

RFC 3424 : IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 Octobre 2007

Date de publication du RFC : Novembre 2002

<http://www.bortzmeyer.org/3424.html>

Le NAT est aujourd'hui une des techniques les plus répandues sur Internet. Motivé à l'origine par le manque d'adresses IPv4, il est devenu tellement répandu que rares sont les utilisateurs qui ne l'ont pas rencontré. Or, le NAT, qui brise le modèle « de bout en bout » qui a fait le succès de l'Internet, est une source sans fin d'ennuis pour les applications et leurs utilisateurs. De nombreuses propositions ont donc été faites pour contourner le NAT et passer malgré lui. Pour que le remède anti-NAT ne soit pas pire que le mal, l'IAB a produit ce RFC, qui explique les contraintes auxquelles doivent se plier toutes les technologies de contournement, spirituellement baptisées UNSAF ("*UNilateral Self-Address Fixing*").

Un protocole UNSAF fonctionne typiquement avec un client situé, pour son malheur, derrière un NAT, et qui communique avec un serveur situé à l'extérieur, pour apprendre sa « vraie » adresse IP, qu'il pourra transmettre à ses pairs.

L'introduction du RFC commence par rappeler les limites de l'exercice. Comme il existe de nombreuses variétés de NAT, aucune solution de la famille UNSAF ne pourra tout résoudre. En outre, le NAT étant un bricolage pour répondre à un problème ponctuel, les solutions anti-NAT ne doivent pas chercher à être pérennes, et à bloquer le déploiement d'une solution propre (IPv6, dont les 2 puissance 128 adresses disponibles dispensent du NAT).

La section 2 du RFC énumère plus précisément les raisons pour lesquelles il n'y aura pas de solution générale. Par exemple, s'il y a plusieurs niveaux de NAT successifs, un client UNSAF doit-il utiliser la première adresse extérieure au NAT le plus proche, ou bien l'adresse la plus éloignée, en comptant qu'elle soit publique ? Un autre problème est le fait que le comportement passé du routeur NAT ne garantit pas son comportement futur. Notons encore que l'introduction d'une nouvelle partie, le serveur UNSAF, rend la communication plus fragile.

La section 3 précise les comportements observés chez les routeurs NAT et leurs conséquences (les RFC 3489¹ ou RFC 4787 sont allés bien plus loin depuis).

Finalement, la section 4 du RFC liste les conditions que devrait satisfaire toute proposition UNSAF :

- Se limiter à un problème à court terme et ne pas essayer d'être trop général,
- Décrire une stratégie de sortie, pour le jour où le NAT ne sera plus utilisé,
- Insister sur le risque de fragilité de la solution UNSAF, si elle introduit des dépendances supplémentaires.

La section 5, sur la sécurité, demande, elle, que la solution UNSAF ne soit pas une occasion pour permettre des traversées du NAT qui n'auraient pas été possibles sans elle.

Tous les RFC sortis depuis se réfèrent donc à celui-ci, en expliquant comment ils répondent aux préoccupations citées (par exemple la section 14 du RFC 3489).

Cinq ans après, ce RFC semble excessivement prudent par rapport aux solutions UNSAF. D'une part, plusieurs d'entre elles, comme STUN sont devenues très répandues et permettent à leurs utilisateurs de passer la plupart des NAT. D'autre part, le rêve d'un déploiement rapide d'IPv6, permettant de se passer rapidement du NAT, ne s'est pas concrétisé. Enfin, les craintes de sécurité ont été relativisées par les analyses montrant que, de toute façon, le NAT n'apporte guère de sécurité réelle.

Le groupe de travail Behave <<http://www.bortzmeyer.org/behave-wg.html>>, créé depuis a donc, logiquement, passé plus de temps à normaliser ce qu'un système NAT doit faire, plutôt que de limiter ce que peut faire un système anti-NAT.

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc3489.txt>