Tópicos avanzados de redes
Comunicaciones NAT

Resumen

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

Introducción

Network Address Translation (NAT) o Traducción de Direcciones de Red es una técnica que módica 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.

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.

1.- Necesidad

La necesidad de la traducción de direcciones IP surge cuando las direcciones IP privadas 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. Afines 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.

- Escasez de direcciones IP reales (Publicas)
- Dificultad en obtener bloques
- Necesidad de NICs regionales - NIC Argentina (Network Information Center Argentina).

  NIC Argentina es una oficina dependiente de la Secretaría Legal y Técnica de la Presidencia de la Nación bajo la órbita de la Dirección Nacional de Registro de Dominios de Internet responsable de administrar el dominio de nivel superior **.ar**, además del registro de nombres de dominio de Internet de las personas físicas y jurídicas.

- Seguridad:

  Los bloques RFC 1918 (redes privadas) no son 'enrutados' hacia internet.

  Se reservan los tres siguientes bloques de direcciones IP para el uso en internets privadas:

```
10.0.0.0        -   10.255.255.255  (prefijo 10/8)
172.16.0.0      -   172.31.255.255  (prefijo 172.16/12)
192.168.0.0     -   192.168.255.255 (prefijo 192.168/16)
```

- Gestión:

  Protegerse de los cambios de bloques del ISP

2.- Funcionamiento

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

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones.

Respecto de su 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 publica (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.

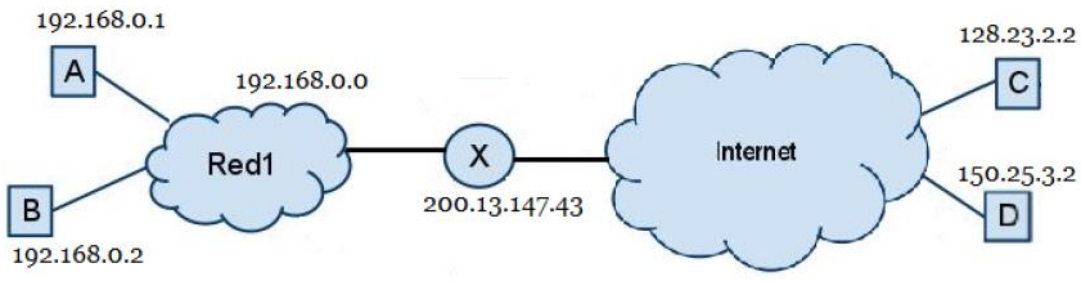
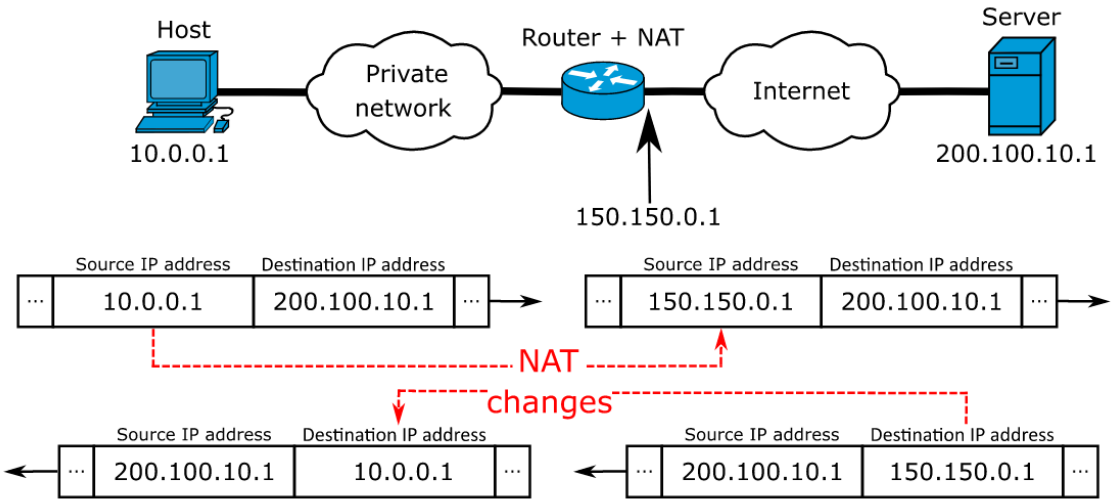


Figura 1: Ejemplo de funcionamiento de NAT.

Generalidad de uso



NAT básico (SNAT - Static Nat)

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 (maquina emisora y maquina 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 maquina 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 publica asignada a la red y guardar registro de dicha modificación.

Direccion Emisor	Direccion Publica	Direccion 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 enviaran 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 quedara de la siguiente manera:

Direccion Emisor	Direccion Publica	Direccion 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 sabrá a que anfitrión deberá 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 maquina exterior a la red.

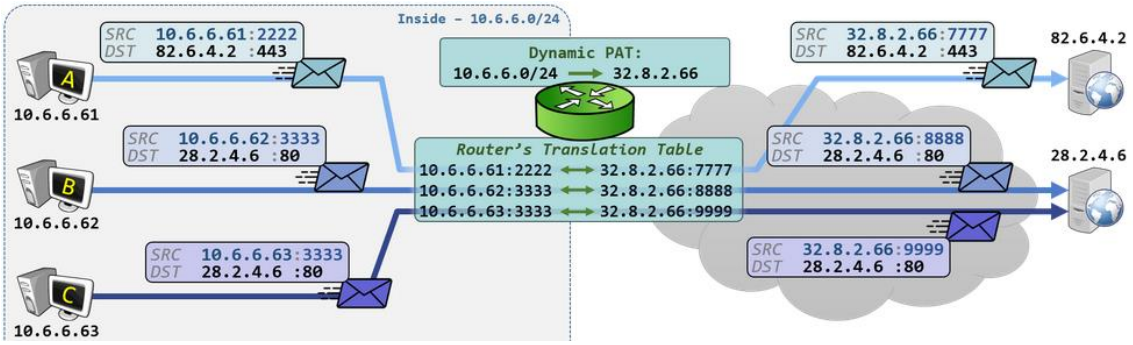
NAPT – PAT (NAT sobre cargado)

Network Address and Port Translation (NAPT) o Port address translation (PAT) 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 maquina externa a la red. 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 maquina 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 publica 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. P□ublica: 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

(Otro ejemplo)



DNAT

Destination NAT (DNAT) o NAT inverso ofrece un servicio similar a NAT pero al revés, es decir, permite que una máquina externa a la red inicie una transmisión hacia un anfitrión de la red.

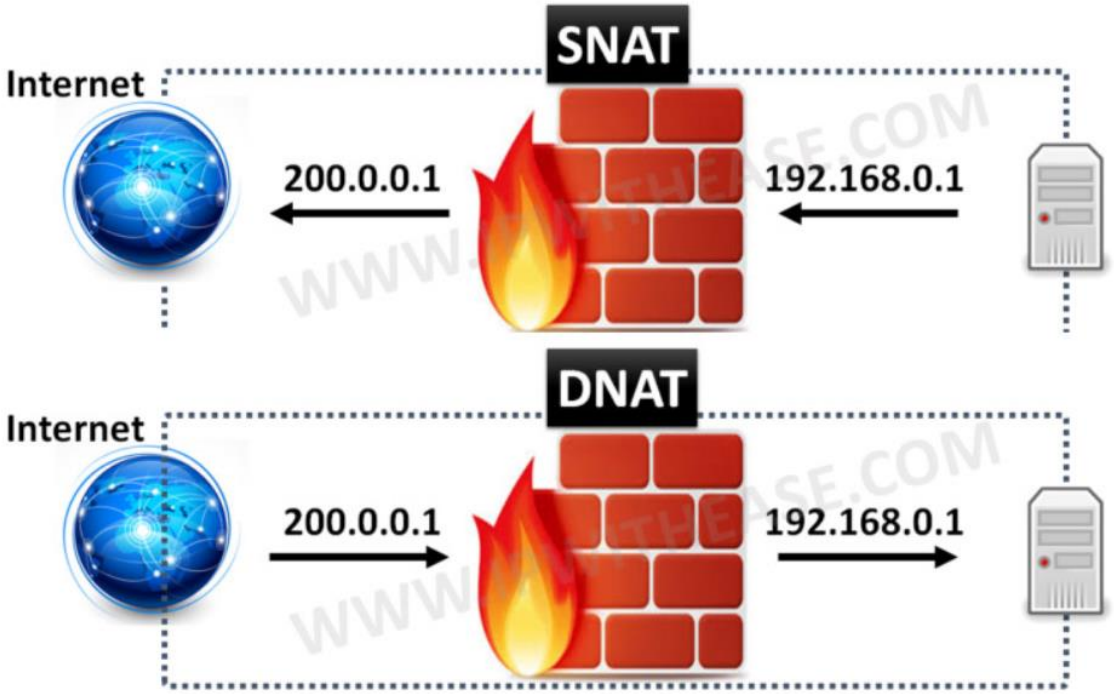
Para permitir conexiones desde el exterior de la red hay que añadir una entrada fija en la tabla de NAT la cual indicará que todo el tráfico que llegue al router dirigido a un determinado puerto sea dirigido a un anfitrión en particular. Dada esta funcionalidad, este estilo de NAT suele ser utilizado 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. Receptor: Puerto	Dir. Publica: Puerto	Dir. Emisor: Puerto
192.168.0.2:80	200.13.147.43:80	*

Referencia de comparación:



Ejemplo de una red hogareña con salida a internet: (PAT)