Le point sur le filtrage DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 octobre 2011

https://www.bortzmeyer.org/dns-filtering.html

À la réunion DNSEASY/SSR <https://www.icann.org/en/security/agenda-dns-ssr-symposium-20oct1
htm> d'octobre 2011 à Rome, une intéressante table ronde portait sur le filtrage du DNS. C'est l'occasion de faire le point sur cette pratique. La réunion ne cherchait pas à obtenir un accord unanime, ni des solutions magiques, mais au moint à définir et délimiter le phénomène.

Comme la réunion se tenait sous la règle de Chatham House, je ne dirai pas ici qui a dit quoi.

Donc, le filtrage DNS est cette pratique qui consiste à substituer aux réponses normales des vrais serveurs DNS des mensonges, de façon à empêcher un utilisateur de communiquer avec les serveurs du domaine filtré. Il est utilisé en entreprise (pour empêcher les employés de regarder Facebook, par exemple) et par les États.

Les points étudiés étaient :

— Aspects politiques, juridiques et éthiques du filtrage (mais rappelez-vous que la majorité des participants étaient des techniciens),
— Efficacité du filtrage (diminue-t-on le nombre de lecteurs de Copwatch <http://www.pcinpact.com/actu/news/66409-refere-ordonnance-copwatch-blocage.htm> en le filtrant ?),
— Conséquences pour DNSSEC (beaucoup d'opposants au filtrage font remarquer qu'il contredit directement une de nos principales techniques de sécurité),
— Effets techniques secondaires (par exemple sur la résilience),
— Effets non-techniques secondaires.

Sur le premier point, l'aspect politique (au sens large), l'accord s'est fait sur l'importance de distinguer **qui** demande le filtrage. Il peut y avoir :

— du filtrage auto-infligé (je bloque google-analytics.com sur mon résolveur car je ne veux pas laisser de trace de ma navigation chez Google). Le consensus est que c'est normal, de même qu'un citoyen a le droit de refuser de lire des livres dont les idées ne lui plaisent pas.
— du filtrage décidé par un prestataire (par exemple le FAI) « pour votre propre bien » (difficile de savoir si c'est le cas, très peu de FAI documentent leur politique).

— un filtrage décidé pour vous par votre employeur (dans un pays comme la France, la légalité de ce filtrage reste toujours à discuter ; mais il ne fait pas de doute que la pratique est répandue, voir par exemple comment une employée parle des problèmes avec le filtrage de sa boîte <http://www.numerama.com/magazine/11879-kosciusko-morizet-teste-le-filtrage-du-net-en-avant-p
html>),
— un filtrage imposé par l'État, que ce dernier soit une dictature (cas de la Chine) ou une démocratie (de nombreuses démocraties filtrent, et il n'y a pas de différence technique avec ce que fait le gouvernement chinois).

Bien sûr, il y a des tas de zones grises. Ainsi, lorsque OpenDNS <https://www.bortzmeyer.org/opendns-non-merci.html> prétend que leur système est "*opt in*" et donc politiquement correct, ils oublient de préciser que, si l'administrateur réseaux d'une école choisit de configurer le relais DNS pour interroger OpenDNS, les enseignants vont être filtrés sans l'avoir demandé... Même chose pour les enfants, mais ils sont mineurs donc le problème est encore différent. À propos d'enfants, un participant a demandé si le cas de l'entreprise était analogue à celui de la famille (où les parents peuvent décider de filtrer ce que peuvent voir leurs enfants) ; les employés sont-ils majeurs ? (En système capitaliste, la réponse est clairement non, l'entreprise n'est pas une démocratie.)

Le cas du filtrage par un prestataire est pour moi nettement un problème de violation de la neutralité du réseau <https://www.bortzmeyer.org/neutralite.html>. Toutefois, beaucoup de participants au débat ont refusé de poser le problème en ces termes car ce débat sur la neutralité est très chargé. Il pose pourtant les mêmes questions : information du client (les FAI qui filtrent, par exemple le port 53 <https://www.bortzmeyer.org/port53-filtre.html>, ne le documentent jamais), et possibilité réelle de changer (la concurrence est souvent insuffisante, par exemple parce qu'il n'existe pas de FAI alternatif, ou bien tout simplement tous les FAI se sont mis d'accord, comme pour les opérateurs mobiles en France qui interdisent tous la voix sur IP).

Certains prestataires se défendent en affirmant que ce filtrage est demandé (ou en tout cas accepté) par la grande majorité de leurs clients (comme disait Camus, « Quelque chose en leur âme aspire à la servitude »). Même si c'est vrai (tout le monde parle de Mme Michu, mais personne ne lui demande jamais son avis), l'opinion dominante était que cela ne change rien : si 0,1 % des clients ne veulent pas de filtrage, ils doivent pouvoir y arriver, par exemple par un système d'"*opt-out*" clair et gratuit. Notez, opinion personnelle, que cela finirait par créer un Internet à deux vitesses, un filtré pour la majorité des citoyens, et un libre pour les 0,1 % de "*geeks*" qui cliqueront sur l'option « "*I know what I do, I understand that I may lose hair, be hacked and see awful things, and I accept the responsability*" » pour désactiver le filtrage.

Un autre cas présenté comme acceptable a été celui d'un FAI qui se vante de fournir du filtrage, comme étant un service. Puisqu'on était à Rome, l'intervenant a pris comme exemple un FAI catholique affirmant qu'il filtrait l'accès à tout ce qui n'était pas approuvé par le Vatican. Le débat sur cette offre est rigolo, mais cet exemple est purement théorique. Comme je l'ai indiqué, les filtreurs n'annoncent jamais qu'ils le font, et un tel FAI n'existe pas (quoiqu'il trouverait peut-être des clients au fin fond des États-Unis).

Une anecdote révélatrice ici : la conférence se tenait dans les locaux de la Poste, qui pratique un filtrage sino-saoudien. Tout utilisateur doit être nommément identifié **et** l'Internet est peu accessible : seuls les ports 80 et 443 sont ouverts (le port 53 est filtré, donc pas question de contourner les résolveurs DNS officiels). Le port 443 a un système de DPI qui envoie des "*resets*" TCP dès qu'il détecte quelque chose qui n'est pas du TLS (par exemple du SSH). Or, quelles que soient leurs opinions sur la légitimité ou non du filtrage (on est dans les locaux de la Poste, on doit accepter leurs règles), la totalité des participants, au lieu d'écouter les exposés, a passé l'essentiel de la première matinée à mettre au point et à déployer (au besoin en créant des comptes pour les voisins) des systèmes de contournement. Pour les gens qui défendaient la légitimité du filtrage, c'était un bonne illustration du principe « le filtrage, c'est pour les autres ».

---

https://www.bortzmeyer.org/dns-filtering.html

Le deuxième point étudié concerne l'efficacité du filtrage. S'il attente aux libertés, est-il au moins efficace ? (Et, question encore plus vicieuse, cette efficacité justifie-t-elle son coût ?) La question est complexe. Bien sûr, pour une minorité de "*geeks*", la question ne se pose pas. Ils trouveront toujours, et souvent assez facilement, un moyen de contourner le filtrage (comme l'a montré l'affaire Copwatch où les miroirs de secours <http://www.pcinpact.com/actu/news/66251-copwatch-effet-streisand-censure-blocage.htm> sont apparus avant même le jugement). Mais cela s'appliquera-t-il aux utilisateurs moins avertis, aux M. et Mme Toutlemonde ? Peut-être pas (sauf si quelqu'un fait un logiciel simple qui met en œuvre les mesures d'évitement). Notez bien que le gouvernement répressif ne cherche pas forcément une efficacité à 100 %. Qu'une poignée de types dans leur garage contournent le filtre n'est pas forcément un problème. D'autant plus que, souvent, le gouvernement ne cherche pas d'efficacité du tout, il veut simplement faire du théâtre et donner l'impression qu'il agit.

Dans le cas où le filtrage est « auto-infligé » (par exemple parce qu'un utilisateur essaie de se prémunir contre la possibilité d'une vision accidentelle d'images qui le choqueraient), la question de l'efficacité ne se pose pas. Celui qui a voulu le filtrage ne va évidemment pas essayer de le contourner. Dans le cas où le filtrage est réellement mis en place pour protéger l'utilisateur (par exemple contre le "*malware*"), l'efficacité a des chances d'être assez bonne, tant que le filtrage n'énerve pas l'utilisateur, le motivant assez pour chercher un contournement. Et dans le cas d'un filtrage obligatoire par l'État ? Si l'État n'est pas trop méchant, l'efficacité du filtrage est faible. On a bien vu, selon un classique effet Streisand, que Copwatch était beaucoup plus lu après la plainte de Guéant qu'avant, où ce site était quasiment inconnu. Si l'État est prêt à cogner, les choses sont différentes. Si on contourne moins le filtrage en Chine qu'en France, c'est parce que le gouvernement chinois a d'autres moyens de persuasion à sa disposition. C'est d'ailleurs une leçon classique en sécurité, bien illustrée par un dessin de XKCD <http://xkcd.com/538/>.

Comme la grande majorité des participants était composée de technophiles, la question des liens entre le filtrage DNS et DNSSEC était inévitable. En effet, le filtrage DNS dans les résolveurs va invalider les signatures DNSSEC et sera donc détecté. À première vue, le filtrage va donc en opposition directe à la tentative de sécurisation du DNS qu'est DNSSEC.

En fait, le problème est plus complexe que cela. D'abord, si le filtrage est fait au niveau du registre (comme lors des cas des saisies ICE), DNSSEC ne protégera pas. Ensuite, DNSSEC ne gènera pas si le censeur veut uniquement bloquer l'accès : un `SERVFAIL` (parce que la validation DNSSEC aura échoué) est aussi bon pour lui qu'un `NXDOMAIN` (d'ailleurs, un des mécanismes de censure pourrait être de bloquer les réponses, au lieu de les remplacer par une réponse mensongère). Ce n'est que si le censeur voulait rediriger discrètement vers une autre destination que DNSSEC le gênerait. Mais il gênerait aussi l'utilisateur : le domaine serait inaccessible. DNSSEC permet de détecter la censure, pas de la contourner.

Néanmoins, DNSSEC est utile : dans beaucoup de pays, le gouvernement ne veut pas qu'on sache qu'il censure (ou, en tout cas, il essaie de rendre plus difficile la preuve) et, même s'il l'avoue, la liste des domaines censurés est en général secrète, ce qui permet de s'assurer que les citoyens ne pourront pas vérifier sa légitimité. DNSSEC permet d'être sûr qu'il y a bien filtrage, et on peut imaginer des logiciels qui utiliseront cette connaissance pour passer automatiquement à un plan B (un navigateur Web pourrait par exemple rereouter les requêtes pour ce domaine via Tor, s'il est sûr que c'est bien un problème de filtrage).

Et la détection qu'offre DNSSEC pourra servir aux opérateurs pour dégager leur responsabilité. « Vilain opérateur du `.com`, vous avez supprimé `example.com` ! » « Ah non, regardez les signatures DNSSEC, ce n'est pas nous, c'est un Homme du Milieu, sans doute l'opérateur du résolveur. »

À noter aussi que, si on imagine un pays dictatorial qui veut faire du filtrage, mais n'a pas le contrôle de tous les registres (contrairement au gouvernement états-unien), et choisit donc d'opérer dans les

résolveurs, mais veut qu'on puisse quand même faire du DNSSEC, il existe toujours des solutions techniques (par exemple forcer les utilisateurs, dans ce pays, à utiliser une clé DNSSEC de la racine qui soit contrôlée par le gouvernement).

Quatrième point étudié pendant l'atelier, les conséquences techniques du filtrage. En fait, la discussion a un peu tourné court. Car, contrairement à un argument parfois entendu, le filtrage ne casse pas en soi le DNS. Il le rend simplement plus lent (traitement supplémentaire) et plus fragile (introduction d'un nouveau composant, qui peut avoir des problèmes). Bref, il peut y avoir des arguments techniques contre le filtrage, mais ils ne sont pas décisifs. Notons tout de même que certains gouvernements font preuve d'une grande schizophrénie en encourageant des travaux visant à améliorer la résilience de l'Internet, tout en prônant ou en imposant le filtrage, qui va certainement diminuer cette résilience.

Enfin, cinquième et dernier point de la discussion, les conséquences non techniques. Elles sont multiples :

— Certains utilisateurs, pour contourner le filtrage, vont utiliser des résolveurs DNS alternatifs comme Google Public DNS <https://www.bortzmeyer.org/google-dns.html> ou Telecomix <http://dns.telecomix.org/> ou comme des résolveurs ouverts par accident. Ces fournisseurs alternatifs ne sont pas forcément de confiance et leur utilisation relève parfois du « je me jette dans le lac pour éviter d'être mouillé par la pluie ». Certains font leur propre filtrage, d'autres analysent vos requêtes, d'autres ajoutent leurs propres TLD.
— Le filtrage peut mener au développement de systèmes de nommage et de résolution radicalement différents. Cela peut être une bonne chose (le filtrage de Napster a certainement puissamment aidé au développement de meilleurs algorithmes P2P). Pour l'instant, il faut bien constater qu'on a surtout du "*vaporware*" <https://www.bortzmeyer.org/dns-p2p.html> dans ce domaine.
— Le filtrage apporte ses propres dangers. Le plus évident, compte tenu de l'expérience des DNSBL, est celui de filtrage excessif. On aura certainement un jour des TLD entiers filtrés, volontairement (certaines entreprises filtrent déjà tout `.ru` ou tout `.cn`) ou par accident.

Compte-tenu de ces différents points, quels sont les scénarios possibles (je n'ai pas dit « souhaitables ») pour le futur de DNSSEC ? La discussion en a identifié trois :

— Un scénario modérement pessimiste. En raison du filtrage massif, la validation DNSSEC sur le poste de travail (ce que permet dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html>) deviendrait à peu près impossible. DNSSEC serait alors limité à protéger les résolveurs/caches des FAI et on ne pourrait pas créer de nouvelles applications sur DNSSEC (elles nécessitent en général une validation locale). Cela ne serait pas sa mort, mais certainement un gros échec.
— Un scénario modérement optimiste. La détection du filtrage par DNSSEC marche (la question des indicateurs à présenter à l'utilisateur pour que cela soit clair reste ouverte), le filtrage, ainsi repéré, fait l'objet d'articles dans Libération ou le Canard enchaîné, ou de protestations au Parlement, le filtrage continue mais reste limité, grâce à la vigilance citoyenne. Des mécanismes de contournement automatiques apparaissent (passer par un relais si DNSSEC montre qu'il y a censure).
— Un scénario optimiste. La démocratie l'emporte, la liberté est rétablie, le filtrage stoppe, et tout est signé avec DNSSEC. On a la sécurité fournie par les signatures. Cela serait très bien, mais c'est hélas peu vraisemblable.

Ah, et puis une dernière chose, qui a fait l'objet d'amusantes discussions. DNSSEC ne permet pas de distinguer facilement du filtrage d'une attaque. Si la recherche de l'adresse de `www.example.com` fait un `SERVFAIL` ("*Server Failure*", indication par le résolveur DNS qu'il y avait un problème), comment discerner si `example.com` a été bloqué par le résolveur (sur demande de l'ARJEL ou d'un autre censeur) ou bien si un attaquant essaie de détourner le trafic vers son propre site ?

Une des suggestions était donc, en cas de censure, de renvoyer un enregistrement spécial, qui indique qu'il y a eu censure. Le résolveur pourrait interroger sans validation (avec dig, c'est l'option `+cd`) et voir ainsi ce qui s'est passé, pour annoncer à l'utilisateur qu'il a été filtré pour son bien.

J'avais suggéré, en cas de requête de type `A` (adresse IPv4), de renvoyer la valeur spéciale `1.9.8.4`. Mais, bon, le préfixe englobant est déjà alloué .

`https://www.bortzmeyer.org/dns-filtering.html`