FIREWALLS

Firewalls

Un firewall es un dispositivo hardware o software que se encarga del filtrado de paquetes.

Opera mediante reglas. Cada regla consiste en un patrón, que selecciona el tráfico a filtrar, y una acción que se ejecuta sobre el tráfico que encaja con el patrón.

Firewalls

Los routers MikroTik agrupan las reglas de filtrado en cadenas.
Cada cadena es un conjunto de reglas que se ejecuta secuencialmente.
Cuando el tráfico encaja con el patrón de alguna de las reglas, se ejecuta la acción y termina el análisis.

```
/ip firewall filter
add chain=input connection-state=invalid action=drop
add chain=input connection-state=established
action=accept
add chain=input protocol=icmp action=accept
add chain=input src-address=192.168.0.0/24 action=accept
add chain=input action=accept
```

Al final de cada cadena hay una regla implícita que deja pasar todo el tráfico.

Firewalls

Hay tres cadenas por defecto que no se pueden borrar:

- **input –** Paquetes entrantes destinados a alguna de las direcciones del router.
- **forward** – Paquetes no destinados al router ni originados en el router.
- **output** – Paquetes salientes originados en el router.

Además es posible crear cadenas adicionales que permiten organizar las reglas de una manera coherente.

Las acciones a realizar en una regla pueden ser: accept, drop, log, reject, jump

La acción `jump` permite saltar de una cadena a otra:

```
add chain=forward protocol=tcp action=jump jump-target=tcp
add chain=forward protocol=udp action=jump jump-target=udp
add chain=forward protocol=icmp action=jump jump-target=icmp
```

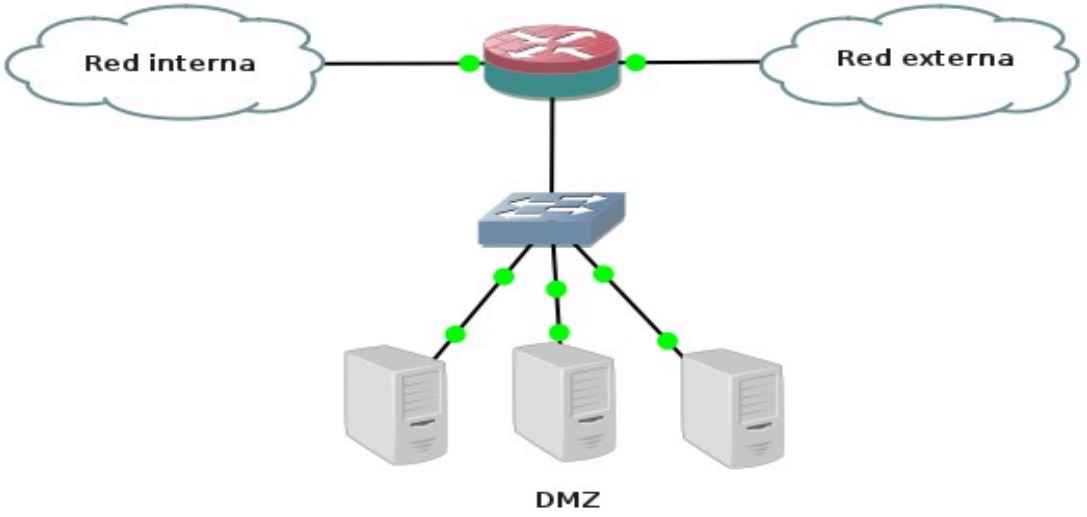
Firewalls

Los patrones se construyen en base a los valores de los campos de las cabeceras de los protocolos.

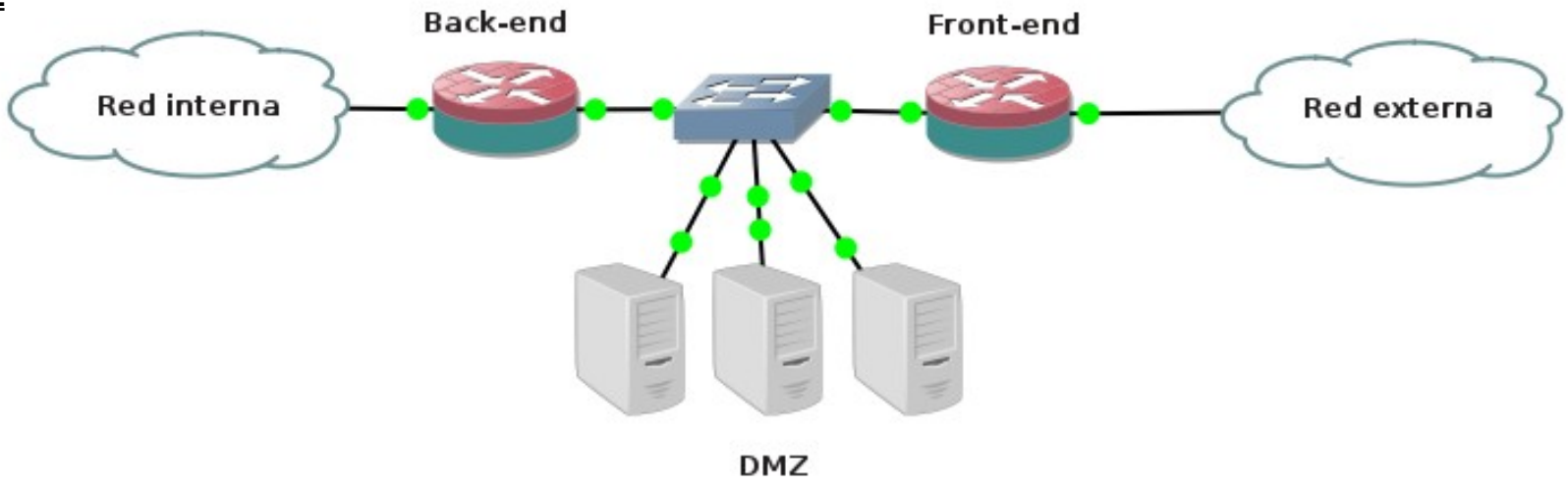
https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

Firewalls

FIREWALL ÚNICO



FIREWALL DUAL



Firewalls

RESTRICCIONES PARA PREVENIR ATAQUES IP SPOOFING

- Las direcciones privadas especificadas
- Direcciones multicast (direcciones de multidifusión)
- Direcciones de loopback
- Direcciones de la clase E (Están reservadas).
- Si las direcciones de la red interna no coinciden con alguno de los bloques de direcciones para redes privadas, también es recomendable restringir el acceso a aquellos paquetes con direcciones de origen correspondientes a la red interna.

CONSIDERACIONES SOBRE TRÁFICO ICMP

- ICMP Echo e ICMP Echo Reply
- ICMP unreachable.
- ICMP Source quench.
- ICMP Time Exceeded.

Firewalls

REGLAS PARA PERMITIR SERVICIOS

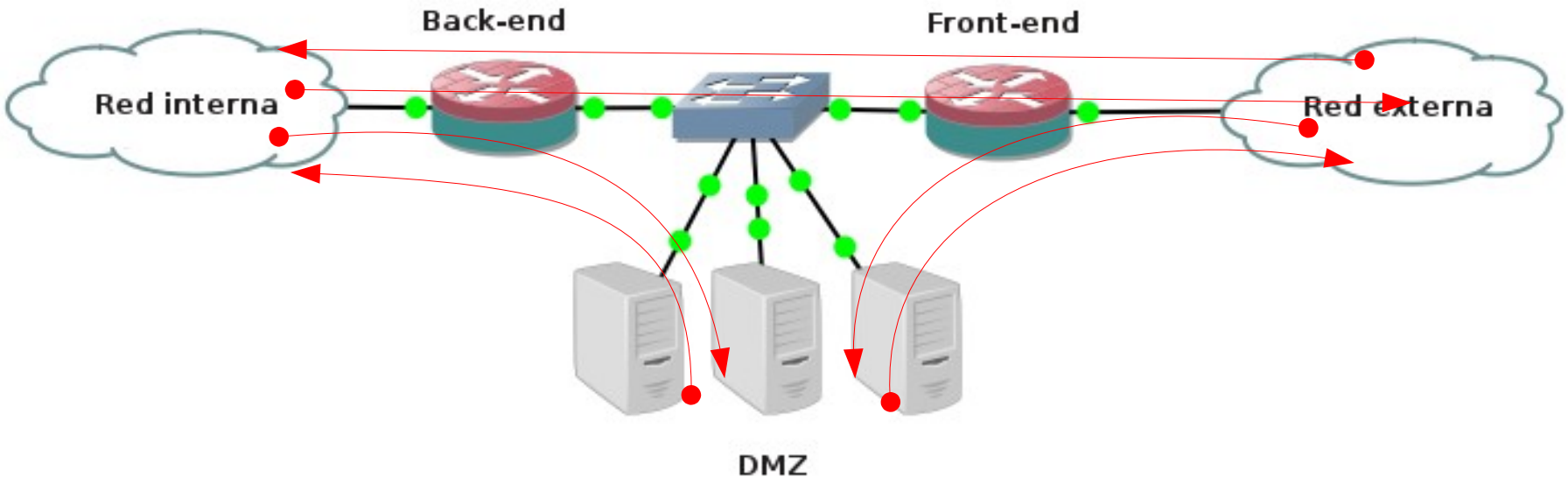
REGLAS BASADAS EN ESTADO

```
add chain=forward connection-state=established action=accept
```

PROTECCIÓN DEL PROPIO ROUTER

Firewalls

HAY QUE CONSIDERAR TODOS LOS POSIBLES FLUJOS DE TRÁFICO



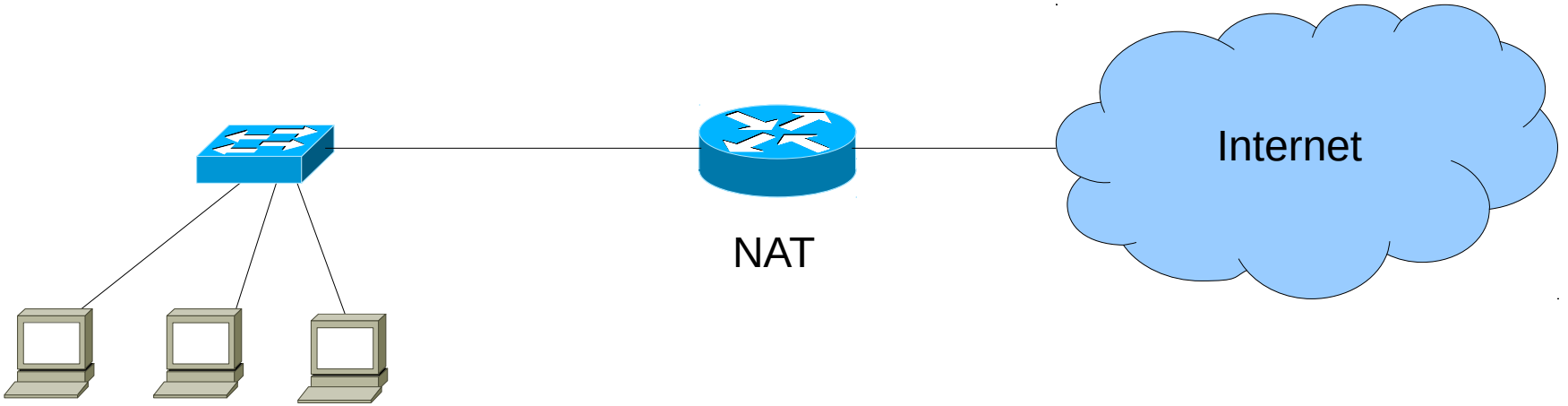
NAT

NAT (Network Address Translation)

Tipos de NAT:

- ***NAT estático:*** Es un mapeo uno-a-uno entre direcciones privadas y públicas y requiere una dirección pública por cada dirección privada.
- ***NAT dinámico:*** Mapea una dirección privada a una dirección pública de un pool, por lo que es necesario disponer de suficientes direcciones públicas.
- ***Overloading (PAT):*** Se mapean las direcciones privadas sobre una única dirección pública. Para diferenciarlas se utilizan los puertos.

NAT (Network Address Translation)



192.168.1.0/24

Direcciones privadas

Direcciones públicas

NAT (Network Address Translation)

¿Cuándo se usa NAT?

- Cuando debemos conectar un host a internet y este no tiene direcciones globalmente únicas.
- Cuando se cambia a un nuevo ISP y requiere renumerar su red.
- Mezcla de dos intranets con direcciones duplicadas.

NAT (Network Address Translation)

Ventajas	Inconvenientes
•Remedia el solapamiento de direcciones. •Mayor flexibilidad a la hora de conectar con Internet. •Evita renumerar cuando cambia la red	•La traducción introduce retardos. •Se pierde la posibilidad de trazar extremo a extremo. •Ciertas aplicaciones no funcionan correctamente.

NAT (Network Address Translation)

Tipos de NAT:

Source NAT(SNAT): Cambia la dirección de origen de los paquetes que atraviesan el router.

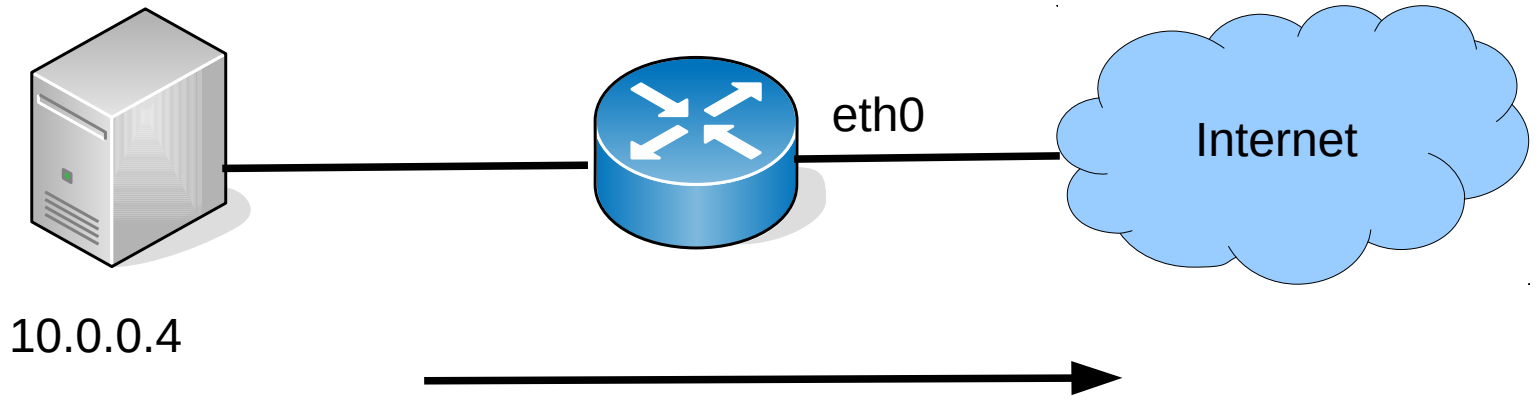
Destination NAT (DNAT): Cambia la dirección de origen de los paquetes que atraviesan el router.

Bidireccional: Cuando se configuran DNAT y SNAT simultáneamente.

NAT (Network Address Translation)

Comandos en MikroTik (SNAT):

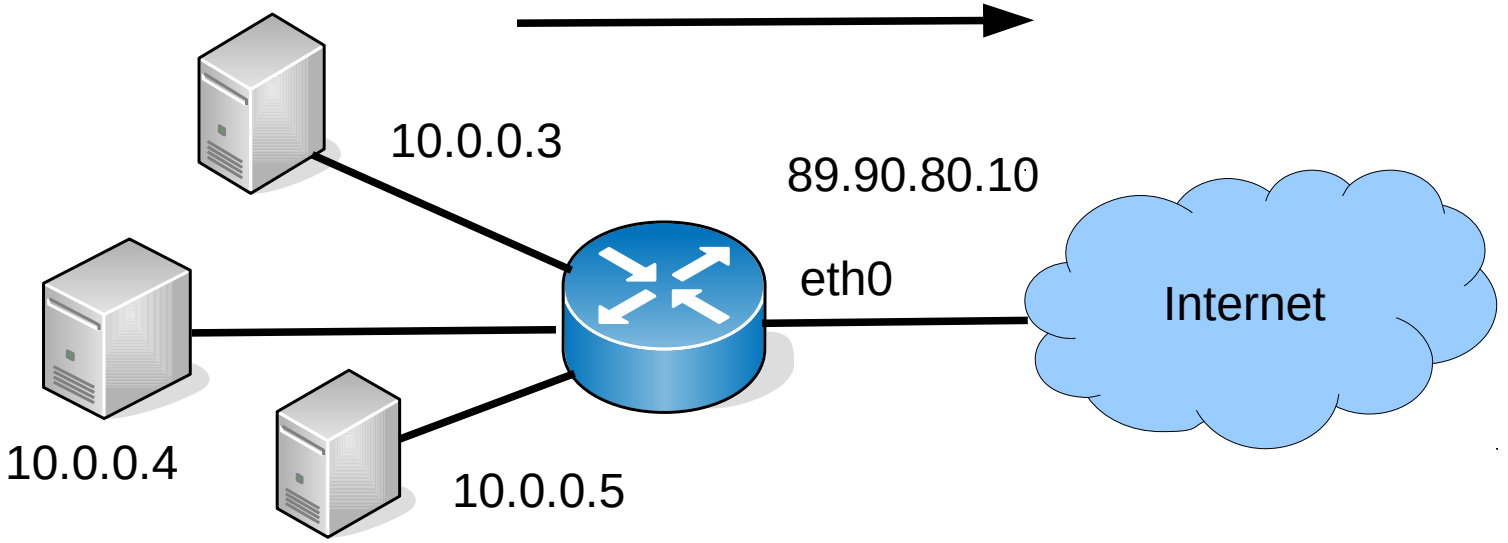
```
/ip firewall nat
add chain=srcnat src-address=10.0.0.4
action=src-nat to-addresses=89.90.80.10 out-
interface=eth0
```



NAT (Network Address Translation)

Comandos en (NAT masquerade):

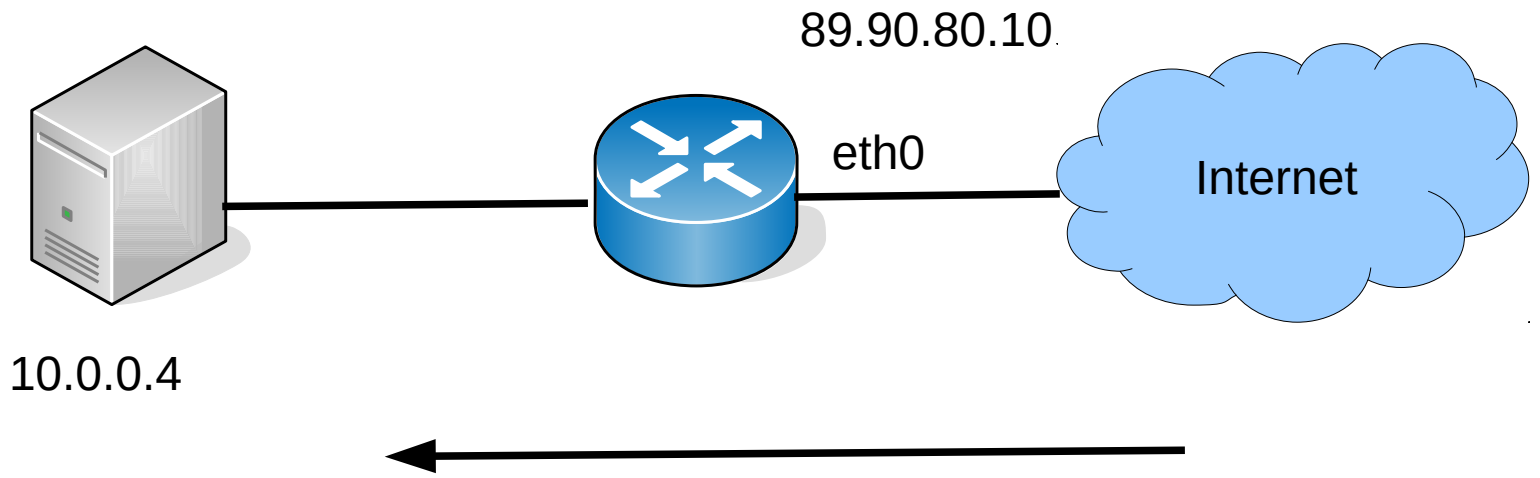
```
/ip firewall nat add chain=srcnat action=masquerade out-interface=eth0
```



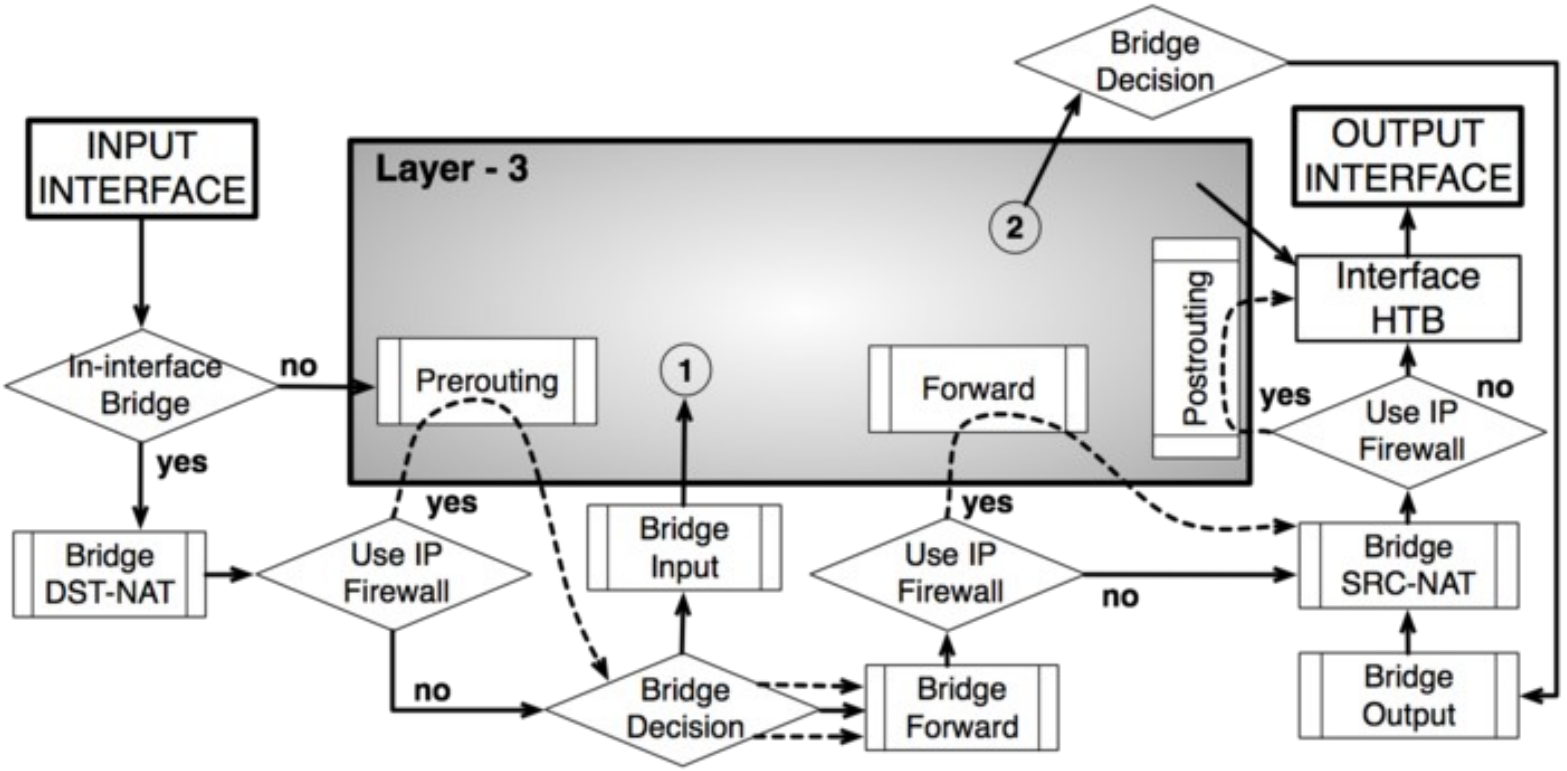
NAT (Network Address Translation)

Comandos en (DNAT):

```
/ip firewall nat add chain=dstnat dst-address=89.90.80.10 action=dst-
nat    to-addresses=10.0.0.4
```



Firewalls


Bridge Decision
INPUT INTERFACE
Layer - 3
OUTPUT INTERFACE
2
Postrouting
Interface HTB
In-interface Bridge
no
Prerouting
1
Forward
yes
no
Use IP Firewall
yes
yes
yes
Bridge DST-NAT
Use IP Firewall
Bridge Input
Use IP Firewall
no
Bridge SRC-NAT
no
Bridge Decision
Bridge Forward
Bridge Output