RPZ, un moyen simple de configurer un résolveur DNS BIND pour qu'il mente

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 mars 2011

http://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html

---

L'exposé le plus controversé lors de la réunion OARC <https://www.dns-oarc.net> de San Francisco était, le 14 mars, celui intitulé simplement « DNS RPZ, Rev 2 », par Paul Vixie (voir ses transparents <https://www.dns-oarc.net/files/workshop-201103/rpz2.pdf>). En effet, traditionnellement, le résolveur DNS BIND servait exactement ce que lui avait envoyé les serveurs faisant autorité. BIND ne **mentait pas**. Les gens qui voulaient des mensonges (par exemple renvoyer l'adresse IP d'un serveur à eux au cas où le domaine n'existe pas) devaient modifier BIND (ce qui était toujours possible, puisque BIND est un logiciel libre mais pas forcément très pratique). Désormais, avec le système RPZ ("*Response Policy Zone*"), BIND peut mentir.

Cette fonction a été ajoutée à partir de la version 9.8.0, sortie le 1er mars. RPZ est un mécanisme de configuration du mensonge dans le résolveur <http://www.bortzmeyer.org/dns-menteur.html>. Il peut être utilisé pour le cas ci-dessus (fausse adresse en cas de domaine non existant) ou, comme le signalent sans pudeur les « "*release notes*" », pour la censure de l'entreprise <http://www.lemonde.fr/technologies/article/2011/03/18/le-filtrage-d-internet-deja-une-realite-dans-l1478252_651865.html> ou de l'État (comme en Chine ou en Loppsiland).

Comment fonctionne RPZ ? Une zone RPZ est une zone DNS normale (on peut donc la distribuer par les mécanismes habituels du DNS, comme par exemple le transfert de zones du RFC 5936 [1]) contenant des règles sur les réponses à donner. Les règles peuvent porter sur la requête (noirlister tous les domaines en send-me-spam.biz ou illegal-gambling.cn) ou sur la réponse.

Du fait du mécanisme de distribution, on verra donc sans doute des fournisseurs de zones RPZ, comme il existe des fournisseurs de listes noires DNS pour la lutte anti-spam. Ainsi, la place Beauveau

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5936.txt

créerait une zone des domaines qui déplaisent au gouvernement, dont les résolveurs des FAI français seraient esclaves. Il ne sera plus possible de retarder de telles demandes en disant « Le logiciel ne sait pas faire ». Notons au passage que ce n'est pas un cas théorique : la LOPPSI est normalement réservée aux cas de pédopornographie mais, si son article 4 prévoit que la décision de mettre un site sur la liste noire est prise par le gouvernement et non pas par un juge indépendant, cela ne peut être que pour une seule raison : étendre discrètement la liste des cas pour laquelle on est mis sur la liste noire. Toujours pour le cas français, notons aussi que l'ARJEL a déjà plusieurs fois envoyé des injonctions aux FAI <http://www.zdnet.fr/actualites/l-arjel-veut-imposer-aux-fai-francais-le-filtrage-d-un-site-e
htm> de barrer l'accès à tel ou tel site de jeux illégal, et que donc la censure ne concerne déjà plus exclusivement la pédopornographie (les intérêts de l'industrie du jeu sont puissants). Des TLD entiers, s'ils sont contestés par certains (comme `.xxx` ou `.ru`) pourraient être victimes de filtrage volontaire.

RPZ peut évidemment être utilisé pour le bien ou pour le mal et Vixie n'a pas manqué de prévenir les critiques en exposant lui-même tous les défauts et les risques de RPZ. Les avantages sont la capacité à bloquer, par exemple, des domaines de hameçonnage (ou des domaines commerciaux inutiles et dangereux comme `google-analytics.com` dans l'exemple plus bas). Les inconvénients sont l'utilisation par la censure mais aussi (point signalé, et à juste titre, par Vixie) la moins grande résilience du DNS <http://www.bortzmeyer.org/eteindre-internet.html> du fait de l'introduction d'un nouveau composant. On peut imaginer d'avance la prochaine grande bogue : un fournisseur RPZ bloque tout `*.fr` par erreur et tous les FAI automatiquement appliquent cette règle...

Passons maintenant à l'utilisation pratique. Comme indiqué, il faut au moins BIND 9.8.0. Quelqu'un doit créer une zone RPZ. Dans tous les exemples ci-dessous, cette zone se trouve sur le même serveur, qui est maître. Dans la réalité, le résolveur sera souvent un esclave, soit d'un maître placé dans la même organisation (centralisation de la censure au niveau d'une entreprise), soit situé à l'extérieur. Dans ce dernier cas, le serveur maître pourra être au gouvernement, dans le cas de la Chine ou de la France, ou bien chez un fournisseur privé de RPZ, comme il existe des fournisseurs privés de DNSBL. (Un point en passant : je sais bien qu'une censure via le DNS est peu efficace, car relativement facile à contourner. Mais la censure ne vise pas à marcher à 100 % : elle vise simplement à rendre les choses pénibles pour la majorité des utilisateurs, qui ne connaissent pas forcément les techniques de contournement).

Cette fourniture des zones RPZ par des organisations extérieures posera probablement les mêmes problèmes qu'avec les listes noires anti-spam d'aujourd'hui : listes gérées par des cow-boys qui vous mettent sur la liste noire pour un oui ou pour un non, listes où on est facilement enregistrés mais jamais retirés, etc.

Revenons à BIND. Pour indiquer que je veux utiliser la RPZ, je dois donner le nom de la zone qui contient les règles de filtrage (ici, `loppsi.gouv.fr`) :

```
options {
        ...
        response-policy { zone "loppsi.gouv.fr"; };
};
```

Et on doit ensuite indiquer où trouver la zone en question. Ici, pour faciliter les tests, le serveur DNS est également maître pour la zone :

```
zone "loppsi.gouv.fr" {
      type master;
      file "loppsi.gouv.fr";
      allow-query {none;};
};
```

La dernière directive, interdisant l'accès direct à la zone, est là pour respecter la LOPPSI, où la liste des sites filtrés n'est pas publique (pour éviter que les citoyens ne puissent la contrôler).

Le contenu de la zone lui-même suit la syntaxe décrite dans la documentation de BIND, dans la section « "*Response Policy Zone (RPZ) Rewriting*" ». Par exemple, pour qu'un nom soit présenté comme non-existant, on met un enregistrement de type CNAME et de valeur `.` (juste un point). Je n'ai pas trouvé de mécanisme simple pour appliquer le traitement à tout l'arbre sous le nom et la documentation ne semble pas en parler. Apparemment, il faut indiquer séparement l'apex et les sous-domaines (avec le caractère `*`, le joker). Imaginons donc qu'on veuille bloquer Google Analytics, système qui non seulement ralentit les accès au site mais en outre est dangereux pour la vie privée : en visitant un site qui n'a rien à voir avec Google, vous donnez des informations à cette entreprise. Bloquons donc ce domaine :

```
; Beginning of the zone, some mandatory values
$TTL 1H

@   SOA gueant.interieur.gouv.fr. root.elysee.fr (2011031800 2h 30m 30d 1h)
    NS gueant.interieur.gouv.fr.

; Filtering rules
; NXDOMAIN will be sent back
google-analytics.com         CNAME   .
*.google-analytics.com         CNAME   .
```

Testons le serveur ainsi configuré, faisons d'abord une vérification avec un résolveur non-menteur :

```
% dig A google-analytics.com
...
;; ANSWER SECTION:
google-analytics.com. 300 IN A 74.125.224.52
google-analytics.com. 300 IN A 74.125.224.48
...
```

Puis essayons avec le résolveur menteur, qui écoute sur le port 9053 de la machine `localhost` :

```
% dig @localhost -p 9053 A google-analytics.com
...
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 20660
...
;; AUTHORITY SECTION:
loppsi.gouv.fr. 3600 IN SOA gueant.interieur.gouv.fr. root.elysee.fr.loppsi.gouv.fr. 10 3600 900 2592000 7200
```

C'est parfait. BIND a répondu que le domaine n'existe pas (`NXDOMAIN`) et a même donné les coordonnées du responsable (le filtrage n'est donc pas caché).

On peut mettre dans la zone RPZ d'autres choses. Par exemple, on peut vouloir une réponse `NOERROR`, `ANSWER=0` au lieu du `NXDOMAIN` :

```
; NOERROR, ANSWER=0 will be sent back
enlarge-your-penis.biz           CNAME   *.
*.enlarge-your-penis.biz         CNAME   *.
```

Et on a bien le résultat attendu :

```
% dig @localhost -p 9053 A buy.enlarge-your-penis.biz
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49450
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

Et si on veut un mensonge encore plus gros, renvoyer l'adresse IP d'un de ses serveurs à la place de la vraie ? On peut :

```
; Replace the address by ours
; Since we provide only a AAAA, A queries will get NOERROR,ANSWER=0
ads.example.net             AAAA 2001:db8::1
```

Ce qui fonctionne :

```
% dig @localhost -p 9053 AAAA ads.example.net
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63798
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
...
;; ANSWER SECTION:
ads.example.net. 3600 IN AAAA 2001:db8::1
```

Il peut être intéressant de mettre une règle générale et d'autoriser ensuite des exceptions. Supposons qu'on veuille défendre la langue française en ne permettant que la consultation du Wikipédia francophone. On met alors une règle générale pour `wikipedia.org` puis une exception pour `fr.wikipedia.org`, ce qui se fait en mettant un `CNAME` vers le domaine lui-même :

```
; Language-enforcement policy: no access to Wikipedia except the
; French-speaking one
wikipedia.org          CNAME .
*.wikipedia.org          CNAME .
; and the exception:
fr.wikipedia.org        CNAME fr.wikipedia.org.
```

Dans tous les exemples précédents, on procédait à la réécriture en fonction de la **question** posée. Mais BIND permet aussi de réécriture selon la **réponse**. Cela se fait en encodant l'adresse IP (et la longueur du préfixe) dans le nom et en la mettant dans le sous-domaine `rpz-ip`. Imaginons qu'on veuille bloquer toutes les réponses lorsque l'adresse IP est dans `192.0.2.0/24` :

```
; Forbidding answers that are the documentation prefix, 192.0.2.0/24
24.0.2.0.192.rpz-ip      CNAME   .
```

Voilà, vous savez l'essentiel désormais. N'oubliez pas, comme aime à le dire Spider-Man, qu'un grand pouvoir implique de grandes responsabilités...

Un bon article en anglais sur le même sujet est « *"How to configure your BIND resolvers to lie using Response Policy Zones (RPZ)"* <`http://jpmens.net/2011/04/26/how-to-configure-your-bind-resolvers-`> ». L'ISC maintient aussi une liste de liens utiles <`https://deepthought.isc.org/article/AA-00525/0/Building-DNS-Firewalls-with-Response-Policy-Zones-RPZ.html`>.

Un des premiers fournisseurs à distribuer sa liste noire via RPZ est Spamhaus. Un autre est SURBL.
