

Routage NAT

I) Introduction

Avec le développement croissant du monde de l'internet, et notamment des liaisons à connexions permanentes comme le câble ou l'ADSL, de plus en plus d'entreprise utilisent la NAT ("Network Address Translation") pour partager leur accès Internet.

L'adresse IP (Internet protocol), est un protocole permet d'identifier les machines et de router les informations sur Internet. Ces adresses sont codées sur 4 octets, soit 32 bits. Ce qui nous permet d'avoir 2^{32} adresses disponibles (un peu plus de 4 milliards d'adresses). D'ici peu, nous allons bientôt manquer d'adresses disponibles.

En attendant un nouveau standard d'adressage qui permette d'avoir plus d'adresses disponibles (IPv6), il a fallu trouver des solutions temporaires. La NAT a notamment été une réponse à cette future pénurie d'adresses.

NAT est souvent utilisé pour représenter différents concepts que nous allons différencier, notamment NAT statique, NAT dynamique, PAT, IP masquering...

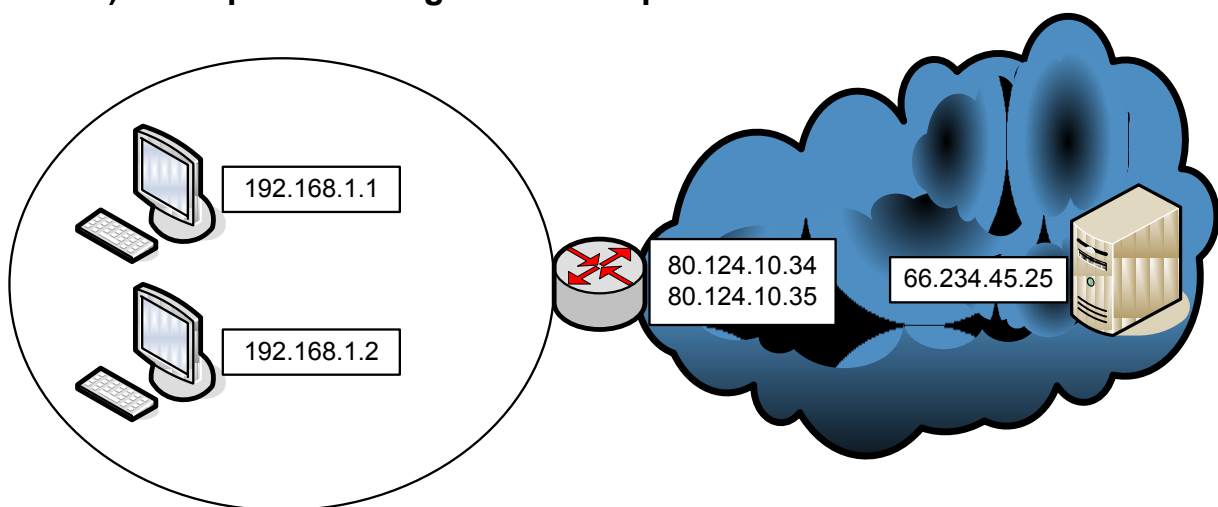
II) La NAT statique

a) Principe

A une adresse IP interne, on associe une adresse IP externe. Par exemple : si il y a trois machines dans le réseau, il faudra trois adresse IP publique, pour 1000 machines il faudra 1000 adresse IP publique.

Dans ce cas, la seule action qui sera effectuée par le routeur sera de remplacer l'adresse source ou destination par l'adresse correspondante.

b) Exemple de routage NAT Statique



- Pour l'exemple suivant, Compléter les tableaux suivant :

Table NAT du routeur :

@ IP Privé source	@ IP Publique source
192.168.1.1	80.124.10.34
192.168.1.2	80.124.10.35

- 1) Les PCs envoient un paquet IP a destination du serveur WEB sur Internet.

Pc -> "routeur NAT"		"routeur NAT" -> serveur	
IP source	IP destination	IP source	IP destination
192.168.1.1	60.234.45.25	80.124.10.34	60.234.45.25
192.168.1.2	60.234.45.25	80.124.10.35	60.234.45.25

- 2) Le serveur répond aux PCs

serveur -> "routeur NAT"		serveur -> "routeur NAT"	
IP source	IP destination	IP source	IP destination
60.234.45.25	80.124.10.34	60.234.45.25	192.168.1.1
60.234.45.25	80.124.10.35	60.234.45.25	192.168.1.2

Seule l'association entre l'adresse privée et l'adresse publique est réalisé par le routeur NAT.

c) Avantages et inconvénients de la NAT statique

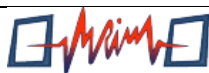
- Avantages

Il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche.

En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible sur Internet.

- Inconvénients

On remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP...



III) *Rappel sur les échanges entre clients et serveurs*

Un numéro de port sert à identifier une application. On peut différencier deux type d'application, les applications serveur et cliente.

a) **Application serveur**

Dans le cas d'application serveur, le numéro de port sert à identifier le type de service, en effet un serveur peut héberger plusieurs services. Pour que les clients contactent le bon service ils doivent utiliser le bon port. A chaque service est associé un numéro de port. Ce numéro de port est généralement inférieur à 1024.

b) **Application cliente**

Dans le cas d'une application cliente le numéro de port ne sert pas à identifier le type d'application mais l'application elle-même. C'est grâce à ce procédé que l'on peut ouvrir, par exemple, deux pages web sur un même site sans que les réponses du serveur soient mélangées. Ce numéro est choisit au hasard parmi les ports libres et il est toujours supérieur à 1024.

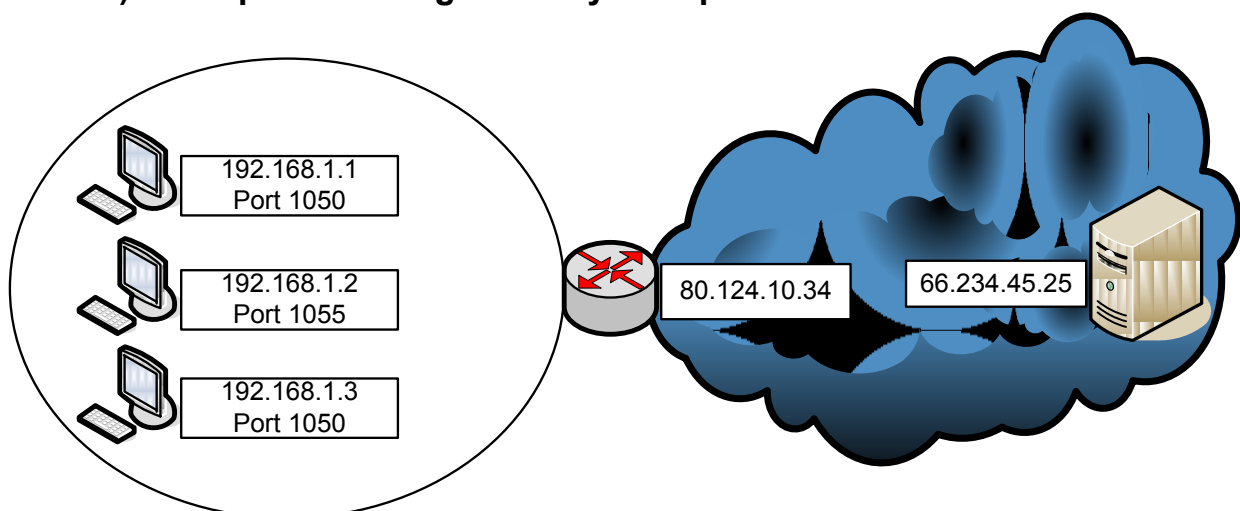
IV) *La NAT dynamique*

a) **Le principe**

La NAT dynamique est aussi appelée IP masquerading. Contrairement à la NAT statique, on peut associer une adresse publique à plusieurs adresses privées et permettre ainsi à un grand nombre de machines ayant des adresses privées d'accéder à Internet.

Par contre, nous verrons que cette méthode possède quelques inconvénients. Et contrairement à la NAT statique, le routeur qui effectue la NAT devra à la fois modifier les adresses IP mais aussi les ports TCP/UDP (on appelle la modification des ports PAT, Port Address Translation).

b) **Exemple de routage NAT dynamique**



- Pour l'exemple, Compléter les tableaux suivant :

1) Les PCs envoient un paquet IP à destination du serveur WEB sur Internet.

Pc -> "routeur NAT"			
IP source	Port Source	IP destination	Port destination
192.168.1.1	1050	60.234.45.25	80
192.168.1.2	1055	60.234.45.25	80
192.168.1.3	1050	60.234.45.25	80

"routeur NAT" -> Serveur			
IP source	Port Source	IP destination	Port destination
80.124.10.34	1050	60.234.45.25	80
80.124.10.34	1055	60.234.45.25	80
80.124.10.34	1051	60.234.45.25	80

Table NAT du routeur :

@ IP Privé source	Port source Privé	@ IP Publique source	Port source public	@ IP Publique Destination	Port destination public
192.168.1.1	1050	80.124.10.34	1050	60.234.45.25	80
192.168.1.2	1055	80.124.10.34	1055	60.234.45.25	80
192.168.1.3	1050	80.124.10.34	1051	60.234.45.25	80

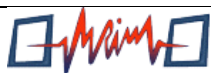
2) Le serveur répond aux PCs

Serveur -> "routeur NAT"			
IP source	Port Source	IP destination	Port destination
60.234.45.25	80	80.124.10.34	1050
60.234.45.25	80	80.124.10.34	1055
60.234.45.25	80	80.124.10.34	1051

Serveur -> "routeur NAT"			
IP source	Port Source	IP destination	Port destination
60.234.45.25	80	192.168.1.1	1050
60.234.45.25	80	192.168.1.2	1055
60.234.45.25	80	192.168.1.3	1050

Que se passe-t-il si deux machines du réseau interne initialisent des connexions vers le même service avec le même port source?

Le routeur remplace le port TCP/UDP source par un nouveau qu'il choisit lui-même. Ainsi, comme c'est lui qui les choisit, il n'en choisira pas deux identiques, et pourra identifier chacune des connexions.



c) Avantages et inconvénients de la NAT dynamique

- Avantages

La NAT dynamique permet à des machines ayant des adresses privées d'accéder à Internet. Etant donné que l'on peut "cacher" un grand nombre de machines derrière une seule adresse publique, cela permet de répondre à notre problème de pénurie d'adresses.

les machines n'étant pas accessibles de l'extérieur, cela donne un petit plus au niveau de la sécurité.

- Inconvénients

La NAT ne permet pas d'être joint par une machine de l'Internet. Effectivement, si la NAT dynamique marche, c'est parce que le routeur qui fait la NAT reçoit les informations de la machine en interne (Adresse IP, port TCP/UDP). Le paquet arrivera, avec comme adresse de destination le routeur, et le routeur ne saura pas vers qui rediriger la requête en interne.

- Conclusions

La NAT dynamique ne permet donc que de sortir sur Internet, et non pas d'être joignable. Elle est donc utile pour partager un accès Internet, mais pas pour rendre un serveur accessible.

V) Statique ou dynamique ?

- Entourer la bonne réponse.

Rendre une application disponible sur Internet, (comme un serveur web, mail ou un serveur FTP.)

Nat Statique	Nat Dynamique
--------------	---------------

Ajouter un petit plus en terme de sécurité.

Nat Statique	Nat Dynamique
--------------	---------------

Economiser les adresses IP.

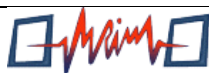
Nat Statique	Nat Dynamique
--------------	---------------

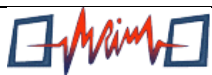
Partager un accès à Internet à des machines qui n'ont pas besoin d'être joignables de l'extérieur.

Nat Statique	Nat Dynamique
--------------	---------------

Peut-on combiner les deux méthodes ?

Oui	Non
-----	-----





Section MRIM
7, avenue Jean Jaures
BP 115
77380 COMBS-LA-VILLE

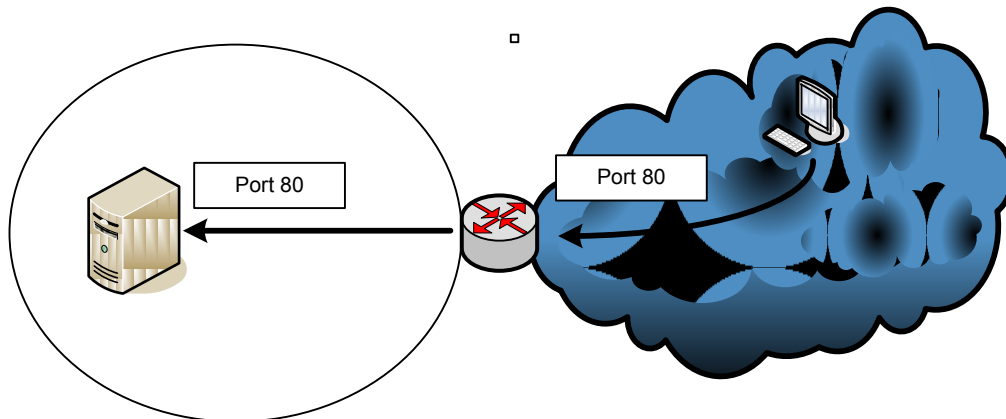
☎ : 01.64.13.42.63
✉ : prof@mrim-combs.com
🌐 : <http://www.sen-tr.fr>
Dernière modification : 24/01/10

VI) *Rendre joignables les machines du réseau local avec une seule adresse publique.*

C'est notamment le cas quand on possède un accès ADSL ou câble, une seule adresse publique vous est fournie, et il devient alors compliqué de rendre disponibles plusieurs serveurs du réseau local. (exemple de la section MRIM) Une solution à ce problème est le port forwarding.

a) **Le port forwarding.**

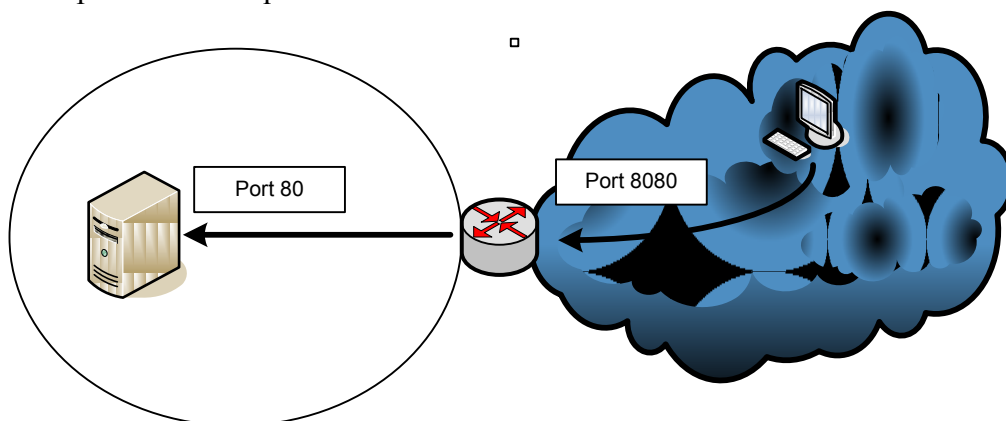
Le port forwarding consiste à rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet.



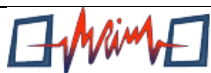
Exemple : Toutes les requêtes venant d'internet à destination du port 80, seront redirigés vers : 192.168.10.254 port 80

b) **Le port mapping.**

Le port mapping est un peu équivalent au port forwarding. Il consiste simplement à rediriger la requête sur un port différent que celui demandé.



Exemple : Toutes les requêtes venant d'internet à destination du port 80, seront redirigés vers : 192.168.10.254 port 8080.



c) Les limites du port forwarding

Le port forwarding ne peut pas non plus répondre parfaitement à toutes les questions qu'amène la NAT dynamique.

Ainsi, on a vu que l'on ne pouvait associer qu'une adresse de machine à un port donné. Si l'on possède plusieurs serveurs FTP en local et que l'on veut les rendre accessibles, il faudra trouver une autre astuce...

VII) Exercice

a) Cahier des charges

- Une entreprise possédant un parc informatique de 1500 machines veut que ces postes aient un accès à internet.
- Pour que les employés puissent communiquer par mail à l'intérieur et à l'extérieur de l'entreprise, un serveur de mail a été mis en service (POP3, SMTP).
- Pour se faire connaître, les dirigeants de l'entreprise décident de mettre en place un serveur web, administrable à distance par FTP.

b) Solutions mise en place

- Proposer des solutions qui permettront de répondre au cahier des charges.

c) Modification

- Les dirigeants de l'entreprise décident d'ajouter un deuxième serveur Web. Proposer une méthode permettant de joindre les deux serveurs web de l'extérieur du réseau.

