Comunicaciones.
NAT

Jesús Mauricio Chimento

Resumen

En este documento se describe el funcionamiento de algunos de los distintos tipos de NAT y las consideraciones generales asociadas a los mismos.

1. Introducción

Network Address Translation (NAT) o **Traducción de Direcciones de Red** es una técnica que modifica la información de dirección IP en la cabecera de un paquete IP mientras el mismo es transmitido de una red a otra por medio de un router.

La necesidad de la traducción de direcciones IP surge cuando las direcciones IP privadas[1] internas de la red no pueden ser usadas fuera de la red, o bien porque no son válidas en el exterior, o bien porque el direccionamiento interno debe mantenerse separado de la red externa.

A fines prácticos, la traducción de direcciones permite, por lo general, que las máquinas de una red privada se comuniquen de manera transparente con destinos en una red externa y viceversa.

Su principal uso hoy en día es el de permitir que las máquinas de una red privada puedan acceder a Internet utilizando una única dirección IP pública.

Si bien hay una diversa cantidad de tipos de NAT, en este trabajo solo nos enfocaremos en las más conocidas.

2. Funcionamiento

Pese a que existen muchas variantes de NAT, todas estas deben compartir las siguientes características [2]:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones.
- Traducción de la carga útil de los paquetes de error ICMP.

[1] Se considera dirección IP privada a las que pertenezcan a los rangos dispuestos en la RFC1918 [1].

Respecto de sus forma de trabajo, a continuación a partir del (posible) escenario planteado en la figura 1 analizaremos el funcionamiento de algunos de los distintos tipos de NAT. Dicha figura consiste en una red privada (red 1) con dos anfitriones (A y B) la cual posee una única dirección pública (200.13.147.43) que fue asignada al router X, el cual provee servicio de NAT. Además, hay dos máquinas (C y D) las cuales son externas a la red y la comunicación entre dichas máquinas y los anfitriones de la red se realiza vía Internet.

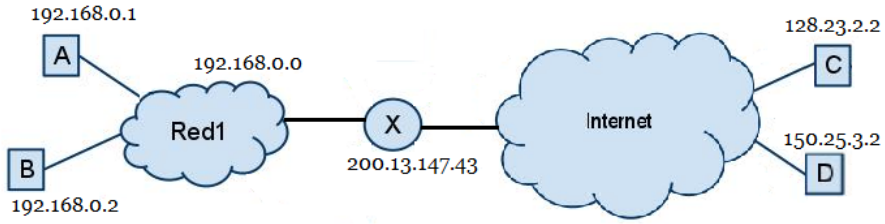

Figura 1: Ejemplo de funcionamiento de NAT.

NAT básico

En este tipo de NAT las sesiones son unidireccionales, salientes desde la red privada. El mismo, modifica dinámicamente las direcciones IP de los nodos finales (máquina emisora y máquina receptora) según corresponda y mantiene el estado de estos cambios en una tabla para que los paquetes pertenecientes a una sesión sean encaminados hacia el nodo final correcto en cualquiera de las redes (interna y/o externa).

Supongamos que el anfitrión A desea comunicarse con la máquina C y que el anfitrión B quiere hacer lo propio con la máquina D. Cuando el router X reciba un paquete proveniente desde A o B deberá cambiar en el mismo la dirección privada del campo *dirección del emisor* por la dirección pública asignada a la red y guardar registro de dicha modificación.

Dirección Emisor	Dirección Pública	Dirección Receptor
192.168.0.1	200.13.147.43	128.23.2.2
192.168.0.2	200.13.147.43	150.25.3.2

Luego, cuando C le responda A o D haga lo propio con B, estas enviarán sus paquetes con el campo *dirección destinatario* seteado en 200.13.147.43 y X deberá encargarse de modificar dicho campo por la dirección de A o B según corresponda para que la transmisión pueda seguir su curso. Ahora bien, ¿qué ocurre si mientras A se está comunicando con C, el anfitrión B desea hacer lo mismo? Si esto ocurriera, la tabla NAT de X quedaría de la siguiente manera:

Dirección Emisor	Dirección Pública	Dirección Receptor
192.168.0.1	200.13.147.43	128.23.2.2
192.168.0.2	200.13.147.43	128.23.2.2

Entonces, cuando X reciba un paquete entrante no sabría a que anfitrión debería rutearlo. Para evitar este problema, cuando se utiliza NAT básico los anfitriones de la red privada no pueden comunicarse al mismo tiempo con la misma máquina exterior a la red.

NAPT

Network Address and Port Translation (NAPT) extiende la noción de traducción del NAT básico un paso más allá dado que también traduce el identificador de transporte (número de puerto TCP/UDP por ejemplo). Esto permite que dos o más anfitriones de la red puedan comunicarse con una misma máquina externa a la red. Además, al combinarse con NAT básico permite que se use un bloque de direcciones externas en conjunto con la traducción de puertos. En otras palabras, se pueden tener múltiples conexiones con máquinas externas a la red.

Nuevamente, supongamos que tanto el anfitrión A como el anfitrión B desean comunicarse con la máquina C. Cuando el router X reciba un paquete proveniente desde A o B deberá cambiar en el mismo la dirección privada del campo *dirección del emisor* por la dirección pública asignada a la red y guardar registro de dicha modificación junto con el número de puerto a utilizar en la transmisión (no necesariamente será el mismo puerto que utiliza A).

Dir. Emisor: Puerto	Dir. Pública: Puerto	Dir. Receptor: Puerto
192.168.0.1:1333	200.13.147.43:1333	128.23.2.2:80
192.168.0.2:1555	200.13.147.43:1000	128.23.2.2:80

Luego, cuando C le responda A o B enviará sus paquetes con el campo *dirección destinario* seteado en 200.13.147.43 y X deberá encargarse de modificar dicho campo por la dirección del anfitrión que corresponda y modificar el puerto a utilizar en el anfitrión receptor por el puerto que corresponda para que la transmisión pueda seguir su curso.

DNAT

Destination NAT (DNAT) o NAT inverso ofrece un servicio similar a NAT pero al revés, es decir, permite que un máquina externa a la red inicie una transmisión hacia un anfitrión de la red. Para permitir conexiones desde el exterior de la red hay que añadir una entrada fija en la tabla de NAT la cual indicará que todo el tráfico que llegue al router dirigido a un determinado puerto sea dirigido a un anfitrión en particular. Dada esta funcionalidad, este estilo de NAT suele ser utilizado para la creación de DMZs.

Supongamos que queremos que todo el tráfico que llegue dirigido al puerto 80 sea derivado al anfitrión B dado que este brinda servicios de servidor web. Entonces, se debe generar una entrada fija en la tabla NAT como la siguiente:

Dir. Emisor: Puerto	Dir. Pública: Puerto	Dir. Receptor: Puerto
192.168.0.2:80	200.13.147.43:80	*

NAT bidireccional

Con el NAT bidireccional, las sesiones pueden iniciarse tanto desde una máquina externa hacia un anfitrión de la red privada como desde un anfitrión de la red privada hacia una máquina externa. Como en los anteriores, las direcciones de la red privada se asocian a direcciones públicas según se establecen las conexiones en cualquier sentido. El espacio de nombres entre las máquinas de las redes privada y externa se supone único extremo a extremo. Las máquinas en el dominio externo acceden a las máquinas del dominio privado usando DNS para la resolución de direcciones.

Referencias

[1] RFC1918. `http://tools.ietf.org/html/rfc1918`.

[2] RFC2663. `http://tools.ietf.org/html/rfc2663`.