Pare-feu

Sous linux : netfilter

Iptables/nftable/firewalld

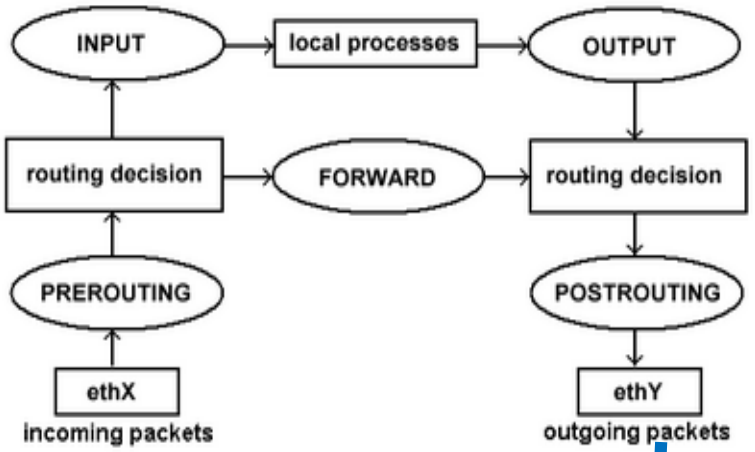
Pare-feu

- Plusieurs pare-feux possibles
  - En coupure de réseaux
    - Filtrage de ce qui entre/sort
    - Ne contrôle que ce qui passe par lui
  - Sur le PC/serveur
    - Attention, ce n'est pas un anti-virus
- Configuration d'un pare-feu
  - **Utilise des règles**
  - Ne peut pas comprendre les flux chiffrés
  - Filtrage au niveau 3 et 4
    - Au-dessus, on parle de proxy ou pare-feu applicatif
    - Filtre @IP, n°port, protocoles, …

Netfilter (1)

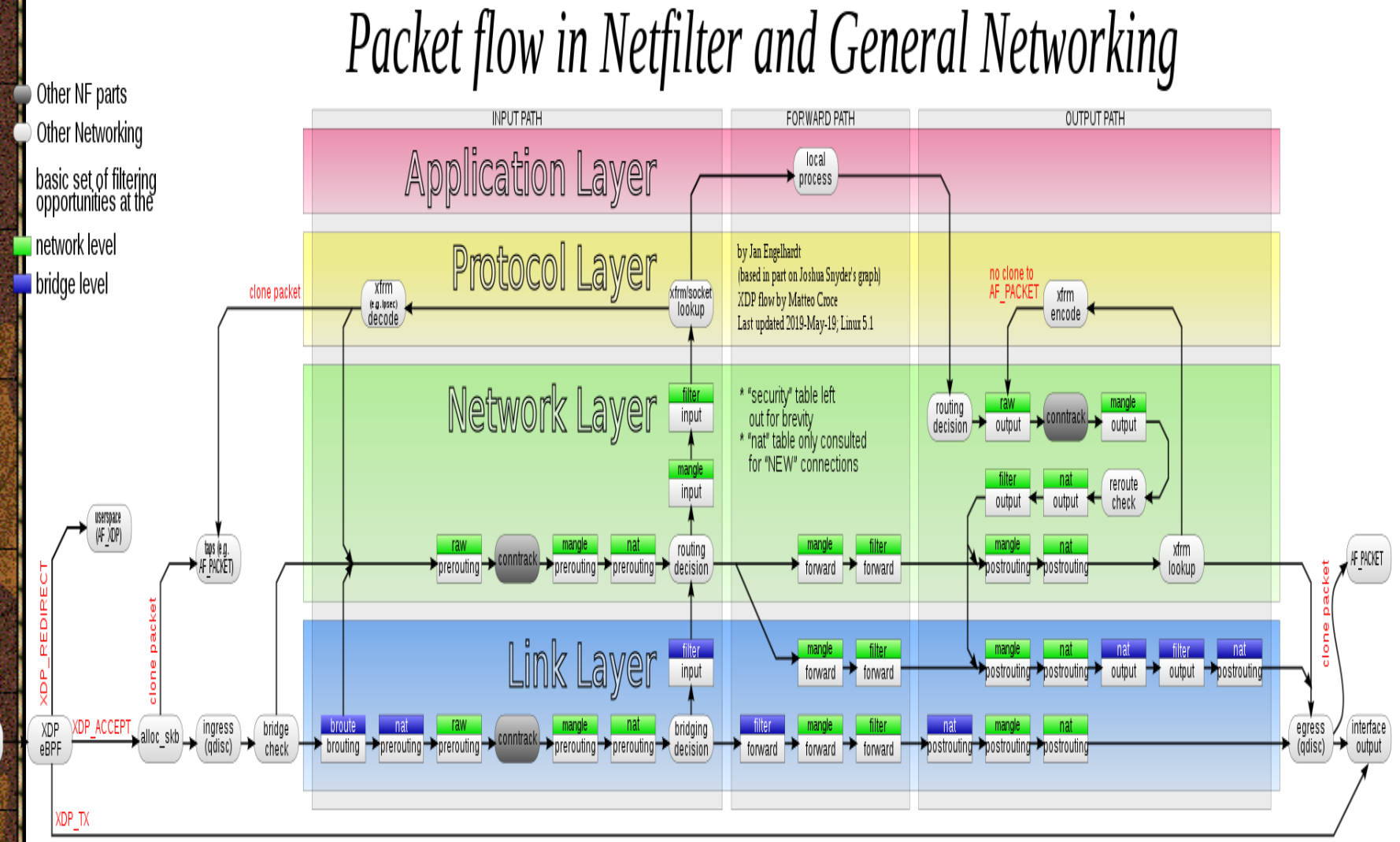
- Utiliser par tous les pare-feux linux
- Directement intégrer au kernel linux

- Flux des informations (très simplifié)
  - 5 chaînes
  - Plusieurs tables
    - Filter (défaut)
    - Nat
    - Raw
    - Mangle



Filter n'existe pas au niveau pre/post routing

Netfilter (2)


Packet flow in Netfilter and General Networking
Other NF parts
Other Networking
basic set of filtering opportunities at the
network level
bridge level
INPUT PATH
FORWARD PATH
OUTPUT PATH
Application Layer
Protocol Layer
Network Layer
Link Layer
local process
by Jan Engelhardt
(based in part on Joshua Snyder's graph)
XDP flow by Matteo Croce
Last updated 2019-May-19, Linux 5.1
* "security" table left out for brevity
* "nat" table only consulted for "NEW" connections
clone packet
no clone to AF_PACKET
xfrm (e.g. ipsec) decode
xfrm/socket lookup
xfrm encode
filter input
mangle input
raw prerouting
conntrack
mangle prerouting
nat prerouting
routing decision
mangle forward
filter forward
raw output
mangle output
filter output
nat output
reroute check
mangle postrouting
nat postrouting
xfrm lookup
userspace (AF_XDP)
taps (e.g. AF_PACKET)
XDP_REDIRECT
clone packet
(start)
XDP eBPF
XDP_ACCEPT
alloc_skb
ingress (qdisc)
bridge check
broute brouting
nat prerouting
bridging decision
nat output
filter output
nat postrouting
egress (qdisc)
interface output
AF_PACKET
clone packet
XDP_TX

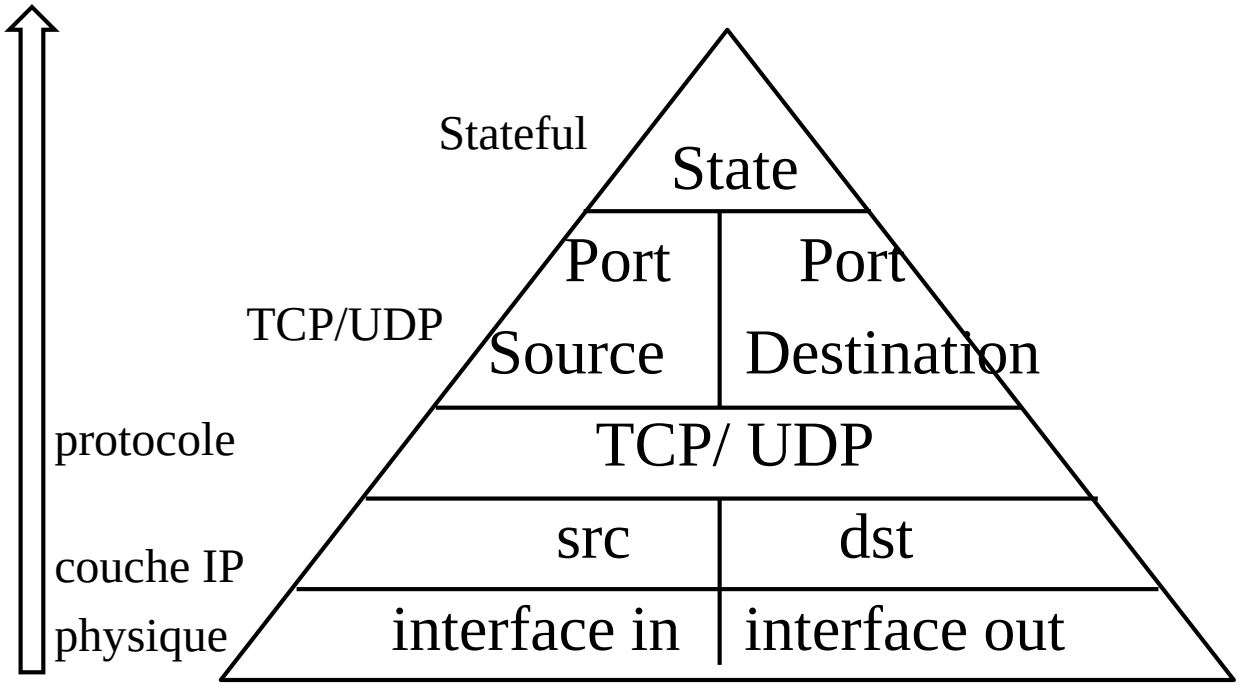
Netfilter (3)

- 3 tables couramment utilisées
  - Filter : input, forward, output
  - Nat : prerouting, input, output, postrouting
  - Mangle : tout, mais opération particulière
- Chaque chaine est indépendante, et ordonnée
- 4 actions possibles : ACCEPT, DROP, REJECT, LOG

  autres : QUEUE, RETURN
- Différents logiciels l'utilisent :
  - Iptables, ip6tables, arptables,…
  - Nftables utilisent une partie

Iptables (1)

- Gestion d'une règle



Pour être complet, toutes ces informations….

Ex : iptables -A forward -i eth0 -o eth1 -s 195.10.15.0/24 -d 192.120.10.2 -p tcp --sport 1024: --dport 80 --syn -m state --state NEW -j ACCEPT

Iptables (2)

Commande	Exemple	Explication
-N "nom de la chaîne"	iptables -N test	Crée une nouvelle chaîne appelée "test".
-X "nom de la chaîne"	iptables -X test	Supprime la chaîne vide "test" ; impossible pour INPUT, OUTPUT et FORWARD.
-L "nom de la chaîne "	iptables -L test	Liste les règles de la chaîne "test".
-F "nom de la chaîne "	iptables -F test	Supprime les règles de la chaîne "test".
-P "nom de la chaîne " "Action"	iptables -P INPUT DROP	Règle à appliquer par défaut.
-A "nom de la chaîne " "Règle"	iptables -A test -s 127.0.0.1 –j ACCEPT	Ajoute une nouvelle règle à la chaîne sélectionnée.
-D "nom de la chaîne " "Règle"	iptables -D test -s 127.0.0.1 -j ACCEPT	Supprime une règle spécifique à la chaîne sélectionnée.
-I "nom de la chaîne " "Position" "Regel"	iptables -I test 1 -s 127.0.0.1 -j DROP	Ajoute une nouvelle règle à une position définie dans la chaîne sélectionnée (position 1 dans l'exemple).
-D "nom de la chaîne " "Position"	iptables -D test 1	Supprime une règle occupant une position prédéfinie dans la chaîne sélectionnée (position 1 dans l'exemple).

Iptables (3)

- Script par défaut (Attention, c'est un parefeu….)
  - iptables –P INPUT DROP
  - iptables –P OUTPUT DROP
  - iptables –P FORWARD DROP
- Accès à l'interface l0
  - iptables –A input –i lo –j ACCEPT
  - iptables –A output –o lo –j ACCEPT
- Plage de port
  - x:y de x à y
  - :y de 0 à y
  - x: de x au max
- Etat d'une connexion
  - NEW, ESTABLISHED, RELATED, INVALID
  - -m state --state …

Iptables (3)

- Autoriser communication sur le réseau local ?

iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.0/24 -j ACCEPT

- Autoriser le passage vers le serveur web 195.10.5.1 ?

iptables -A FORWARD -s 192.168.x.0/24 -d 195.10.5.1 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A FORWARD -s 195.10.5.1 -d 192.168.x.0/24 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT