Le NAT

Network Address Translation

Aurélien BONNARDON

29/04/2008

Ce document présente le NAT, système mis en place en 1994 pour palier au manque d'adresses IP publiques sur Internet.

Introduction

Le Network Address Translation (NAT) (ce qu'on peut traduire de l'anglais en « traduction d'adresse réseau ») fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques 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 la carence d'adresses IPv4 d'Internet. Le NAT est décrit dans les RFC 1631 et 3022.

1 Théorie

Sur l'Internet actuel, les machines sont identifiées grâce à une adresse IP qui doit être unique pour chaque machine. Celle-ci est codée sur 32 bits, il est donc possible d'adresser 2^32 machines, soit environ 4 milliards. Malheureusement, un grand nombre de ces adresses sont réservées et il en existe un nombre disponible largement inférieur à la demande. Pour résoudre ce problème, il a été imaginé de segmenter les machines en réseaux privées (Intranet) derrière une machine qui possède une adresse publique. Celle-ci remplace l'adresse source des paquets en provenance du réseau privé par la sienne avant de les envoyer sur Internet. C'est ce qu'on appelle le NAT.

On peut définir le NAT dans les deux sens (entrée et sortie). Il existe deux méthodes de NAT de sortie, le NAT basic utile avec plusieurs adresses IP publiques (souvent utilisé en entreprise) et le NAT par port lorsqu'il n'y a qu'une seule adresse publique (particulier).

1.1 Le NAT en sortie

Le NAT en sortie consiste à modifier l'adresse IP source du paquet pour y mettre l'adresse IP publique de la passerelle ou routeur. On l'appelle également SNAT, pour Source NAT.

1.1.1 Le NAT basic

Le NAT basic est utilise si l'on possède plusieurs adresse publiques. Il permet d'associer, statiquement ou dynamiquement, une adresse privée à une adresse publique. Le système utilise une table dans laquelle il ajoute une notion de durée de vie:

Adresses privées	Adresse publiques	Durée de vie en seconde
192.168.0.3	192.168.1.2	3200
192.168.0.7	192.168.1.3	1400

1.1.2 Le NAT par port

La deuxième méthode, nommée NAT par port, est utile si l'on ne possède qu'une seule adresse publique. En plus de l'adresse source, la passerelle enregistre le port source de la connexion (au sens TCP). Ces informations sont donc stockées dans une table de ce format:

Adresses privées	Ports sources	Ports associés
192.168.0.3	1025	2000
192.168.0.7	1456	2001

1.2 Le NAT en entrée

Le NAT a également une importance dans le sens inverse. En effet, si l'on veut mettre en place un serveur accessible depuis l'extérieur dans notre réseau privé, il faut que les machines extérieures puissent ouvrir une connexion avec celui-ci. Ce mécanisme s'appelle la redirection port (*port forwarding*), voir également, par abus de langage, ouverture de port. On le note DNAT, pour Destination NAT, puisqu'il modifie l'adresse de destination du paquet.

Prenons un exemple concret pour mieux comprendre, imaginons que nous aillons un serveur Web à l'adresse 192.168.0.2 en écoute sur le port 80. Une station du réseau externe veut se connecter à celui-ci, or, elle ne connaît que l'adresse de la passerelle. Cette dernière reçoit un paquet destiné à son adresse sur le port 80, elle ne sera pas le traiter par défaut. Il faut donc lui indiquer de rediriger ce paquet vers la station possédant le serveur.

Il se présente également sous forme de table, de ce format:

Port destination	Adresse privée	Port destination privé
80	192.168.0.2	80

On remarque qu'il est possible que le port privée soit différent du port public.

On note SNAT le NAT de source où seule la source est traduite et on note DNAT le NAT de destination où seule la destination est traduite.

2 Pratique

Etudions maintenant comment mettre en place du NAT sur différente plateforme.

2.1 Linux

Sous Linux, on utilise principalement l'outil Netfilter pour faire du NAT. Netfilter est le module qui fournit à Linux les fonctions de pare-feu, de traduction d'adresse et d'historisation du trafic réseau. Il intercepte et manipule les paquets IP avant et après le routage.

La commande suivante permet de mettre en place du SNAT par port :

```
iptables -A POSTROUTING -t nat -o <Interface de sortie> -j SNAT --to <Adresse IP publique>
```

Analysons les options de cette commande :

- **-A POSTROUTING** permet de traiter les paquets après la décision de routage, juste avant que le paquet soit expédié. Il permet la modification de la source de la connexion.
- **-t** permet de spécifier la table dans laquelle les informations seront stockées. Ici: nat.
- **-o** permet de préciser l'interface de sortie.
- **-j SNAT** permet de spécifier l'utilisation d'un NAT de source. L'option j précise ce qu'il faut faire si le paquet correspond à la règle.
- **--to** permet de préciser l'adresse IP à mettre dans la source du paquet. Il est également possible de modifier le port en ajoutant ":PORT" à la fin de l'adresse. Il faut mettre l'adresse publique de la station.

La commande suivante permet de mettre en place du DNAT :

```
iptables -A PREROUTING -t nat –p tcp ––dport <Port externe> -j DNAT --to
<Adresse IP publique>:<Port interne>
```

Analysons les options de cette commande :

- **-A PREROUTING** permet de traiter les paquets avant la décision de routage, juste avant que le paquet soit expédié. Il permet la modification de la destination.
- **-t** permet de spécifier la table dans laquelle les informations seront stockées. Ici: nat.
- **-p** permet de préciser le protocole.
- **--dport** permet de préciser le port externe, celui visible depuis le réseau public.
- **-j DNAT** permet de spécifier l'utilisation d'un NAT de destination. L'option j précise ce qu'il faut faire si le paquet correspond à la règle.
- **--to** permet de préciser l'adresse IP à mettre dans la destination du paquet ainsi que le port. Il faut mettre l'adresse du serveur dans le réseau privé.

Il ne faut pas oublier d'autoriser ces paquets avec la commande suivante :

```
iptables -A FORWARD -p tcp -d <Adresse IP du serveur> --dport <Port
interne> -j ACCEPT
```

Si vous rencontrez des difficultés avec *iptables*, référez-vous à mon document sur la mise en place d'une Passerelle avec NAT et DNSmasq.

2.2 Windows

Pour les plateformes Windows, je vous conseille *WinRoute Lite* qui est facile d'utilisation, léger et gratuit. Vous le trouverez à l'adresse suivante :

http://download.kerio.com/dwn/wrl4-fr-win.exe

Je ne vais pas détailler son installation et sa configuration qui est assez simple. Si certains d'entre vous rencontrent des problèmes, merci de m'en informer.

3 Problèmes liés au NAT

Le NAT pose des problèmes avec certains protocoles. Notamment ceux qui ne respectent pas l'indépendance des couches du modèle OSI.

Le protocole FTP utilise deux connexions en parallèle. L'une pour le contrôle de la connexion, l'autre pour le transfert des données. Le premier problème intervient lors de la connexion, en mode actif, c'est le serveur qui initialise le canal de données. Or, il est impossible d'initialiser une connexion de l'extérieur avec le NAT, à moins de faire de DNAT, mais comme le port est n'est pas fixe, cela est impossible. Il faut utiliser le mode passif où les deux canaux sont initialisés par le client. Le deuxième problème est que le protocole FTP intègre l'adresse IP des stations dans sa trame. Il faut donc lire le contenu de celle-ci pour pouvoir lui appliquer le NAT correctement. Cela prend du temps et va à l'encontre du modèle OSI.

De plus, certains protocoles n'utilisent pas TCP ou UDP, alors que NAT se base sur les numéros de ports. On peut citer ICMP, PPP, Netbios, … Prenons l'exemple d'ICMP. Au lieu d'utiliser de numéro de port, on utilise l'identifiant ICMP présent dans l'en-tête, le mécanisme est ensuite le même. De plus, certains paquets ICMP contiennent des adresses IP, il faut également les modifier.

Conclusion

Le NAT est une solution pour résoudre le problème de manque d'adresses IP publiques. Celui-ci va disparaitre dans quelques années quand l'IPv6 se sera imposé, mais cela risque de ne pas être pour un futur proche. Nous pourrons alors avoir tous notre plage adresses IP publiques et ainsi adresser toutes nos machines.

Sources

- La Nat,
  http://www.frameip.com/nat/

- Network address translation,
  http://fr.wikipedia.org/wiki/Network_address_translation