TEMA 1.3. Servicios de Red: Filtrado de paquetes y NAT

PROFESORES:

Rubén Santiago Montero
Eduardo Huedo Cuesta
Rafael Rodríguez Sánchez

Firewalls y Filtrado de Paquetes

- **Firewall**, componente de seguridad que analiza el tráfico de red y determina si debe permitir su paso. Funciones:
  - Filtrado de paquetes de red
  - Registro de actividad
  - Traducción de direcciones
- **Tipos de firewalls**:
  - En función del estado (*stateless*/*stateful*): Si consideran únicamente las características de los paquetes individuales o si además consideran el estado de la conexión
  - En función de la capa (de red o de aplicación): Si comprueban las cabeceras de los protocolos de red de los paquetes (IP, ICMP, TCP o UDP) o si también consideran sus datos que pertenecen a protocolos de aplicación (ej. HTTP)
- **Filtrado de paquetes** (Netfilter/`iptables`)
  - Permite manipular las reglas asociadas a cada tabla de firewall
  - Las tablas de firewall es una funcionalidad ofrecida por el núcleo del SO
  - Incluye un programa en el espacio de usuario para la gestión

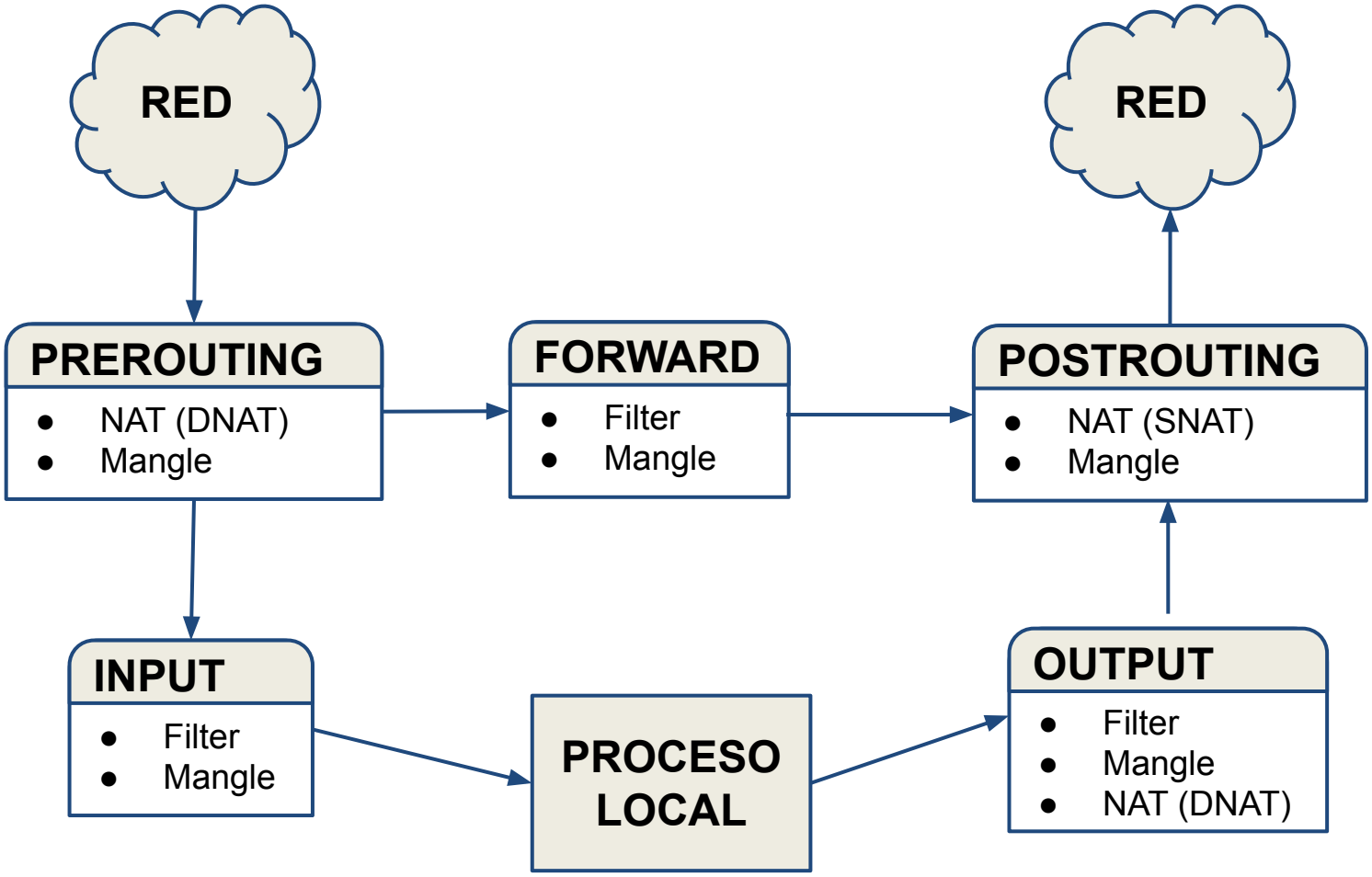
iptables: Tablas, cadenas y reglas

- **Reglas**: definen qué hacer (ej. descartar o aceptar) con un paquete que cumple unos determinados criterios (ej. puerto origen, dirección IP destino...)
- **Cadenas**: listas de reglas que se aplican en orden a los paquetes en un punto determinado de su procesamiento
  - Una regla puede mover un paquete a otra cadena
  - Todo paquete de entrada/salida del sistema atraviesa al menos una cadena
  - Si un paquete no encaja en ninguna de las reglas, se aplica la política de la cadena
- **Tablas**: conjuntos de cadenas destinados a diferentes tipos de procesamiento

iptables: Tablas y cadenas predefinidas

- **Tabla Filter**
  - Bloquea o permite el tránsito de un paquete
  - Todo paquete del sistema atraviesa esta tabla
    - Cadena INPUT: paquetes destinados al sistema
    - Cadena OUTPUT: paquetes generados en el sistema
    - Cadena FORWARD: paquetes que atraviesan el sistema (encaminados)
- **Tabla NAT**
  - Re-escribe las direcciones origen/destino y puertos de un paquete
    - Cadena PREROUTING: paquetes de entrada antes de la decisión de encaminamiento
      - Usada en DNAT (Destination NAT)
    - Cadena POSTROUTING: paquetes de salida después de la decisión de encaminamiento
      - Usada en SNAT (Source NAT)
    - Cadena OUTPUT: paquetes de salida generados localmente
- **Tabla Mangle**
  - Sirve para cambiar algunos campos de un paquete (ej. TOS o MSS)
  - Tiene las 5 cadenas anteriores

iptables: Tablas y cadenas predefinidas



Versión simplificada de cadenas y tablas

iptables: Definición de Reglas

- Las reglas se pueden definir según la información del paquete o el estado de la conexión
- Se debe indicar la cadena a la que se añade la regla
- Debe incluir un **objetivo** *(rule target)*

Opción/Ejemplo	Significado
-A INPUT -A OUTPUT -A FORWARD	Añade regla a cadena de entrada Añade regla a cadena de salida Añade regla a la cadena forward (sólo en caso de routers)
-s 192.168.1.1 -d 140.10.15.1	Filtrado por dirección IP origen Filtrado por dirección IP destino
-p tcp -p udp -p icmp	Filtrado de paquetes TCP Filtrado de paquetes UDP Filtrado de paquetes ICMP
--sport 3000 --dport 80 --icmp_type 8	Filtrado por nº de puerto origen (para TCP o UDP) Filtrado por nº de puerto destino (para TCP o UDP) Filtrado por tipo de mensaje (para ICMP)
-i eth0 -o eth1	Filtrado por interfaz de red de entrada Filtrado por interfaz de red de salida

iptables: Definición de Reglas

- Definición de reglas según el estado de la conexión:

Opción	Significado
-m state --state NEW	Filtrado de paquetes correspondientes a conexiones nuevas (el primer paquete)
-m state --state ESTABLISHED	Filtrado de paquetes correspondientes a conexiones ya establecidas
-m state --state RELATED	Filtrado de paquetes relacionados con otras conexiones existentes
-m state --state INVALID	Filtrado de paquetes que no pertenecen a ninguno de los estados anteriores

- Objetivo (target) de una regla (-j, jump)
  - DROP
  - ACCEPT
  - REJECT, como DROP pero envía un mensaje ICMP (--reject-with define el tipo, ej. connection-administratively-filtered, icmp-port-unreachable)
  - LOG

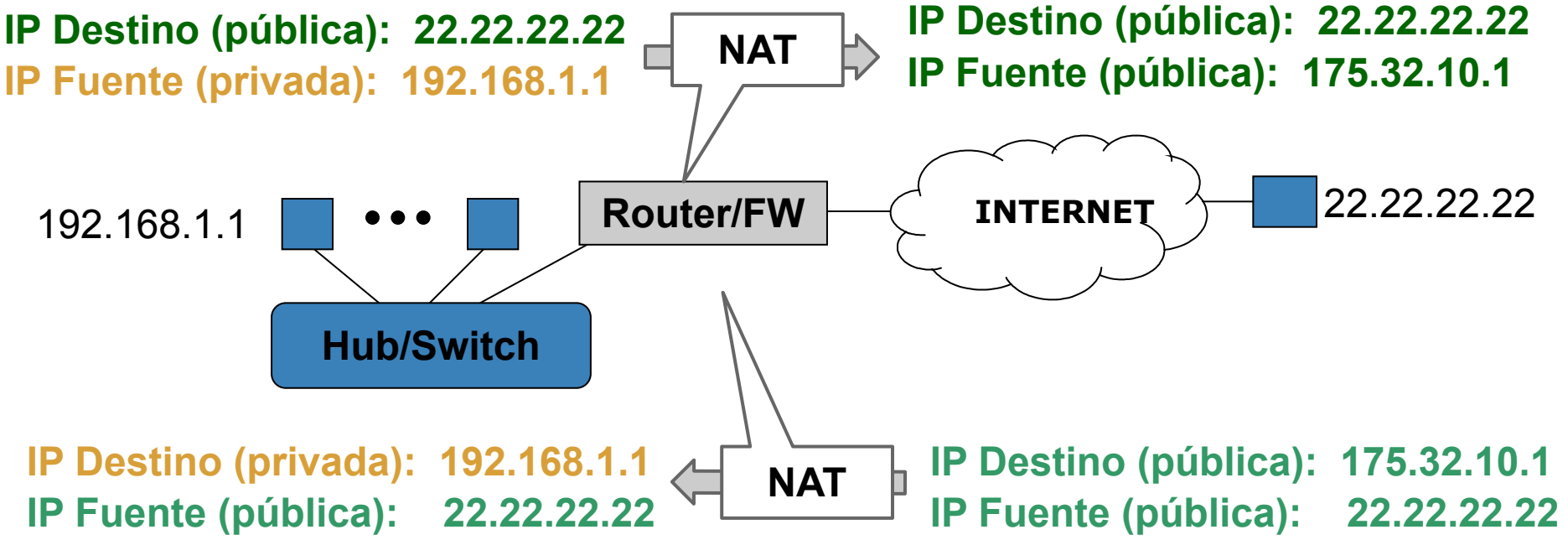
iptables: Ejemplos de Reglas

```
# Establecer política por defecto para cadenas INPUT, OUTPUT y FORWARD
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# Dejar entrar o salir cualquier paquete correspondiente a
# conexiones establecidas o relacionadas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Permitir conexiones entrantes SSH (tcp/22) desde pc-oficina
iptables -A INPUT -s 200.1.1.1 -p tcp --dport 22 -m state \
     --state NEW -j ACCEPT
# Permitir conexiones web salientes (tcp/80) a cualquier destino
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
# Permitir conexiones pop3 salientes (tcp/110) con servidor de correo
iptables -A OUTPUT -d 22.1.1.1 -p tcp --dport 110 -m state \
      --state NEW -j ACCEPT
# Permitir conexiones DNS salientes (udp/53) con servidor DNS
iptables -A OUTPUT -d 22.1.1.2 -p udp --dport 53 -m state \
      --state NEW -j ACCEPT
```

NAT: Network Address Translation

Redes Privadas IPv4

- Permite aliviar el problema del número limitado de direcciones IPv4
- El objetivo es dar acceso a Internet a máquinas en redes privadas



NAT: Traducción Estática

- Asignación de N direcciones privadas a N direcciones públicas
- Asignación fija
- Ejemplo de tabla de traducción estática para N=7

IP Privada	**IP Pública**
192.168.1.3	147.96.80.132
192.168.1.23	147.96.80.12
192.168.1.2	147.96.80.122
192.168.1.5	147.96.81.2
192.168.1.4	147.96.81.23
192.168.1.7	147.96.81.77
192.168.1.56	147.96.81.4

NAT: Traducción Dinámica

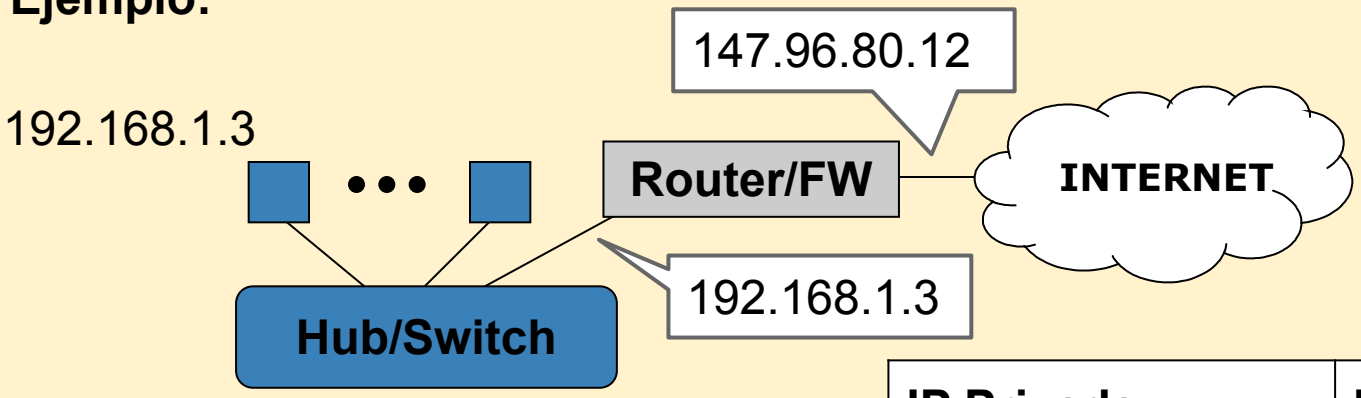
- Asignación de N direcciones privadas a M direcciones públicas (M < N)
- Asignación dinámica, sólo pueden acceder a Internet M máquinas a la vez
- Ejemplo de tabla de traducción dinámica para N=7, M=3

IP Privada	**IP Pública**
192.168.1.3	147.96.80.132
192.168.1.23	147.96.80.12
192.168.1.2	147.96.80.122
192.168.1.5	Sin posibilidad de acceso a Internet hasta que se libere una IP pública
192.168.1.4	
192.168.1.7	
192.168.1.56	

NAT: NAPT - Masquerading

- NAPT (Network Address and Port Translation)
- Asignación de N direcciones privadas a **1 dirección pública**
- **Funcionamiento:**
  - La única dirección IP pública disponible es la dirección IP pública del Router
  - El nº de puerto origen del cliente se traduce a un puerto libre del Router

Ejemplo:



IP Privada	IP Pública
192.168.1.3:3453	**147.96.80.12**:6782
192.168.1.7:2380	147.96.80.12:3342
192.168.1.5:6790	147.96.80.12:4390

NAT: NAPT - Masquerading

- El objetivo SNAT de la tabla NAT permite cambiar la dirección origen
- Se aplica a la cadena POSTROUTING
- El resultado se aplica a todos los paquetes posteriores de la conexión
- Permite implementar NAPT con dirección IP pública fija

```
iptables -t nat -A POSTROUTING -o ppp0 -j SNAT --to 175.20.12.1
```

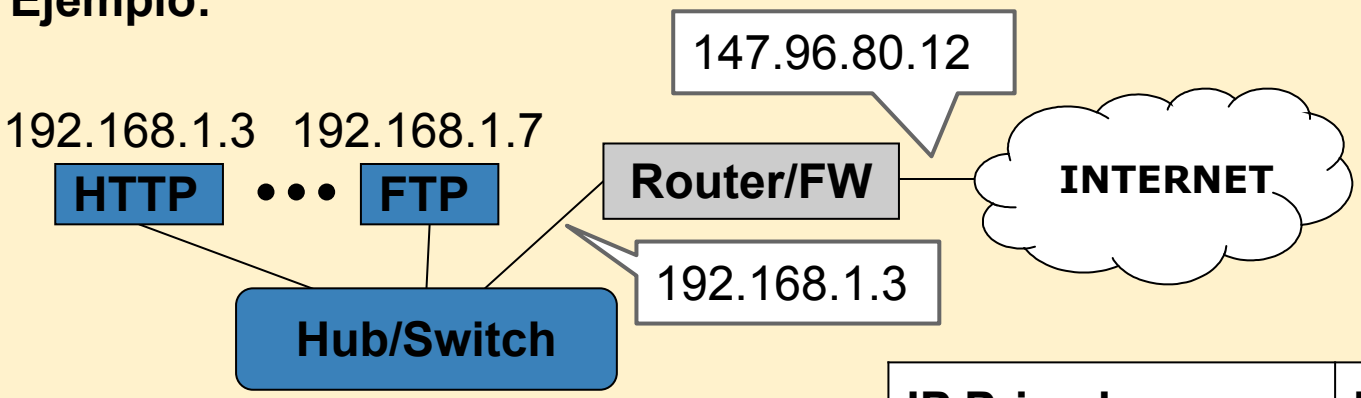
- El objetivo MASQUERADE de la tabla NAT permite usar una dirección IP pública dinámica
  - Usa la dirección IP del interfaz como dirección IP origen, que puede cambiar de una conexión a otra, al ser dinámica
  - Además, mantiene pista de las conexiones activas para aplicar también el cambio

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

NAT: Port Forwarding - Virtual Servers

- Asignación de **1 dirección pública** a N direcciones privadas
- Permite tener servidores en la red privada “visibles” desde Internet
- **Funcionamiento:**
  - Desde Internet, todos los servidores usan la dirección IP pública del Router
  - El Router traduce y reenvía los paquetes al servidor real de la red interna

Ejemplo:



IP Privada	IP Pública
192.168.1.3:8080	**147.96.80.12**:80
192.168.1.7:20	147.96.80.12:20
192.168.1.7:21	147.96.80.12:21

NAT: Port Forwarding - Virtual Servers

- El objetivo DNAT de la tabla NAT permite modificar la dirección de destino de un paquete y, opcionalmente, el puerto
- Se aplica a las cadenas OUTPUT y PREROUTING
- El resultado se aplica a todos los paquetes posteriores de la conexión
- **Ejemplo:**

```
iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 80 \
          -j DNAT --to 192.168.1.1:8080

iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 25 \
          -j DNAT --to 192.168.1.2

iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 20 \
          -j DNAT --to 192.168.1.7

iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 21 \
          -j DNAT --to 192.168.1.7
```