NETFILTER IPTABLES

Netfilter es un framework de linux que **permite interceptar y manipular paquetes de red.** Iptables es **su componente más popular y actúa como cortafuegos.**

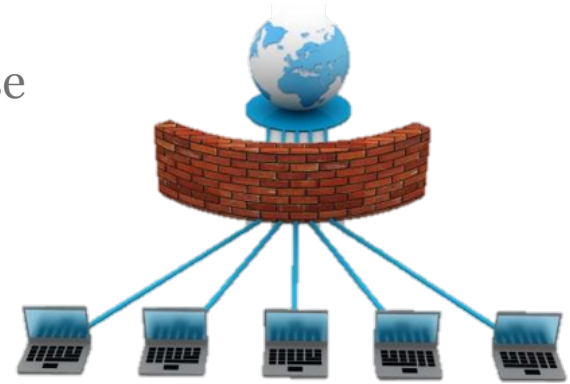
1.

FIREWALL

Descripción del Firewall (Cortafuegos)

Un cortafuegos es un sistema (hardware o software) usado para separar una subred protegida de otra red de riesgo estableciendo políticas de control entre ambos entornos.

El **filtrado de paquetes** es un proceso que deniega o permite el flujo de información y datos entre la red que se desea proteger (interna) del resto.



Descripción del Firewall (Cortafuegos)

- Trabajan sobre las **cabeceras de los paquetes IP**.
- Según las reglas podrá realizar distintos tipos de acciones (aceptar, rechazar…) sobre los paquetes.
- Tipos de filtrado de paquetes:
  - Estático (*stateless*): analiza las cabeceras de cada paquete sin establecer relación con otros.
  - Dinámico (*stateful*): permite el control de un flujo de datos relacionados dentro de una misma conexión TCP o varias conexiones haciendo uso de la memoria

2.

NAT

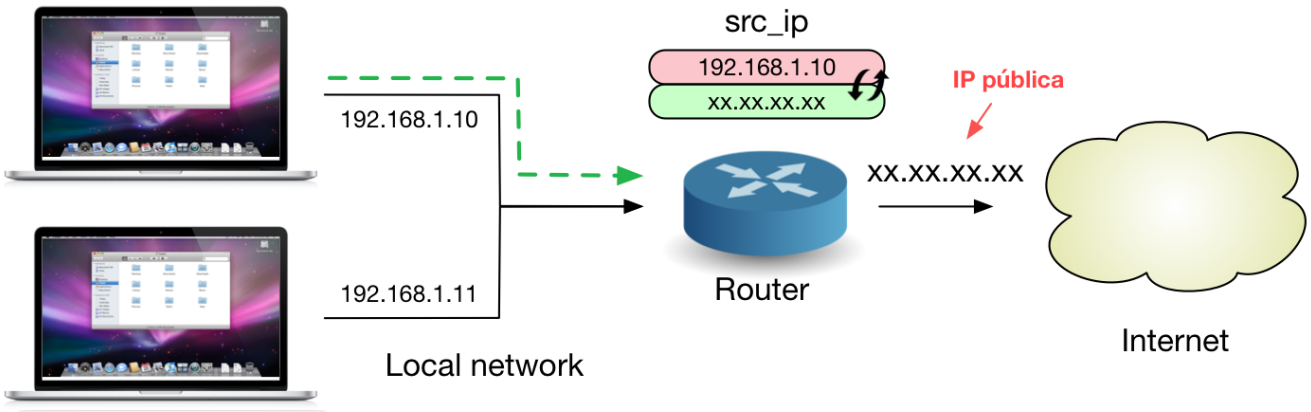
Enmascaramiento NAT

Network Address Translation

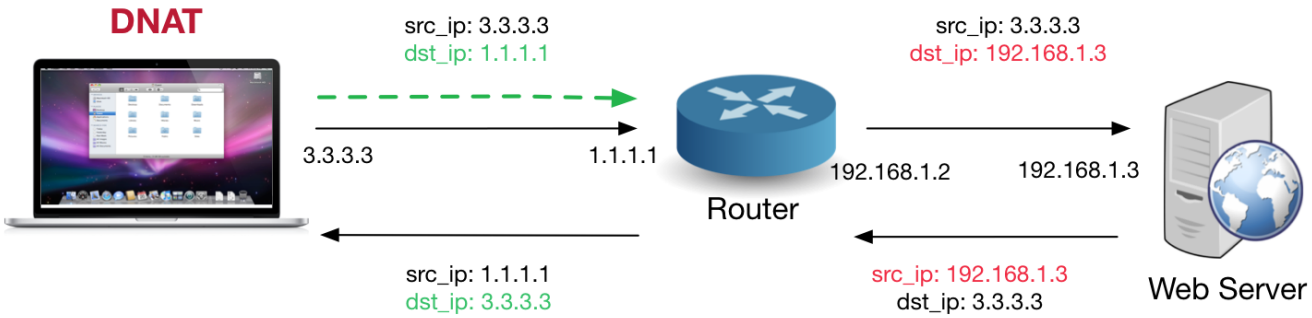
Mecanismo que altera las cabeceras de los paquetes IP soliendo cambiar las direcciones IP y puertos origen o destino.

- *Source NAT (SNAT)*: Se altera el origen del datagrama, realizado después del encaminamiento del mismo y antes de su reenvío.
- *Destination NAT (DNAT)*: Se altera el destino del datagrama, realizado antes del encaminamiento del mismo.

SNAT


src_ip
192.168.1.10
xx.xx.xx.xx
IP pública
192.168.1.10
192.168.1.11
Local network
Router
xx.xx.xx.xx
Internet

DNAT


src_ip: 3.3.3.3
dst_ip: 1.1.1.1
3.3.3.3
1.1.1.1
Router
192.168.1.2
src_ip: 3.3.3.3
dst_ip: 192.168.1.3
192.168.1.3
Web Server
src_ip: 1.1.1.1
dst_ip: 3.3.3.3
src_ip: 192.168.1.3
dst_ip: 3.3.3.3

3.

PROCESAMIENTO DE PAQUETES

Filtrado de paquetes

Con Netfilter e Iptables se puede realizar:

- Filtrado de paquetes
- Traducción de direcciones y puertos NAT
- Manipulación sobre datagramas IP
- Seguimiento de conexiones

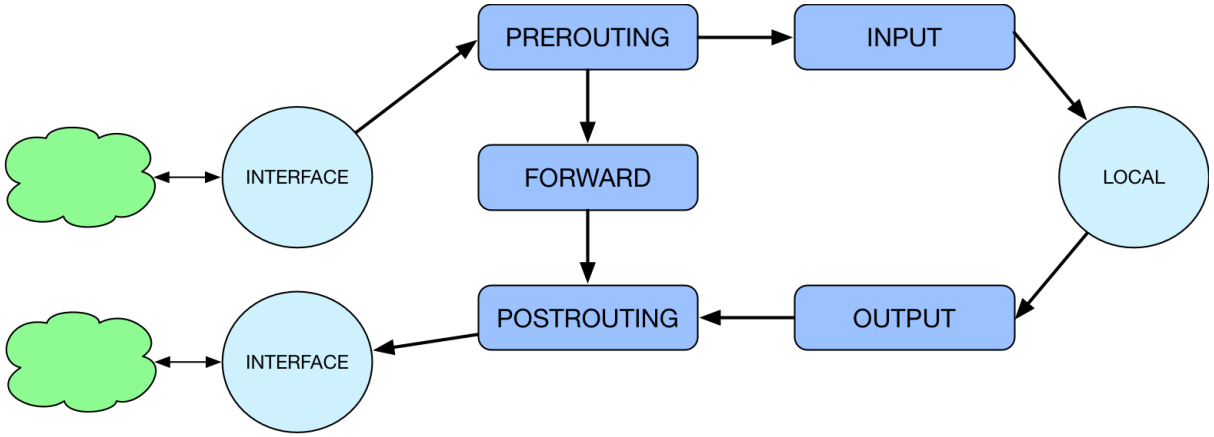
Netfilter permite el uso de distintas tablas de IP para el filtrado: *nat*, *filter*, *mangle* y *raw*.

Funciona con IPv4 e IPv6

Cadenas (*chains*)

Netfilter gestiona el filtrado mediante tablas organizadas en cadenas y éstas a su vez compuestas por reglas.

- Las cadenas son agrupaciones de reglas que se aplican a los paquetes en momentos concretos.



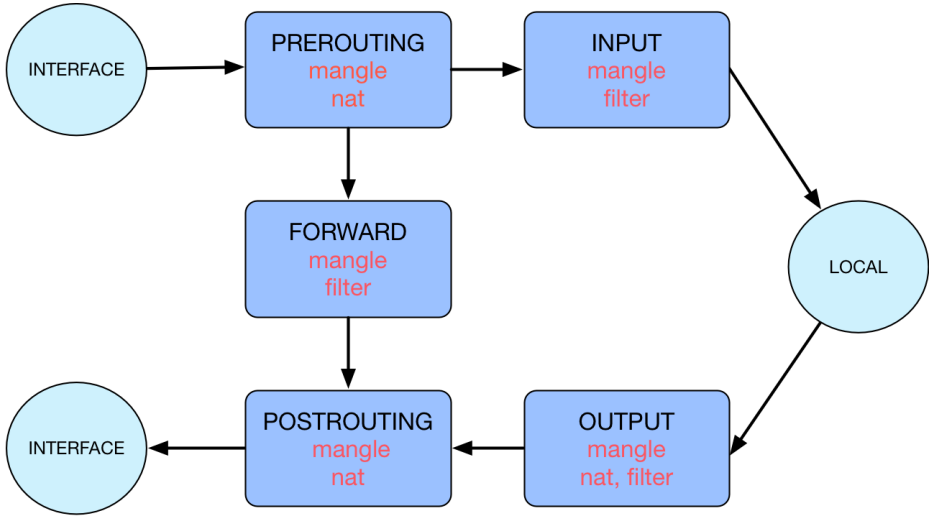
Cadenas (*chains*)

- *INPUT*: acción a realizar cuando un paquete coincide con la regla a la entrada de la interfaz. Se aplica a paquetes destinados a la propia máquina.
- *OUTPUT*: acción a realizar cuando un paquete coincide con la regla, a la salida de la interfaz. Se aplica a paquetes originados en la propia máquina.
- *FORWARD*: Cuando un paquete se envía de una interfaz a otra. Cadena intermedia entre las dos siguientes.
- *PREROUTING*: primera acción a realizar antes de que el paquete entre en el sistema.
- *POSTROUTING*: acción a realizar justo antes de enviar el paquete a la interfaz destino.

Tablas

Tipo de procesamiento que se debe aplicar a los paquetes

- *Tipos*: *filter*, *mangle*, *nat* y *raw*



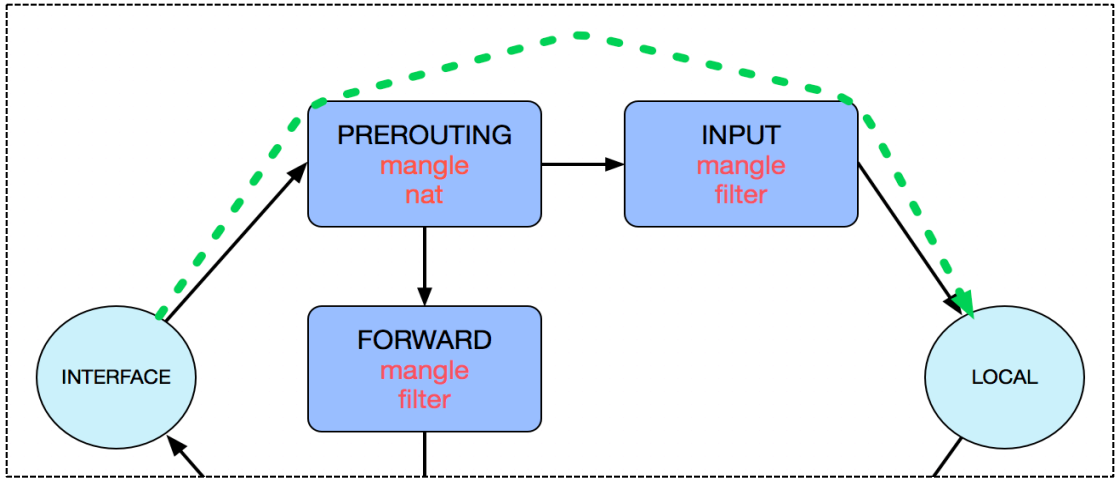
Tablas

- *FILTER*: filtrado general de paquetes. Decide los paquetes que pasan y los que no. Compuesta por las cadenas *input*, *output* y *forward*.

- *NAT*: traducción de direcciones. Permite cambiar las direcciones origen y destino de los datagramas. Compuesta por las cadenas *prerouting*, *postrouting* y *output*.

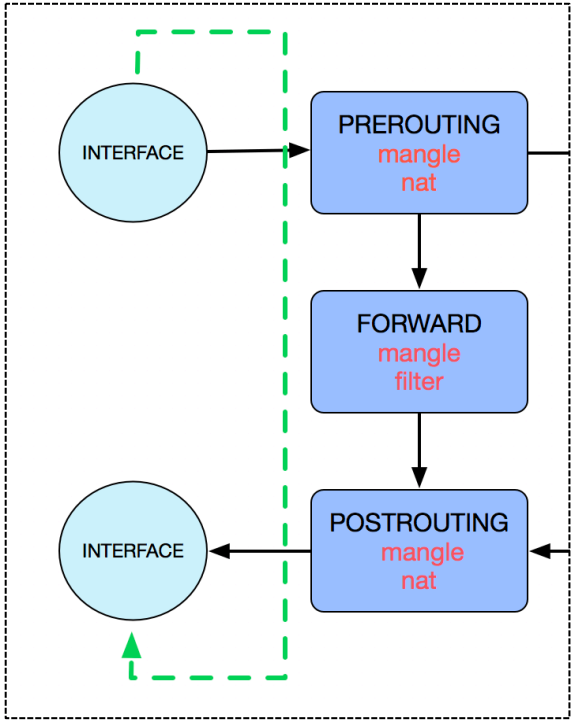
- *MANGLE*: analiza el paquete y lo etiqueta para que reciba un tratamiento concreto. Compuesta por las cadenas *prerouting*, *postrouting, input, forward* y *output*.

Paquetes entrantes, destino Local



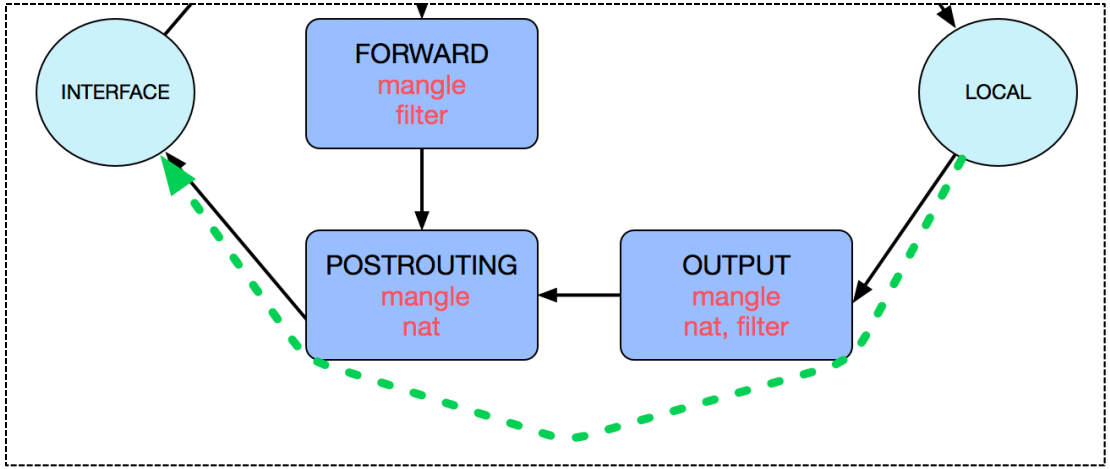
[PRE] *Mangle*: cambios en cabecera (TOS), *Nat*: DNAT y decisión de camino.
[INPUT] *Mangle*: cambios antes del procesamiento, *Filter*: filtrado tráfico entrante

Paquetes entrantes, destino reenvío



[PRE] *Mangle*: cambios en cabecera, *Nat*: DNAT y decisión de camino.
[FORW] *Mangle*: cambios en cabecera, *Filter*: filtrado del tráfico reenviado.
[POST] *Mangle*: cambios antes del envío, *Nat*: SNAT

Paquetes salientes, origen Local



[OUT] *Mangle*: cambios en cabecera, *Nat*: cambios en direcciones, *Filter*: filtrado del tráfico saliente
[POST] *Mangle*: cambios antes del procesamiento, *Nat*: SNAT

4.

REGLAS

Creación de reglas

Sintaxis del comando *iptables*:

1. Comando *iptables*
2. Tabla a usar: *filter, nat, mangle*
3. Comando sobre la cadena: *insertar, modificar, eliminar reglas…*
4. Cadena a usar: *input, output, forward, prerouting o postrouting*
5. Condición: criterios que deben cumplir los campos
6. Acción a realizar (para los que cumplan la condición previa)
7. Opciones extra para ajustar la acción