Elementos de iptables

Alberto Molina

@alberto_molina

Elementos principales

- Módulos del kérnel linux
  - Todas las distros los incluyen
- Herramientas del espacio de usuario
  - Paquete iptables, normalmente ya instalado
  - CLI: `iptables`

Flujo del tráfico

- Se puede hacer la siguiente clasificación del tipo de tráfico:
  - Entrante con destino el equipo
  - Saliente, originado en el equipo
  - Que atraviesa el equipo (entra por una interfaz de red y sale por otra)
- Esto, junto a lo que queramos hacer, nos permite agrupar las reglas en iptables

Jerarquía de elementos

- Reglas
- Las reglas se agrupan en cadenas
- Las cadenas se agrupan en tablas

Tablas

- **`filter`** Cortafuegos. Tabla por defecto
- **`nat`** Para hacer NAT
- **`mangle`** Marcar y modificar paquetes
- **`raw`** Depurar seguimiento conexión
- **`security`** Usada para MAC (SELinux)

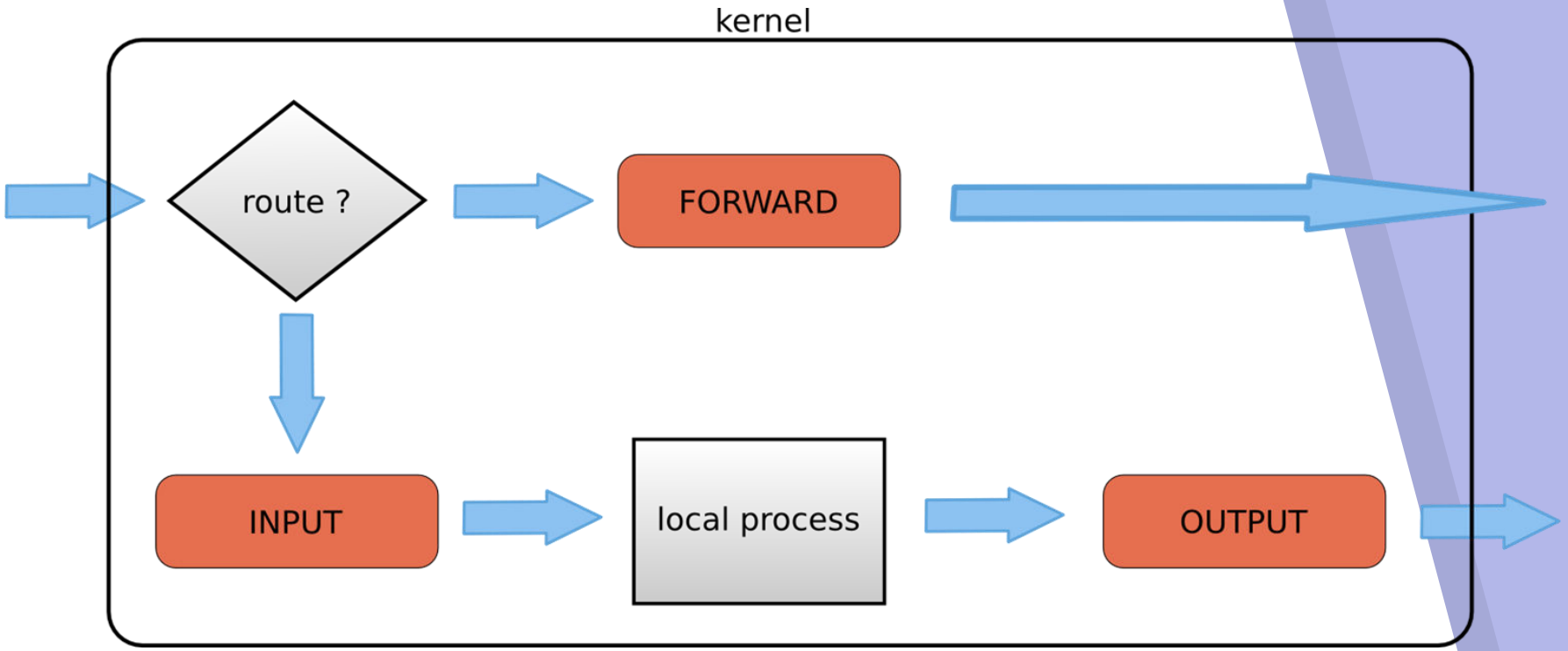
Cadenas de filter

- INPUT
- OUTPUT
- FORWARD

Cadenas de nat

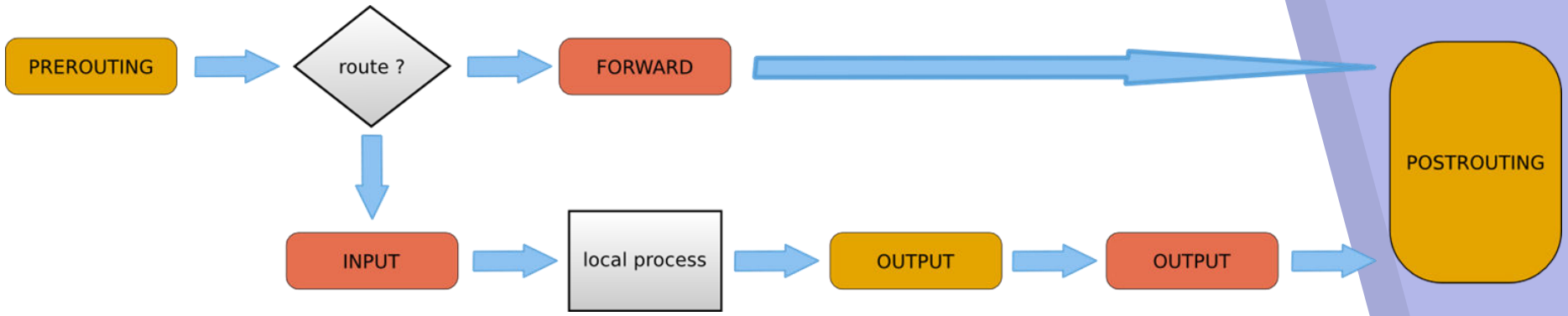
- PREROUTING
- INPUT
- OUTPUT
- POSTROUTING

Diagrama de Flujo tabla filter



Fuente: http://linux-training.be/networking/ch14.html

Diagrama de Flujo tablas filter y nat



Fuente: http://linux-training.be/networking/ch14.html

Tipo de tráfico y flujo

- Paquete del exterior con destino el equipo:
  - POSTROUTING de nat e INPUT de filter
- Paquete originado en el equipo que sale
  - OUTPUT de nat, OUTPUT de filter y POSTROUTING de nat
- Paquete que atraviesa el equipo
  - PREROUTING de nat, FORWARD de filter y POSTROUTING de nat