IPTABLES

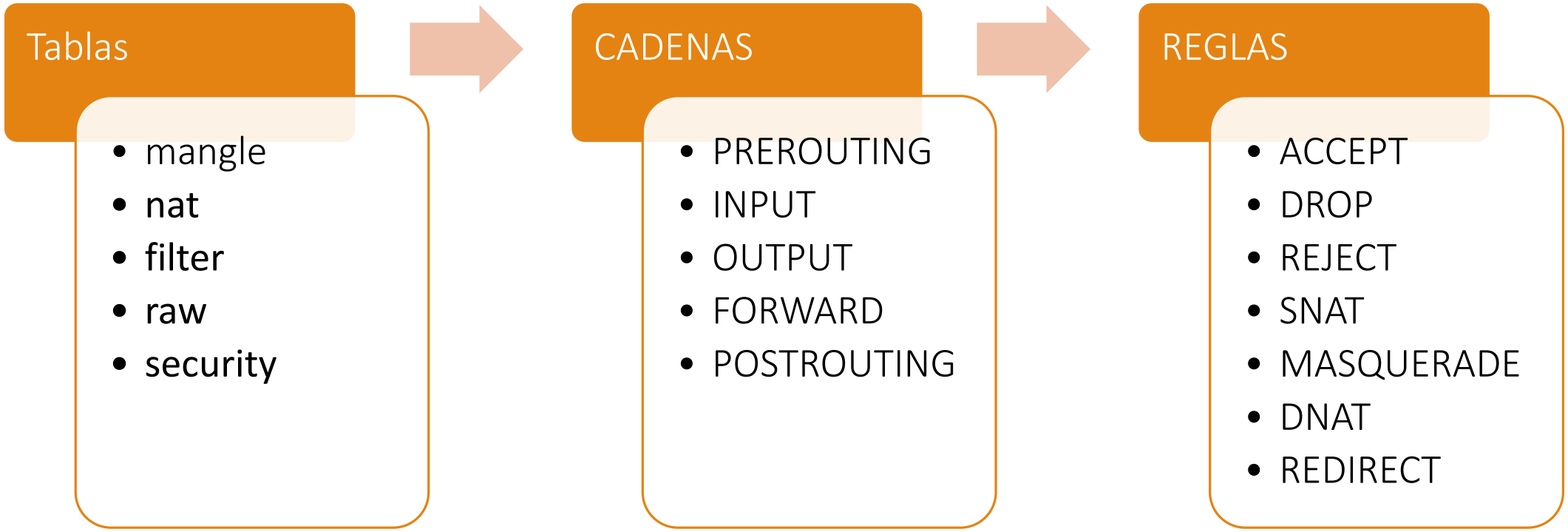
PROYECTO NETFILTER.ORG

Índice

¿Qué es IPTABLES?

- Herramienta de software libre, desarrollada bajo el proyecto Netfilter.org.
- Sus funciones son:
  - Monitorización del tráfico de red.
  - Filtrado del tráfico, permitiendo o denegando acceso.
  - Traducción de direcciones de red.
  - Marcar y modificar paquetes.

Elementos de IPTABLES



Elementos de IPTABLES: Tablas

Las tablas contenidas en IPTABLES son:

- filter: Usada para filtrar el tráfico de red.
- nat: Realiza traducciones de direcciones de red.
- mangle: Usada para marcar y modificar el tráfico de red.
- raw: para realizar el depuramiento de la conexión.
- security: Usada para un tratamiento especial de seguridad.

Elementos de IPTABLES: Cadenas

filter	nat
• INPUT • OUTPUT • FORWARD	• PREROUTING • INPUT • OUTPUT • POSTROUTING

Elementos de IPTABLES: Reglas

La estructura de todas las reglas de IPTABLES es la siguiente:

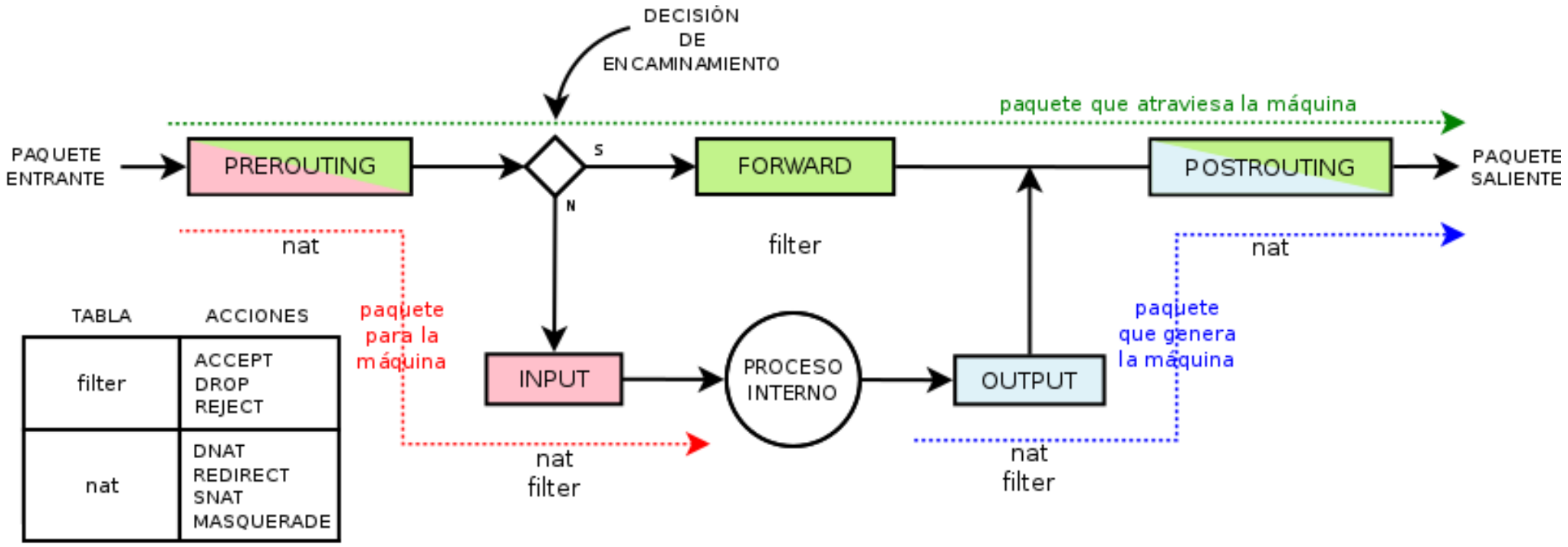
```
iptables [-t TABLA] [opciones] COMANDO_SOBRE_CADENA [condiciones] [-j OBJETIVO [opciones_del_objetivo]]
Ejemplos:
# iptables –t filter –A INPUT –i eth0 –p tcp --dport 80 –j ACCEPT
# iptables –t nat –A POSTROUTING –o eth0 –j SNAT --to-source 80.56.14.2
```

OBJETIVO FILTER

- ACCEPT
- DROP
- REJECT
- LOG

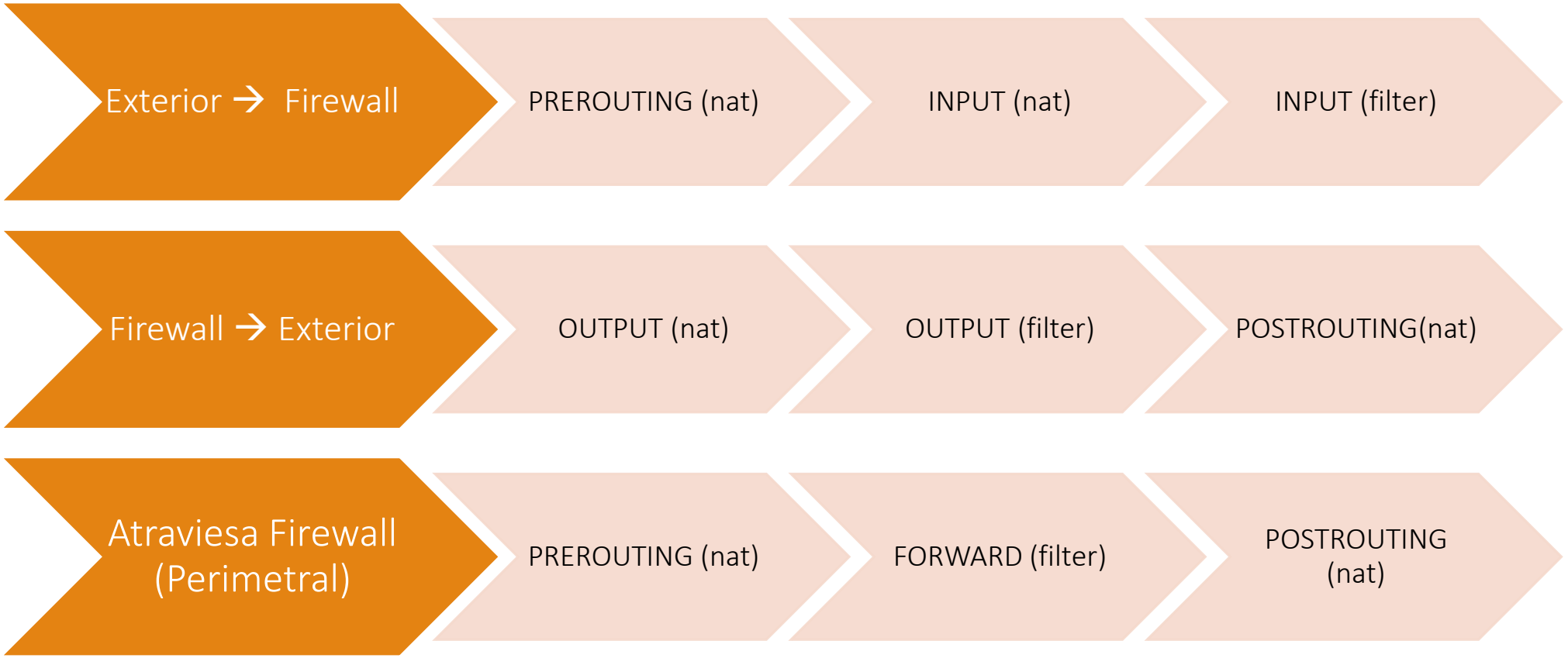
OBJETIVO NAT

- DNAT
- SNAT
- MASQUERADE
- REDIRECT



IPTABLES: Relación entre elementos

Flujo del tráfico por el firewall



Habilitar Forwarding (Perimetral)

- Se debe habilitar en casos de implementación de un firewall perimetral.
- Permite el tráfico entre las interfaces del firewall.
- El firewall deberá tener tantos interfaces de red como redes esté conectado.
- Ponemos a 1 el valor del archivo "ip_forward":
  - echo 1 > /proc/sys/net/ipv4/ip_forward

Sintaxis: Política del firewall

Todas las reglas de IPTABLES se ejecutan de forma secuencial de la lista de la tabla. En el momento que una regla cumple sus condiciones y es ejecutada ya no se siguen comprobando el resto de reglas de la tabla.

iptables [-t TABLA] [opciones] COMANDO_SOBRE_CADENA [condiciones] [-j OBJETIVO [opciones_del_objetivo]]

Establecer la política por defecto:

```
# iptables [-t tabla] -P [CADENA] ACCEPT|DROP
```

- -t [table]: indicamos la tabla. Si no se indica se toma filter.
- -P [CADENA]: se puede indicar cadena o no, si no se indica se aplica a todas las cadenas de la tabla.
- ACCEPT|DROP: ACCEPT permite todo el tráfico y DROP lo deniega.
- **NOTA: La política DROP implica que deben realizarse reglas de permisión por parejas.**
  - Para comunicaciones hacia/desde el firewall reglas en INPUT y OUTPUT.
  - Para comunicaciones que atraviesan el firewall: dos reglas en FORWARD.

Sintaxis: Añadir reglas (filter)

Añadir reglas al final de la tabla:

```
# iptables [–t tabla] -A [CADENA][-p PROTOCOLO] [-s IP_Origen] [-d IP_Destino] [-i int_Entr] [-o Int_salida] -j ACCEPT|DROP
```

- -p: protocolo al que se aplica.
- -s: dirección IP o subred de origen.
- -d: dirección IP o subred de destino.
- -i: interfaz de entrada de los paquetes.
- -o: interfaz de salida de los paquetes.

Añadir reglas en una determinada posición de la tabla:

```
# iptables [–t tabla] -I [indice] [CADENA][-p PROTOCOLO] [-s IP_Origen] [-d IP_Destino] [-i int_Entr] [-o Int_salida] -j ACCEPT|DROP
```

- -i: Se indica la posición en la que se quiere insertar. Si no se especifica un número pues se inserta en la primera posición.

Sintaxis: Ejemplos de inserción de reglas

Recordemos que en el caso de política drop debemos crear reglas por pares. Ejemplos:

INPUT y OUTPUT. Permitir ping:

- Regla en INPUT: # iptables -I INPUT –p icmp -i eth0 -j ACCEPT
- Regla en OUTPUT: # iptables -I OUTPUT –p icmp -o eth0 -j ACCEPT

FORWARD. Permitir ping creando dos reglas:

- # iptables –I FORWARD –p icmp –i eth0 –o eth1 –j ACCEPT
- # iptables –I FORWARD –p icmp –i eth1 –o eth0 –j ACCEPT

Sintaxis: Listar reglas

Listar las reglas de una tabla:

```
# iptables –t tabla -L [CADENA] [-n] [-v] [--line-numbers]
```

- -L: Muestra la lista de reglas de una cadena.
- -n: muestra direcciones IP.
- -v: Muestra información adicional valiosa.
- --line-numbers: muetra el número ordinal de regla.

Listar las reglas de una tabla en el mismo formato de entrada de reglas:

```
# iptables -S [CADENA] [-v]
```

Sintaxis: Borrar reglas

Borrar una regla de una cadena:

```
# iptables [–t tabla] -D CADENA [N]
```

- N: Número de la regla que se quiere borrar. Si no se especifica se borra la primera.

Borrar todas las reglas de una cadena:

```
# iptables [-t tabla] -F [CADENA]
```

- -F [CADENA]: Borra todas las reglas de la cadena especificada. Si no se especifica borra todas las reglas de todas las cadenas de la tabla.

Poner los contadores a cero:

```
# iptables –Z [CADENA]
```

- -Z [CADENA]: si no se especifica la cadena se pone a cero todos los contadores de todas las cadenas de la tabla.

Sintaxis: SNAT (POSTROUTING)

Realizar SNAT para acceder al exterior desde una red privada:

```
# iptables –t nat -I POSTROUTING –s [origen] -o [int_Salida] -j SNAT [--to-source DIR_IP]|[MASQUERADE]
```

Ejemplo:

```
# iptables –t nat –I POSTROUTING –s 192.168.2.0/24 –o eth0 –j SNAT --to-source 172.2.10.4
```

- -s: se indica la dirección IP o la red de origen.
- -o: se indica la interfaz de salida de la conexión.
- SNAT|MASQUERADE: Se usa SNAT si tenemos una IP pública estática. Si no es así usamos MASQUERADE.

Sintaxis: DNAT (PREROUTING)

Realizar DNAT para ofrecer servicios al exterior desde una red privada. Ejemplo de servidor web en 192.168.2.10:

```
# iptables –t nat -I PREROUTING –p tcp --dport 80 -i eth0 -j DNAT --to 192.168.2.10:80
```

- -s: se indica la dirección IP o la red de origen.
- -o: se indica la interfaz de salida de la conexión.
- SNAT|MASQUERADE: Se usa SNAT si tenemos una IP pública estática. Si no es así usamos MASQUERADE.

Sintaxis: Extensiones

Extienden la funcionalidad base.

Algunos ejemplos con protocolos udp y tcp:

- -d protoclo --sport N: se indica el número del puerto origen de la conexión.
- -d protocolo --dport N: se indica el número del puerto destino de la conexión.

Ejemplos con el protocolo icmp:

- [-d|-m] icmp --icmp-type echo-request: para indicar que se está realizando una petición de ping.
- [-d|-m] icmp --icmp-type echo-reply: para indicar que se está realizando una respuesta de ping.

Para el registro de paquetes:

- -j LOG --log-prefix “Texto”: incluye el texto como prefijo en el log de eventos.

Para control en la capa de “Acceso a red”:

- -m --mac-source Dir_MAC: Filtra por la dirección MAC origen.

Sintaxis: Extensiones

Limitar el número de conexiones simultáneas:

- `-m connlimit –connlimit-above X –j REJECT --reject-with tcp-reset`
- Si se supera el número de conexiones indicada mandaría un “reject”.

Establecer reglas para múltiples puertos:

- `-p tcp|udp –m multiport --sports 1024:65535 --dports 80,443`
- Habilita muchos puertos simultáneamente, mediante rangos o listas.

Limitar el uso horario de servicios:

- `-m time --timestart 10:00 --timestop 12:00 –j ACCEPT|DROP|REJECT`
- Se ejecuta la regla durante la hora establecida entre “timestart” y “timestop”.

Comprobar el estado de la conexión:

- `-m state --state NEW|STABLISHED`
- Permite el control de la conexión para saber si son conexiones nuevas o ya preestablecidas.

¡Gracias por vuestra atención!

JOSÉ ANTONIO SANTOS GÓMEZ