Échec de RPZ à l'IETF

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 janvier 2021

https://www.bortzmeyer.org/echec-rpz.html

RPZ ("*Response Policy Zones*") est une technologie permettant de configurer les mensonges d'un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html>. Il était prévu de la normaliser à l'IETF mais le projet a finalement échoué. Pourquoi ?

Un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> est censé transmettre fidèlement les réponses envoyées par les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>. S'il ne le fait pas, on parle de résolveur menteur <https://www.bortzmeyer.org/censure-francaise.html> ou, pour employer le terme plus "*corporate*" du RFC 8499[1], de « résolveur politique ». De tels résolveurs menteurs sont utilisés pour de nombreux usages, du blocage de la publicité (par exemple avec Pi-hole) à la censure étatique ou privée. L'administrateur d'un tel résolveur menteur peut configurer la liste des domaines où un mensonge sera fait à la main. Mais c'est évidemment un long travail que de suivre les changements d'une telle liste. Il peut être préférable de sous-traiter ce travail. RPZ ("*Response Policy Zones*") est conçu pour faciliter cette sous-traitance.

Pour les principes techniques de RPZ, je vous laisse lire mon article technique <https://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html>, ou bien regarder le site « officiel » <https://dnsrpz.info/>. RPZ est mis en œuvre dans plusieurs logiciels résolveurs comme BIND, Unbound (depuis la version 1.10, cf. cet article <https://medium.com/nlnetlabs/response-policy-zones
ou Knot <https://www.knot-resolver.cz/>.

Comme RPZ est là pour permettre la communication entre le fournisseur de listes de mensonges et le résolveur, il serait intéressant techniquement qu'il soit normalisé. Un effort a donc été fait à l'IETF pour cela. Sur l'excellent "*DataTracker*" <https://datatracker.ietf.org/> de l'IETF, vous pouvez suivre l'histoire de ce projet depuis 2016 <https://datatracker.ietf.org/doc/draft-vixie-dnsop-dns-r
> : d'abord une contribution individuelle, draft-vixie-dns-rpz, puis après adoption par un groupe de travail de l'IETF, une version de groupe (qu'on reconnait à son nom commençant par draft-ietf-NOMDUGROUPE),

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8499.txt

draft-ietf-dnsop-dns-rpz puis, après une interruption d'une année, à nouveau un retour à la contribution individuelle, draft-vixie-dnsop-dns-rpz, finalement abandonnée depuis aujourd'hui plus de deux ans.

Pourquoi cet échec ? Notez d'abord que l'IETF ne documente pas explicitement les échecs. Il n'y a pas eu de décision officielle « on laisse tomber », avec un texte expliquant pourquoi. Il s'agit plutôt d'un document qui a eu à faire face à tellement de problèmes que plus personne n'avait envie de travailler dessus.

Quels étaient ces problèmes ? Commençons par le plus gros, le problème politique. Beaucoup de gens ne sont pas d'accord avec la censure faite via le DNS et craignaient que RPZ n'aide les méchants davantage que les gentils. À ce problème politique (tout le monde n'étant pas d'accord sur la légitimité de la censure) s'ajoutait un problème classique lors des débats politico-techniques, celui de la neutralité de la technique (j'en ai parlé dans mon livre <https://cyberstructure.fr/>, p. 148 et suivantes de l'édition papier). Le débat est récurrent à l'IETF et peut se simplifier en deux positions opposées :

— Nous normalisons juste des techniques, les gens peuvent ensuite les utiliser pour le bien ou pour le mal <https://www.bortzmeyer.org/internet-est-il-de-gauche.html> et, de toute façon, si l'IETF ne normalise pas cette technique dans un RFC, elle sera utilisée quand même, et peut-être normalisée par des organismes moins scrupuleux comme l'UIT.
— Nous ne pouvons pas nier les conséquences des décisions que nous prenons (RFC 8890), tout est politique (RFC 8280), et un RFC sera interprété comme une approbation ou quasi-approbation par l'IETF.

Pris entre ces deux positions, le document a ainsi été adopté par le groupe de travail DNSOP <https://datatracker.ietf.org/wg/dnsop/>, puis abandonné, après de longues et parfois vigoureuses discussions.

Une autre raison de la non-normalisation de RPZ est peut-être le fait qu'en pratique, ce protocole n'a été adopté que par des acteurs commerciaux. Je n'ai pas trouvé de flux RPZ librement accessible, par exemple avec une liste de domaines liés à la publicité (ce serait bien pratique pour les bloquer). Peut-être ? Mais, s'ils ont bien le format RPZ, ils ne rendent pas ces flux accessibles en AXFR, ce qui complique leur mise à jour.

Un problème supplémentaire est également survenu dans la discussion : le contrôle du changement. Normalement, une fois un protocole publié par l'IETF, c'est l'IETF qui gouverne les évolutions futures. Or, ici, les auteurs originaux de RPZ avaient écrit dans le document qu'ils gardaient le contrôle et pouvaient donc empêcher telle ou telle évolution de la norme. En contradiction avec les règles de l'IETF, cette mention a contribué à l'échec de RPZ dans le groupe de travail. Il aurait quand même pu être publié en RFC non-IETF mais le projet est finalement mort d'épuisement.