NAT - Firewalls

Redes de Ordenadores para Robots y Máquinas Inteligentes

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Febrero de 2024

Contenidos

Introducción

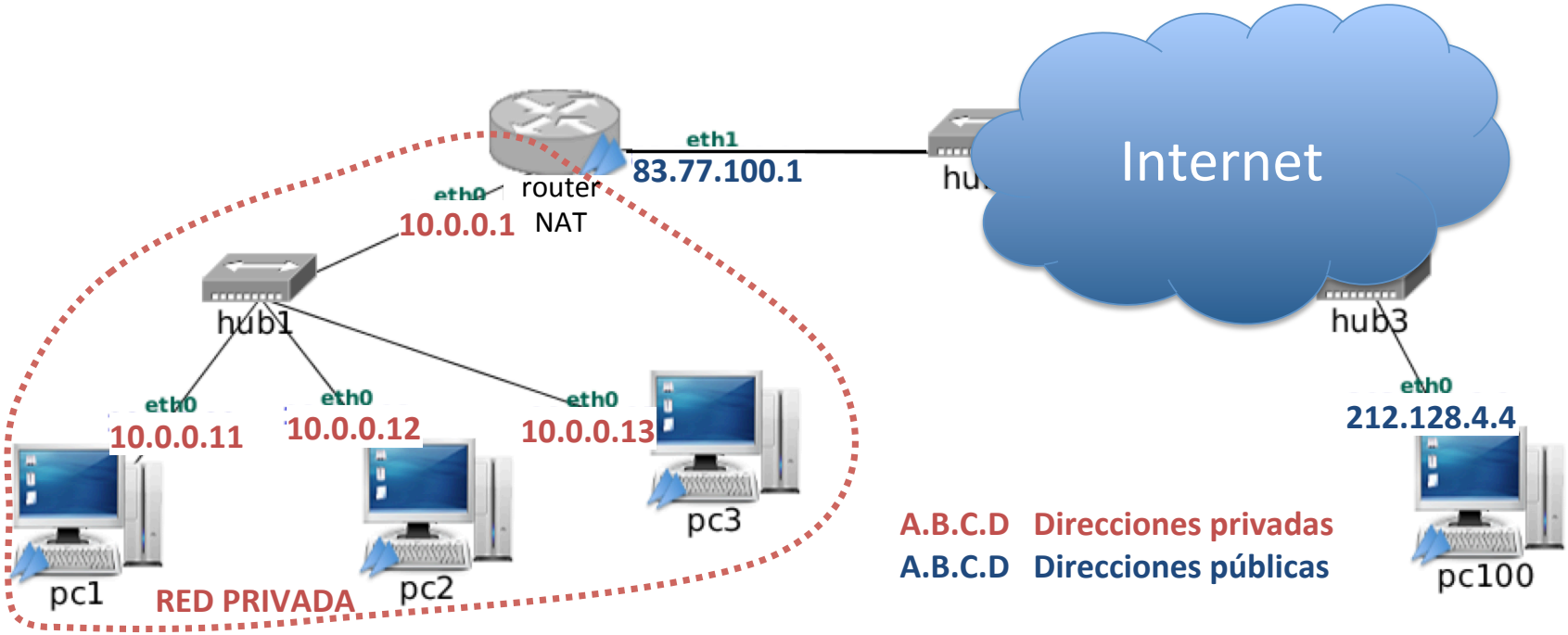
- Una máquina conectada a una red TCP/IP debe tener configurada una dirección IP que la identifica.
- En los años 90, debido a la escasez de direcciones IPv4 se diseñó un mecanismo para que un conjunto de máquinas pudieran compartir una misma dirección IP:
  - Dentro de una organización las máquinas usan direccionamiento privado para comunicarse entre ellas.
  - Para comunicaciones con otras máquinas externas a la organización, todas las máquinas utilizan una única dirección IP pública para comunicarse con el exterior.
  - Existe un dispositivo que debe realizar la traducción de direcciones entre el rango privado y la dirección IP pública cada vez que un paquete IP sale/entra de/en la organización.

Contenidos

NAT (*Network Address Translation*)

- Se denomina NAT a la reescritura por parte de un *router* de algunos campos de la cabecera de los paquetes que encamina:
  - cambia dirección IP origen y puerto origen en el tráfico saliente
  - cambia dirección IP destino y puerto destino en el tráfico entrante
- Esta técnica se desarrolla con el propósito principal de paliar la escasez de direcciones IP: Gracias al NAT, una organización puede usar direcciones privadas internamente, y tener una sola dirección IP global (pública) en el *router* que le da acceso a Internet (RFC 2663).
- Pero la técnica ha tenido también el objetivo secundario de la seguridad: Un *router* NAT es (también) un *firewall* básico.
- Direcciones IP para redes «privadas»:
  - De `10.0.0.0` a `10.255.255.255`: 1 red de clase A
  - De `172.16.0.0` a `172.31.255.255`: 16 redes de clase B
  - De `192.168.0.0` a `192.168.255.255`: 256 redes de clase clase C

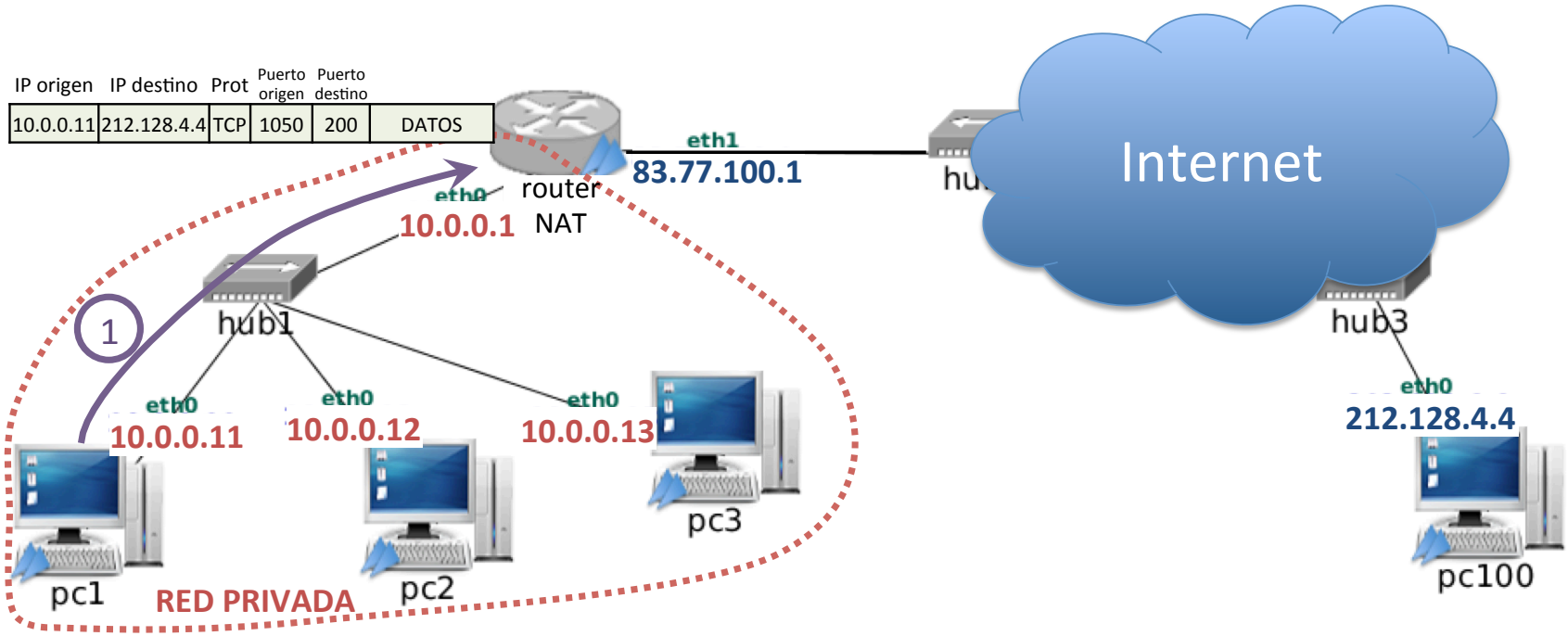
Direccionamiento



- Todos los ordenadores de la red interna utilizan direcciones «privadas», que no son válidas en Internet.
- El router que da acceso a Internet tiene una dirección «pública», válida en Internet.
  - En algunos casos, el router podría disponer de más de una IP pública. Siempre que haya disponibles menos IPs públicas que máquinas en la red interna habrá que utilizar NAT.

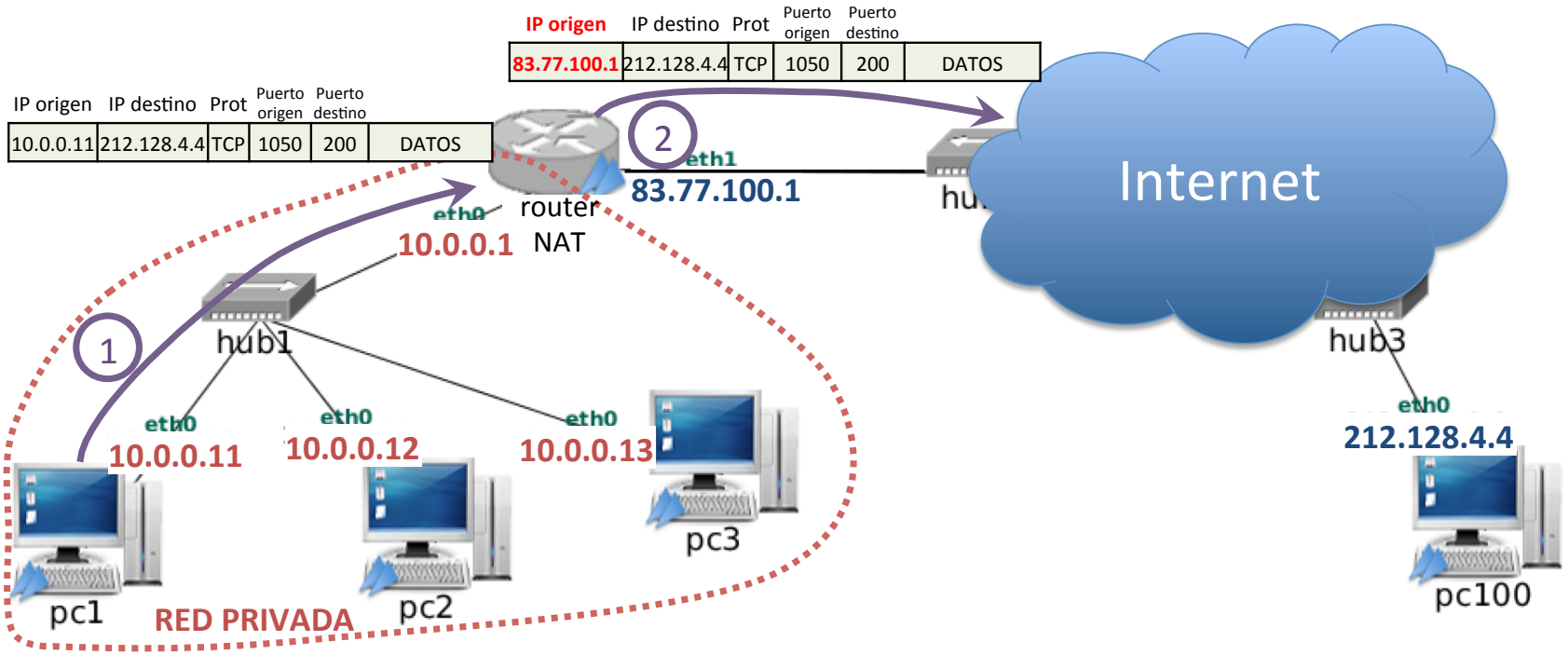
Contenidos

Tráfico saliente, mecanismo básico (1/3)



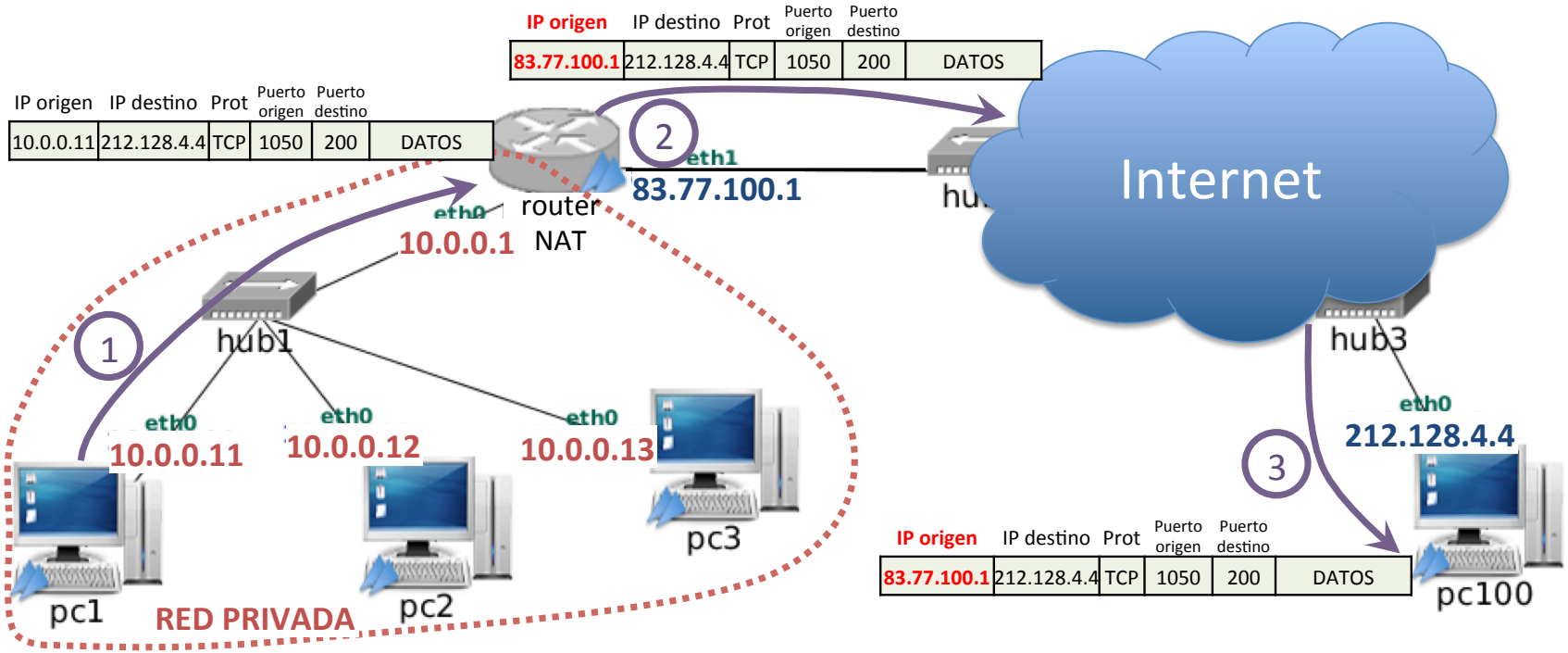
- La máquina pc1 envía un datagrama IP dirigido a pc100
- pc1 usa como IP origen su dirección IP privada, que no es válida en Internet (pues los *routers* de Internet no tienen rutas hacia esas direcciones).

Tráfico saliente, mecanismo básico (2/3)



- El router NAT cambia la **IP de origen** sustituyendo la IP privada de la máquina que creó el datagrama (10.0.0.11) por la IP pública del router (83.77.100.1).
- El seguimiento de conexiones del router NAT tendrá en cuenta el cambio para hacerlo a la inversa en el tráfico de respuesta.

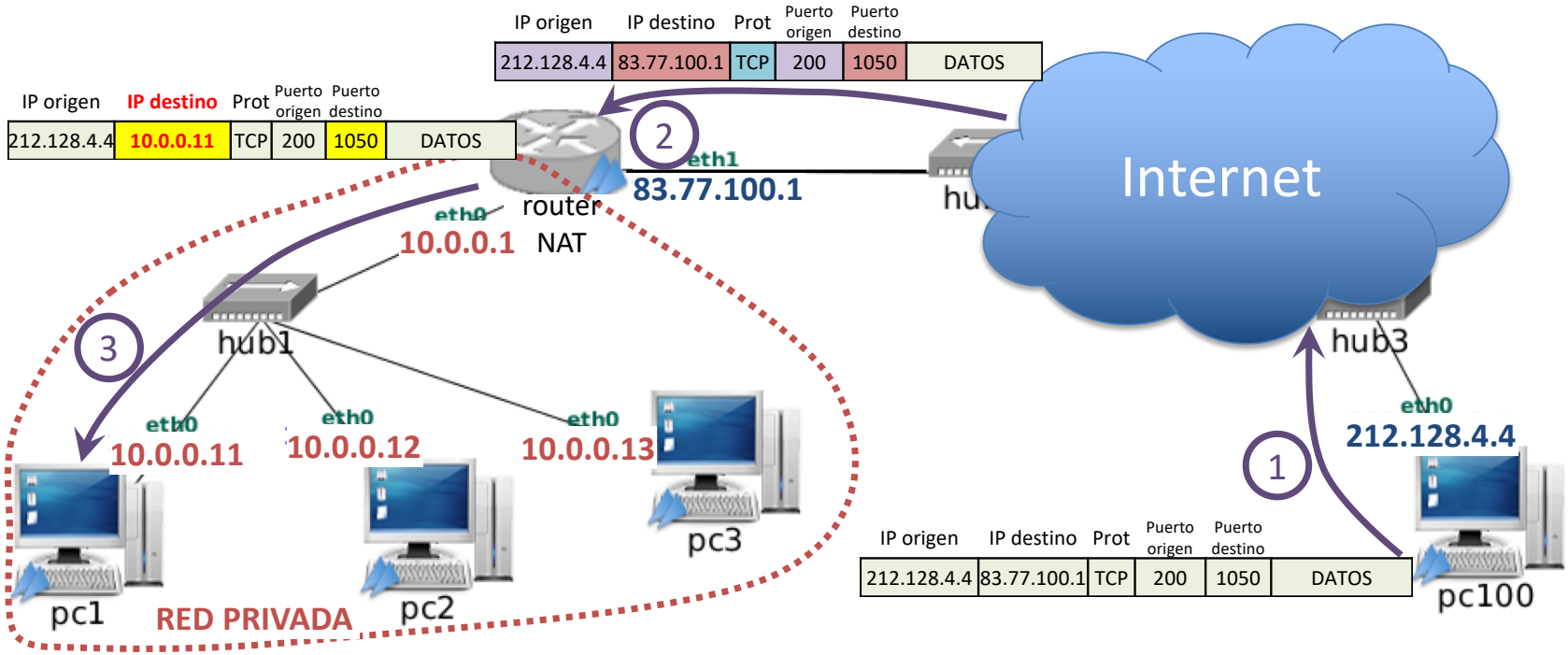
Tráfico saliente, mecanismo básico (3/3)



- La máquina que recibe el datagrama cree que el origen del mismo es el propio router NAT.

Contenidos

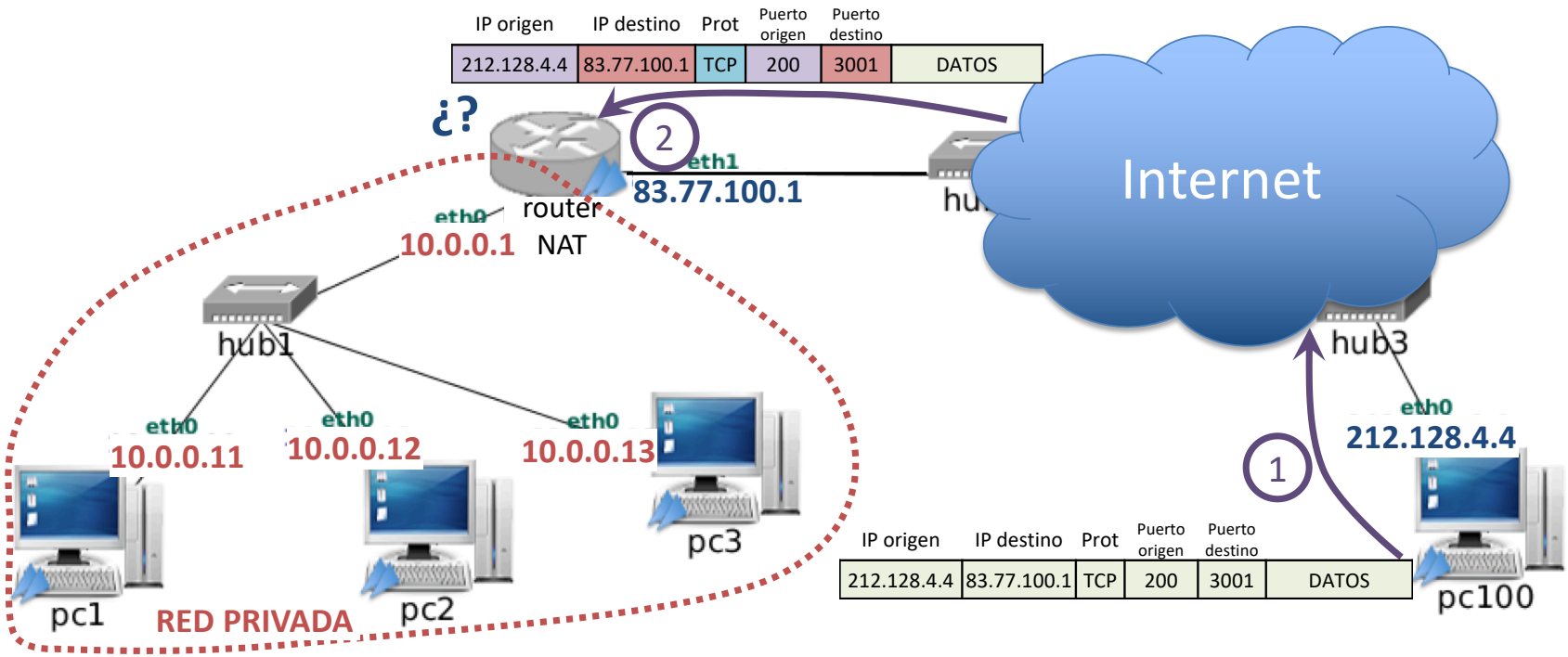
Tráfico entrante que responde al saliente



- El router NAT reenvía a la red privada el datagrama cambiando los campos de destino que ha recibido (dirección IP y puerto del router NAT `IP=83.77.100.1, puerto=1050`) por los que extrae del seguimiento de conexiones.

Contenidos

El problema del tráfico entrante nuevo



- Cuando llega al router NAT el datagrama, el router NAT no tiene forma de saber a qué máquina interna redirigirlo, pues no el seguimiento de conexiones no reconoce a dicho tráfico
- En este caso la configuración por defecto de un router NAT es descartar el datagrama recibido (*firewall*)

Tráfico entrante nuevo: abrir puertos

- **Solución**: En la configuración del router NAT se añade **a priori** una regla de traducción de direcciones para el tráfico entrante, reenviándolo a una máquina interna concreta.
- Para elegir a qué máquina concreta se reenvía se utiliza como criterio el **puerto de destino** del tráfico entrante: según el puerto de destino del paquete que llega al router, se decide a qué máquina interna se reenvía, cambiando la IP de destino. También podría cambiarse el puerto de destino para usar otro en la máquina interna.
- Esta solución se conoce informalmente como **"abrir puertos"** en el router NAT.
- Si en la red privada hubiera otro servidor que utilizara el mismo puerto, sería necesario que las reglas de traducción usaran puertos de destino diferentes para distinguir el tráfico para cada servidor.
- Nótese que desde los clientes de Internet las comunicaciones necesariamente se realizan dirigidas a la IP pública del router y al puerto de destino abierto.
- Las reglas de apertura de puertos pueden configurarse "a mano" en el router NAT, o bien utilizar un protocolo como **UPnP** (*Universal Plug and Play*) para que los puertos se abran automáticamente en el router bajo demanda de las máquinas internas.

Contenidos

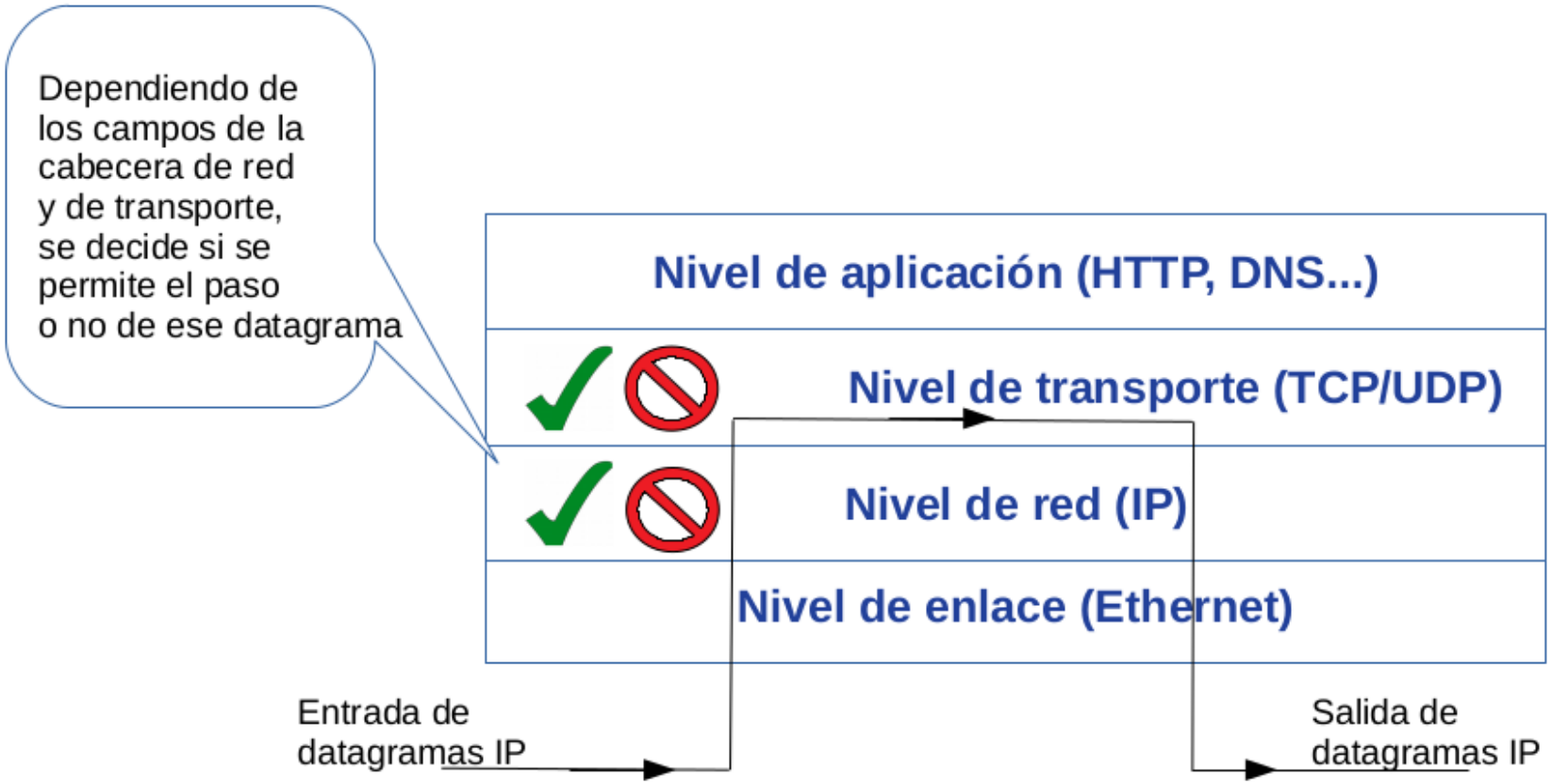
Firewall o cortafuegos

- Se denomina **red frontera** es la parte de la red que comunica la red interna de una organización con otras redes externas.
- La seguridad en la red frontera es clave para proteger los equipos y servicios de la organización de ataques externos. Para ello, las organizaciones instalan **firewalls** que permiten filtrar el tráfico y detectar posibles ataques maliciosos desde el exterior. Adicionalmente los *firewalls* permiten restringir el tráfico que sale de los equipos internos de la organización.
  - Un *firewall* necesita inspeccionar los campos de las cabeceras de los paquetes. Sólo el tráfico que cumple una serie de condiciones atraviesa el *firewall*.
- Existen otro tipo de firewalls, *Personal firewalls*, que se instalan en la máquina final del usuario y que controlan el acceso a los servicios y trafico dirigido a esa máquina exclusivamente.

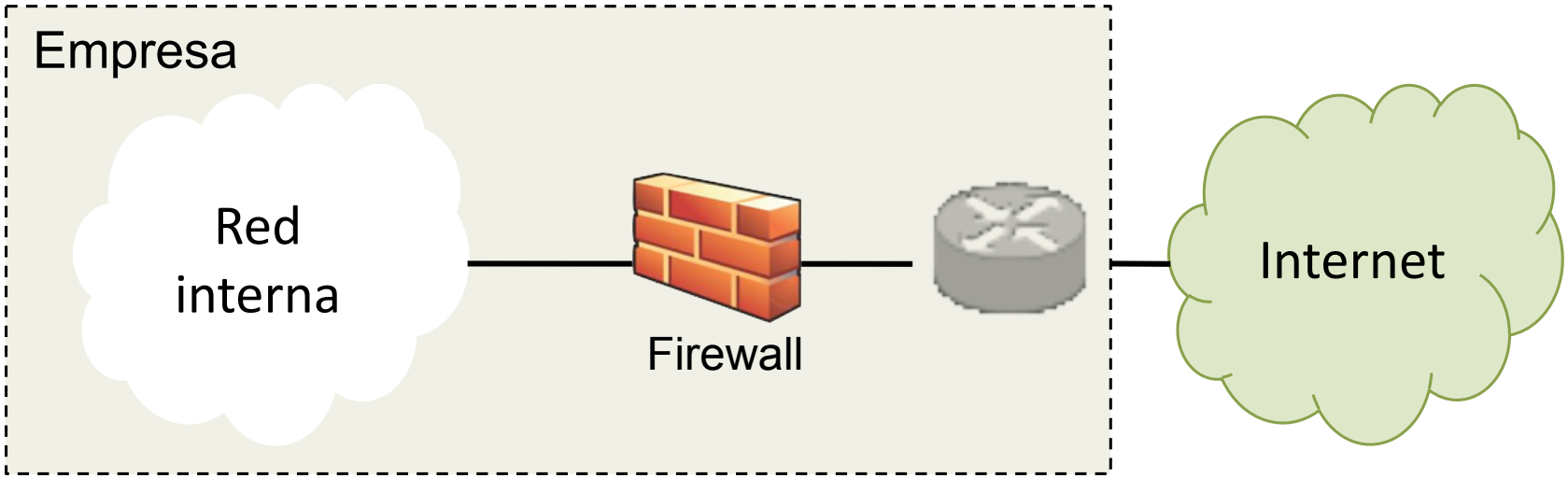
Funcionalidad de un firewall

- Función básica: Filtrado de tráfico.
- Además se han ido incorporando otras funcionalidades:
  - NAT
  - Sistema de detección de intrusos (IDS): notifican si hay tráfico que ha sido registrado previamente como tráfico malicioso.
  - Servidor de VPN (Virtual Private Network): servicio para permitir conexión segura desde usuarios o sedes remotas con una determinada organización a través de una red no fiable.

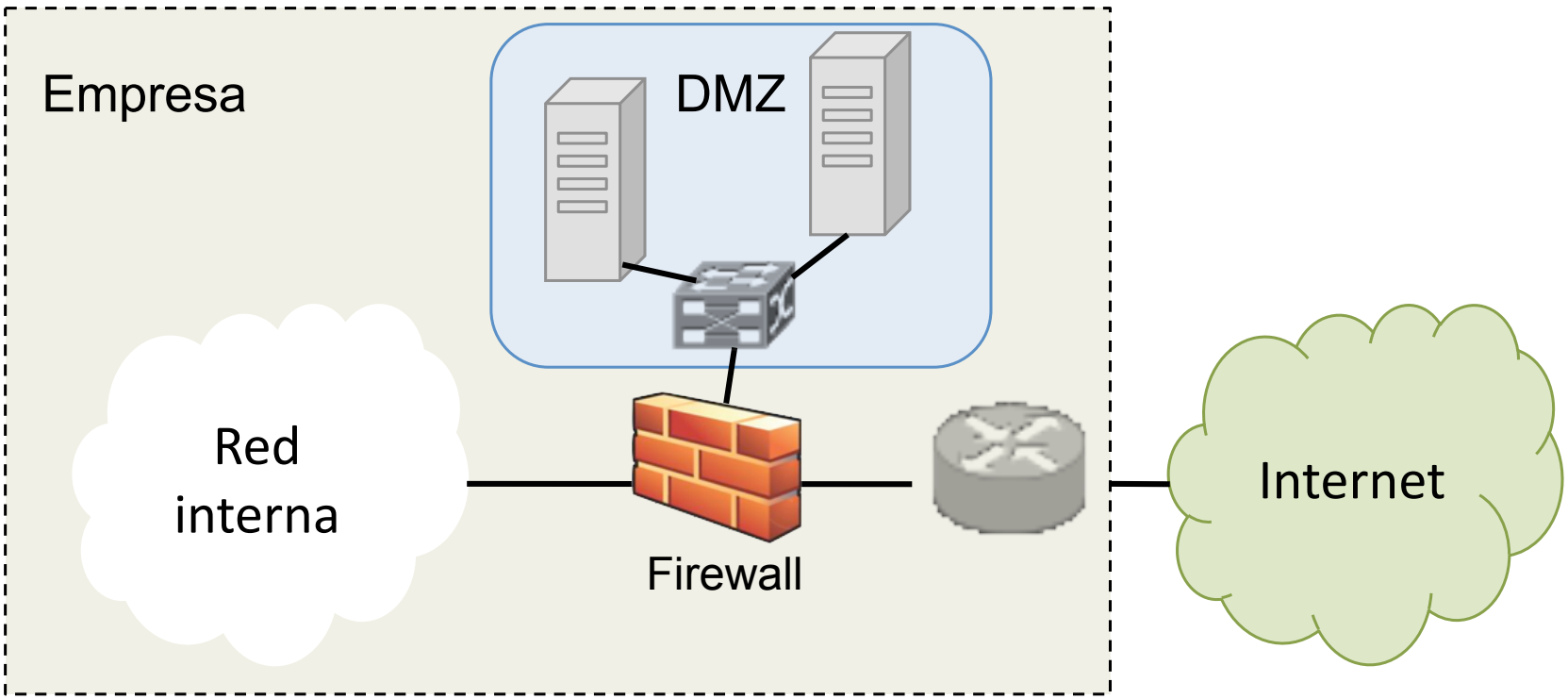
Filtrado en un firewall



Un único firewall



Un único firewall con zona DMZ



DMZ: DeMilitarized Zone. Es una zona de la red de la organización en la que se colocan los servicios públicos de la empresa a los que puede acceder cualquier cliente desde Internet. A diferencia del resto de equipos de la red interna la empresa, a los que en general no se podrá acceder desde Internet.

Dos firewalls