RFC 7857 : Network Address Translation (NAT) Behavioral Requirements Updates

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 avril 2016

Date de publication du RFC : Avril 2016

http://www.bortzmeyer.org/7857.html

Le mécanisme de traduction d'adresses IPv4 connu sous le nom de NAT (et qui devrait plutôt être appelé NAPT pour "*Network Address and Port Translation*", car il ne se contente pas de traduire les adresses IP) cause beaucoup de problèmes, car il casse le modèle normal de fonctionnement d'IP, modèle de bout en bout. Pour limiter les problèmes dus à ce mécanisme, plusieurs RFC posent certaines exigences que doivent respecter (en théorie) les routeurs NAT. Ce nouveau document met à jour certaines de ses exigences. Il met donc légèrement à jour les règles des RFC 4787 [1], RFC 5382 et RFC 5508.

Ce RFC de maintenance ne s'applique qu'au « NAT44 » traditionnel, où une adresse IP publique n'est partagée que par les membres d'un même foyer, ou bien les employés d'une même entreprise. Pour le CGN, les exigences sont dans le RFC 6888.

D'abord, le suivi de connexions TCP (section 2 du RFC). Notre RFC formalise rigoureusement la machine à états que doit suivre un routeur NAT (elle est proche de celle du RFC 6146). Le RFC 5382 spécifiait bien des délais pour certains états mais sans décrire précisement la machine complète. Par exemple, l'exigence 5 du RFC 5382 donne un délai pour le temps minimum d'attente avant de considérer une connexion partiellement ouverte, ou fermée, comme abandonnée, mais il n'était pas clair si ces deux cas devaient avoir le même délai. Notre RFC tranche donc : le cas des connexions partiellement ouvertes et celui des connexions fermées sont différents et les délais devraient pouvoir être configurés différemment.

Et les paquets TCP `RST` ("*ReSeT*"), on en fait quoi ? Notre RFC précise clairement (suivant ce que faisait déjà le RFC 6146) qu'un paquet RST doit être considéré comme détruisant la connexion TCP et

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4787.txt`

donc comme mettant fin à la correspondance dans le routeur NAT (après un délai, pour tenir compte du fait que le paquet `RST` a pu être reçu par le routeur NAT mais pas par la machine terminale). Attention, il faut d'abord vérifier que ce paquet `RST` correspond bien à une connexion existante, sinon, on permet des attaques par déni de service faciles (RFC 5961).

Les RFC 4787 et RFC 5382 précisaient qu'on pouvait utiliser le même couple {adresse IP externe, port externe} pour des connexions allant vers des machines extérieures différentes. Mais ils ne traitaient que du cas où il n'y avait qu'une machine interne qui allait vers ces machines extérieures. Désormais, on précise (section 3 de notre RFC) que cette utilisation est également valables si plusieurs machines internes se connectent. Sans cette règle, il faudrait beaucoup plus de ports externes disponibles, ce qui poserait un problème avec les environnements où le facteur de partage d'adresses est important (cf. RFC 6269).

Est-ce qu'un routeur NAT doit/peut utiliser les mêmes correspondances pour UDP et TCP (section 5 de notre RFC) ? Ce n'est pas précisé dans les RFC 4787 (exigence 1) et RFC 5382 (exigence 1). On fait une connexion TCP sortante, est-ce qu'un paquet UDP sortant va réutiliser la même correspondance ? La règle est désormais explicite : non, il ne faut pas ; par défaut, les correspondances doivent être spécifiques à un protocole (donc, différentes pour UDP et TCP).

Autre piège du NAT, le fait qui peut parfois changer une distribution aléatoire des ports en une distribution prévisible. Cela pose un problème pour certaines méthodes de sécurité qui dépendent du caractères imprévisible (par exemple le RFC 5452). Notre RFC reprend (section 9) une recommandation de la section 4 du RFC 6056 : un routeur NAT ne doit pas choisir les ports de sortie de manière prévisible ou régulière.

Comme d'habitude, la fragmentation est une source d'ennuis (section 10). Notre RFC rappelle donc qu'il faut suivre les règles de la section 5.3.1 du RFC 6864, notamment sur le caractère unique et imprévisible de l'identificateur de fragment.

Le routeur NAT voit parfois passer des paquets en « épingle à cheveux » (”*hairpinning*”). Cela désigne les paquets (section 12) qui, venus du réseau interne, y retournent, après être passés par le routeur. Si le réseau interne est `172.17.42.0/24`, et qu'un serveur HTTP est sur la machine `172.17.41.1` et accessible de l'extérieur en `192.0.2.71`, alors, une machine interne qui tente d'aller en `http://192.0.2.71/` va envoyer des paquets qui iront au routeur NAT, prendront un virage en épingle à cheveux et reviendront dans le réseau interne, vers `172.17.41.1`. Historiquement, pas mal de routeurs NAT étaient incapables de gérer ce cas. La situation est désormais meilleure mais il reste des cas limites. Ainsi, l'exigence 7 du RFC 5508 devait rappeler que le virage en épingle à cheveux était possible même en ICMP. Notre RFC insiste sur le respect de cette règle.

Enfin, la sécurité (section 13). Notre RFC estime que ses exigences renforcées vont améliorer la sécurité. Par exemple, des règles strictes (sections 7 et 11) sur la suppression des correspondances dans la table du routeur NAT évitent qu'un attaquant puisse garder ouvertes des correspondances qui devraient être fermées (et la mémoire récupérée). Les règles sur les ports sources imprévisibles de la section 9 rendront (entre autres) plus difficile le suivi des machines situées derrière un routeur NAT.

Notez enfin qu'il y a des gens qui prétendent avoir un brevet sur certaines de ces recommandations `<https://datatracker.ietf.org/ipr/1917/>`...