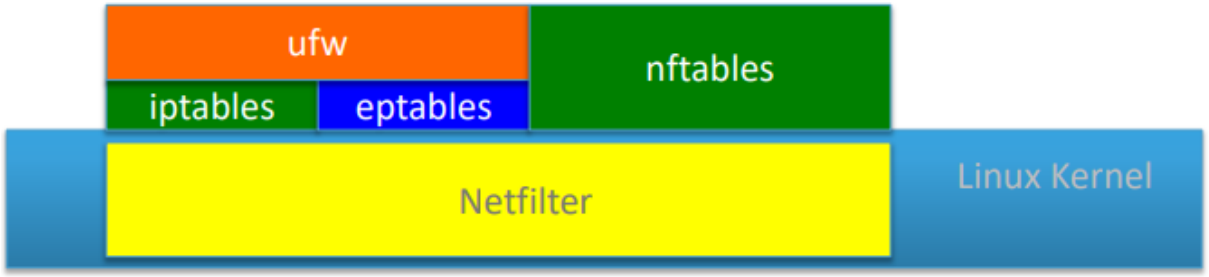
1 Firewall iptables

Il est nécessaire d'activer netfilter dans la configuration du kernel. Un hook est une étape lors du passage d'une trame dans le stack de protocoles. Le framework netfilter sera appelé à chaque hook



On peut configurer netfilter avec la commande `iptables`. `ebtables` permet de configurer la couche 2 uniquement (Linux bridge). `nftables` vise à remplacer tout le framework



1.1 Features

1. Stateless packet filtering (table filter et ACCEPT, DROP, REJECT). Permet de protéger au niveau réseau (bloquage d'une ip en particulier, ou ports). Les paquets sont analysés de manière individuelle
2. Stateful packet filtering. Permet de protéger au niveau du paquet en fonction du contexte (précédents paquets). Il est possible d'accepter des paquets venant de l'extérieur seulement si ils sont des réponses à des requêtes venant de l'intérieur
   - Utilisation de connection tables pour traiter les différentes parties des protocoles.
   - NEW : Nouveau paquet qui n'est pas lié à une connexion active
   - ESTABLISHED : Une connexion passe de NEW à ESTABLISHED losrque la connexion est validée par la direction opposée
   - RELATED : Paquets qui ne font pas partie d'une connexion existante mais qui sont liés à une autre. (Par exemple réponses ICMP pour une communication FTP).
3. Translation d'adresses / ports (NAT)
4. API pour autres applications

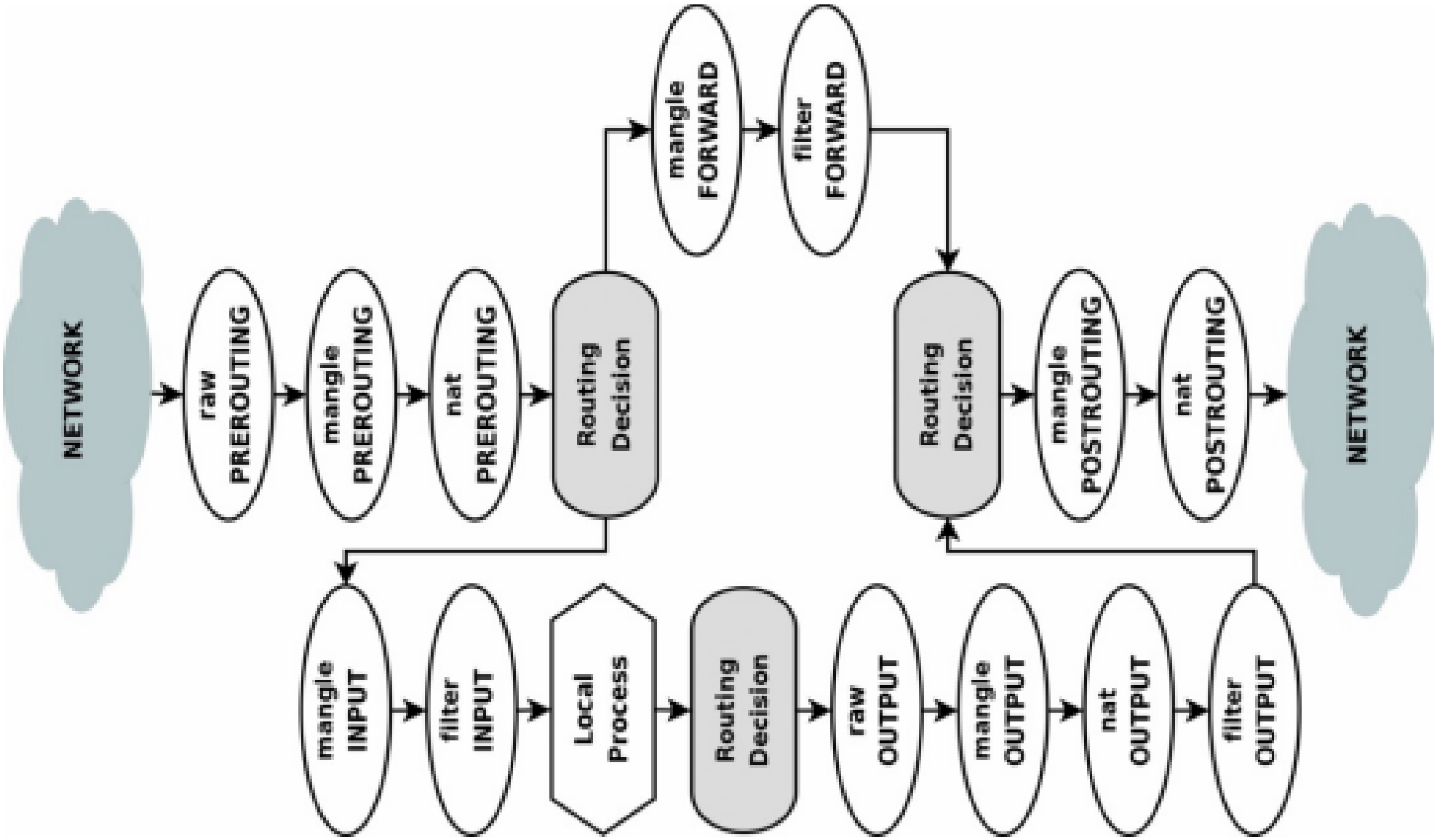
1.2 Chain

la combinaison Chain-Table constitue les hooks

Chains : INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING

1.2.1 Tables

- raw
- mangle (modification spéciales sur des paquets)
- nat (consultée lorsqu'un paquet créé une nouvelle connexion)
- filter (table de base)



1.3 NFQUEUE

NFQUEUE permet de passer un paquet au userspace

1.4 knockd

Configuration dynamique du parefeu netfilter. Lorsque des séquences sont reconnues (par exemple des ports spécifiques), le pare-feu est ouvert.

1.5 fwknop

Même système que knockd mais il utilise le contenu des paquets TCP / UDP (frame SPA). Si un SPA est valide, le pare-feu est ouvert pendant un certain temps (par exemple 30s)

1.6 Commande iptables

```
iptables -t table -COMMAND chain ... -j TARGET
```