Práctica 2 – Servicios básicos de red II: NAT

1. Introducción

Network Address Translation (NAT), o traducción de dirección de red en castellano, es un servicio que permite usar en una red un conjunto de direcciones IP para las comunicaciones internas y otro conjunto de direcciones IP distinto para las comunicaciones externas. Para ello, en toda red que use NAT, debe haber una pasarela (*gateway*) o enrutador (*router*) NAT encargada de reescribir ("traducir") en la cabecera IP la dirección IP origen en los paquetes salientes y la dirección IP destino en los paquetes entrantes. La pasarela NAT utiliza una tabla de traducción NAT para mapear las direcciones IP internas en direcciones IP externas.

Este mapeo puede ser estático o dinámico. En el mapeo **estático** se define explícitamente la correspondencia uno a uno entre el conjunto (*pool* en inglés) de direcciones IP internas y el conjunto de direcciones IP externas, mientras que en el mapeo **dinámico** se define algún criterio para establecer esta correspondencia según las condiciones de la red. Así, por ejemplo, para el último caso, se podría asignar una de las direcciones IP externas disponibles (que no estén actualmente en uso por alguno de los equipos de la red) de forma aleatoria a un dispositivo de la red que inicie un periodo de actividad (genere tráfico). Del mismo modo, se podrían liberar direcciones IP de aquellos dispositivos que tengan una de ellas asignada actualmente y que hayan estado inactivos durante un cierto periodo de tiempo.

Una de las principales motivaciones de usar NAT es paliar el problema de la falta de direcciones IP *version* 4. Por ejemplo, un conjunto de direcciones IP públicas puede compartirse con una relación 1:N (hay más interfaces IP en la red privada que direcciones públicas disponibles) usando un criterio de asignación dinámica de IP públicas como en el ejemplo descrito anteriormente. Sin embargo, en estos escenarios una misma dirección IP pública sólo puede ser usada por uno de los equipos de la red privada en un instante dado. Este problema se solventa con *Network Address Port Translation* (NAPT). NAPT va un paso más allá de NAT para soportar la traducción de identificadores de transporte tales como los puertos TCP/UDP y los identificadores de consulta ICMP. Esto le permite a un conjunto de estaciones finales compartir una misma dirección IP externa simultáneamente. Para tal fin, los identificadores de transporte de un conjunto de estaciones de la red NAT (puertos) se multiplexan en los identificadores de transporte (puertos) de una única dirección IP externa (véase la Figura 1).

En el caso de NAPT, la tabla de traducción o mapeo NAT establece una correspondencia uno a uno entre los pares *<IP interna, puerto interno>* y los pares *<IP externa, puerto externo>* (véase la Figura 1).

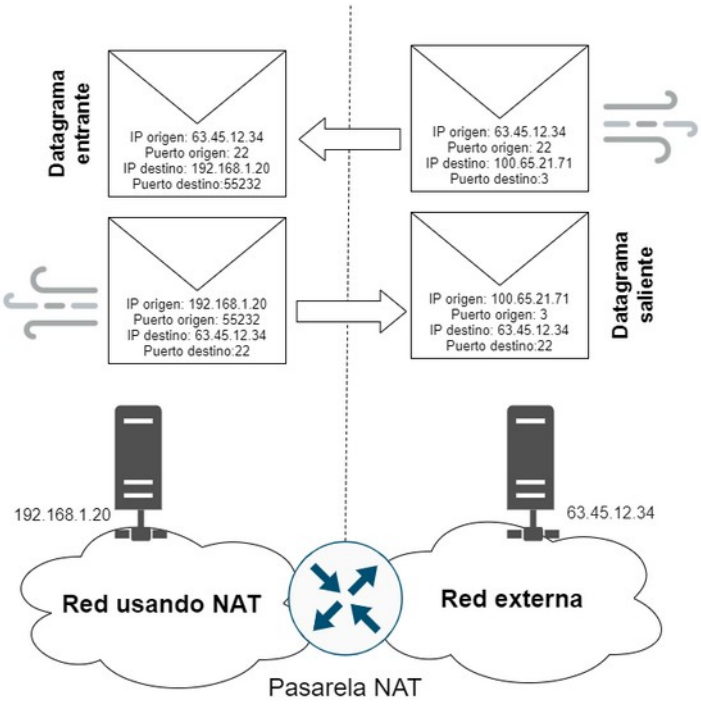

Tabla de mapeo NAT

Dirección IP local	Puerto local	Dirección IP externa	Puerto externo
192.168.1.10	55232	100.65.21.71	1
192.168.1.20	62301	100.65.21.71	2
192.168.1.20	55232	100.65.21.71	3
192.168.1.20	7888	100.65.21.71	4

Figura 1: Operación de la funcionalidad NAT.

Considerando el origen de la comunicación, podemos diferenciar dos tipos de NAT:

***Source* NAT (*srcnat*)**: Este tipo de NAT aplica a las comunicaciones originadas dentro de la propia red NAT. El *router*NAT reemplaza la dirección IP origen de los paquetes salientes originados en la red NAT. Posteriormente realizará la operación inversa para los paquetes entrantes.

***Destination* NAT (*dstnat*)**: Este tipo de NAT aplica a las comunicaciones originadas en redes externas y que van destinadas a la red NAT. En este caso, el *router* NAT deberá realizar primero una traducción de la dirección IP destino de los paquetes entrantes. Posteriormente realizará la operación inversa para los paquetes salientes.

Observe que en *srcnat* la pasarela NAT puede identificar perfectamente quienes son los equipos finales de la comunicación a partir de la información que contiene el primer paquete IP de dicha comunicación, mientras que esto no es posible en *dstnat*.

Es decir, la pasarela NAT no tendrá forma de saber cuál es el equipo de la red NAT al que va dirigido el primer paquete de una comunicación entrante (originada en una red externa) si se basa exclusivamente en la información contenida en dicho paquete. Este hecho junto a la protección requerida para mitigar las vulnerabilidades creadas por permitir las comunicaciones entrantes a la red NAT hacen que las configuraciones en los *routers* NAT asociadas a *dstnat* sean en general más complejas.

1.1 Información básica para la realización de la práctica

En esta sección se ofrece información básica y las referencias necesarias para llevar a cabo las tareas que se proponen en la práctica.

1.1.1 Acceso al puesto de usuario y elección de sistema operativo

Para la realización de esta práctica, es necesario formar grupos de tres. Después, arrancar su puesto de usuario con la opción "Redes"→"Ubuntu 20.04".

Una vez que se haya identificado como "**operador**"/"**finisterre**", puede pasar a modo *superusuario* mediante el siguiente comando, y utilizando la contraseña "**finisterre**"

```
$ sudo  su
```

1.1.2 Escenario de trabajo y dispositivos implicados

En las Figuras 2 y 3 se observan los diferentes escenarios de trabajo para efectuar SRC-NAT o DST-NAT, respectivamente. El direccionamiento IP de los elementos que aparecen en las figuras, se corresponde con aquellas direcciones que se encontrarían en la isla 1. La práctica se realizará en grupos de tres, ubicándose cada miembro en cada uno de los PC que están sin sombrear en ambas figuras.

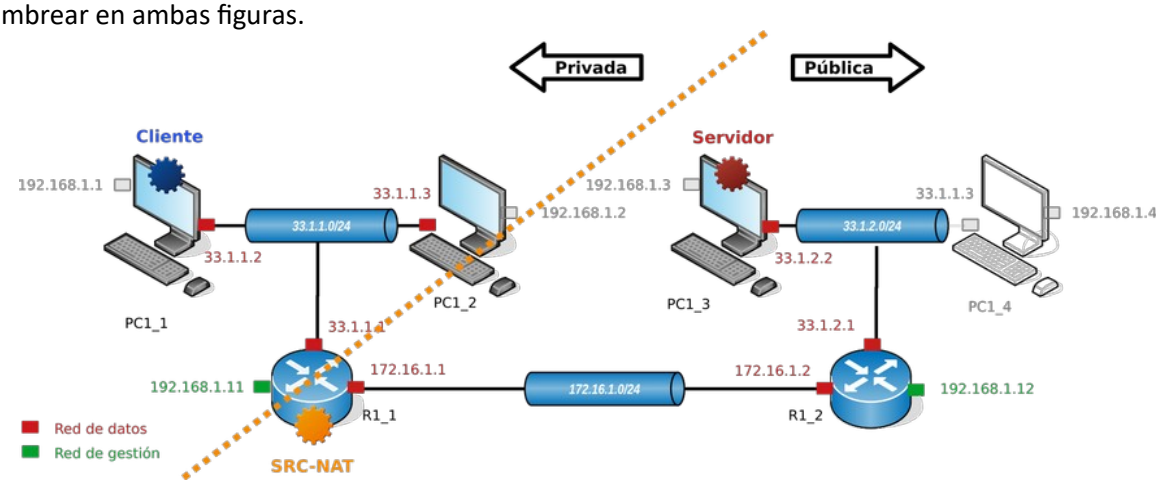

Figura 2: Escenario de trabajo y dispositivos implicados para SRC-NAT.

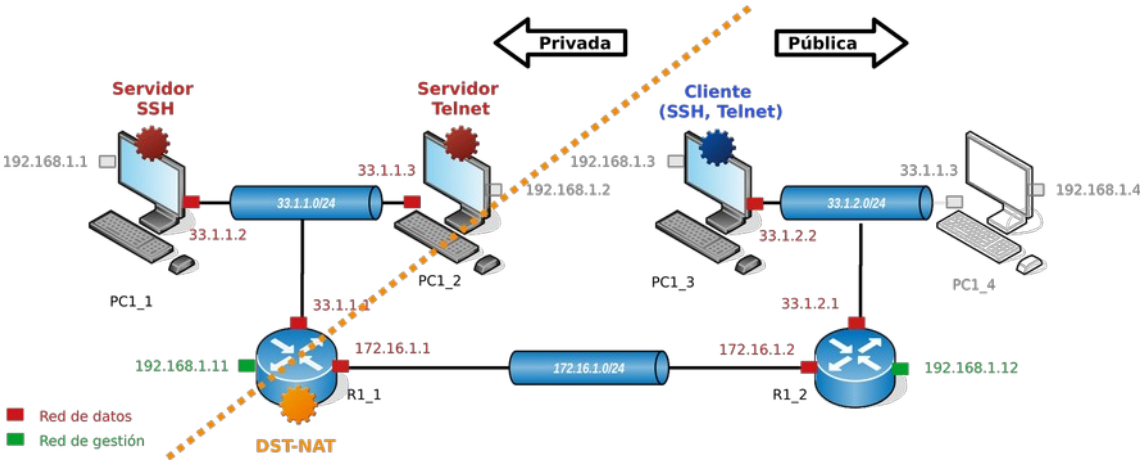

Figura 3: Escenario de trabajo y dispositivos implicados para DST-NAT.

1.1.3 Configuración de *srcnat*

Para llevar a cabo la configuración en los *routers MikroTik,* de modo que actúen como *router* NAT, será necesario acceder al dispositivo en cuestión a través de su IP de gestión mediante la aplicación Winbox. La dirección IP de la interfaz de gestión en los *routers MikroTik* tiene el formato 192.168.X.1Y, donde *X* es número de isla e *Y* es el número de subred dentro de dicha isla. La configuración NAT se lleva a cabo desde el menú *IP -> Firewall -> NAT*. En caso de usarse la interfaz de línea de comandos del *router* mediante Telnet, se puede ejecutar el siguiente comando para activar `masquerade` en la interfaz `etherF` de un *router Mikrotik.*

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

La acción `masquerade` (única subversión de la acción `src-nat`) está específicamente diseñada para escenarios *srcnat* en los que la dirección IP externa es dinámica (puede cambiar).

Del mismo modo se pueden traducir direcciones IP internas (privadas) a una IP externa (pública) específica con el siguiente comando:

```
/ip firewall nat add chain=srcnat src-address=33.X.Y.0/24 action=src-nat to-addresses=172.168.X.Y out-interface=ether2
```

A modo de resumen, el comando de arriba habilita *srcnat* usando una de las direcciones IP (`172.168.X.Y`) asignadas a la interfaz de salida ether2 para la subred `33.X.Y.0/24`. De este modo, el *router MikroTik* correspondiente actuará como *router* NAT y traducirá las direcciones IP origen de todas las conexiones salientes desde la red `33.X.Y.0/24` a la dirección IP `172.168.X.Y`.

Configuraciones similares a las comentadas anteriormente se pueden llevar a cabo desde Winbox en el menú *IP-> Firewall -> NAT* y pulsando sobre el icono con el símbolo "+" en azul para añadir la regla NAT correspondiente.

1.1.4 Configuración de *dstnat*

Para dirigir todas las solicitudes a un *host* (servidor) dentro de una red interna (privada) cuando estas tienen un determinado puerto destino (acción comúnmente conocida como "*abrir un puerto*" o "*mapeo de puerto*") se puede activar la siguiente regla dentro I*P->Firewall-NAT*:

```
/ip firewall nat add chain=dstnat dst-port=23 action=dst-nat
protocol=tcp to-address=33.X.Y.2 to-port=23 in-interface=ether2
```

Activando la regla de arriba, el router *MikroTik* redirigirá todos los paquetes con puerto TCP destino 23 (puerto utilizado generalmente por el servicio Telnet) al *host* con dirección IP 33.X.Y.2 dentro de la red interna (privada). Además, no hará traducción de puerto, sino que lo mantendrá al mismo valor (to-port = 23).

1.2 Realización práctica

Es necesario configurar las tablas de encaminamiento tanto en los *routers* como en los PC para que estos últimos tengan conectividad entre ellos.

1) Configure su *router*, el que está directamente conectado a su subred, para habilitar *srcnat* en dicha subred. Note que la dirección IP externa será la que tenga asignada su *router* en la subred 176.16.X.0/24 (vier Figura 2). Ejecute Wireshark en cada uno de los *hosts* implicados para ver el intercambiando mensajes ICMP sobre la interfaz `datos` y aplique el filtro "`icmp`" en ambas instancias de Wireshark. Después, use la utilidad *ping* para generar mensajes `ICMP` entre un *host* de su subred y un *host* de la subred que formada por los PC PCX_3 y PCX_4 así como el RX_2. Observe las diferencias que existen en las cabeceras de los protocolos IP e ICMP de un paquete capturado en el *host* de su subred y ese mismo paquete capturado en un *host* de una subred distinta. Analice los resultados.

2) Configure el mismo *router*, el que está directamente conectado a su subred, para habilitar *dstnat*. Concretamente, configure el *router* de modo que las conexiones SSH entrantes desde externas vayan a uno de los equipos de su subred y las conexiones Telnet entrantes a otro equipo diferente de su subred (ver Figura 3). Conéctese vía SSH y Telnet a dichos equipos desde cualquier equipo de otra subred. Por último, ejecute instancias de Wireshark en cada uno de los equipos (cliente SSH, servidor SSH, cliente Telnet y servidor Telnet), capture el tráfico en la interfaz `datos`, aplique el filtro correspondiente y compare las diferencias entre el tráfico capturado en los clientes y servidores.

 Tenga en cuenta que los protocolos SSH y Telnet transportan sus mensajes sobre TCP sobre los puertos 22 y 23 respectivamente.

1.3 Bibliografía

[1] Manual de MikroTik: NAT.
https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT#Summary
[2] RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations.
https://datatracker.ietf.org/doc/html/rfc2663