RFC 7754 : Technical Considerations for Internet Service Blocking and Filtering

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 mars 2016

Date de publication du RFC : Mars 2016

http://www.bortzmeyer.org/7754.html

Normalement, l'Internet est **ouvert**. C'est même une de ses principales caractéristiques : un outil de communication ouvert, où tout le monde peut s'exprimer. C'est cette ouverture qui est à la base de son succès. Mais une de ses conséquences est que certaines communications vont être indésirables pour certains. Il y a donc une demande pour du « blocage » ou du « filtrage », afin d'empêcher ces communications. Ce nouveau RFC, dû à l'IAB, examine les techniques de blocage et de filtrage et cherche lesquelles sont le plus compatibles avec une architecture saine et robuste de l'Internet. Évidemment, les techniques qui menacent le moins la robustesse de l'Internet sont celles qui se déroulent entièrement aux extrémités. Si je ne veux pas voir les publicités, j'installe un logiciel qui télécharge sur ma machine une liste noire de serveurs distribuant ces publicités, et je peux ainsi bloquer et filtrer sans risques pour l'utilisation de l'Internet par les autres. Mais, hélas, pas mal de gens puissants se moquent de fragiliser l'Internet (ou la démocratie) et bien d'autres méthodes de blocage ou de filtrage existent.

On voit tout de suite que ce RFC est très politique. Les filtrages dont il parle sont évidemment ceux de gens ayant du pouvoir (entreprises, États) et qui vont essayer d'empêcher M. Michu de voir ce qu'il veut. Mais l'IAB essaie de ne pas faire trop de politique, et se limite à analyser le problème technique. Ce RFC est un excellent document, analysant très finement les systèmes de filtrage et blocage, et restant sous l'angle technique, à la fois par désir de ne pas prendre position trop clairement et aussi parce que, pour l'Internet, une censure légale/légitime et une attaque ne sont pas différentes.

Le problème des « communications non souhaitées » est vaste. Il ne se limite pas aux pages Web qui déplaisent aux ministres et que ceux-ci souhaitent censurer. Il y a aussi le logiciel malveillant (qui remonte à loin), les attaques, le spam, etc. C'est donc depuis longtemps qu'il existe des techniques de blocage et de filtrage, et depuis aussi longtemps qu'elles sont vigoureusement contestées.

Le RFC 4084 [1] notait déjà que certains FAI bloquaient l'accès à certains services. Parfois, cela se fait avec le consentement de l'utilisateur, consentement parfois très contestable : si, pour avoir un accès Internet à l'hôtel, vous devez cliquer « J'accepte » après un texte de vingt pages, y a-t-il réellement eu consentement ? Mais, souvent, il n'y a même pas de semblant de consentement : certains voudraient bloquer sans que l'utilisateur soit d'accord, et parfois sans même qu'il soit informé. Si ces « certains » ne contrôlent pas le réseau, ils cherchent à atteindre leurs fins en agissant sur des intermédiaires (comme les résolveurs DNS), et tant pis pour les dommages collatéraux.

J'ai parlé de « blocage » et de « filtrage », quelle est la différence ? On dit en général « blocage » quand on interdit complètement l'accès à un agrégat de ressources et « filtrage » quand il s'agit de sélectivement empêcher l'accès à certaines ressources seulement, dans cet agrégat. Si on empêche l'accès à tout YouTube, c'est du blocage. Si on empêche seulement l'accès à certaines vidéos, c'est du filtrage. Pour l'analyse dans ce RFC, cela ne change pas grand'chose, et on parlera indifféremment de filtrage ou de blocage.

Selon le pays, l'époque, les opinions politiques de la personne à qui on parle, ce filtrage peut être vu comme légal, illégal, éthique, acceptable, dégueulasse, souhaitable, stupide, scandaleux et contraire aux droits de l'homme, indispensable, etc. Mais, pour l'analyse technique qui est faite par l'IAB, cela ne fait pas de différence. Notamment, la distinction légale/illégale est non seulement très complexe (le gouvernement turc a-t-il le droit de détourner l'adresse IP d'un serveur états-unien ? <http://www.bortzmeyer.org/turquie-dns-frnog.html>) mais également sans conséquences pour la technique. (Un logiciel ne sait pas ce qui est légal ou illégal et il travaille de la même façon dans les deux cas.)

C'est encore plus vrai pour la distinction éthique/pas éthique, que notre RFC considère comme hors sujet, et sur laquelle il ne prend donc pas position.

La section 2 du RFC donne plusieurs exemples de filtrage ou blocage. Historiquement, les premiers systèmes qui se mettaient sur le trajet entre Alice et Bob étaient les pare-feux (RFC 2979). Ils peuvent être déployés sur les machines terminales (c'est aujourd'hui le cas du Netfilter de Linux) ou bien sur le réseau (souvenir personnel lointain : les débuts avaient été difficiles car certains systèmes supportaient mal qu'une machine soit joignable via certains ports et pas d'autres : c'est ainsi qu'au début des années 1990, Ultrix coupait toute communication avec une machine dès qu'il recevait un ICMP indiquant qu'un port était bloqué).

Il y a bien des sortes de pare-feux, le RFC 4949 contient des définitions, et le RFC 4948 décrit les différents types de trafic non souhaités, ceux qu'on veut typiquement bloquer avec le pare-feu. Notamment, on distingue traditionnellement (ces termes sont absents du RFC 4949, qui est assez ancien) :

- Les pare-feux sans état, où chaque paquet est traité indépendemment des autres. Ce sont les plus simples à réaliser et les premiers apparus. Ils permettent, par exemple, de bloquer toute connexion sortant vers le port 25 (celui de SMTP), pour empêcher les zombies d'envoyer du spam.
- Les pare-feux avec état, qui ont une mémoire des précédents paquets, ce qui permet des politiques plus subtiles comme de bloquer tout paquet entrant qui ne correspond pas à un flot de données déjà établi (une connexion TCP, par exemple). Ils sont plus complexe à réaliser (et donc plus fragiles) et l'état nécessite de la mémoire, les rendant très vulnérables en cas d'attaque par déni de service (le pare-feu à état plante souvent avant le serveur qu'il était censé protéger).
- Les pare-feux capables de DPI. Le terme est assez flou mais il désigne en général, de façon assez arbitraire, les pare-feux qui examinent au-delà de la couche 4, par exemple en regardant le contenu applicatif.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4084.txt

Autre exemple de filtrage, celui du Web. Comme les dirigeants, en général, ne connaissent de l'Internet que le Web, c'est souvent sur celui-ci que portent les efforts de censure. Il est donc fréquent que le filtrage soit spécifique à certains URI, soit en détournant tout le trafic HTTP vers un "*proxy*" qui examine les URI, soit par DPI. Évidemment, HTTPS rend bien plus compliqué ce filtrage. Mais ne l'empêche pas complètement, en raison des failles du modèle de sécurité de X.509 : par exemple, le filtreur peut obtenir un faux certificat d'une autorité existante <http://www.01net.com/actualites/comment-le-ministere-des-f
html>, ou bien faire installer sur les ordinateurs une autorité de certification qui validera les faux certificats générés par le système de filtrage.

Le filtrage n'est pas forcément fait par des méchants dictateurs voulant empêcher les citoyens d'accéder à des informations honnêtes. Un bon exemple d'un filtrage que la majorité des utilisateurs apprécie, et même réclame, est le filtrage du spam. C'est même sans doute dans la lutte contre le spam que le filtrage a trouvé une de ses premières applications. Une des armes utilisées, les listes noires, est, techniquement, tout à fait comparable aux outils de la censure (RFC 5782).

Un autre exemple cité dans le RFC d'un filtrage volontaire par les utilisateurs est le "*safe browsing*", quand le navigateur Web connait une liste de sites Web méchants ou dangereux, et refuse de s'y connecter.

Et le filtrage des noms de domaine ? Cela peut se faire en supprimant ledit nom, par exemple par la procédure de justice privée UDRP (cf. Moore, T. et R. Clayton, « "*The Impact of Incentives on Notice and Take-down*" <http://www.econinfosec.org/archive/weis2008/papers/MooreImpact.pdf> », "*Workshop on the Economics of Information Security 2008*", et Chachra, N., McCoy, D., Savage, S., et G. Voelker « "*Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting*" <http://www.econinfosec.org/archive/weis2014/papers/Chachra-WEIS2014.pdf> », "*Workshop on the Economics of Information Security 2014*". Cette approche nécessite de disposer d'un moyen politique d'action contre le registre qui gère le nom (notez que c'est la loi du pays du registre qui compte, pas la loi du titulaire, comme l'avait illustré l'affaire RojaDirecta <http://www.techdirt.com/articles/20110201/10252412910/homeland-security-seizes-spanish-domain-name-that-had-already-been-d
shtml>).

Mais la censure d'un nom de domaine peut aussi se faire dans le DNS. (Au passage, arrêtez de lire ici et allez, si ce n'est pas encore fait, allez voir l'excellent rapport du conseil scientifique de l'AFNIC « Conséquences du filtrage Internet par le DNS » <https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6573/show/le-conseil-scientifique-de-l-afnic-partage-sur-
html>.) Dans ce cas, un résolveur menteur <http://www.bortzmeyer.org/dns-menteur.html> va donner, pour ce nom de domaine, un autre résultat que celui prévu par le titulaire du nom (c'est ainsi que fonctionne la censure administrative française <http://www.bortzmeyer.org/censure-francaise.html>). Cette technique est utilisée dans de nombreux pays <https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes>, même si elle fragilise l'Internet, par exemple en perturbant le déploiement de DNSSEC.

Une autre technologie d'**infrastructure** qui risque d'être utilisée pour le filtrage est le routage. En manipulant le routage de l'Internet, on peut empêcher l'utilisateur d'accéder où il veut. Un exemple typique a été l'action aux Pays-Bas <http://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-rip
ripe-ncc-blocks-registration-in-ripe-registry-following-order-from-dutch-police> contre le RIPE-NCC dans l'affaire DNSChanger.

Après ce tour des exemples de filtrage (le RFC en cite plusieurs autres que je n'ai pas repris ici), passons maintenant à la théorie et essayons de classer ces systèmes de blocage. Il y a quatre critères de classement importants :

— **Qui** bloque ?

— **Pourquoi** bloque-t-il ?
— **Quelle** est la cible technique du blocage ?
— **Quoi**, quel composant de l'Internet est utilisé pour le blocage ?

La liste des cas présentés à la section 2 était délibérement très variée, utilisant des cas qui se classent très différemment selon ces critères.

Commençons, par le premier critère, **qui** bloque. On a vu des blocages par la police, par des tribunaux, par des entreprises, par des opérateurs réseau et par des utilisateurs individuels. Souvent, la décision est prise par une entité et ensuite appliquée par une autre. Par exemple, le ministère de l'Intérieur décide de bloquer un site Web « djihadiste » mais c'est un FAI qui, via son résolveur DNS menteur, effectue le blocage. (Le RFC n'en parle pas mais un autre exemple est celui où une entreprise choisit d'utiliser un résolveur menteur, par exemple OpenDNS, comme résolveur. OpenDNS affirme toujours que leurs clients ont choisi le blocage. Mais, dans ce cas, l'employé de base a-t-il réellement choisi ?)

Second critère, **pourquoi** on bloque. On peut bloquer « pour des raisons de sécurité » (c'est souvent une excuse pipeau mais il y a aussi des vraies raisons de sécurité). Par exemple, on va bloquer les sites Web qui distribuent du logiciel malveillant. Ou bien on va bloquer les communications avec tel préfixe IP, d'où partent souvent des attaques.

On peut aussi bloquer un contenu dont on ne veut pas. Le RFC ne cite pas cet exemple mais on pense évidemment aux bloqueurs de pub. Il y a aussi bien sûr les cas de censure étatique, où l'État ne veut pas que les citoyens accèdent à tel site Web. Les raisons sont nombreuses, de la pédopornographie au jeu en ligne en passant par la vente de drogues, la propagande raciste ou la violation des droits sacrés des ayant-droits.

Le blocage peut aussi se faire pour des raisons économiques, par exemple un service d'accès à l'Internet gratuit mais qui bloquerait la plupart des sites, nécessitant une option payante pour y accéder.

Le blocage peut se faire par liste noire (on laisse passer par défaut, et on a une liste des choses interdites, c'est typiquement le cas avec la censure) ou carrément par liste blanche (on bloque par défaut et on a une liste des choses autorisées, c'est typiquement le cas des offres limitées). Une entreprise qui ne veut pas que ses employés passent du temps sur autre chose que les tâches qui leur sont affectées pourrait utiliser une liste noire (interdire ce qui leur ferait « perdre » du temps) ou la liste blanche (limiter les employés à quelques destinations connues).

Troisième critère de classification, **quelle** est la cible exacte ? Veut-on bloquer un service entier (par exemple la voix sur IP, pour protéger la vache à lait des opérateurs téléphoniques) ? Ou un contenu très spécifique (une seule vidéo sur YouTube) ? Certaines techniques bloquent facilement plus que la cible visé. Par exemple, supprimer un nom de domaine parce que le site Web sert un contenu à problèmes va aussi couper tous les services associés à ce nom de domaine (le courrier par exemple). Les demandes de "*take down*" (« le site Web en `http://example.com/` vend de la contrefaçon, supprimez immédiatement ce nom ») prennent rarement en compte ce problème. Si on les écoutait, chaque fois que le WordPress d'une mairie est piraté et sert à du hameçonnage, on supprimerait le nom de domaine, coupant ainsi l'accès des citoyens à leur ville.

Enfin, quatrième cas, le **comment**, quels composants de l'Internet vont être utilisés pour le blocage. Cela peut être :

— La machine terminale <`http://www.bortzmeyer.org/terminal-host.html`>, client ou serveur (ou pair, dans le cas du pair à pair),
— Le réseau, par exemple les routeurs,

— Et un composant auquel on ne pense pas toujours, les services de rendez-vous, comme le DNS ou comme une DHT, qui ne sont pas dans le chemin direct entre les machines terminales, mais qui sont en général indispensables à l'établissement d'une communication.

Par exemple, lorsque M. Michu veut accéder à `http://example.com/comment-partir-en-syrie` avec son navigateur Web, les machines terminales sont son PC et le serveur HTTP, le réseau, ce sont tous les routeurs et autres équipements actifs sur le trajet, le service de rendez-vous, c'est le DNS (par exemple le registre de `.com`). Autre exemple, Alice appelle Bob en SIP, les machines terminales sont le "*smartphone*" d'Alice et le PC de Bob, le réseau, ce sont tous les routeurs et autres équipements actifs sur le trajet, le service de rendez-vous, c'est le "*proxy*" SIP.

Dans l'exemple HTTP ci-dessus, on peut empêcher M. Michu de regarder la page Web à de très nombreux endroits. Le RFC donne la liste complète mais voici quelques extraits, aux trois endroits possibles :

— On peut empêcher le navigateur de faire des requêtes vers cet URL (c'est ce que font les bloqueurs de pub),
— On peut configurer le réseau pour envoyer tout le trafic vers le serveur dans un trou noir,
— On peut supprimer le nom de domaine `example.com`.

Le choix dépendra souvent de qui bloque. Si c'est l'utilisateur (cas des bloqueurs de pub), il fera en général le blocage sur sa machine terminale. Si c'est l'État, il utilisera plus souvent le réseau ou bien le système de rendez-vous (s'il est sur son territoire, ainsi, un `.com` peut être saisi par les autorités états-uniennes).

Le gros du RFC est représenté par la section 4, qui évalue les différentes techniques. Les critères d'évaluation sont la **portée**, la **granularité**, l'**efficacité** et la **sécurité**. Commençons par la **portée** (qui est affecté).

Si je configure Shorewall <`http://www.bortzmeyer.org/filtrage-avec-shorewall.html`> sur ma machine Linux pour bloquer le trafic vers `2001:db8:bad:1:ef5:34:aba1:96`, je n'affecte qu'une toute petite partie de l'Internet. Si le gouvernement des États-Unis décidait de supprimer `.ir` de la racine du DNS, il affecterait bien plus de monde (« "*About 35,400,000 results*" » me dit Google). D'une manière générale, le blocage fait aux bords de l'Internet affecte peu de gens, celui fait dans le réseau affecte beaucoup de monde, sans doute bien plus que ce qui était nécessaire. Les exemples de « bavures » (le blocage « bave » au delà de sa portée normale) sont nombreux, de l'Inde censurant Oman <`https://citizenlab.org/2012/07/routing-gone-wild/`>, au célèbre cas de Pakistan Telecom bloquant YouTube <`http://www.bortzmeyer.org/pakistan-pirate-youtube.html`>, en passant par la censure chinoise débordant en Allemagne <`https://labs.ripe.net/Members/pk/denic-case-study-using-ripe-atlas`>. Le « bon » blocage devrait avoir la portée la plus petite possible.

Et la **granularité** ? Est-ce qu'on pourra bloquer un service sans bloquer les autres ? Par exemple, si une machine héberge un serveur SMTP qui envoie du spam, peut-on la bloquer sans empêcher l'accès aux autres ressources qu'elle héberge, comme un serveur HTTP ? Idéalement, là encore, on souhaite que le blocage puisse être fait avec la granularité la plus fine possible.

Et l'**efficacité** ? Si on bloque, on veut qu'il ne soit pas facile de « débloquer », c'est-à-dire d'accéder aux ressources bloquées. Évidemment, si le blocage est fait par l'utilisateur (comme dans le cas des bloqueurs de publicité), pas de problème : il ne va évidemment pas chercher à contourner ce blocage. Mais si le blocage est imposé, l'expérience de l'Internet montre que les utilisateurs vont chercher à le contourner (voir par exemple les articles « "*Failures in a Hybrid Content Blocking System*" <`http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf`> » et « "*Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting*" <`http://www.econinfosec.org/archive/weis2014/papers/Chachra-WEIS2014.pdf`> »). Un service bloqué se déplace facilement, comme le montre les fréquents changements de TLD de The Pirate Bay. Du côté client, les solutions de contournement sont également nombreuses, du passage par Tor, à l'utilisation de son propre résolveur DNS <`http://www.bortzmeyer.org/`

son-propre-resolveur-dns.html> pour contourner les résolveurs menteurs. Ces contournements mènent parfois à une escalade puis à une course aux armements comme dans le cas turc où le DNS menteur était contourné par l'utilisation de Google Public DNS <http://www.bortzmeyer.org/google-dns.html>, ce qui avait mené au piratage du routage de Google <http://www.bortzmeyer.org/dns-routing-hijack-turkey.html>. Un autre exemple de course aux armements est le blocage des services par leur numéro de port, poussant les applications à toujours utiliser le port 80, celui de HTTP, poussant les bloqueurs à faire du DPI, poussant les applications à chiffrer, poussant les bloqueurs à faire de l'analyse de trafic pour essayer de détecter, sous le chiffrement, certains type de trafic, etc. Une telle course ne peut pas avoir de fin.

Certains de ces contournements ont d'ailleurs des conséquences pas forcément positives pour l'architecture de l'Internet. C'est ainsi que beaucoup d'applications se pressent sur le port 443, celui de HTTPS, car il est rarement filtré. Ou bien que des victimes d'un blocage de SIP passent à des solutions fermées comme Skype. Le RFC note au passage que le chiffrement rend évidemment plus difficile tout filtrage sélectif, et que cela va donc jouer dans la diabolisation du chiffrement.

Dernier exemple de technique de contournement du blocage, citée par le RFC mais jamais vue en pratique (mais elle amusera les "*nerds*"), l'ajout d'en-têtes d'extension dans les paquets IPv6 (par exemple une option Destination <http://www.bortzmeyer.org/destination-options-ipv6.html>) suffit souvent aujourd'hui à rendre aveugles les filtres (ces en-têtes sont parfois difficiles à analyser <http://www.bortzmeyer.org/analyse-pcap-ipv6.html>).

Dans l'évaluation du blocage, reste la question de la **sécurité** : les techniques de sécurité sur l'Internet cherchent à empêcher toute interférence d'un tiers. Le blocage ne va-t-il pas entrer en conflit avec ce souhait ? Techniquement, rien ne distingue une attaque légale d'une attaque illégale : les mêmes techniques de sécurité vont réagir contre les deux. C'est le cas des protocoles qui visent (entre autres) à assurer l'intégrité des communications (TLS - RFC 5246 ou IPsec - RFC 4301). Lorsqu'on accède au site de sa banque en TLS, c'est précisement pour empêcher un tiers de modifier les données, justement ce que la censure aimerait bien faire.

La sécurité sur l'Internet repose en général sur des techniques de bout en bout, les seules sûres (RFC 4924). Certains blocages (comme le détournement des sessions TLS <https://www.schneier.com/blog/archives/2010/04/man-in-the-midd_2.html>) nécessitent d'insérer dans le trafic un intermédiaire non prévu à l'origine, ce qui casse cette sécurité.

La section 4 du RFC se penche ensuite sur les trois lieux où on peut faire le blocage, le réseau, puis le rendez-vous, puis la machine terminale. D'abord, le réseau, par exemple via un pare-feu. Est-ce un bon endroit pour bloquer ? Si on bloque dans un réseau périphérique, proche d'une des machines terminales qui communiquent, la portée reste faible. Si, par contre, on bloque dans l'épine dorsale d'un grand réseau, la portée sera bien plus étendue (dans le cas d'une censure volontaire, une portée importante n'est pas un défaut...) Notez que le blocage dans le réseau nécessite que le réseau ait accès à suffisamment d'informations pour prendre sa décision. Cela peut mener à des pratiques comme le DPI.

Notez qu'un filtrage dans le réseau peut être complexe car rien ne dit qu'un point du réseau verra passer tout le trafic entre Alice et Bob. Pour des blocages sommaires (« couper toute communication avec 192.0.2.0/24 »), ce n'est pas un problème. Mais cela interdit des choses plus subtiles, par exemple de bloquer certains URI sur un site Web mais pas tous. Le routage dans l'Internet étant ce qu'il est, un point donné peut ne voir qu'une partie des paquets d'une même communication. C'est d'ailleurs pour cela que les censeurs essaient toujours d'obtenir que les réseaux soient architecturés de manière à faciliter le blocage, notamment en limitant le nombre de points de sortie vers l'extérieur et en empêchant l'asymétrie du routage (en se moquant des conséquences que cela peut avoir pour les performances et la fiabilité).

Quant à l'efficacité et la sécurité du blocage dans le réseau... Le chiffrement suffit à gêner une grande partie de ces blocages. Il ne laisse que quelques métadonnées comme les adresses IP, qui peuvent être trop grossières pour le système de filtrage.

Et les techniques de contournement sont nombreuses, comme cela a pu être vu dans la lutte des ayant-droits contre The Pirate Bay <http://staff.science.uva.nl/~vdham/research/publications/1401-Baywatch.pdf>. Le site visé peut changer d'adresse IP, ou de nom, ses clients peuvent passer par Tor ou par un VPN, etc. Évidemment, plus le blocage reste en place longtemps, plus les techniques de contournement se développeront et seront déployées. Si on bloque dans le réseau, c'est en général parce que les deux parties qui communiquent ne sont pas d'accord avec ce blocage. Elles ont donc des bonnes motivations pour le contourner et la lutte de l'épée et de la cuirasse va donc durer longtemps.

Le bloqueur peut essayer de bloquer l'accès aux services qui permettent un contournement. Par exemple, il peut interdire TLS vers certains sites. Comme l'a montré le projet Telex <https://telex.cc/>, même cela n'est pas forcément suffisant : on peut toujours, avec la participation d'un pair accessible, faire des tunnels peu repérables. Plus radical, le censeur peut interdire tout le chiffrement (en France, des tas de politiciens ne demanderaient pas mieux <http://www.liberation.fr/futurs/2015/09/13/cryptographie-la-justice-cherche-la-cle_1381801>). Cela serait évidemment catastrophique pour la sécurité de l'Internet.

Le RFC conclut donc que le blocage dans le réseau est en général une mauvaise idée.

Bon, mais alors, se dit le censeur qui lit les RFC (cela doit être rare...), pourquoi ne pas bloquer via les systèmes de rendez-vous à la place ? En effet, on a beau parler de pair à pair, presque toutes les communications réelles sur l'Internet nécessitent un mécanisme mettant en rapport les machines de Bob et d'Alice. C'est souvent le DNS mais cela peut être un moteur de recherches (Pirate Bay joue ce rôle, mettant en rapport un utilisateur de BitTorrent et le contenu convoité) ou bien d'autres mécanismes (comme les DHT ou une "*blockchain*").

Le blocage sur le service de rendez-vous est surtout utile pour un État si ledit service est sous sa juridiction. Si vous utilisez un `.ly`, vous dépendez logiquement des lois libyennes <http://www.racknine.com/blog/internet/the-dangers-of-foreign-tlds/>. Si le service est global (c'est le cas d'un registre de noms de domaine), la portée du blocage est également globale. C'est ce qui fait qu'un service légal dans son pays a pu perdre <http://www.numerama.com/magazine/23558-le-site-de-strea
html> son `.com` et donc tous ses clients. Si par contre le service est local (un résolveur DNS), la portée est limitée aux utilisateurs de ce service.

Lorsque le système de rendez-vous est le DNS, la granularité du blocage est mauvaise : supprimer le nom de domaine supprime tous les services associés. Quant à l'efficacité, elle n'est jamais parfaite (voir mon article pour une étude sur le cas du DNS <https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes> ou bien le rapport de l'ISOC <http://www.internetsociety.org/what-we-do/issues/dns/finding-solutions-illegal-line-acti
les utilisateurs peuvent souvent changer de point de rendez-vous (passer à un autre résolveur DNS, par exemple), d'autant plus que la plupart des systèmes de rendez-vous n'ont aucune sécurité (des techniques d'authentification comme DNSSEC pour le DNS changeront peut-être partiellement les choses).

Un autre système de rendez-vous est souvent oublié : les IRR et, d'une manière plus générale, le mécanisme d'allocation d'adresses IP. Dans au moins un cas <http://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-ripe/ripe-ncc-blocks-registration-in-ripe-registry-following-orde
(déjà cité plus haut), un État a essayé de l'utiliser pour bloquer un service illégal.

En résumé, le blocage par action sur un service de rendez-vous est simple (et donc tentant pour les autorités) car on n'agit que sur un seul point, ou un petit nombre de points, mais n'est pas très efficace et, comme il consiste à bricoler l'infrastructure de l'Internet, il est dangereux pour le bon fonctionnement de celui-ci.

Reste un dernier endroit, dans l'une des machines terminales. Quelles sont les propriétés d'un blocage fait à cet endroit ? À chaque instant, le logiciel installé sur ces machines ou bien leur utilisateur prend des décisions sur le fait de communiquer ou pas. Les utilisateurs choisissent (ou pas) de cliquer sur un lien hypertexte. Le logiciel de messagerie décide si un message doit être montré ou classé dans le dossier Spam. Netfilter jette les paquets ou pas. L'utilisateur installe un nouveau logiciel de communication (ou pas). Les choix du logiciel sont guidés par l'utiisateur (cas d'un filtre bayésien à qui l'utilisateur dit « ce message est un spam ») mais le contraire arrive aussi ("*SafeBrowsing*" <https://developers.google.com/safe-browsing/>).

La portée d'un tel blocage est strictement locale. Si j'installe Ghostery pour bloquer les mouchards, cela n'affecte (en bien ou en mal) que moi.

La granularité est très fine : la machine terminale maitrise tous les aspects de la connexion contrairement à, par exemple, le serveur DNS, qui n'a aucune idée de pourquoi on demande ce nom de domaine. Elle peut donc ne bloquer qu'un seul service. Encore mieux si le blocage est fait dans l'application (le cas, là encore, des bloqueurs de publicité) car ils ont la totalité de l'information sur la connexion, sous une forme qui permet des traitements sans ambiguité (cf. RFC 7288).

L'efficacité est bonne. D'abord, puisque le blocage est décidé par l'utilisateur, il ne va évidemment pas chercher à le contourner. Ensuite, les services bloqués peuvent, évidemment, essayer de s'adapter (le point de distribution d'un "*malware*" va changer souvent de nom de domaine et d'adresse IP, pour disparaitre des listes noires) mais la machine terminale ayant une visibilité complète (y compris de ces changements) est dans une meilleure position que quiconque pour s'y adapter. Comme le blocage se fait aux extrêmités, il ne gêne pas l'architecture de bout en bout (chacun est bien sûr libre d'accepter de communiquer avec qui il veut).

À noter qu'il existe deux extrêmités à la communication : le blocage peut aussi être fait de l'autre côté, par le serveur (dans le cas d'une communication client/serveur). Voici par exemple les compteurs du nombre de paquets rejetés sur le serveur qui porte ce blog. On voit que je n'accepte pas tout :-)

```
% sudo iptables -n -v -L net-fw
Chain net-fw (2 references)
 pkts bytes target     prot opt in     out     source               destination
9360K  659M blacklst   all  --  *      *       0.0.0.0/0            0.0.0.0/0
 679K   49M smurfs     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID,NEW
9041K  625M tcpflags   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
74720   11M Drop       all  --  *      *       0.0.0.0/0            0.0.0.0/0
 8881  631K DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

On peut faire la même chose de tas de façons. Par exemple, un serveur HTTP comme Apache a plein de techniques permettant toutes sortes de blocages des visiteurs importuns. Et, évidemment, pour bloquer un service entier sur le serveur, c'est très facile, on ne fait tout simplement pas tourner le logiciel correspondant.

Bien sûr, ce blocage nécessite l'accord de la personne qui utilise ladite machine terminale et les censeurs ne seront donc pas enthousiastes à l'idée de lui demander.

Bref, le blocage sur une des machines terminales est de loin celui qui a le moins de chances de causer des dommages collatéraux sur l'Internet.

Comme tous les RFC, notre RFC 7754 contient une section dédiée à la sécurité, la section 5. Son point essentiel est que le blocage dans le réseau ou dans les services de rendez-vous est un danger pour la sécurité de l'Internet : il s'oppose frontalement aux mesures de sécurité. Par exemple, pour bloquer, on va essayer de casser le chiffrement, avec une attaque de l'homme du milieu, comme le font beaucoup d'entreprises, avec les produits de société comme Blue Coat, en fabriquant de faux certificats <http://www.01net.com/actualites/comment-le-ministere-des-finances-espionne-le-trafic-web-de-ses-coll
html> pour que les logiciels ne détectent pas cette attaque.

En outre, le système qui effectue cette attaque devient lui-même une cible tentante pour un attaquant extérieur puisqu'il donne accès à tout le trafic en clair. On a donc mis en péril toutes les machines de l'entreprise en introduisant cette « machine du milieu ». (En tant qu'ancien ingénieur système, je suis également sensible à la remarque du RFC comme quoi l'administrateur de cette machine court un gros risque juridique personnel, puisqu'il va avoir accès à des tas de données sensibles.)

La conclusion du RFC (section 6) est que, si on tient à faire du blocage, il faut le faire sur les machines terminales et laisser le réseau tranquille, afin qu'il puisse faire son travail avec rapidité et sécurité. Gageons que cet avis ne sera pas suivi. Parmi toutes les discussions sur le blocage, le filtrage et la censure, beaucoup de temps a été passé sur la légitimité ou non de ces blocages (« si vous vous opposez à la Main Rouge <http://interieur2.eu.org/>, c'est que vous sympathisez avec les terroristes ») et nettement moins sur les conséquences techniques de ces blocages. En gros, si on veut faire de la censure efficace, il faut ré-architecturer l'Internet pour la censure et non pas pour la communication. (Cf. mon exposé à l'Assemblée Générale de France-IX <https://www.youtube.com/watch?v=Juj8Tdd1YA0>, et les supports <https://www.franceix.net/media/cms_page_media/851/The_necessary_restructuring_of_the_Internet_by_Stephane-BORTZMEYER_AFNIC.pdf>.)

Un des auteurs du RFC, Olaf Kolkman, a écrit ses réflexions personnelles <https://www.internetsociety.org/blog/tech-matters/2016/03/blocking-and-filtering-rfc-7754-collaborative-security-cont