

NAT (*Network Address Translation*)

© 2014 tv <tvaira@free.fr> - v.1.0 - produit le 18 novembre 2014

Sommaire

NAT (<i>Network Address Translation</i>)	2
Définition	2
La NAT statique	2
La NAT dynamique	3
Problèmes liés à la NAT dynamique	3
<i>Port forwarding</i>	4
<i>Port mapping</i>	4
IPv6	4

Lire : www.frameip.com/nat/

NAT (*Network Address Translation*)

Définition

Un routeur fait du NAT (*Network Address Translation* soit « traduction d'adresse réseau ») lorsqu'il fait correspondre les adresses IP internes privées (non-unicques et souvent non routables) d'un intranet à un ensemble d'adresses externes publiques (unicques et routables). Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4. [Wikipedia]

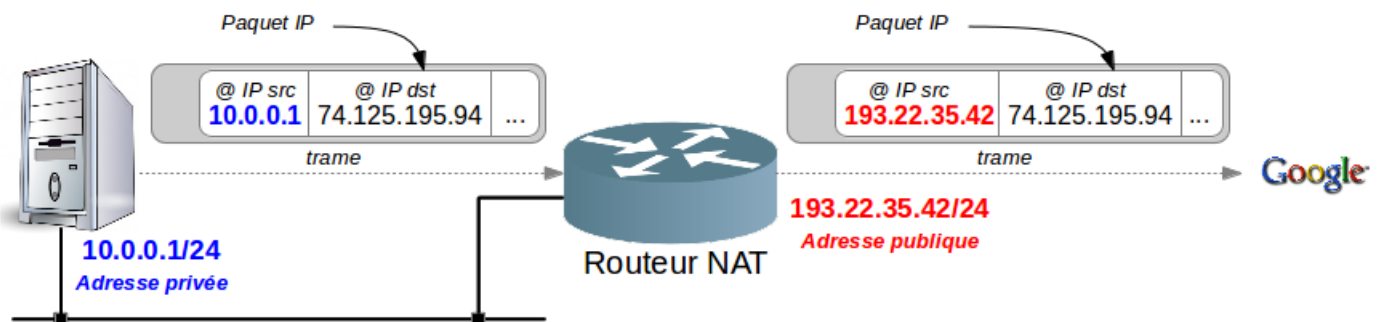


Si l'on s'en tient intrinsèquement à la définition du terme NAT, cela représente la modification des adresses IP dans l'en-tête d'un datagramme IP effectuée par un routeur. On parlera de SNAT quand c'est l'adresse source du paquet qui est modifiée, et de DNAT quand il s'agit de l'adresse destination.

La NAT statique

La NAT statique, se base sur l'association de N adresses internes avec N adresses externes. C'est à dire qu'à UNE adresse IP interne, on associe UNE adresse IP externe. Dans ce cas, la seule action qui sera effectuée par le routeur sera de remplacer l'adresse source ou destination par l'adresse correspondante.

Exemple : La NAT statique permet de rendre une machine accessible sur Internet alors qu'elle possédait une adresse privée. On fait simplement une association entre une adresse privée et une adresse publique :
 $10.0.0.1 \leftrightarrow 193.22.35.43$




Les correspondances entre les adresses privées (internes) et publiques (externes) sont stockées dans une table sous forme de paires (adresse interne, adresse externe). Il est possible de réutiliser une entrée dans la table de correspondance du NAT si aucun trafic avec ces adresses n'a traversé le routeur pendant un certain temps paramétrable.

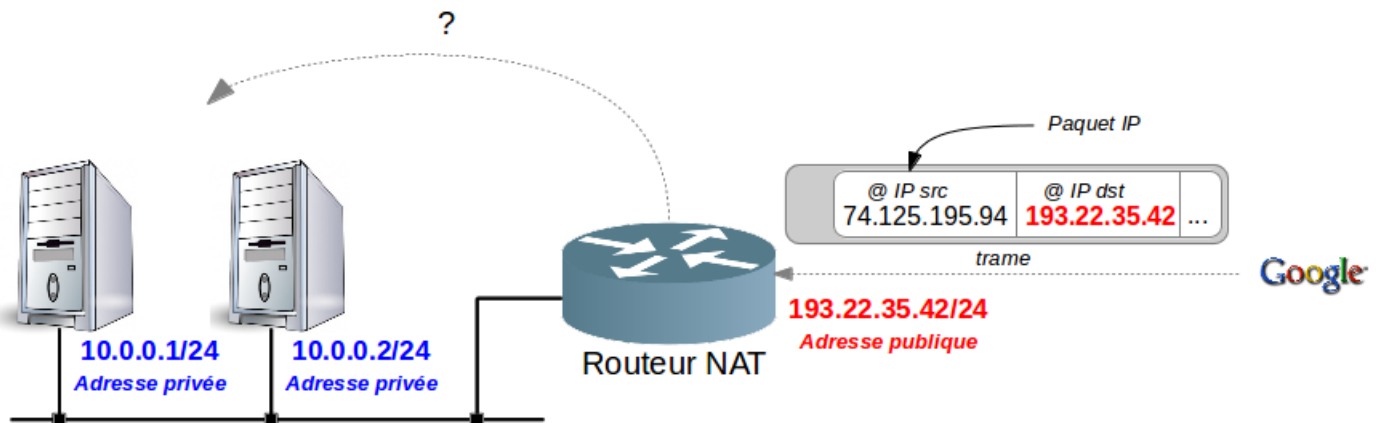
IP interne	IP Externe	Durée	Réutilisable
10.0.0.1	193.22.35.43	1200	non
10.0.0.2	193.22.35.44	3601	oui
10.0.0.3	193.22.35.45	0	non


Ces NAT servent à donner accès à des serveurs en interne (DMZ) à partir de l'extérieur.

La NAT dynamique

La NAT dynamique est aussi appelée *IP masquerading*. Contrairement à la NAT statique, la NAT dynamique associe M adresses internes à N adresses externes où $M > N$ (les adresses pour sortir étant choisies dans un *pool*). Ainsi, on peut associer UNE adresse publique à M adresses privées et permettre ainsi à un grand nombre de machines ayant des adresses privées d'accéder à Internet.


 Les adresses internes des machines se retrouvent ainsi masquer derrière une seule adresse publique. Cela a un effet sur la sécurité car les adresses internes sont ainsi dissimulées.



 Contrairement à la NAT statique, la NAT dynamique va modifier aussi les ports TCP/UDP (que l'on appelle PAT (*Port Address Translation*)).

Ce sont les numéros de ports qui vont servir à résoudre le problème d'identification des adresses internes : le numéro du port source (celui de la machine interne) va être modifié par le routeur (un nouveau qu'il choisit lui-même). Il va s'en servir pour identifier la machine interne.

Internal				External				Protocol Used
Source IP Address	Source Port	Destination IP Address	Destination Port	Source IP Address	Source Port	Destination IP Address	Destination Port	
192.168.2.1	12000	a.b.c.d	20	64.33.104.180	14000	a.b.c.d	20	TCP
192.168.2.1	12001	a.b.c.d	21	64.33.104.180	14001	a.b.c.d	21	TCP
192.168.2.2	12000	a.b.c.d	20	64.33.104.180	14002	a.b.c.d	20	TCP
192.168.2.2	12001	a.b.c.d	21	64.33.104.180	14003	a.b.c.d	21	TCP

 Cependant, contrairement à la NAT statique, la NAT dynamique ne permet pas d'être joint par une machine de l'Internet. En effet, elle a besoin d'un numéro de port source pour établir sa table de correspondance. Elle est donc utile pour partager un accès Internet, mais pas pour rendre un serveur accessible (cf. *port forwarding*).

Problèmes liés à la NAT dynamique

La NAT dynamique demande l'utilisation des ports TCP/UDP, cependant, tous les protocoles utilisés sur un réseau n'utilisent pas obligatoirement ces ports, notamment les protocoles ICMP, PPTP, Netbios...

Certains protocoles sont dits « passant difficilement les pare-feu », car ils échangent au niveau applicatif (FTP par exemple) des informations du niveau IP (échange d'adresses) ou du niveau TCP (échange de ports), ce qui transgresse le principe de la séparation des couches réseaux. Dans ce cas et pour un service donné, il faudra passer par un serveur mandataire (*proxy*) qui est capable alors de travailler sur l'ensemble des couches. C'est à dire qu'il sert d'intermédiaire dans une communication entre un client et un serveur.

Les communications entre postes (client/serveur) qui se situent derrière des NAT posent un problème, c'est le cas des protocoles pair à pair (*peer to peer*).

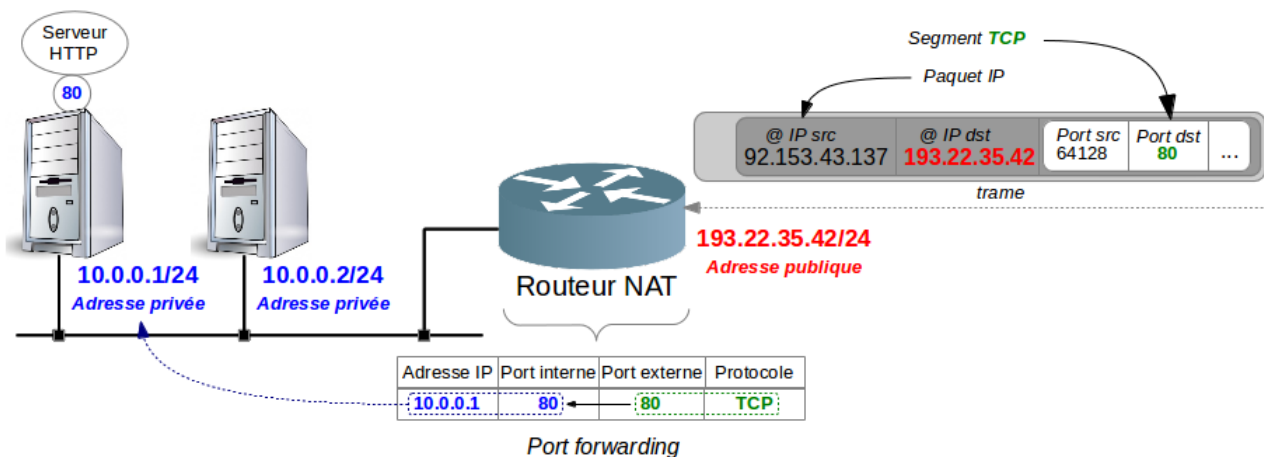
La fragmentation éventuelle des paquets dans le réseau pose également un problème quand un NAT est traversé, car il n'est pas possible pour un hôte qui reçoit des fragments avec le même *fragment id* et des adresses IP source identiques d'identifier qu'ils appartiennent en réalité à deux hôtes différents derrière un NAT.

Certains protocoles imposent que le port source soit fixé (comme `rlogin` à 512). La traversée d'un NAT empêche alors plus d'une session sortante par adresse publique.

Port forwarding

Le *port forwarding* est une solution pour joindre des machines internes (serveurs) à partir d'Internet avec la NAT dynamique. Cela consiste à rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet (une seule par port TCP/UDP).

Exemple : la machine 10.0.0.1 possède un serveur HTTP, il faut donc configurer le *port forwarding* du routeur pour qu'il redirige les connexions arrivant sur le port 80 vers la machine 10.0.0.1.



Port mapping

Le *port mapping* consiste simplement à rediriger la requête sur un port différent que celui demandé.

Par exemple, si on possède un serveur web sur le réseau local sur le port 8080 et qu'on veut le rendre accessible pour les internautes. On redirige le port 80 (port par défaut) vers le serveur sur le port 8080.

IPv6

L'IETF décourage le NAT avec IPv6 en raison des problèmes liés à certains protocoles et du fait que l'espace d'adresse IPv6 est tel que l'économie d'adresse n'est pas nécessaire.