MINISTÈRE
DE LA DÉFENSE

NetFilter & Iptables
Le pare-feu selon Linux

Premier Maître Jean Baptiste FAVRE
DCSIM / SDE / SIC / Audit SSI
jean-baptiste.favre@marine.defense.gouv.fr

sersim

MINISTÈRE
DE LA DÉFENSE

Au menu

- Concept du pare-feu sous Linux
- Netfilter - Iptables
- Iptables
  - Principe
  - Syntaxe
- Application

sersim

MINISTÈRE
DE LA DÉFENSE

Concept du pare-feu sous Linux

- Principales fonctionnalités
  - DNAT & SNAT
  - Filtre les couche MAC, IP, TCP
  - Prise en charge de protocoles « particuliers »
  - Modification de paquets « à la volée »
  - « Statefull enabled »
  - Modulaire
  - ...
- Intervient en environnement noyau (NetFilter)
  - Droits étendus
  - Vitesse d'exécution

sersim

Concept pare-feu sous Linux

- La mise au point des règles s'effectue en espace utilisateur
  - Programme /sbin/iptables
- Il faut être root (ouf !!) ou un utilisateur autorisé (sudo)
- Sauvegarde et restauration au démarrage possible
  - Soit par un script shell (ce que nous ferons)
  - Soit directement les règles compilées

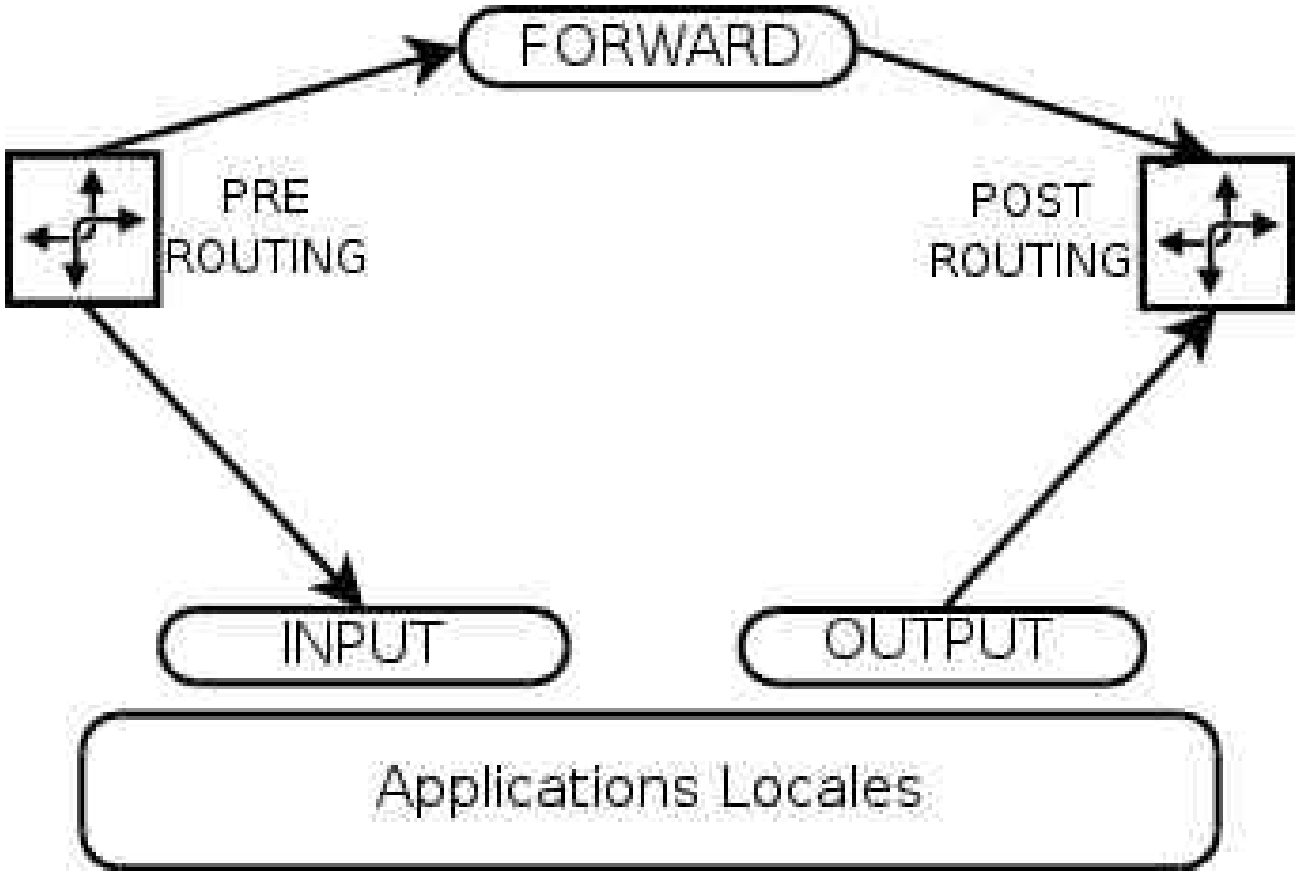
MINISTÈRE
DE LA DÉFENSE

Principe de Netfilter

- 3 tables
  - Filter (table par défaut): module iptables_filter.o
  - NAT: module iptables_nat.o
  - Mangle: module iptables_mangle.o
- 5 chaînes basiques
  - PRE-ROUTING, INPUT, FORWARD, OUTPUT, POST-ROUTING
- Des cibles (décisions)
  - ACCEPT, DROP, LOG, REJECT, MASQUERADE, SNAT, DNAT, ... en fonction des tables

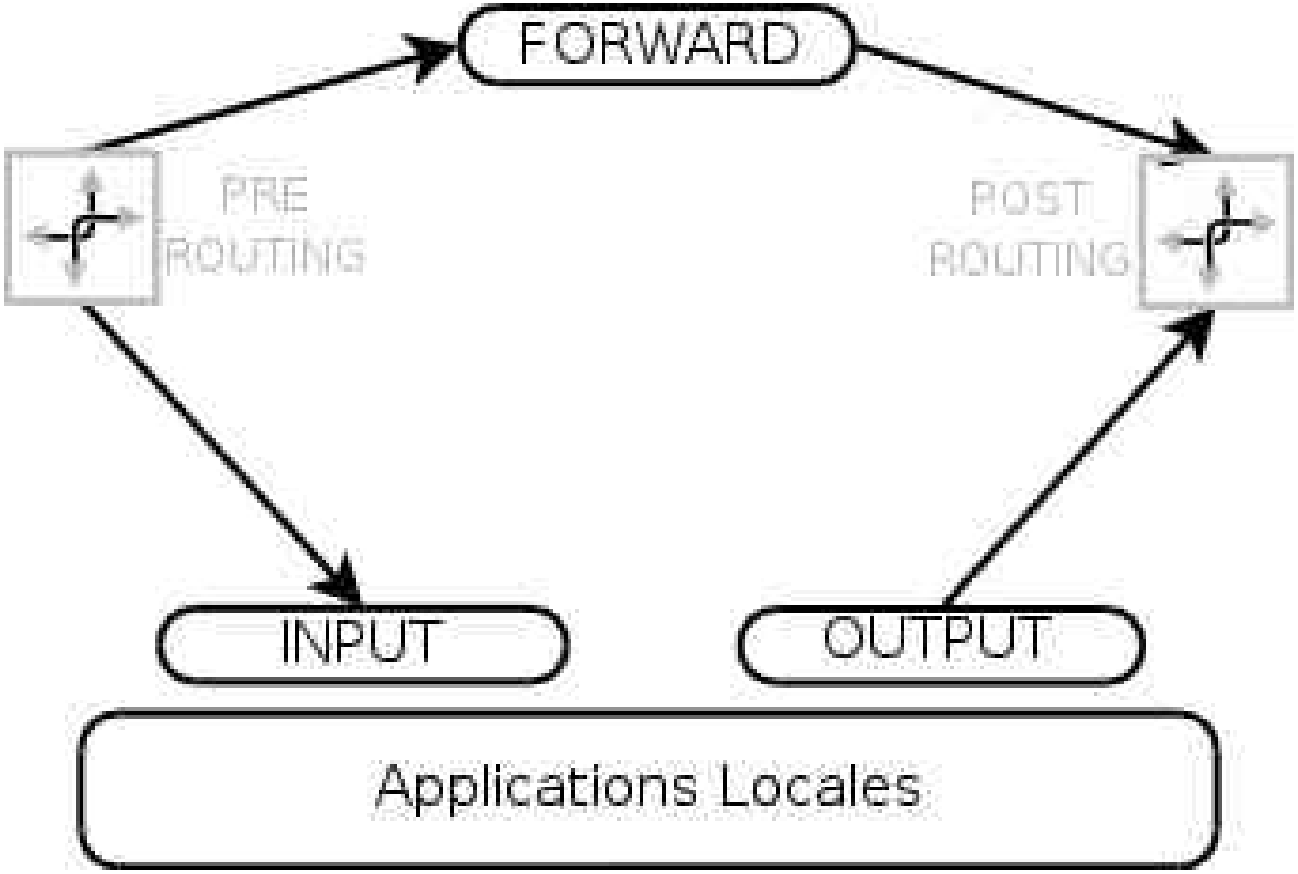
MINISTÈRE
DE LA DÉFENSE

Architecture de Netfilter



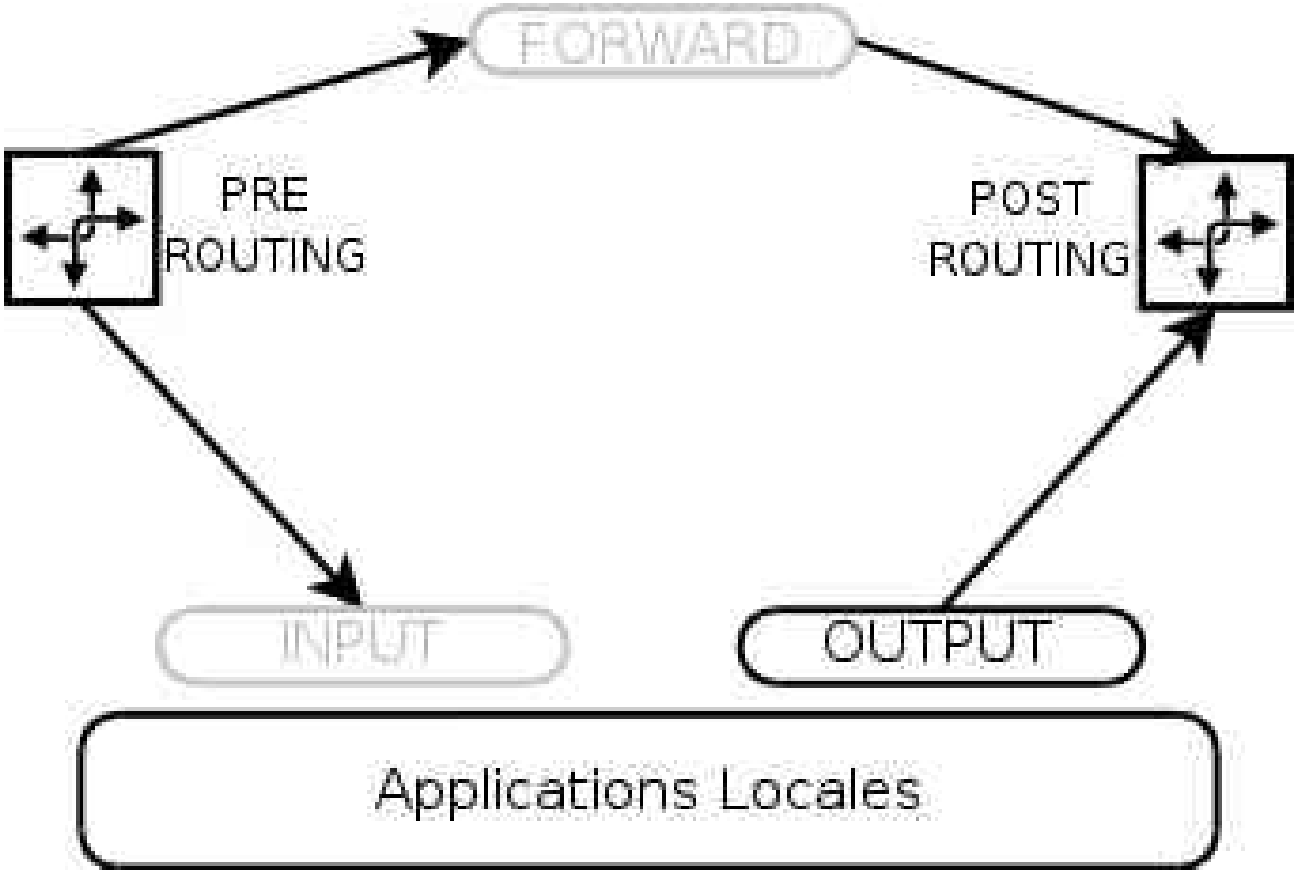
La table FILTER

- Chaînes par défaut:
  - INPUT, FORWARD, OUTPUT



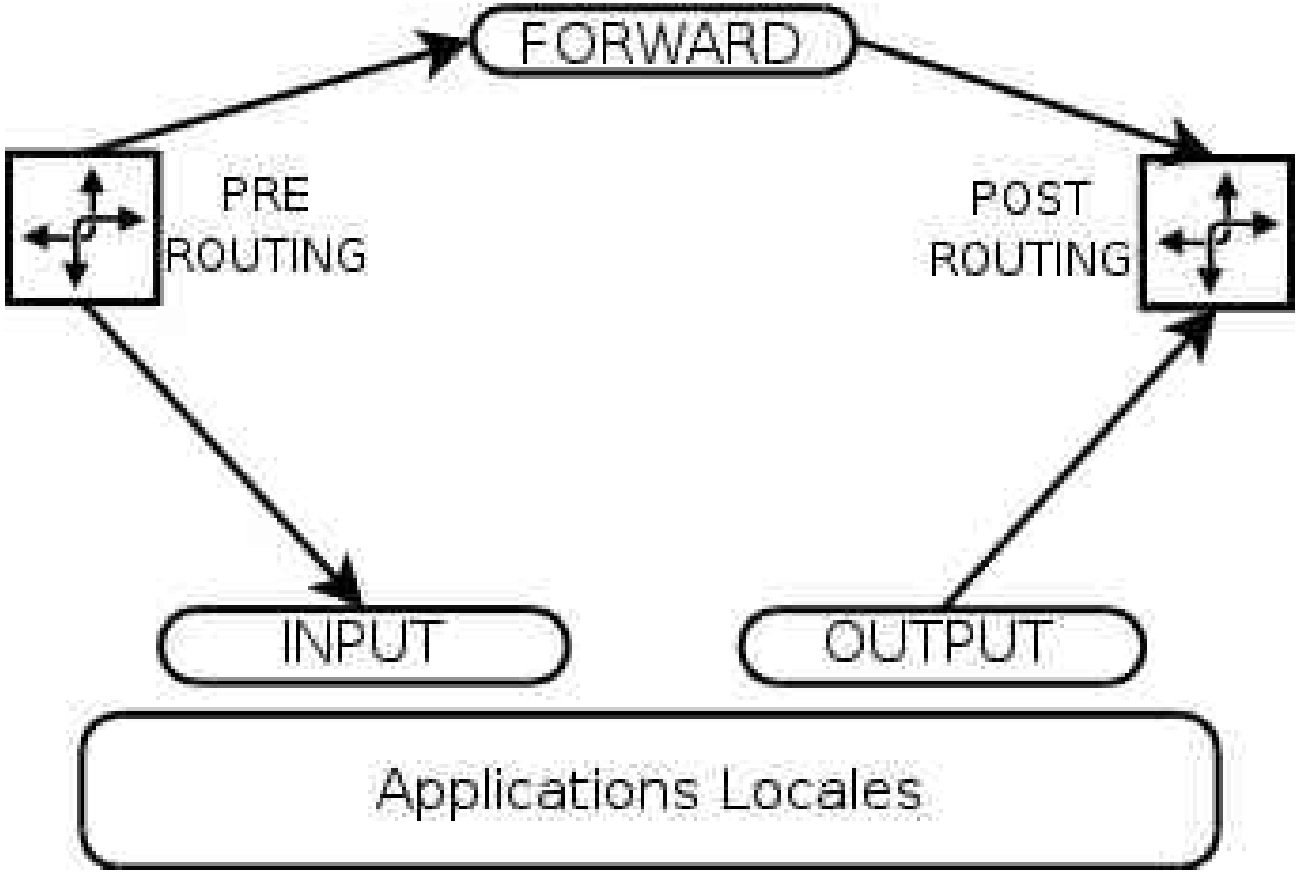
La table NAT

- Chaînes par défaut:
  - PREROUTING, OUTPUT, POSTROUTING



La table MANGLE

- Chaînes par défaut:
  - PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING

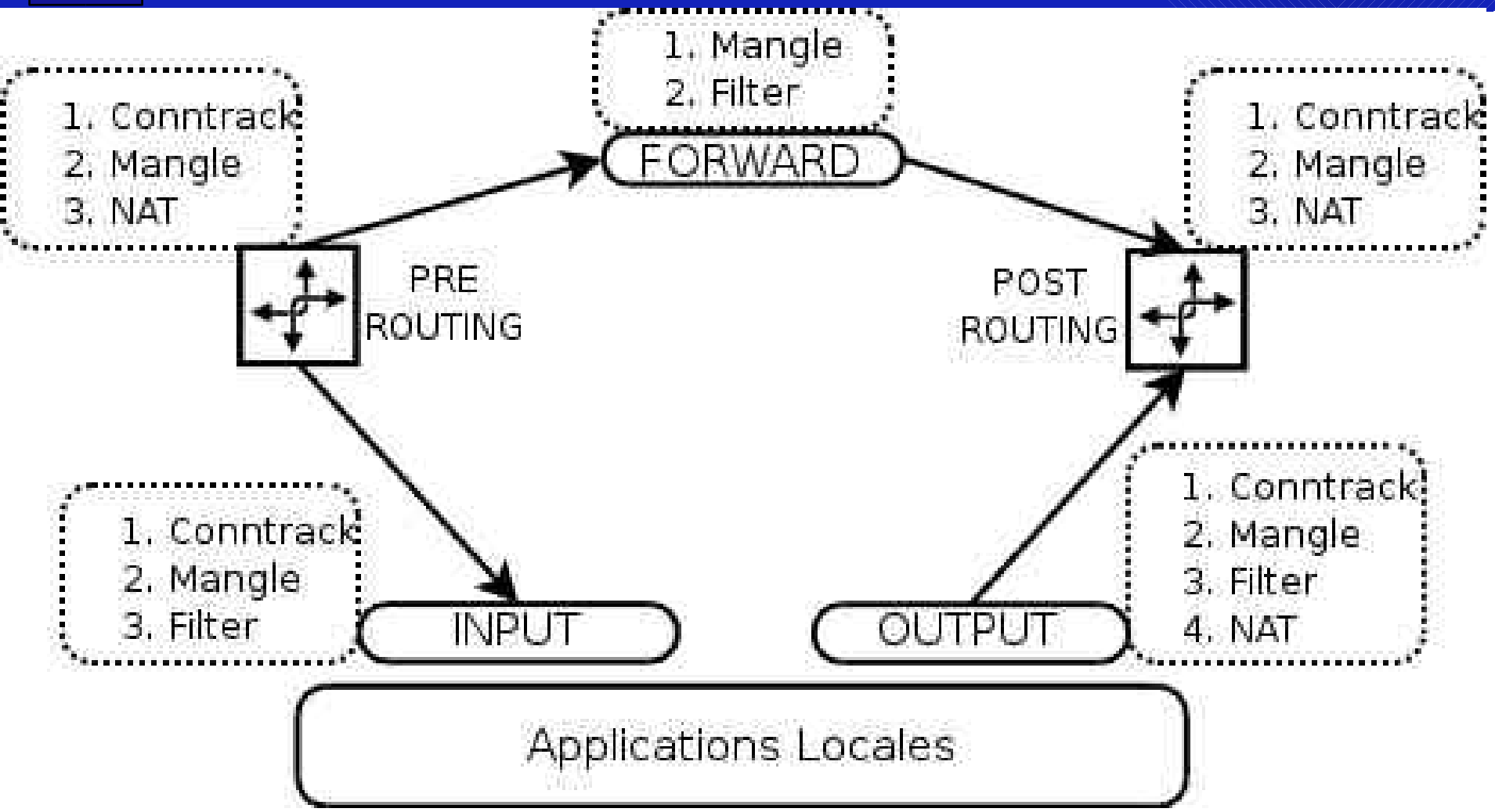


MINISTÈRE
DE LA DÉFENSE

Priorité des tables

- Par défaut:
  - Conntrack
  - Mangle
  - Nat
  - Filter
- En fonction du point d'entrée:
  - Ex: point d'entrée PRE-ROUTING
    - Conntrack
    - Mangle
    - NAT

Priorité des tables



MINISTÈRE
DE LA DÉFENSE

Le suivi de sessions

- Géré par un module: ip_conntrack
- Forme une pseudo-table
- Maintient en mémoire un tableau des connexions « en cours »
  - Connexions TCP basées sur le premier paquet
  - Connexions UDP basées sur un timeout

sersim

La création de règles: syntaxe iptables

- /sbin/iptables
  - La table d'application (FILTER par défaut)
  - La chaîne d'application
  - Un motif de reconnaissance
  - La cible représentant la décision à prendre
- Ex:
  - /sbin/iptables
    -t FILTER
    -A INPUT
    -p tcp --syn -s 192.168.0.2 --sport 1024: --dport 80
    -j ACCEPT

Les opérations sur les chaînes

- -N <chaîne>
  - Crée (Nouvelle) <chaîne>
- -L <chaîne>
  - Liste les règles de <chaîne>
- -F <chaîne>
  - Vide (Flush) les règles de <chaîne>
- -Z <chaîne>
  - Remet à Zéro les compteurs de <chaîne>

MINISTÈRE
DE LA DÉFENSE

Les opérations sur les chaînes (2)

- -P <chaîne>
  - Fixe la cible (Politique) par défaut de <chaîne>
  - Limité aux tables « basiques » (FILTER, NAT et MANGLE)
- -E <ancienne_chaîne> <nouvelle_chaîne> *
  - Renomme (Échange) <ancienne_chaîne> en <nouvelle_chaîne>
- -X <chaîne> *
  - Supprime <chaîne>

* Ne fonctionnent pas avec les tables par défaut (FILTER, NAT et MANGLE)

MINISTÈRE
DE LA DÉFENSE

Les opérations sur les règles

- -A <chaîne> [Règle]
  - Ajoute [Règle] à la fin de <chaîne>
- -I <chaîne> n [Règle]
  - Insère [Règle] à la n^{ième} position dans <chaîne>
- -R <chaîne> n [Règle]
  - Remplace la n^{ième} règle par [Règle] dans <chaîne>
- -D <chaîne> n
  - Détruit la n^{ième} règle dans <chaîne>

Motif de reconnaissance

- Basiques:
  - -p: protocole de niveau 4 (tcp, udp, icmp)
  - -s: adresse IP/réseau source
  - -d: adresse IP/réseau destination
  - --sport: port TCP/UDP source
  - --dport: port TCP/UDP destination
  - -i: interface d'entrée
  - -o: interface de sortie
  - -f: paquet fragmenté
  - --icmp-type: type de paquet ICMP
    - --icmp-type:

MINISTÈRE
DE LA DÉFENSE

Motif de reconnaissance (2)

- Modules de concordance (switch -m)
  - state, mac, owner, ttl, multiport, limit, ...
    - Exemple:
      -m multiport --dport 80,443
      -m state --state NEW
      -m state --state RELATED, ESTABLISHED
- Valables dans toutes les tables, ...
  ... mais pas toutes les chaînes
  - Exemple:
    - mac: PREROUTING, INPUT
    - owner: POSTROUTING, OUTPUT

sersim

MINISTÈRE
DE LA DÉFENSE

Les cibles

- DROP
  - Supprime le paquet
- ACCEPT
  - Laisse passer le paquet
- LOG
  - A utiliser conjointement à la concordance LIMIT
- REJECT
  - Comme DROP mais envoie un message ICMP

MINISTÈRE
DE LA DÉFENSE

Les cibles (2)

- -j <chaîne utilisateur>
  - Envoyer le paquet dans <chaîne utilisateur>
- -j RETURN
  - Sort de <chaîne utilisateur> et retourne dans la chaîne appelante
- -j QUEUE
  - Envoie le paquet en espace utilisateur pour traitement

sersim

Netfilter - Iptables

Questions ?