La traduction d'adresses (NAT) apporte-t-elle vraiment de la sécurité ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 septembre 2012

https://www.bortzmeyer.org/nat-et-securite.html

Lors des discussions techniques sur la sécurité des réseaux informatiques, on entend très souvent l'affirmation comme quoi la traduction d'adresses (le NAT) apporterait une certaine sécurité au réseau local, bloquant par défaut les connexions entrantes et protégeant ainsi un peu les machines situées derrière. Cet argument a par exemple été souvent cité lors des débats sur le déploiement d'IPv6 (dans ces débats, l'argument pro-NAT est « Avec IPv4, le réseau local dispose d'une certaine sécurité grâce au NAT, qu'il perdrait lors du passage à IPv6 où le NAT est inutile »). Quelle est la part de vérité dans cette affirmation ?

D'abord, un petit rappel pour ceux et celles qui ne connaissent pas bien le NAT. Le nom est déjà une erreur. En effet, ce qui est déployé chez l'écrasante majorité des particuliers, qui accèdent à l'Internet via une "*box*", ce n'est pas du NAT, c'est du NAPT (voir aussi mon article sur le zoo des NAT <https://www.bortzmeyer.org/nats.html>). La différence est énorme en pratique car, avec le NAPT, il y a partage d'adresses IP ce qui n'est pas le cas avec le NAT et cela entraîne une rupture du principe « connexion de bout en bout », qui est à la base de l'Internet. NAT signifie "*Network Address Translation*" et désigne une technique où les machines du réseau local ont des adresses privées, adresses qui sont dynamiquement remplacées par des adresses publiques lors de la traversée d'un routeur NAT. Celui-ci fait la traduction dans les deux sens, vers l'extérieur (remplacement des adresses privées par des adresses publiques) et vers l'intérieur (remplacement des adresses publiques par des adresses privées). Si le NAT peut perturber certains protocoles (qui indiquent l'adresse IP utilisée dans le paquet transmis, ce qui ne marche plus si un routeur réécrit les adresses), il ne pose pas en soi de problème philosophique fondamental. L'Internet pourrait fonctionner avec le NAT (voir le RFC 6296 [1] pour un bon exemple de NAT bien conçu).

Mais ce qui est déployé actuellement sous le nom de NAT n'est **pas** du NAT ! La technique que doivent supporter les utilisateurs de base, chez eux ou dans les petites entreprises ou associations est tout autre chose. Son nom exact est NAPT ("*Network Address and Port Translation*") et, contrairement au NAT, le NAPT a deux énormes défauts :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6296.txt

— Il partage les adresses publiques. Typiquement, en raison de la pénurie d'adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, on n'a qu'une seule adresse publique et **toutes** les adresses privées du réseau interne sont mises en correspondance avec cette unique adresse publique. Cela a des tas de conséquences fâcheuses, détaillées dans le RFC 6269.
— Comme toutes les adresses internes sont fusionnées en une seule adresse externe, comment le routeur NAPT sait-il, lorsqu'un paquet IP revient, à quelle machine interne il est destiné ? Il regarde pour cela le numéro de port qu'il a mémorisé à l'aller. Cela entraine encore d'autres conséquences désagréables, comme la difficulté pour faire marcher les protocoles sans port (par exemple ICMP).

Bon, mais je m'éloigne du sujet, va-t-on me dire, j'avais promis de parler de la sécurité, pas de faire un éreintement du NAPT. Je reviens donc sur le second point : lorsqu'un paquet sort, le routeur NAPT doit traduire {Adresse IP source privée, port source} vers {Adresse IP source publique, autre port source} et se souvenir de la correspondance qui lui permettra, lorsqu'un paquet de réponse reviendra, de trouver vers laquelle des adresses IP privées il doit le diriger. Résultat, un paquet entrant **non sollicité**, qui n'est pas la réponse à un paquet sortant, ne sera pas accepté puisqu'il n'y a aucune entrée dans la table pour lui.

C'est ce point qui est souvent présenté comme un avantage de sécurité. Comme un pare-feu à état, le routeur NAPT ne laisse pas passer les **nouvelles** connexions entrantes. Cela transforme le réseau interne en un réseau purement client, qui ne peut accéder au réseau qu'en consommateur. (Cela perturbe également les services de type pair-à-pair où tout le monde est « serveur », cf. RFC 5128. Vu la diabolisation du pair-à-pair par le puissant lobby de l'industrie du divertissement, ce défaut du NAPT peut plaire à certains...) Mais, disent les partisans de cette configuration minitélienne, cela a des conséquences positives pour la sécurité ; si des machines du réseau interne sont complètement ouvertes à tous vents, pas de problème, le routeur NAPT empêchera le méchant extérieur d'y accéder. C'est d'autant plus important que certains systèmes (Windows...) sont très peu protégés et pourraient être piratés en quelques heures, ne laissant même pas le temps d'installer les "*patches*" nécessaires. (Voir l'excellent article « "*Know your Enemy : Tracking Botnets*" <http://www.honeynet.org/papers/bots/> ».)

Mais les avantages de sécurité du NAPT sont largement exagérés. Voyons en quoi.

Le NAPT a des limites (qui sont aussi celles des pare-feux, malheureusement souvent présentés comme des solutions miracles) :

— Le NAPT ne protège pas contre les attaques effectuées par le contenu (« charge utile ») comme les chevaux de Troie, le virus contenu dans un courrier, le "*malware*" dans une page HTML lue avec IE6...
— Et il ne protège pas contre les attaques venues de l'**intérieur** du réseau, pourtant les plus fréquentes. Rappelez-vous que l'attaquant humain peut être à l'extérieur et quand même lancer une attaque depuis l'intérieur, avec des techniques comme le changement DNS <https://www.bortzmeyer.org/dns-rebinding-pinning.html>.

Il ne manque d'ailleurs pas d'outils automatisant tout cela <http://www.bit-tech.net/news/hardware/2010/04/05/hacker-releases-nat-traversal-tool/1> et permettant à un attaquant de faire une attaque sur un réseau privé situé derrière un routeur NAT.

Aujourd'hui, il y a de moins en moins d'attaques utilisant les connexions réseau, au profit des attaques « charge utile ». C'est logique quand on voit que sur un système récent (j'ai testé avec un Android et un Ubuntu, systèmes conçus pour M. Toutlemonde), il n'y a **aucun** service qui écoute sur l'Internet par défaut. Testez avec nmap :

```
# nmap -6 2a01:e35:8bd9:8bb0:6d07:5fdb:89e9:7d00

Starting Nmap 5.00 ( http://nmap.org ) at 2012-09-16 22:00 CEST
Interesting ports on 2a01:e35:8bd9:8bb0:6d07:5fdb:89e9:7d00:
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
```

(le service SSH a été ajouté explicitement après l'installation, il n'était pas activé par défaut). Bien des services tournaient certes sur cette machine Ubuntu mais tous n'écoutaient que sur les adresses locales à la machine (`127.0.0.1` et `::1`) et n'étaient donc pas vulnérables. Le NAPT n'aurait donc protégé contre rien.

Néanmoins, en matière de sécurité, ce n'est jamais tout blanc ou tout noir. Les programmes qui écoutent sur des ports inférieurs à 1024 sont en général particulièrement sensibles et l'idée de les protéger ne me semble pas mauvaise. On peut donc imaginer des règles plus subtiles que celle du NAPT actuel.

Mais le refus de certains d'abandonner le NAT « pour des raisons de sécurité » n'est pas rationnel, puisque le NAT n'empêche pas ces attaques. Même si on tient à la sécurité qui découle de l'usage du NAPT, rien n'interdit de faire pareil si on n'a pas de NAPT, avec un simple pare-feu avec état (c'est ce que recommande le RFC 6092 pour IPv6.)

Cette question de l'utilisation du NAT (ou plutôt, comme on l'a vu, du NAPT) pour améliorer la sécurité a fait couler beaucoup d'électrons. Parmi tous les articles existants, je préfère :

— « "*Is NAT a security feature ?*" <`http://blog.ioshints.info/2011/12/is-nat-security-feature.html`> »,
— Et bien sûr le RFC 4864, premier à discuter de la question des bénéfices de sécurité du NAT.