

Network Address Translation (NAT)

Álvaro González Sotillo

22 de marzo de 2018

Índice

1. Introducción	1
2. Enrutamiento	1
3. NAT	3
4. Ventajas de NAT	6
5. Redirección permanente de puertos	6
6. Ejemplo NAT: ICS de Windows	7
7. DMZ	8
8. Referencias	10

1. Introducción

- En un enrutamiento normal IP los paquetes siempre conservan su IP origen y destino, aunque pasen por diferentes routers
 - ¿Qué pasaría si un *router* cambiase la dirección IP de origen por la suya propia?
 - El destino de la comunicación pensaría que el origen de la misma es ese *router*
 - La información de vuelta se enviaría al *router*, no al origen real
 - ¿Esto es deseable? ¿Esto es útil?

2. Enrutamiento

En un enrutamiento normal IP los paquetes siempre conservan su IP origen y destino, aunque pasen por diferentes routers

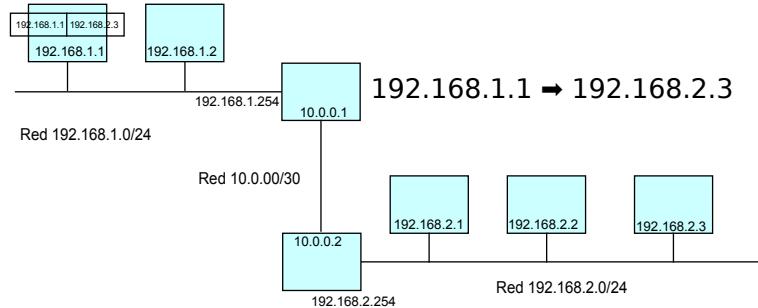


Figura 1: Se envía un paquete a otra red

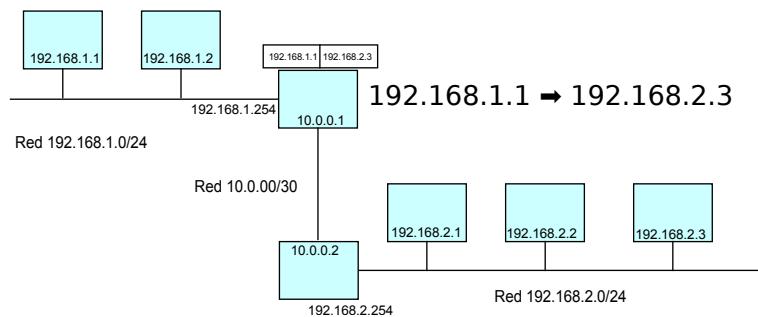


Figura 2: El paquete pasa por el *router* local

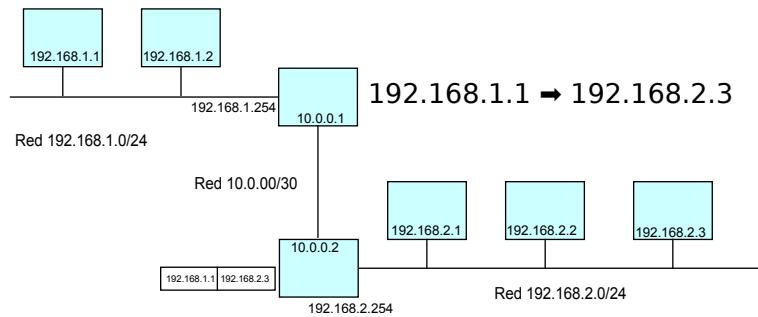


Figura 3: El *router* local lo envía al siguiente *router*

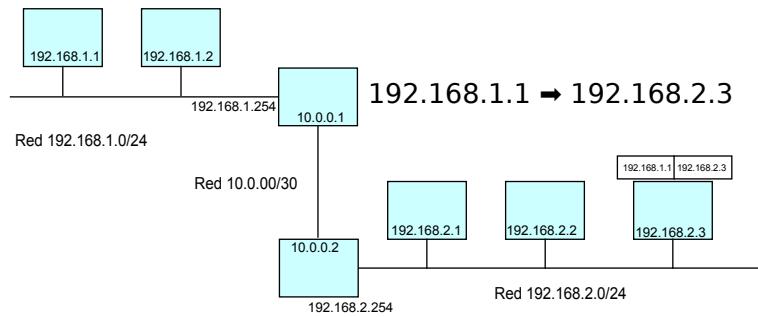


Figura 4: El *router* de la red remota lo envía al destino

3. NAT

- NATP cambia la dirección IP de origen
 - El origen está en una red privada interna
 - La reemplaza por la IP externa del *router*
 - También puede cambiar el puerto de origen
- Deja anotados estos cambios en una tabla de correspondencias
 - Al recibir un paquete de respuesta, deshace el cambio antes de enrutar

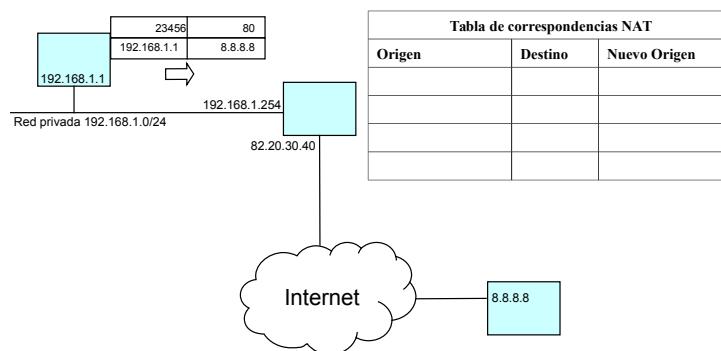


Figura 5: Se envía un paquete de la red interna a Internet

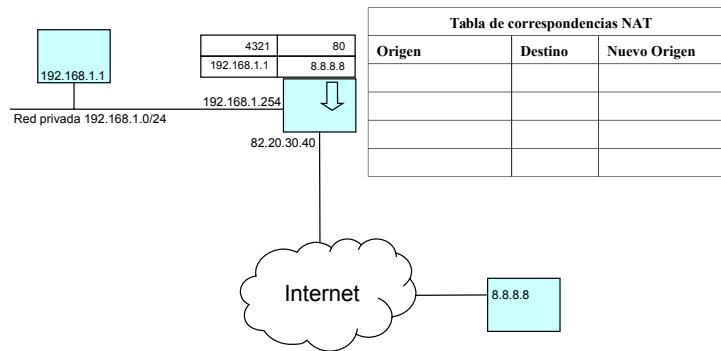


Figura 6: El *router* recibe el paquete

- ¿Podría 8.8.8.8 comenzar una comunicación con 192.168.1.1?
 - el *router* no tendría en su tabla NAT una correspondencia para hacer la traducción
 - Solo las comunicaciones internas añaden entradas a la tabla NAT de correspondencias
 - 8.8.8.8 ni siquiera sabe que 192.168.1.1 existe
- ¿Cuántas direcciones IP públicas (de pago) necesito utilizar?
 - Solo una, la del *router*, ya que el resto de ordenadores tendrán una IP privada que será traducida por la tabla NAT

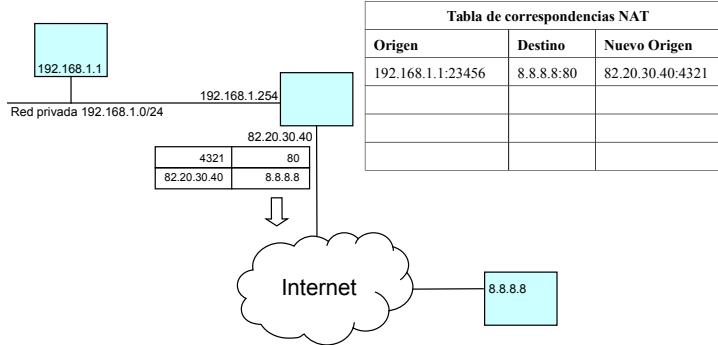


Figura 7: Lo envía sustituyendo la dirección IP de origen por la IP pública

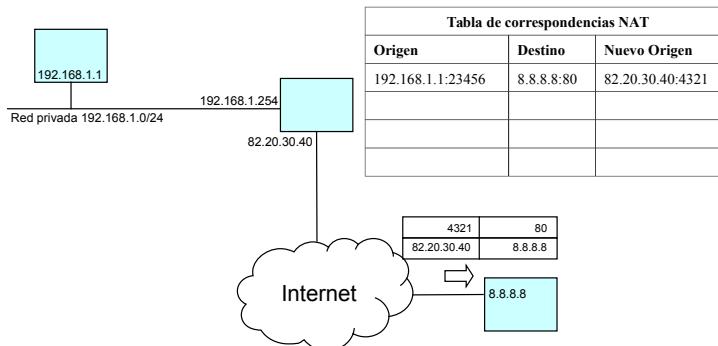


Figura 8: El paquete llega a su destino en Internet

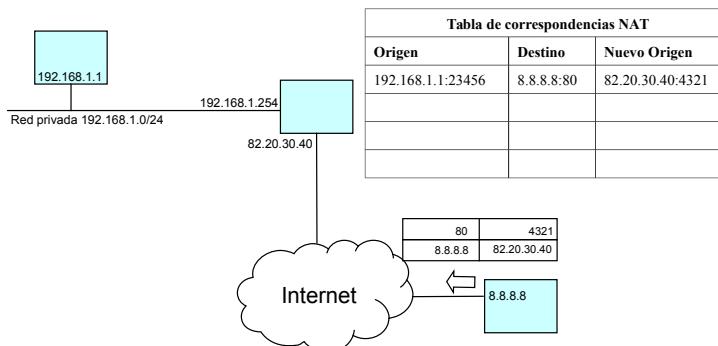


Figura 9: El servidor de Internet responde al origen del paquete

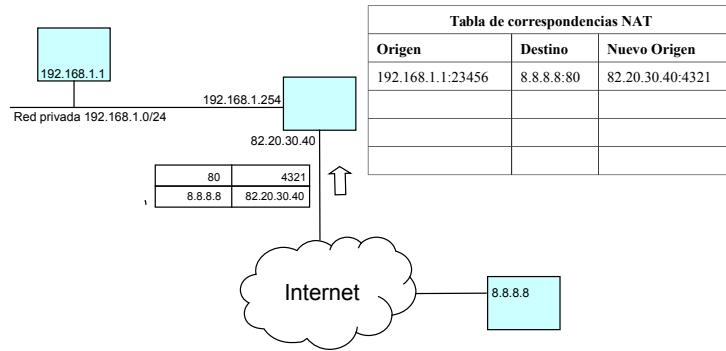


Figura 10: El paquete llega a la IP pública del *router*

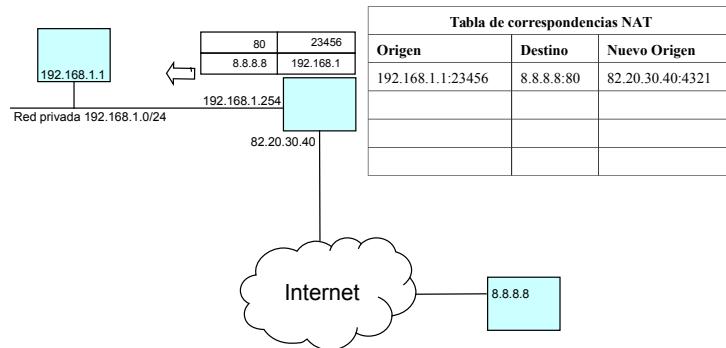


Figura 11: El *router* sabe que él no es el destino final, y deshace el cambio de direcciones

4. Ventajas de NAT

- El NAT crea un *firewall* automático y casi imposible de saltar
 - Los equipos externos no pueden iniciar comunicaciones, sólo los internos
 - Los equipos internos ni siquiera existen en Internet
- El NAT permite compartir una sola IP pública entre muchos ordenadores
 - Ahorro en direcciones IP públicas

5. Redirección permanente de puertos

- Puede ser interesante que haya entradas NAT permanentes en la tabla de correspondencias
 - Un servidor web en nuestra red local debería recibir todo el tráfico que tenga como destino la IP del router y el puerto 80
 - Programas P2P pueden funcionar mejor redireccionando directamente el tráfico al programa, para que otros *peers* puedan encontrarnos
- El puerto interno expuesto no tiene por qué coincidir con el externo

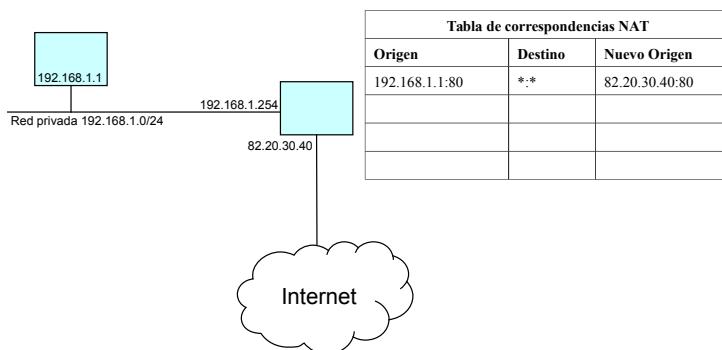


Figura 12: Servidor Web en 192.168.1.1 expuesto a Internet

5.1. ¿Qué puertos exponer?

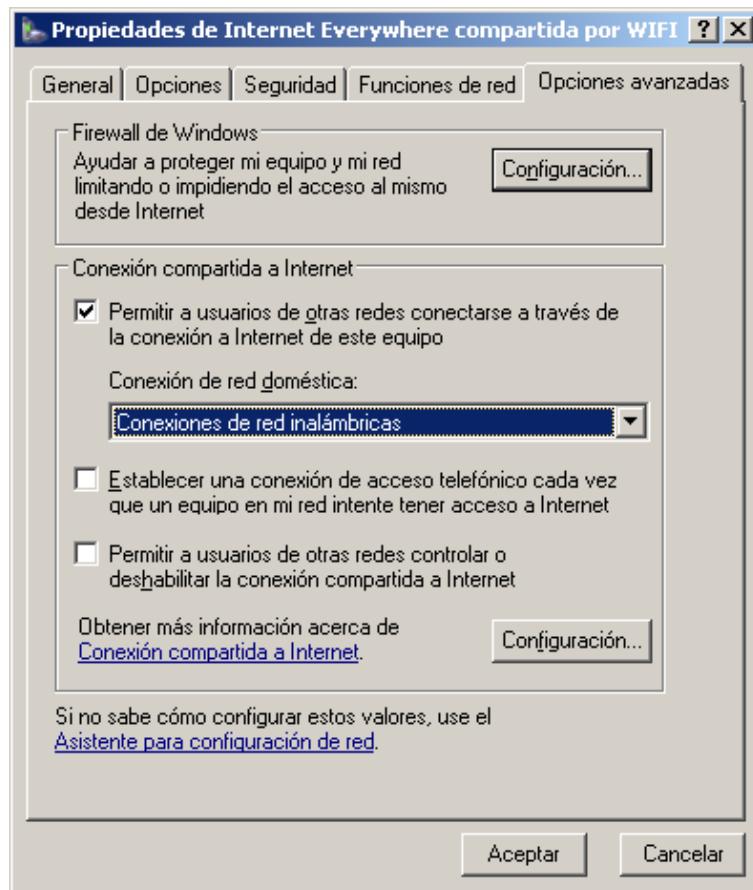
- Cada protocolo tiene un puerto asignado (aunque algunos pueden cambiarse)
- Hay que referirse a la documentación de cada servicio (o a [/etc/services](#))

Protocolo	Puerto(s)
Continúa en la siguiente página	

Continúa de la página anterior	
Protocolo	Puerto(s)
SSH	22
HTTP	80
HTTPS	443
SMTP	25
POP3	110
IMAP	143
FTP	20, 21
VNC	5900
RDP	3389
DNS	53

6. Ejemplo NAT: ICS de Windows

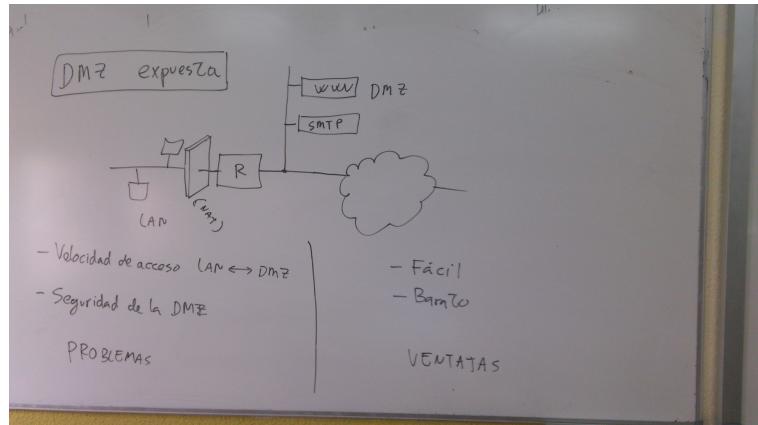
- *Internet Connection Sharing* permite compartir una conexión Internet entre muchos ordenadores
- Un equipo tiene una conexión a Internet (por ejemplo, LAN), y la comparte mediante una conexión (por ejemplo, Wifi)
- Habilita el enrutamiento, y en la conexión Wifi instala
 - Un servidor DHCP
 - Un servidor NAT
 - Un servidor DNS



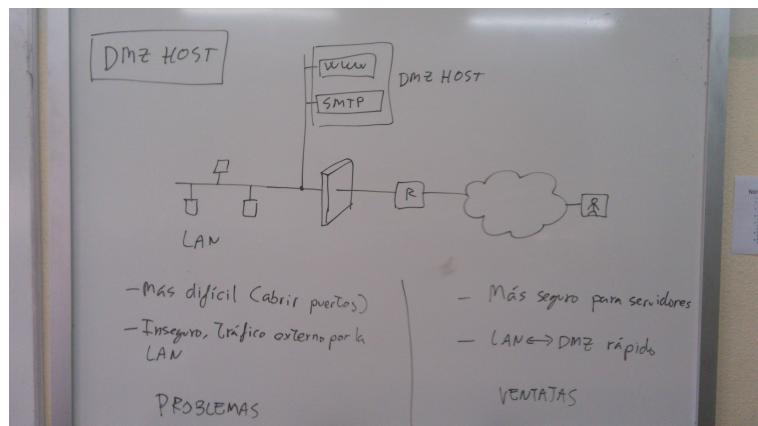
7. DMZ

- La *zona desmilitarizada* la componen los hosts que una empresa expone a Internet
- Puede configurarse de varias maneras

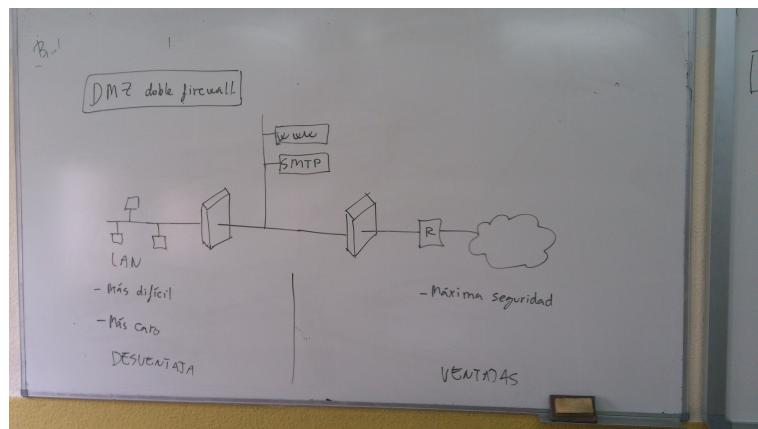
7.1. DMZ expuesta



7.2. DMZ Host



7.3. DMZ doble firewall



8. Referencias

- Formatos:

- [Transparencias](#)
- [PDF](#)

- Creado con:

- [Emacs](#)
- [org-reveal](#)
- [Latex](#)