LA NAT – TRANSLATION D'ADRESSE IP

1 – Introduction à la NAT

1.1 – Objet de ce cours

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 de particuliers utilisent de la NAT pour partager leur accès Internet, parfois même sans le savoir.Il m'a donc semblé opportun de faire un petit cours rassemblant les idées principales qui tournent autour de la NAT, et d'essayer de les clarifier. Ce cours se limitera à l'étude de la NAT sur le modèle TCP/IP. Pour comprendre les mécanismes mis en oeuvre dans la NAT, vous aurez besoin d'avoir quelques connaissances sur le modèle TCP/IP, et notamment sur les couches 3 et 4 du modèle OSI (IP et TCP/UDP).

1.2 – Réutilisation de ce cours

1.3 – Décharge

L'auteur décline toute responsabilité concernant la mauvaise utilisation ou compréhension du cours qui engendrerait l'écroulement de votre réseau.

1.4 – Votre travail

La seule et unique tâche que je vous demanderai d'accomplir sera de corriger mes erreurs (aussi bien dans la cohérence des éléments avancés que pour l'orthographe), me donner des conseils sur ce qui est mal expliqué pour le rendre plus accessible, ajouter des éléments qui ont trait à la NAT et rendent l'exposé plus complet, combler tout manque pour améliorer ce cours.

2 – Définitionsde la NAT

2.1 – L'identification des machines

Pour envoyer du courrier à un ami, vous utilisez son adresse postale. Ainsi vous êtes sûr que le paquet que vous envoyez arrivera à la bonne personne. Et bien pour les ordinateurs, c'est pareil. Quand vous connectez votre ordinateur à un réseau (Internet par exemple), il possède une adresse qui l'identifie d'une façon unique pour que les autres ordinateurs du réseau puissent lui envoyer des informations.

2.2 – L'adressage IP

Nous avons parlé d'adresses pour les machines, il est temps maintenant de définir ces adresses. On parle d'adresse IP (Internet protocol), car il s'agit du protocole qui 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). Même si ce chiffre dépasse de loin le nombre de machines présentes sur Internet, nous allons bientôt manquer d'adresses disponibles, notamment parce qu'un grand nombre de ces adresses sont gâchées. 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. Nous allons voir en quoi elle consiste, et quels sont ses avantages et inconvénients.

2.3 – Qu'est-ce que la NAT ?

Le terme barbare NAT représente les initiales de « Network Address Translation », ou « Traduction d'Adresse réticulaire » en français. Mais il est souvent utilisé pour représenter différents concepts que nous allons différencier, notamment NAT statique, NAT dynamique, PAT, IP masquerading… Si l'on s'en tient intrinsèquement à la définition du terme NAT, cela représente la modification des adresses IP dans l'entête d'un datagramme IP effectuée par un routeur. On verra par la suite quelles sont les différentes applications possibles. 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.

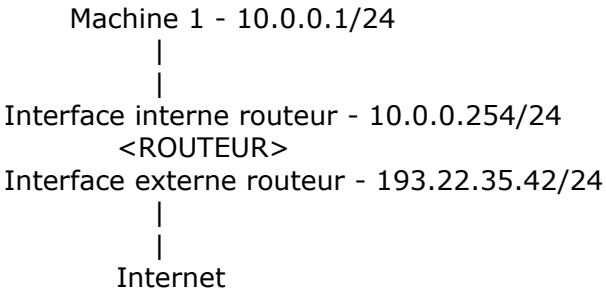
3 – La NAT statique

3.1 – Le principe

La NAT statique, se base sur l'association de n adresses avec n adresses. 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.

3.2 – Pourquoi je ne peux pas accéder à Internet avec une adresse privée ?

On prend l'exemple suivant :



La machine 1 veut envoyer un paquet sur Internet, vers www.ohmforce.com, par exemple. Donc dans l'entête IP, l'adresse en destination est celle de www.ohmforce.com, et en source c'est 10.0.0.1. Si jamais il n'y avait pas de translation d'adresse, le paquet arriverait bien a la machine www.ohmforce.com, mais celle-ci essaierait de renvoyer sa réponse a 10.0.0.1 qui n'est pas une adresse routée sur Internet !! (Elle fait partie d'une classe d'adresses réservées pour les réseaux privés). Et notre machine 1 n'obtiendrait jamais de réponse… Ainsi, une machine ayant une adresse privée ne pourra pas recevoir de réponse à ses requêtes sans un mécanisme supplémentaire.

3.3 – Le fonctionnement de la NAT statique

Nous avons vu qu'une machine ayant une adresse privée ne pouvait pas dialoguer sur Internet avec celle-ci, donc pour résoudre ce problème, on va lui donner une adresse publique virtuelle qui va lui permettre d'accéder à Internet. Ainsi, un routeur (la plupart du temps la passerelle d'accès à Internet) va modifier dans l'entête IP du paquet l'adresse source 10.0.0.1 pour mettre une adresse valide sur Internet 193.22.35.43 (dans notre exemple). Le paquet va donc arriver à sa destination, et celle-ci va pouvoir le renvoyer à 193.22.35.43 qui est une adresse valide sur Internet. Le paquet va arriver jusqu'au routeur qui a fait l'association entre 193.22.35.43 et 10.0.0.1, il va donc modifier l'adresse destination 193.22.35.43 et mettre à la place 10.0.0.1, et renvoyer le paquet sur le réseau local. Ainsi, la machine 1 est vue de l'Internet avec l'adresse 193.22.35.43. S'il s'agit d'un serveur web, il suffit d'envoyer une requête HTTP vers cette adresse pour obtenir le site web.

La NAT statique nous a permis de rendre une machine accessible sur Internet alors qu'elle possédait une adresse privée. On a simplement fait une association entre une adresse privée et une adresse publique: 10.0.0.1 <–> 193.22.35.43

3.4 – Avantages et inconvénients de la NAT statique

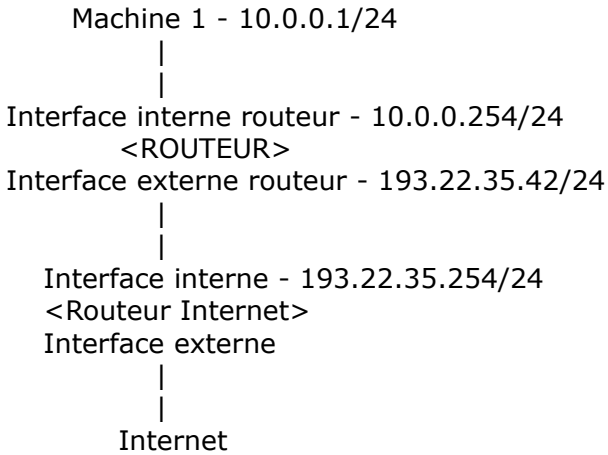
En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible sur Internet. Par contre, on remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant

accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP… D'autre part, tant qu'à donner une adresse publique par machine, pourquoi ne pas leur donner cette adresse directement plutôt que de passer par un intermédiaire ? A cette question, on peut apporter plusieurs éléments de réponse. D'une part, 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 adresse privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche. D'autre part, on gâche un certain nombre d'adresses lorsqu'on découpe un réseau en sous-réseaux (adresse de réseau, adresse de broadcast…), comme lorsqu'on veut créer une DMZ pour rendre ses serveurs publiques disponibles. Avec la NAT statique, on évite de perdre ces adresses.

Malgré ces quelques avantages, le problème de pénurie d'adresses n'a toujours pas été réglé. Pour cela, on va se pencher sur la NAT dynamique (Pour ceux qui ne veulent pas rentrer dans les détails techniques, vous pouvez directement passer au paragraphe 4)

3.5 – Problèmes de routage liés à l'utilisation de la NAT statique (proxy ARP)

Les problèmes montrés ne sont pas toujours rencontrés lors de l'implémentation de la NAT statique. Si celle-ci est bien faite, tous les mécanismes décrits devraient être implémentés de façon transparente pour l'utilisateur. Ce qui va suivre demande d'avoir quelques notions sur le fonctionnement de la pile TCP/IP. Un premier problème rencontré est celui de la redirection d'un paquet vers l'adresse virtuelle de la NAT statique. On considèrera l'exemple précédent auquel on ajoute le premier routeur rencontré sur Internet.



La machine 1 fait une requête vers le site www.ohmforce.com. Le paquet est NATé au niveau du routeur avec comme adresse source 193.22.35.43, ainsi, le site web www.ohmforce.com renvoie sa réponse vers cette adresse. Le paquet est routé sur Internet et arrive sur le routeur Internet (celui qui précède le routeur de l'entreprise ou du particulier). Celui-ci regarde l'adresse de destination et observe qu'elle se situe sur le même réseau qu'une de ses interfaces. Ainsi, elle a maintenant besoin de l'adresse MAC de la machine 193.22.35.43 pour lui envoyer le paquet. Elle fait donc une requête ARP en demandant « Quelle est l'adresse MAC de la machine ayant 193.22.35.43 comme adresse IP ? ». Or, sur ce réseau, aucune machine n'a cette adresse puisqu'il s'agit d'une adresse virtuelle. Il faut donc que le routeur (193.22.35.42) réponde lui-même à cette requête ARP. C'est ce que l'on appelle faire proxy ARP. Quand vous faites de la NAT statique, le proxy ARP est souvent automatiquement implémenté, cependant, il est bon de connaître ce mécanisme si ce n'est pas le cas.

Il y a plusieurs façons de pallier ce problème. Soit mettre en place soit même un mécanisme de proxy ARP sur la machine faisant la NAT statique.

- Soit ajouter une entrée statique dans la table ARP du routeur Internet (pas le routeur faisant la NAT, mais le premier routeur rencontré après celui-ci sur Internet). Commande arp sous windows :
  arp -s 193.22.35.43 @MAC_routeur

- Soit ajouter une route host statique pour chacune des adresses virtuelles. Sous windows:
  Route add -p 193.22.35.43 mask 255.255.255.255 193.22.35.42

3.6 – Problèmes de routage liés à l'utilisation de la NAT statique (routage sur la passerelle)

Un second problème peur survenir sur l'équipement qui fait la NAT. Revenons à l'exemple précédent. Le routeur Internet envoie le paquet au routeur de l'entreprise. Celui-ci reçoit la trame Ethernet, voit que c'est son adresse MAC qui est en destination, il envoie donc le contenu des données à la couche IP. Celle-ci voit que c'est l'adresse 192.22.35.43 (l'adresse virtuelle de notre machine) qui est en destination. Il va voir dans la table de routage, et là, il peut y avoir un problème… Soit une route spécifique existe pour cette adresse pour rediriger le paquet vers le réseau interne, soit ce n'est pas le cas, et il sera renvoyé sur l'interface externe du routeur, vu que l'adresse de destination appartient au même réseau que son interface externe 193.22.35.42 !! Pour que la NAT fonctionne, il faut donc qu'il y ait une route spécifique vers le réseau interne. Dans notre cas :

- Route add -p 193.22.35.43 mask 255.255.255.255 10.0.0.1

Ainsi, quand le routeur recevra un paquet à destination de l'adresse virtuelle 193.22.35.43, il le redirigera bien vers l'adresse réelle de la machine, 10.0.0.1. Et hop, ça marchera.

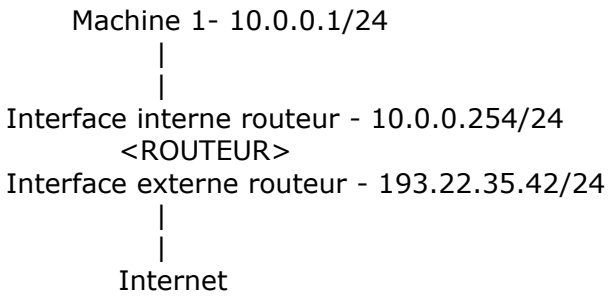
4 – La NAT dynamique

4.1 – Le principe

La NAT dynamique est aussi appelée IP masquerading. Contrairement à la NAT statique, la NAT dynamique associe une seule adresse à n adresses (ou pour être plus précis, M adresses à N adresses, les adresses pour sortir étant choisies dans un pool). Ainsi, on peut associer une adresse publique à n 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 (que l'on appelle PAT, Port Address Translation).

4.2 – Le fonctionnement de la NAT dynamique

Le fonctionnement est un peu différent de celui de la NAT statique. Nous allons notamment voir pourquoi il faut faire de la PAT et non pas une simple traduction des adresses IP. Reprenons l'exemple précédent :



Cette fois, c'est l'adresse publique de l'interface externe du routeur 193.22.35.42 qui va être utilisée pour sortir. Ainsi, lorsque le paquet arrive à la machine de destination, www.ohmforce.com par exemple, celle-ci le renvoie vers l'adresse 193.22.35.42. Le routeur reçoit donc ce paquet et voit que l'adresse de destination est lui-même !! Comment peut-il alors savoir si le paquet est pour lui ou une machine en interne ?

C'est grâce aux ports TCP/UDP qu'il va pouvoir faire la différence. Ainsi, si une machine en interne fait une requête avec comme port TCP source 2356, le routeur pourra savoir que lorsqu'il recevra un paquet avec comme port destination 2356, il faut le rediriger vers la machine en interne qui a initialisé la connexion. Mais je vois déjà pointer les questions: « oui, mais si deux machines du réseau interne initialisent des connexions avec le même port TCP/UDP ?hein ? alors ? comment qu'on fait pour savoir qui est qui ? hein ? alors ? »

Et vous auriez raison de vous les poser ! Mais tout a été prévu pour pallier à ce problème. En fait, 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, magisme… On reprend donc depuis le début le fonctionnement.

La machine 10.0.0.1 veut se connecter au site www.ohmforce.com, elle envoie donc un paquet avec comme adresse source la sienne, 10.0.0.1, et comme port source un port quelconque supérieur à 1024, soit par exemple 5987. Le paquet arrive au routeur qui fait la NAT, il remplace donc l'adresse IP source par la sienne 193.22.35.42, et la PAT en remplaçant le port TCP/UDP source 5987 par un de son choix, 10000 par exemple. Il garde ces informations de correspondance bien au chaud dans une table NAT. Le paquet arrive a www.ohmforce.com qui le renvoie a 193.22.35.42. Le paquet arrive au routeur, il voit que l'adresse destination est lui-même, il regarde donc le port destination TCP/UDP qui est 10000. Il va regarder dans la table NAT pour avoir la correspondance, et bingo !! il sait qu'il faut envoyer ce paquet à 10.0.0.1, tout en ayant modifié le port destination 10000 en 5987 qui est le port sur lequel 10.0.0.1 a initialisé la connexion.

Et voilà. On peut ainsi masquer autant de machines que l'on veut derrière une seule adresse publique !

4.3 – Avantages et inconvénients de la NAT dynamique

Comme nous l'avons vu, la NAT dynamique permet à des machines ayant des adresses privées d'accéder à Internet. Cependant, contrairement à la NAT statique, elle 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). Par contre, il n'aura aucune de ces informations si la connexion est initialisée de l'extérieur… Le paquet arrivera avec comme adresse de destination le routeur, et le routeur ne saura pas vers qui rediriger la requête en-interne.

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. De plus, étant 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.

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

4.4 – Problèmes liés à la NAT dynamique (ICMP)

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… Prenons par exemple le protocole ICMP. Se limitant à la couche 3 il n'utilise pas de ports TCP ou UDP. Il n'est donc pas possible de faire de la NAT dynamique de façon classique.

Une méthode spécifique doit être implémentée pour permettre la NAT du trafic

ICMP. Pour cela, au lieu de se baser sur les ports TCP/UDP, on peut se baser sur l'identifiant ICMP présent dans l'entête du message ICMP. Ainsi, le mécanisme est exactement le même, mis à part que l'on utilise cet identifiant, plutôt que les ports TCP/UDP. Il faut donc implémenter spécifiquement ce type de NAT pour le protocole ICMP. Par ailleurs, certains paquets ICMP contiennent dans leur payload des informations concernant les datagrammes IP qui ont causé l'erreur. Le routeur faisant la NAT doit donc aussi modifier les informations contenues dans le payload pour que l'information apportée à la machine émettrice soit pertinente.

4.5 – Problèmes liés à la NAT dynamique (FTP)

Le protocole ftp a un fonctionnement un peu particulier. Il utilise deux connexions en parallèle. L'une pour le contrôle de la connexion, l'autre pour le transfert des données. Le ftp peut fonctionner selon deux modes différents, actif ou passif. En mode passif, pas de problème, les connexions sont initialisées de l'intérieur pour chacun de ces deux canaux. Par contre, pour le mode actif, la connexion de contrôle est d abord initialisée de l intérieur, et quand des données sont demandées, c'est le serveur qui initialise la connexion de données à partir de l'extérieur. Et comme nous le savons, il n'est pas possible d'initialiser de connexions à partir de l'extérieur du réseau avec de la NAT dynamique. Un autre problème du protocole ftp est qu'il contient des données se rapportant aux adresses des machines. Ainsi quand les adresses sont NATées, cela pose problème… Donc pour que le ftp puisse fonctionner, on est obligés d'utiliser un module qui soit capable de lire les informations contenues dans les données ftp. Pour faire cela, on utilise un proxy (Voir paragraphe 7) qui sera capable de suivre la connexion et de modifier les données ftp pour la rendre possible.

Dans un cas comme celui-ci, ce n'est plus un simple module NAT à ajouter, mais un proxy à part entière.

5 – Statique ou dynamique ?

5.1 – Quand faire de la NAT statique ?

Nous avons vu que la NAT statique permettait de rendre disponible une machine sur Internet, mais qu'il fallait par contre une adresse IP pour que ce serveur soit joignable. Il est donc utile d'utiliser la NAT statique quand vous voulez rendre une application disponible sur Internet, comme un serveur web, mail ou un serveur FTP.

5.2 – Quand faire de la NAT dynamique ?

La NAT dynamique permet d'une part de donner un accès à Internet à des machines possédant des adresses privées, et d'autre part d'apporter un petit plus en terme de sécurité. Elle est donc utile pour économiser les adresse IP, donner un accès à Internet à des machines qui n'ont pas besoin d'être

joignables de l'extérieur (comme la plupart des utilisateurs). D'autre part, même quand on possède assez d'adresses IP, il est souvent préférable de faire de la NAT dynamique pour rendre les machines injoignables directement de l'extérieur. Par exemple, pour un usage personnel de partage de l'ADSL ou du câble, on utilise souvent la NAT dynamique pour partager sont accès, étant donné que les machines n'ont pas besoin d'être jointes de l'extérieur.

5.3 – Puis-je combiner ces deux méthodes ?

Oui, et c'est même souvent la meilleure solution lorsque l'on a à la fois des machines offrant un service, et d'autres qui n'ont besoin que de se connecter à Internet. Ainsi, on économisera les adresses IP grâce aux machines NATées dynamiquement, et on utilisera exactement le bon nombre d'adresses IP publiques dont on a besoin. Il est donc très intéressant de combiner ces deux méthodes.

6 – Comment rendre joignables les machines de mon réseau local alors que je n'ai qu'une seule adresse publique ?

6.1 – Explication du problème

Nous avons vu que dans le cas de la NAT dynamique, les machines du réseau local ne pouvaient pas être jointes de l'extérieur. Cela est plutôt un plus pour la sécurité, mais si on doit offrir des services comme un serveur FTP ou web, ça devient problématique. 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.

Une solution à ce problème est le port forwarding.

6.2 – Le port forwarding, qu'est-ce que c'est ?

Le port forwarding consiste à rediriger un paquet vers une machine précise en fonction du port de destination de ce paquet. Ainsi, lorsque l'on n'a qu'une seule adresse publique avec plusieurs machines derrière en adressage privé. On peut initialiser une connexion de l'extérieur vers l'une de ses machines (une seule par port TCP/UDP). Prenons l'exemple précédent et disons que la machine 10.0.0.1 possède un serveur FTP. Maintenant, on configure le routeur pour qu'il redirige les connexions arrivant sur le port 21 vers la machine 10.0.0.1. Et hop, on rend notre machine ayant une adresse privée disponible depuis l'extérieur !!

Ainsi, le port forwarding nous a permis de rendre nos machines du réseau local joignables d'Internet, même si l'on ne possède qu'une seule adresse IP publique !!

6.3 – Le port mapping, qu'est-ce que c'est ?

Le port mapping est un peu équivalent au port forwarding. Il consiste simplement à rediriger la requête sur un port différent que celui demandé. Par exemple, si on fait tourner 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 vers notre serveur sur le port 8080. Ainsi, les clients externes auront l'impression de s'adresser à un serveur sur le port usuel pour le web, 80.

6.4 – Les limites du port forwarding

Hé oui, 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…

7 – Les proxys

7.1 – Qu'est-ce qu'un proxy ?

Un proxy est un mandataire pour une application donnée. C'est à dire qu'il sert d'intermédiaire dans une connexion entre le client et le serveur pour relayer la requête qui est faite. Ainsi, le client s'adresse toujours au proxy, et c'est lui qui s'adresse ensuite au serveur. Une proxy fonctionne pour une application donnée, http, ftp, smtp, etc. Il peut donc modifier les informations à envoyer au serveur, ainsi que celles renvoyées par celui-ci. La contrepartie est qu'il faut un proxy par application. Cependant, beaucoup de proxys sont en fait des multi-proxys qui sont capables de comprendre la plupart des applications courantes.

7.2 – Qu'est-ce qu'un proxy n'est pas ?

Un amalgame est souvent fait entre les fonctionnalités qu'on peut apporter à un proxy, et au proxy lui-même. Ainsi, on pense souvent qu'un proxy doit faire de la NAT, ou serveur de cache, mais ce ne sont que des fonctionnalités ajoutées. Effectivement, il est souvent utile d'ajouter des fonctions de cache à un proxy vu que c'est lui qui centralise l'accès au web. Ainsi, si 15 personnes demandent le même site web, il ne sera chargé qu'une fois puis gardé dans le cache du proxy. D'autre part, la NAT est elle aussi souvent indispensable pour qu'un proxy fonctionne, vu qu'il est censé être un intermédiaire, il faudra qu'il modifie l'adresse source du paquet pour que la réponse passe par lui. Cependant, même si c'est ce qui est le plus souvent utilisé, ce n'est pas obligatoire. Si ces fonctionnalités sont souvent utiles et utilisées, ce n'est pas pour autant qu'il faut penser qu'elles sont synonymes de proxy.

8 – Vaut-il mieux faire de la NAT ou avoir un proxy ?

8.1 – Avantages du proxy

Comme nous l'avons vu, un proxy est dédié à un protocole (une application) particulier. Ainsi, il est capable d'interpréter le trafic et notamment de cacher les informations. On diminue ainsi le trafic et augmente la bande passante de la même occasion. On peut aussi autoriser ou non l'accès à certaines partie d'un site, à certaines fonctionnalités, etc. On a donc un bon contrôle de ce qui transite sur le réseau, et on sait quels protocoles peuvent circuler.

8.2- Avantages de la NAT

Contrairement au proxy, la NAT est indépendante des applications utilisées. On peut donc faire passer la plupart des protocoles que l'ont veut.

8.3 – Alors ? NAT ou proxy ?

La réponse est bien sur… ça dépend !! Vous êtes déçus ? Il ne faut pas, car si vous avez bien lu et compris ce qui précède, vous devriez être en mesure de faire votre choix vous même en fonction de ce que vous avez (adresses, matériel, etc.) et de ce que vous voulez faire (applications, politique de sécurité, etc.). Personnellement, j'ai une petite préférence pour la NAT car elle ne limite pas ce que je peux faire sur le réseau, je n'ai donc pas de mauvaises surprises quand j'utilise un nouveau protocole un peu exotique.

9 – La sécurité et la NAT

9.1 – La NAT dynamique permet-elle d'améliorer ma sécurité ?

La NAT dynamique permet de rendre les machines d'un réseau local inaccessibles directement de l'extérieur, on peut donc voir cela comme une sécurité supplémentaire. Mais cela n'est pas suffisant et il est indispensable d'utiliser un filtrage si l'on veut obtenir un bon niveau de sécurité. La NAT dynamique seule ne peut pas être considérée comme une sécurité suffisante.

9.2 – Est-ce utile pour la sécurité d'utiliser un proxy ?

Un proxy travaille au niveau 7 du modèle OSI, c'est à dire qu'il est capable d'interpréter et de modifier les informations du protocole sur lequel il travaille. Ainsi, il peut vérifier le contenu de ce qui est reçu de la part du serveur et en interdire ou modifier le contenu selon la politique choisie. L'utilisation d'un proxy pour des protocoles critiques est donc souvent utile si on veut avoir une bonne vision de ce qui se passe.

9.3 – La NAT est elle compatible avec IPSEC ?

Si on veut être précis, la réponse est oui. Cependant, la norme IPSEC ayant différentes implémentations, ce n'est pas toujours le cas. D'ailleurs la plupart des constructeurs ont créé leur propres solutions IPSEC pour traverser de la NAT. Le problème vient de l'encryption de l'entête IP par les participants au tunnel IPSEC. Si l'adresse IP est modifiée pendant le trajet du paquet, elle ne sera pas la même à l'arrivée que celle qui a été encryptée au départ, et après comparaison, le paquet sera détruit. Cependant, en se plaçant en mode ESP et en faisant du tunneling, c'est la totalité du paquet qui est encryptée, et une nouvelle entête est ajoutée à celui-ci. Ainsi, la comparaison ne se fera pas sur l'entête modifiée, mais sur celle contenue dans les données du paquet. Mais cette solution n'est pas toujours possible.

Je ne crois pas qu'il existe de norme pour résoudre ce problème, mais une solution semble apporter une réelle satisfaction au problème cité. Elle est aujourd'hui utilisée par beaucoup de constructeurs, la NAT traversal ou NAT-T. Il s'agit d'encapsuler les données dans un tunnel UDP. Ainsi, de la même façon qu'en mode tunnel et ESP, l'entête modifiée par la NAT ne sera pas utilisée pour le test d'authentification. Ainsi, il est souvent possible de mettre en place un VPN IPSEC, même si on utilise de la NAT.

10 – Utilitaires pour faire de la NAT

10.1 – Sous windows

Voici quelques noms de produits qui permettent entre autres de faire de la NAT, une présentation plus précise sera peut-être faite par la suite si cela s'avère utile. Je n'ai pas testés ces produits, vos remarques et expériences sont donc les bienvenues.

Wingate, winroute lite, NAT32, TCPrelay…

10.2 – Sous Unix

IPchains, ipfilter, netfilter…

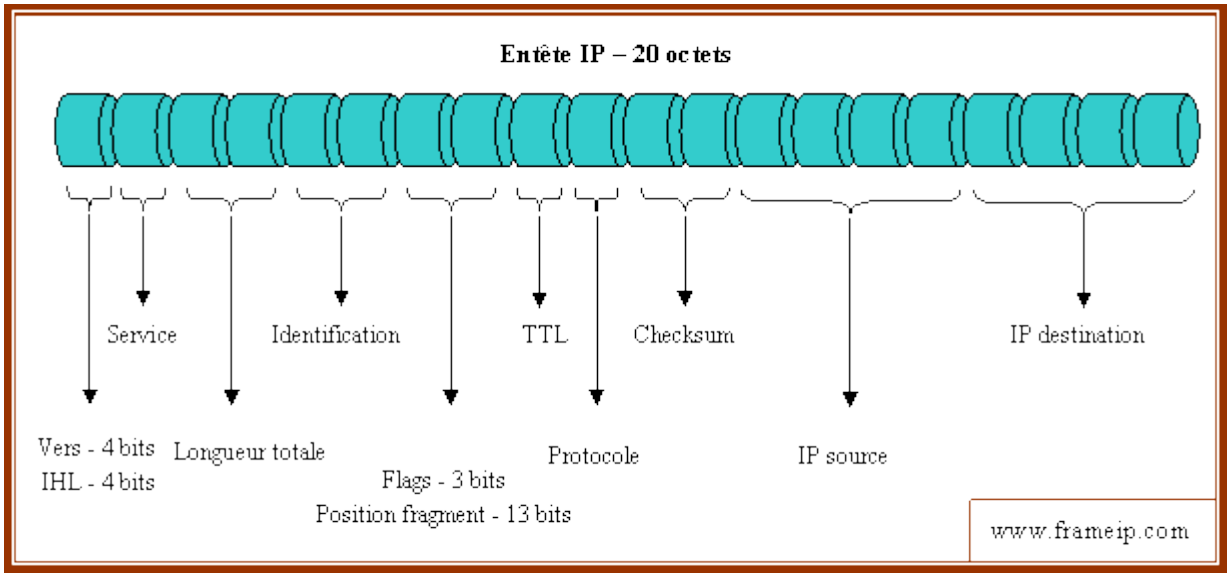
11 – Mini lexique

11.1 – Modèle OSI

Le modèle OSI a été créé dans le but d'uniformiser les réseaux et de permettre l'interopérabilité entre systèmes hétérogènes. Il définit sept couches ayant chacune un rôle spécifique. Ces couches permettent donc de rendre un service les unes par rapport aux autres, tout en étant chacune indépendante des autres.

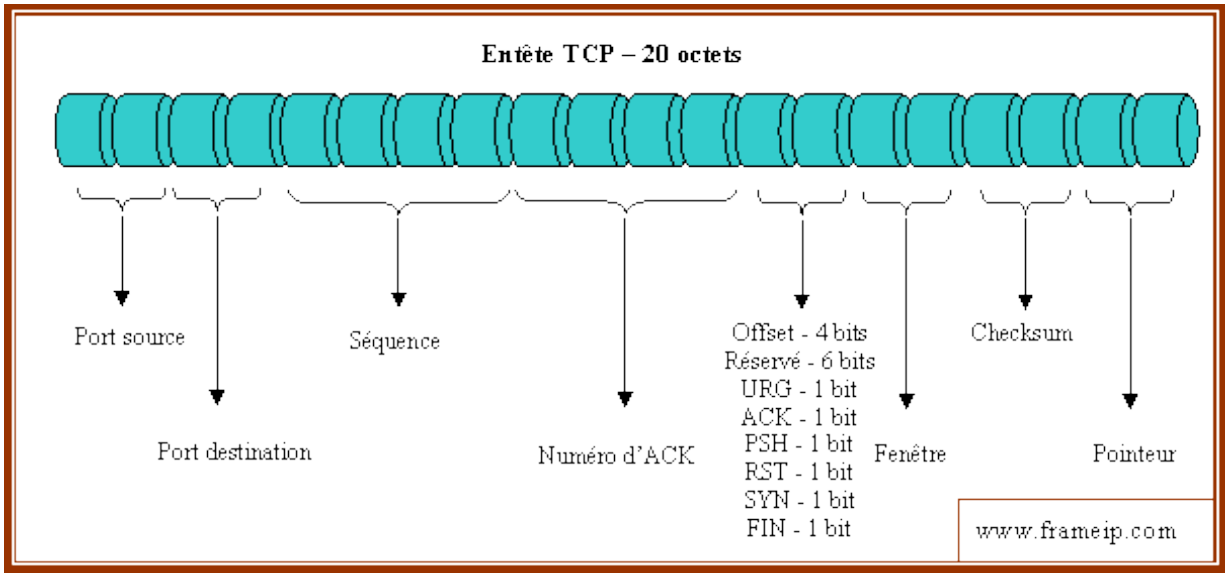
11.2 – IP

IP est un protocole de couche 3 qui permet principalement d'identifier les machines à l'aide d'adresses et de router les informations entre réseaux logiques. Il permet aussi de faire de la fragmentation de paquets. Voici l'entête IP :



11.3 – TCP

TCP est un protocole de couche 4 qui permet d'identifier et de contrôler les connexions entre machines. La gestion des flux et des erreurs est aussi intégrée à ce protocole. Dont voici l'entête TCP :



11.4 – SNAT ou Source NAT

Le Source NAT correspond à la modification de l'adresse source dans un paquet translaté. Il est notamment utilisé pour la NAT dynamique, mais aussi pour la NAT statique lorsqu'on veut sortir du réseau local.

11.5 – DNAT ou Destination NAT

Le Destination NAT correspond à la modification de l'adresse destination dans un paquet translaté. Il est utilisé pour la NAT statique, lorsqu'on veut accéder à un serveur sur un réseau local.

12 – Annexes

12.1 – Ressources utilisées

Je n'ai pas utilisé beaucoup de documents aussi bien en ligne que sur papier. Les réponses et connaissances apportées proviennent en majeure partie des informations que j'ai pu glaner en furetant sur le net, et notamment sur les newgroups fr.comp.reseaux.ip et fr.comp.reseaux.ethernet.

Je me suis quand même inspiré de la RFC 1631. Et notamment de l'excellente faq sur les firewalls de Stéphane Catteau dont je me suis inspiré pour la mise en forme. N'hésitez pas à la consulter, on y apprend plein de choses.

12.2 – Remerciements

Je remercie notamment les personnes suivantes pour leur lecture assidue de la faq durant sa réalisation et leurs conseils précieux. Diane Guinnepain, Pep, Ifragu, Cédric Blancher.

13 – Conclusion

La NAT est aujourd'hui un élément important en réseau étant donné son énorme déploiement à travers le monde suite à l'annonce de la pénurie d'adresses IPv4. J'ai essayé de rendre la compréhension de cette technique la plus accessible possible. Cependant, il faut impérativement avoir quelques notions en réseau pour pouvoir bien comprendre les points délicats qu'elle engendre. Il y a et il y aura sûrement encore beaucoup de choses à dire sur le sujet. Vos remarques sont donc encore et toujours les bienvenues, aussi bien pour y ajouter des idées, que pour enlever le superflu. Maintenant, si je revois passer des questions sur la NAT, j'aurai au minimum un droit de flagellation sur les personnes incriminées.