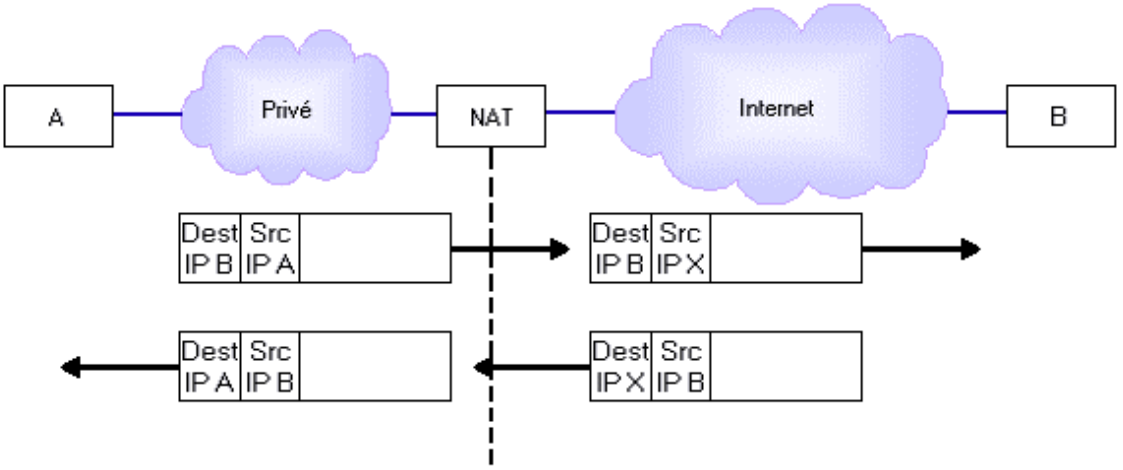
NAT : Network Address Translation

Overview

La technique de translation d'adresses (NAT en anglais, RFC 3022) est une pratique courante qui est apparue à l'origine pour palier au manque croissant d'adresses IPv4 libres. En effet, ces adresses sont codées sur 4 octets et sont du type 0.0.0.0 à 255.255.255.255 (certaines valeurs étant réservées et par conséquence inutilisables); il y a donc peu d'adresses disponibles en comparaison du nombre croissant de machines sur Internet. Il fut donc décidé de réserver des intervalles d'adresses à des usages privés uniquement (RFC 1918). Ce sont les adresses :

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

En conséquence, ces adresses ne sont pas routables sur Internet et ne doivent pas être utilisées par des machines de ce réseau. Par contre, tous les réseaux privés peuvent utiliser ces adresses sans restrictions.
Comme ces adresses ne sont pas routables sur le réseau public, la translation d'adresse est utilisée pour permettre aux machines du réseau privé d'accéder à Internet, et de façon générale à d'autres réseaux. Le principe de base est simple puisqu'il s'agit de remplacer à la volée les champs d'adresses dans les paquets qui sont destinés à un autre réseau (ce qui implique que le NAT soit effectué entre les 2 interfaces réseau, entre le réseau privé et les autres).



Comme le montre le schéma, le NAT va effectuer le remplacement de l'IP source de A par son IP X puis il va router le paquet vers le réseau extérieur. La réponse lui parviendra, et suivant la technique utilisée que nous allons détailler plus loin, il va cette fois-ci modifier l'adresse de destination X pour celle de A sur son réseau privé.

Techniques de translation :

Il existe plusieurs variantes de NAT suivant la topologie du réseau privé, le nombre de machines privées, le nombre d'adresses IP publiques et les besoins en termes de services, d'accessibilité et de visibilité de l'extérieur.

Le NAT de base est statique et attribue de façon automatique une adresse IP à une autre. Aucune information liée à la connexion n'est nécessaire, il suffit de modifier le paquet suivant la règle prédéfinie de translation. L'idéal dans ce cas-ci est d'avoir le même nombre d'IP extérieures que d'IP privées.
Le NAT dynamique ne considère aucune association prédéfinie entre l'IP publique et l'IP privée de la requête qu'il reçoit. Il peut d'ailleurs y avoir plusieurs IP extérieures tout comme il y a plusieurs IP privées. Cela entraine nécessairement un suivi de la connexion car le NAT attribue l'IP extérieure lors de la requête initiale qui provient de son réseau privé; il doit ensuite

pouvoir discriminer les paquets entrants de façon à pouvoir leur attribuer à chacun l'IP correspondante sur le réseau privé (celle de la connexion). Le but étant de rester transparent vis-à-vis de l'ordinateur source ou distant; un problème se pose si l'on ne dispose pas du même nombre d'adresses IP externes que d'adresses privées, car si toutes les adresses externes sont déjà en cours d'utilisation, aucune machine supplémentaire ne pourra accéder au réseau extérieur.

Le NAPT MASQ (Network Address and Port Translation) permet de résoudre le problème cité précédement et s'avère donc particulièrement utile si le nombre d'adresses externes est limité; c'est le cas typique d'une connexion Internet simple où plusieurs machines vont devoir partager la même adresse IP publique (externe).

Le problème technique derrière cette méthode est bien de savoir à quelle machine privée les paquets entrants sont destinés, puisqu'ils ont tous -à priori- la même adresse IP de destination (celle de la passerelle). Pour permettre leur différenciation, le NAT va devoir conserver une trace plus complète des paramètres de chaque connexion de façon établir un véritable contexte pour chacune de ces dernières. Parmi ces critères de séparation, citons :

- l'adresse source est le premier élément qui est regardé; chaque machine du réseau privé aura tendance dans la majorité des cas à communiquer avec une machine extérieure différente. Donc les paquets entrants seront porteurs de cette information et permettront au NAT d'identifier la machine à l'origine de chaque échange. Mais cela ne fonctionnera pas si les machines extérieures ne sont pas toutes différentes.
- le protocole supérieur peut également être régardé par le NAT pour pouvoir identifier le contexte. Ce sera par exemple de l'UDP ou du TCP, et si une machine utilise le premier et une autre utilise TCP, alors le NAT saura retrouver la machine initiale de la connexion.
- le port et d'autres informations liées aux protocoles supérieurs peuvent être utilisés pour identifier chaque contexte. Ainsi le NAT pourra faire la différence entre des paquets entrants qui présentent la même IP source, le même protocole de transport mais un port de destination différent.

Il reste un dernier cas dans lequel tout cela ne suffira pas, c'est celui où les 2 contextes basés sur ces informations sont identiques, c'est-à-dire quand les paquets entrants présentent la même IP source, le même protocole de transport et le même port de destination. Dans ce cas-là, le NAT effectue une translation de port en même temps que d'adresse pour pouvoir identifier les flux de façon certaine. Cela consiste à modifier les paramètres de connexion avec la machine distante de façon à utiliser le port voulu sur la passerelle où se situe le NAT. Cette opération reste transparente pour la machine locale (privée) puisque cela est effectué au niveau du NAT qui rétablit ensuite les paramètres initiaux pour cette machine.

Comme il existe 65535 ports disponibles (moins les 1024 réservés), cela laisse une grande marge de sécurité. La dénomination MASQ provient du fait que cette opération est comparable à une attaque du type man-in-the-middle sauf qu'elle ne vise pas à obtenir quelqu'information que ce soit (la législation à ce niveau est stricte, voir les recommandations de la CNIL).

Le NAPT Redirect/Port Forwarding est identique au précédent sauf qu'il présente des services additionnels de redirection des flux entrants ou sortants. Ainsi, le Port Forwarding permet à l'extérieur d'accéder à un service (serveur WEB ou autre) qui est en fait basé sur une machine de réseau privé : la machine distante pense communiquer avec la machine hébergeant le NAT alors qu'en fait celui-ci redirige le flux vers la machine correspondant réellement à ce service. Le Redirect permet quant à lui de rediriger les flux sortants vers des services particuliers commes des proxies, firewalls, etc...

Le Bi-directional NAT diffère des précédents puisqu'il permet à des machines distantes d'accéder à des machines du réseau privé, et ce directement contrairement au Port forwarding. Le principe fait appel au service DNS pour interpréter les requêtes; celles-ci sont initiées par la machine distante et reçues par le NAT. La passerelle répond par sa propre adresse IP tout en gardant en mémoire l'association entre l'IP distante et l'IP requise pour le service. Ainsi, les paquets provenant de la machine distante seront transférés vers la machine correspondante.

Le problème de cette technique est l'utilisation du service DNS qui peut être couteux dans le cas d'un utilisateur de base accédant au réseau public Internet. Par contre, cette solution pourra se révéler utile dans le cas d'une entreprise interconnectant plusieurs réseaux privés car les serveurs DNS sont alors mieux maitrisés.

Le Twice-NAT est, comme son nom l'indique, une technique de double translation d'adresses et de ports. A la fois les paramètres de destination et ceux de la source seront modifiés. Concrètement, on peut dire que le NAT cache les adresses internes vis-à-vis de l'extérieur ainsi que les adresses externes vis-à-vis du réseau privé. L'utilité de cette technique apparait quand plusieurs réseaux privés sont interconnectés : comme nous l'avons expliqué précédement, les machines doivent utiliser des plages d'adressage bien précises ce qui peut créer des conflits et des collisions entre plusieurs réseaux privés (c'est-à-dire plusieurs machines utilisant la même adresse IP privée). Le Twice-NAT permet de résoudre ces problèmes de collisions en modifiant les 2 adresses du paquet.

Le NAT avec Serveurs Virtuels/Load Balancing est une évolution des techniques de NAT qui permet d'optimiser leurs implémentations. L'utilisation de serveurs virtuels est actuellement très répandue; cela correspond à une machine inexistante représentée uniquement par son adresse IP et prise en charge par une ou plusieurs machines réelles qui ont également leurs propres adresses (différentes). Ainsi, les requêtes des machines distantes sont adressées à une ou plusieurs adresses virtuelles correspondant à la passerelle où est implémenté le démon effectuant le NAT. Celui-ci remplace alors l'adresse virtuelle par une des adresses réelles appartenant aux machines implémentant le service NAT, puis leur transmet la requete et la connexion associée.

La sélection de l'adresse réelle peut se faire sur la base de la charge de travail de la machine correspondante: si le serveur NAT est surchargé, on choisira un autre serveur NAT moins chargé. Cette technique est à la base du load balancing et il existe de nombreux algorithmes de sélection et de répartition de la charge.

Enfin, comme le service NAT est habituellement placé sur la machine chargée du routage, une évolution possible est l'utilisation de routes virtuelles tout comme nous avons vu les adresses virtuelles. Dans ce dernier cas, la passerelle possède plusieurs interfaces vers le réseau externe et peut choisir laquelle utiliser en fonction de la charge de traffic sur chaque brin.

Avantages et inconvénients

N'oublions pas que l'utilité principale du NAT est d'économiser les adresses IP nécessaires pour connecter un réseau à Internet par exemple. Cela s'avère particulièrement utile pour tout particulier possédant une connexion Internet simple (modem, ADSL, cable) avec allocation d'une adresse dynamique. Si ce particulier possède plusieurs machines sur son réseau privé, il pourra utiliser la fonctionnalité de NAT pour partager l'adresse IP de sa machine principale.

D'autre part, les fonctionnalités avancées du NAT permettent d'interconnecter plusieurs réseaux privés de façon transparente même s'il existe des conflits d'adressage entre eux.

Par contre, dans la majorité des techniques citées précédement, la connexion est nécessairement initiée à partir d'une machine locale. Les machines externes ne verront que l'adresse de la passerelle et ne pourront pas se connecter directement aux machines locales; cela est bien sûr résolu avec les techniques plus évoluées de translation, mais celles-ci restent couteuses et peu accessibles.
Enfin, l'opération même de translation peut poser un certain nombres de problèmes que nous allons aborder dans le paragraphe suivant.

Sécurité et NAT

Le NAT présente à la fois des inconvénients et des avantages au niveau de la sécurité pour les machines du réseau privé.

Tout d'abord, comme nous l'avons vu précédement, le NAT n'est pas une opération anodine et ce bien qu'il ait pour vocation d'être transparent. En effet, le NAT modifie les paquets IP et cela a pour conséquence directe de casser tout contôle d'intégrité au niveau IP et même aux niveaux supérieurs puisque TCP par exemple inclue les adresses dans ses checksums! Concrètement, on se rend compte qu'un protocole de sécurisation des datagrammes comme IPSec est totalement incompatible avec le NAT, que ce soit en mode tunneling ou transport (voir fiche IPSec).

Une autre raison simple est qu'un NAT évolué a tendance à remonter les couches pour étudier les protocoles de transport afin de rassembler assez d'informations pour chaque contexte. Tout chiffrement à ce niveau empêcherait donc le NAT de fonctionner, puisque les informations seraient alors cryptées.

Un des avantages du NAT est de protéger les machines du réseau privé d'attaques directes puiqu'elles ne sont en fait pas accessibles de l'extérieur. De plus dans la majorité des cas, les requêtes de connexion ne peuvent provenir que de ces machines privées. Cela permet également de se prémunir contre un monitoring du traffic qui viserait à scruter les communications entre 2 machines particulières, un serveur sur Internet par exemple et une machine du réseau privé. Comme cette dernière n'est plus identifiable, l'opération devient impossible à moins de remonter au niveau applicatif (d'où l'utilité d'utiliser une protection/chiffrement à ce niveau également).

Conclusion

Le NAT est aujourd'hui incontournable dans la plupart des topologies réseau, à partir du moment où l'on souhaite connecter le réseau à d'autres. Comme nous l'avons vu, les techniques correspondant au service NAT ont évolué pour répondre aux besoins croissants de transparence, connectivité, disponibilité, etc... Quoiqu'il en soit, l'utilisation d'une telle technique ne doit pas être prise à la légère car elle implique autant d'inconvénients que d'avantages. Enfin, on peut s'interroger sur la pérennité du NAT sachant que cette technique n'était à l'origine destinée qu'à palier les lacunes d'IPv4. Or, il y a fort à parier qu'elle sera toujours effective avec les nouvelles adresses IPv6, autant à cause de ses qualités de sécurisation que du fait de la lenteur prévisible de la migration des terminaux d'un système d'adressage à l'autre.