

Le filtrage sur Internet

Comment contourner les filtres mis en place sur
Internet par les gouvernements?

Samuel Bouchet

06/04/2008

Avant-propos	3
Introduction.....	4
I/ Méthodes de filtrage	6
1. Pré-requis : la structure du réseau Internet	6
2. Filtrage par liste noire	8
3. La redirection DNS / L’empoisonnement DNS	9
4. Le rôle des moteurs de recherche et des sociétés étrangères	10
II/ Les Contre-mesures.....	11
1. Les systèmes de contournement en ligne publics.....	11
a. Fonctionnement.....	11
b. Limites.....	12
c. Exemples.....	13
d. Récapitulatif.....	13
2. Les serveurs <i>proxys</i>	14
a. Fonctionnement.....	14
b. Limites.....	16
c. Exemples.....	16
d. Récapitulatif.....	16
3. Le tunneling	17
a. Fonctionnement.....	17
b. Limites.....	18
c. Exemples.....	18
d. Récapitulatif.....	18
4. Les systèmes de communication anonymes.....	19
a. Fonctionnement.....	19
b. Limites.....	20
c. Exemples.....	21
d. Récapitulatif.....	21
Conclusion	22
Références bibliographiques.....	24

Le filtrage sur Internet... C'est quoi ? D'une façon générale, c'est un ensemble de solutions employées pour restreindre le contenu accessible via Internet. Cette restriction peut-être nécessaire dans un certain nombre de contexte : Pour les parents, empêcher leurs enfants d'accéder à du contenu pornographique ou d'être contacté par des pédophiles ; Pour les entreprises et les écoles, éviter les activités illicites des utilisateurs, les chutes de productivité, la diminution de la bande passante ou la fuite d'information ; Pour éviter l'abus sur les bornes d'accès public.

Malheureusement, les applications sont parfois moins légitimes voire complètement liberticides. En effet, certains gouvernements appliquent des filtres plus ou moins subtils pour contrôler l'information dans leur propre intérêt, en laissant apparaitre une fausse liberté d'information ou en bloquant complètement certains sites.

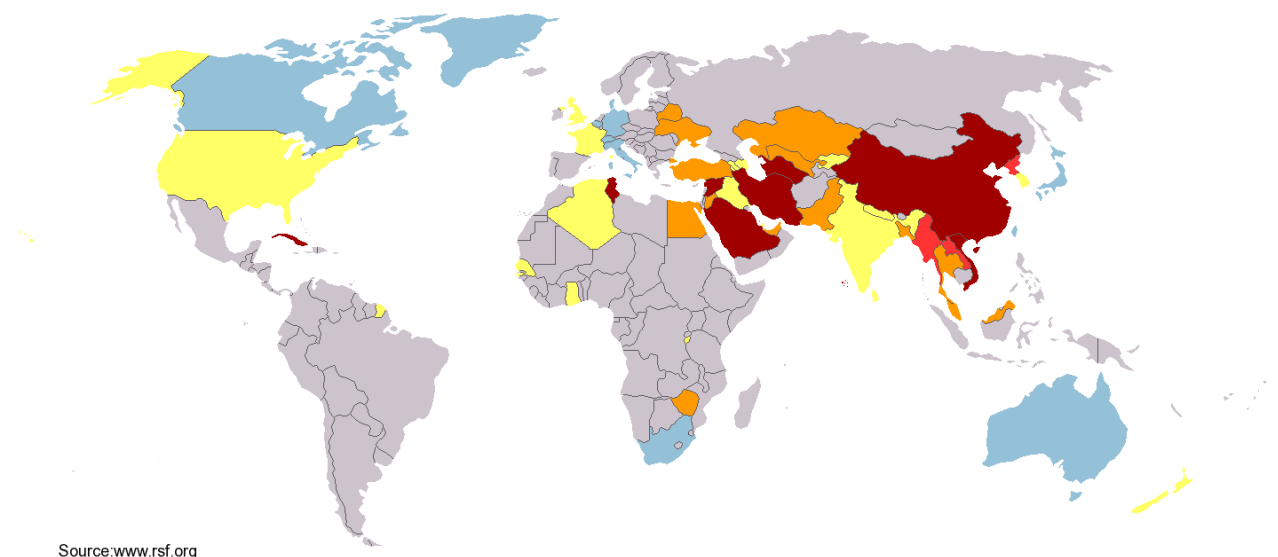
Le présent document s'intéressera uniquement aux filtrages sur Internet appliqués par les gouvernements dans la mesure où ils vont à l'encontre des libertés d'expression. Il se contentera d'aborder le filtrage d'un point de vue technique mais n'entrera pas dans les débats de fond concernant la liberté d'expression.

Introduction

La montée rapide d'Internet inquiète. Elle inquiète notamment plusieurs gouvernements autoritaires à travers le monde. Comment lutter face une source de diffusion libre de l'information lorsqu'on souhaite la brider, la contrôler ? Comment garder son emprise face à un media si ouvert ? Ce sont les problématiques auxquelles ces gouvernements ont du trouver des solutions, et malheureusement, ils en ont trouvé.

Le monde d'aujourd'hui est donc composé de plusieurs Internet. *The Internet*, celui que nous connaissons, le réseau le plus étendu et le plus libre qui soit ; et les autres sous réseaux d'Internet, qui ne donnent accès qu'à une toute petite partie des informations voire à des informations manipulées. Des pays tout entiers à travers le monde sont déconnectés de la toile géante, des peuples vivent dans la désinformation et le mensonge le plus complet, des événements mondiaux sont cachés, déformés, ou même inventés.

Parmi ces pays, reporters sans frontières accuse dans un article du 7 novembre 2006 [1] : L'Arabie saoudite, la Biélorussie, la Birmanie, la Chine, la Corée de Nord, Cuba, L'Égypte, l'Iran, l'Ouzbékistan, la Syrie, la Tunisie, le Turkménistan et le Viêt-Nam d'œuvrer contre la liberté d'information et contre le réseau Internet. Depuis 2008, L'Éthiopie et de Zimbabwe sont également accusés.



Pays mettant des obstacles au libre accès à l'information sur Internet

■ Très grave ■ grave ■ difficile ■ moyenne ■ situation bonne

Reporters sans frontière les accusent entre-autre de surveiller, bloquer, rediriger et manipuler certains sites ayant du contenu lié au sexe, à la religion, à la politique, à l'actualité, mais aussi d'emprisonner des internautes pour leurs opinions politiques ou religieuses. Certains pays tel que la Birmanie se permettent également de surveiller les utilisateurs des cybercafés en prenant des captures d'écran des ordinateurs à intervalles réguliers. D'autres pouvoirs politiques, plus extrémistes, refusent de connecter leur pays au réseau et réservent à une poignée de privilégiés un accès très limité. D'une façon générale, il semblerait que la censure et le filtrage sur Internet soient en forte hausse... [2]

La mise en place de telles mesures de filtrage peuvent avoir des aspects techniques assez complexes. On peut se demander comment il est possible de contrôler un aussi grand réseau, et si les installations mises en place peuvent être contournées.

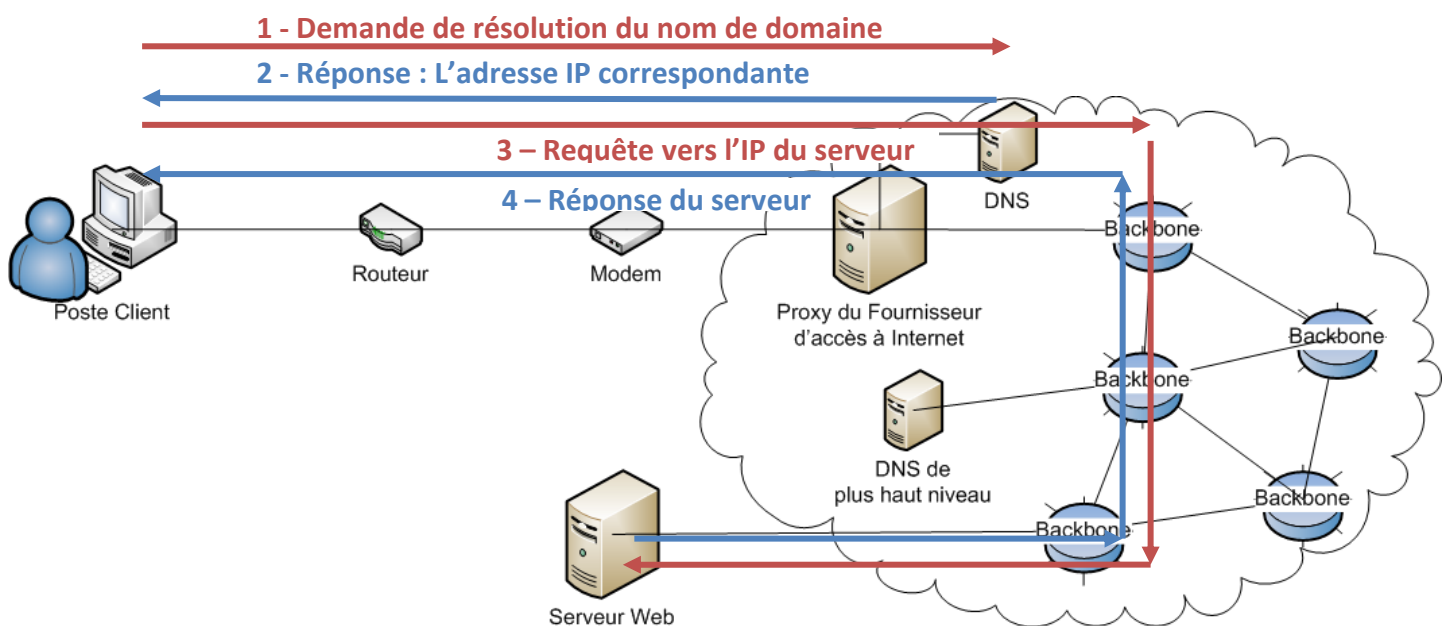
Le présent document expliquera le fonctionnement de ces différentes techniques de filtrage, et comment il est possible de les contourner pour permettre aux internautes du monde entier de se connecter au même Internet non filtré que nous connaissons.

I/ Méthodes de filtrage

1. Pré-requis : la structure du réseau Internet

Pour comprendre comment fonctionnent les technologies de filtrage d'Internet, il faut d'abord avoir une vue d'ensemble du fonctionnement du réseau Internet. Pour l'expliquer, prenons l'exemple de Mr Toutlemonde.

Mr Toutlemonde souhaite à partir de son ordinateur aller visiter son site favori. Il tape donc dans son navigateur l'adresse « <http://monsitfavoris.fr/> » puis valide. L'ordinateur ne connaissant pas l'adresse IP correspondant à monsitefavoris.fr, envoie une demande au DNS qui lui retourne l'IP du site. L'ordinateur de Mr Toutlemonde envoie alors une requête au routeur du réseau local pour rejoindre l'IP de monsitefavoris.fr. Le routeur transmet alors le message par le modem. Le message passe par la boucle locale (segment du réseau entre la prise de l'abonné et le répartiteur téléphonique du fournisseur d'accès à Internet) puis le proxy du fournisseur d'accès redirigera la demande vers le réseau de *backbones* (ou dorsales).



Cheminement d'une requête http sur le réseau Internet

Les *backbones* sont des routeurs à très haute capacités reliés entre eux par des supports sur des longues distances au niveau international. Ce sont des points clés du réseau se sont eux qui donnent sa portée mondiale au web.

Une fois le message arrivé au *backbone* le plus proche, il est redirigé vers les autres *backbones* puis vers le serveur ayant l'IP de monsitefavoris.fr. Ce serveur qui héberge le site pourra ensuite répondre à la requête de l'ordinateur de Mr Toutlemonde en envoyant un message qui fera le chemin inverse.

Maintenant que nous avons vu la structure du réseau Internet, nous pouvons répondre à la question : Où agissent les gouvernements pour contrôler Internet ? Il s'agit en effet des *backbones*. Ces dorsales sont situées généralement dans des grandes villes et appartiennent à des fournisseurs d'accès à Internet ou d'autres sociétés privées mais peuvent être sous contrôle de l'Etat. Le blocage de Youtube en Chine par exemple, se fait par le contrôle de 5 *backbones* Internationaux chinois [3].

2. Filtrage par liste noire

Comme expliqué précédemment, les gouvernements ont accès à leurs dorsales internet. Le blocage par adresse IP ou par nom de domaine est effectué au niveau de ces serveurs. Des serveurs *proxys*¹ sont installés pour filtrer le flux de données passant par chaque dorsale du pays. Ce système vérifie si l'adresse IP ou le nom de domaine demandé n'est pas sur liste noire. S'il l'est, la demande est rejetée ou ignorée.

La liste noire est une liste de toutes les adresses IP et noms de domaines interdits par le gouvernement. Cette méthode de blocage nécessite un grand nombre de personnes pour surveiller et mettre à jour la liste noire. Dans chaque pays appliquant cette méthode, des agents sont chargés de trouver et filtrer tous les sites internet Déplaisants pour le gouvernement. Par exemple, le corps de la « police d'Internet » en Chine serait composé de 30 000 à 40 000 agents selon Le Monde [4].

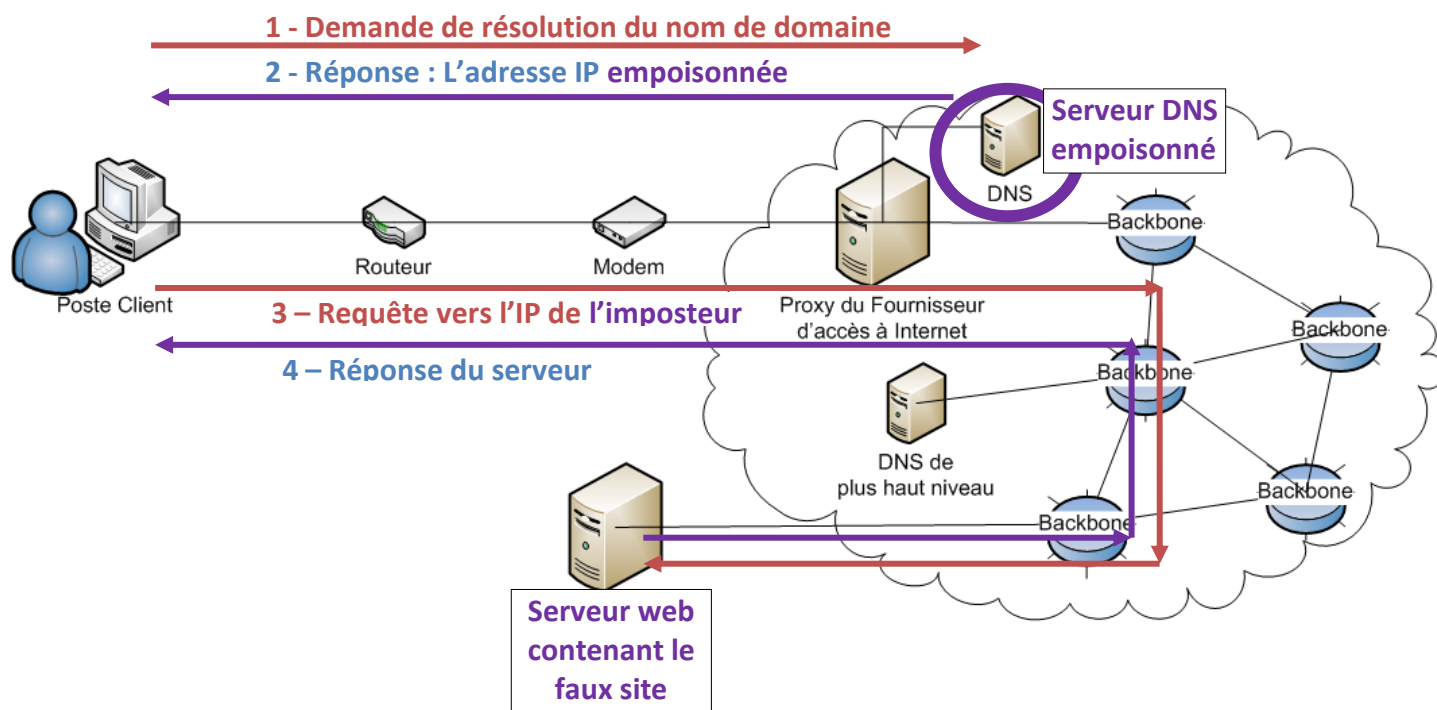
Selon les sites, la demande peut être purement rejetée (l'utilisateur recevra alors un message de demande refusée) ou être plus subtilement ignorée. Dans ce cas il est impossible de savoir si la demande est ignorée à cause d'un pare-feu ou si le site distant est hors ligne.

¹ Aussi appelé « serveur mandataire ». Il permet de relayer des informations entre 2 branches d'un réseau et intègre des fonctionnalités telles que la mise en cache, le filtrage, l'authentification, etc....

3. La redirection DNS / L'empoisonnement DNS

La redirection (ou empoisonnement) DNS est une méthode plus discrète et plus manipulatrice que le blocage par liste noire. Cela consiste à rediriger la demande d'un site Internet vers un autre site en modifiant l'adresse IP associée à un nom de domaine au niveau du DNS.

Par exemple, imaginons que <http://monsitefavoris.fr/> soit hébergé sur un serveur web ayant l'adresse IP 88.1.1.1 et qu'une copie modifiée du site par le gouvernement soit hébergée sur un serveur d'adresse 88.2.2.2. Lorsqu'on tape l'URL <http://monsitefavoris.fr/> dans le navigateur, le serveur DNS renvoi normalement comme IP associée 88.1.1.1. Dans le cas d'une redirection DNS, le gouvernement aura modifié le serveur DNS pour que toute demande vers monsitefavoris.fr soit redirigée vers 88.2.2.2.



Cheminement d'une requête http dans le cas d'une redirection DNS

Résultat : l'internaute croit naviguer sur le site qu'il a demandé alors qu'il est en fait sur un site modifié où l'information est manipulée. On se retrouve en fait dans une situation ressemblant à du phishing (ou hameçonnage en français). La différence étant dans le but : On ne souhaite pas voler des informations personnelles à l'internaute mais le désinformer pour le manipuler. Cette technologie serait utilisée en Ouzbékistan par exemple [1].

L'inconvénient majeur de cette technique est qu'elle nécessite de refaire entièrement le site à rediriger ce qui peut être long et coûteux si l'opération doit être réalisée de façon vraiment convaincant.

4. Le rôle des moteurs de recherche et des sociétés étrangères

Les gouvernements font également pression pour interdire certains mots sur les moteurs de recherches, qu'ils soient internationaux, tel Yahoo! ou Google, ou nationaux comme Baidu en Chine [5]. Une recherche qui contient un mot clé interdit affiche une page d'erreur et une répétition de la même recherche bloque temporairement l'adresse IP de celui effectuant la demande.

Pékin filtrera 400 à 500 mots tabous ou sensibles en rapport avec le Tibet, La Révolution culturelle ou la pornographie [5].

L'expérience est facile à réaliser : faites la recherche d'image « Tiananmen » sur google.com traduit en chinois, sur Google.cn, puis sur Baidu. Le premier site présente des images de guerre et de révolution, les deux autres présentent un endroit festif et coloré. Le rôle du moteur de recherche dans la censure est évident.

Les résultats des recherches ne sont pas toujours filtrés. Des pages provenant de sites censurés peuvent figurer dans les réponses, mais ne sont pas accessibles pour autant. La fonction "cache" (qui affiche une copie de la page indexée, mémorisée sur le site du moteur de recherche) est toujours neutralisée.

Le gouvernement chinois utilise ici un moyen de pression économique pour forcer Google et Yahoo! à mettre en place des solutions de filtrage par mots clés.

II/ Les Contre-mesures

Pour permettre aux internautes de passer au-delà de ces restrictions, des méthodes de contournement ont été mises en place. Ces méthodes sont détaillées et présentées par Reporter sans frontière [6] ainsi que par les développeurs de ces solutions (détaillés en exemple dans chaque section). Ces technologies ont été développées pour aider les citoyens à lutter contre la censure et la surveillance sur Internet.

En général, ces techniques fonctionnent en transmettant la requête d'un internaute vivant dans un pays qui filtre le Web vers une machine intermédiaire qui n'est pas bloquée. Cet ordinateur récupère le contenu demandé par l'utilisateur, qui devrait être bloqué par les filtres, et le lui retransmet. Parfois, ces technologies peuvent être conçues spécifiquement pour contourner la censure dans un pays donné, ou pour lutter contre une technique spécifique de filtrage.

1. Les systèmes de contournement en ligne publics

a. Fonctionnement

Les systèmes de contournement en ligne sont des pages Web qui affichent un formulaire. Ce formulaire propose à l'utilisateur d'entrer l'URL du site Internet qu'il veut visiter. Le système va alors récupérer puis afficher le contenu de la page demandée. Il n'y a de cette façon aucun lien direct entre l'utilisateur et le site Internet demandé : le système relaie de façon transparente la requête et permet à l'internaute de naviguer librement sur des sites habituellement bloqués. Cette technologie réécrit les liens inclus dans la page Web demandée à l'aide d'expressions régulières pour que l'utilisateur puisse continuer de naviguer normalement.

L'utilisateur final n'a besoin d'installer aucun logiciel ni de changer les réglages de son navigateur. Sa seule tâche consiste à se rendre sur le site du système de contournement, à saisir l'adresse qu'il souhaite visiter dans le formulaire en ligne et à cliquer sur le bouton "Soumettre". (Ces systèmes peuvent avoir des aspects différents, mais leur fonctionnalité essentielle ne change pas). Ainsi, aucune expertise n'est requise et ce système peut être utilisé à partir de n'importe quel point d'accès, public ou privé.

La plupart des services publics de contournement en ligne offrent une version limitée gratuite et une version avec davantage d'options (comme l'accès crypté) disponible sur abonnement. Certains services sont gérés par des entreprises, d'autres par des volontaires et en particulier des groupes de hackers luttant pour la liberté d'expression.

b. Limites

Dans la mesure où les adresses Internet de ces services sont largement connues, la plupart des applications de filtrage, de même que les systèmes de censure installés au niveau national, les ont déjà incluses dans leurs listes noires. Or, si les adresses de ces services sont bloquées, ils ne peuvent pas fonctionner. Les utilisateurs doivent aussi être prudent, certains de ces services ne cryptent pas le trafic entre le système de contournement et l'utilisateur du système. Les informations transmises peuvent être interceptée par le fournisseur du service.

Il peut également se poser certains problèmes de sécurité. En effet, il est à noter que les systèmes de contournement n'assurent pas toujours l'anonymat. L'identité des utilisateurs est masquée des responsables des sites visités. Par contre, si la requête http entre l'utilisateur et le fournisseur de contournement n'est pas cryptée, comme c'est souvent le cas pour les services gratuits, son contenu peut être facilement intercepté et analysé par un intermédiaire comme le fournisseur d'accès à Internet. Aussi, même si le contournement a bien réussi, les autorités peuvent toujours pister l'utilisateur et découvrir qu'il a utilisé un système de contournement en ligne. De plus, tout le contenu échangé entre le système de contournement et l'utilisateur final peut être déterminé.

Pour assurer un minimum de sécurité, les systèmes de contournement en ligne qui ne cryptent pas les échanges utilisent parfois un brouillage de l'URL pour contrer les techniques de filtrage qui recherchent les mots-clés dans l'URL. Par exemple, avec l'utilisation d'une technique simple comme ROT-13, où une lettre est remplacée par la lettre située treize places plus haut dans l'alphabet, l'URL `http://ice.citizenlab.org` devient `uggc://vpr.pvgvmrayno.bet/`. De cette façon aucun mot clé ne peut être reconnu et filtré. Cependant, le contenu de la session peut toujours être intercepté, même si le contournement a réussi.

On note également des risques associés à l'utilisation des cookies et des scripts. De nombreux systèmes de contournement en ligne sont configurés pour supprimer les cookies et les scripts, mais certains sites (toujours les *webmails*, par exemple) nécessitent leur utilisation. Un autre risque est lié à l'utilisation de services nécessitant un nom d'utilisateur et un mot de passe : l'internaute accède au système de contournement via une connexion en clair puis utilise le système pour faire une demande d'information à partir d'un serveur crypté. Dans ce cas de figure, le système de contournement récupère l'information demandée via une transmission cryptée, mais envoie ensuite son contenu en clair à l'utilisateur, exposant ainsi les données sensibles en cas d'interception.

Cependant, bien que la connexion de l'utilisateur au système de contournement puisse être sécurisée, il faut garder à l'esprit que toute information qui passe par un système de contournement peut être interceptée par celui qui a mis en place ce système. Les archives du système de contournement constituent donc un problème de sécurité supplémentaire. Selon la localisation du système de contournement ou de son serveur, les autorités peuvent avoir accès à son historique et à ses archives électroniques.

Les utilisateurs doivent aussi être informés quand ils utilisent un système de contournement en SSL que l'utilisation du cryptage peut attirer l'attention sur les activités de l'internaute. Ce cryptage n'est pas forcément légal partout. De plus, les autorités assurant le filtrage ont la possibilité de déterminer quels sont les sites qui ont été visités grâce au contournement, même lorsqu'un cryptage SSL est utilisé, en aillant recours à des techniques connues sous les noms de « prise d'empreinte » HTTPS et d'attaques dites de « l'homme du milieu » (MITM ou Man in the Middle). Toutefois, les pages ayant un contenu dynamique ou les systèmes de contournement qui ajoutent au hasard du faux texte et de fausses images au contenu demandé peuvent rendre ces techniques d'interception inefficaces. Si les utilisateurs disposent de la signature sécurisée du certificat SSL, ils peuvent vérifier manuellement que celui-ci est authentique et ainsi éviter une attaque de « l'homme du milieu » [7].

c. Exemples

Quelques exemples de services de contournement en ligne :

- www.anonymizer.com
- www.unipeak.com
- www.anonymouse.ws
- www.proxyweb.net
- www.guardster.com
- www.webwarper.net
- www.proximal.com
- www.the-cloak.com

d. Récapitulatif

Avantages :

- Facilité d'utilisation : aucun programme n'est à installer par l'utilisateur.
- Ne nécessite pas, comme les autres méthodes, d'avoir un contact étranger dans un pays sans censure.

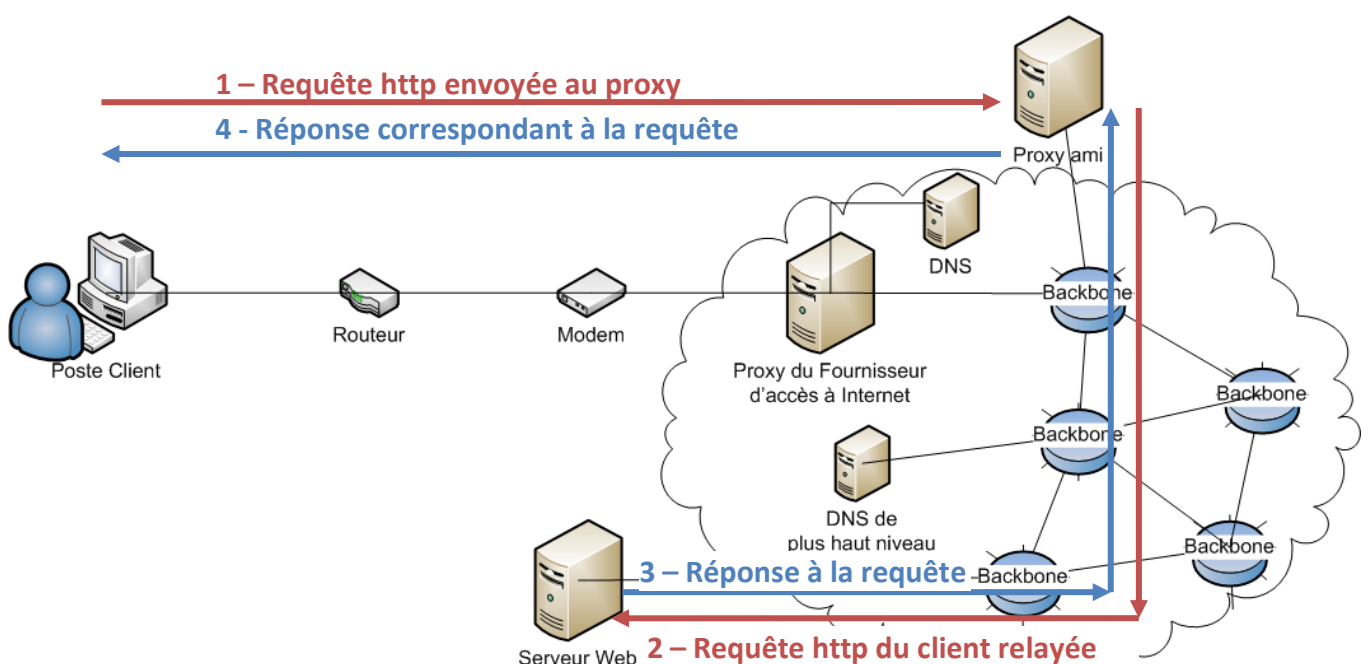
Inconvénients :

- Les systèmes de contournement en ligne ne peuvent pas accéder à plus que des pages Web (HTTP) et supporte pas les technologies d'accès crypté (SSL). Des services Internet nécessitant une authentification peuvent ne pas être pleinement fonctionnels, comme par exemple les *webmails*.
- Lorsque ce sont des systèmes publics, ils sont généralement connus des autorités et peuvent être bloqués. Un grand nombre de ces services sont rendus inaccessibles par des logiciels de filtrage.
- Même avec un cryptage complet (utilisateur/service de contournement et service de contournement/site internet), il existe des risques d'interception.

2. Les serveurs *proxys*

a. Fonctionnement

Un serveur *proxy* est un serveur situé entre le client (par exemple le navigateur internet de l'utilisateur) et un autre serveur (serveur Web ou autre). Le *proxy* agit comme tampon entre le client et le serveur, et gère différentes demandes comme les requêtes Internet (http), les transferts de fichier (ftp) et le trafic crypté (SSL). Les *proxys* sont utilisés par des individus, des institutions et des Etats pour la sécurité, l'anonymat, la mise en cache ou encore le filtrage. Pour utiliser un serveur proxy, l'utilisateur doit configurer son navigateur Internet avec l'adresse IP et le nom du serveur proxy ainsi qu'avec le numéro de port utilisé par le serveur. Bien que cela soit relativement simple, il peut s'avérer impossible de modifier les réglages du navigateur depuis des points d'accès publics tels que des cybercafés, des bibliothèques ou sur les lieux de travail.



Contournement par l'utilisation d'un proxy

Un logiciel de serveur *proxy* peut être installé par des contacts de confiance qui disposent de certaines compétence technique (l'installation d'un serveur proxy nécessite de bonnes connaissances en réseau) et qui sont basés dans un pays qui n'est pas soumis au filtrage. Le logiciel de serveur proxy doit être mis en place sur un ordinateur qui dispose d'une bande passante importante et doit être configuré pour utiliser une technologie de cryptage. Sans cela, il ne pourrait être utilisé pour contourner un quelconque filtrage.

Cette solution est particulièrement adaptée pour un bureau ou une petite organisation ayant besoin d'une solution de contournement stable. Bien qu'il ne s'agisse pas de la solution de contournement la mieux cachée, les serveurs *proxys* privés représentent une solution plus stable et efficace que les systèmes de contournement en ligne. Ils sont également préférables pour accéder aux sites nécessitant une authentification ou l'installation de cookies. Les serveurs proxys sont très modulables et peuvent répondre aux besoins spécifiques de l'utilisateur et s'adapter à l'environnement local de filtrage.

De plus, le serveur proxy permet également de contourner un autre type de filtrage : le filtrage par port. En effet, certains pays effectuent un filtrage au niveau national et bloquent l'accès aux ports proxys standards. Un port est un point d'entrée de connexion utilisé par des protocoles spécifiques. Les numéros standards de ces ports sont attribués par une organisation spécialisée, la « Internet Assigned Numbers Authority » (IANA). Le port 80 est, par exemple, réservé au trafic HTTP. Les serveurs proxys ont également des ports qui leur sont attribués par défaut. Pour les bloquer, de nombreuses technologies de filtrage ne permettront pas l'accès à ces ports. Pour réussir un contournement, il peut être nécessaire de configurer le proxy pour qu'il fonctionne sur un port non standard.

Pour les personnes n'ayant pas de contacts dans les pays étrangers, il existe également des *proxys* ouverts. Ce sont des serveurs qui sont volontairement ou involontairement laissés ouverts pour servir de relais à d'autres ordinateurs afin de se connecter à Internet. Leur avantage est qu'ils ne nécessitent pas de connaître la personne qui l'a mis en place. On ne sait jamais si les *proxys* ouverts ont été réglés dans le but d'être utilisés par tous ou s'ils ont été simplement mal configurés.

A cause de leurs désavantages trop nombreux, ils ne sont pas recommandés. Les risques sont : transmission de scripts et cookies nocifs, attaques « Man in the Middle » et prises d'empreintes HTTPS (comme pour le contournement en ligne), transmissions de données sensibles vers un serveur *proxy* de type *sock* (serveur capable de manipuler d'autres flux que les flux http pour le web), redirection DNS si le nom de domaine est résolu avant la demande au proxy.

b. Limites

La configuration des serveurs *proxys* est extrêmement importante : elle conditionne la sécurité et l'anonymat de la connexion. En l'absence de cryptage, les données échangées en clair peuvent être interceptées et servir à identifier l'utilisateur et à contrôler ses actions sur Internet.

L'utilisateur doit avoir les autorisations nécessaires pour modifier les paramètres de son navigateur. De plus, si le FAI demande que tout le trafic passe par son propre serveur *proxy*, l'utilisation d'un autre *proxy* ouvert peut être impossible.

Selon certaines législations nationales, l'utilisation d'un serveur *proxy* ouvert peut être considérée comme un « accès non autorisé » et les utilisateurs de serveurs *proxys* ouverts peuvent ainsi être l'objet de poursuites judiciaires. La recherche et l'utilisation de serveurs *proxys* publics peut donc être illégale et n'est pas recommandée.

c. Exemples

Voici quelques exemples de logiciels de serveur *proxy* :

- <http://www.squid-cache.org> & www.stunnel.org
- <http://ice.citizenlab.org/projects/aardvark>
- <http://www.privoxy.org>
- <http://www.openssh.com>

d. Récapitulatif

Avantages :

- On peut choisir parmi de nombreux logiciels capables de relayer le trafic http de façon transparente et pouvant être configurés selon les besoin
- Il existe un grand nombre de serveurs *proxys* accessibles au public.
- Solution fiable et efficace pour des groupes
- Permet de contourner le filtrage par port si le *proxy* est configuré sur un port non standard

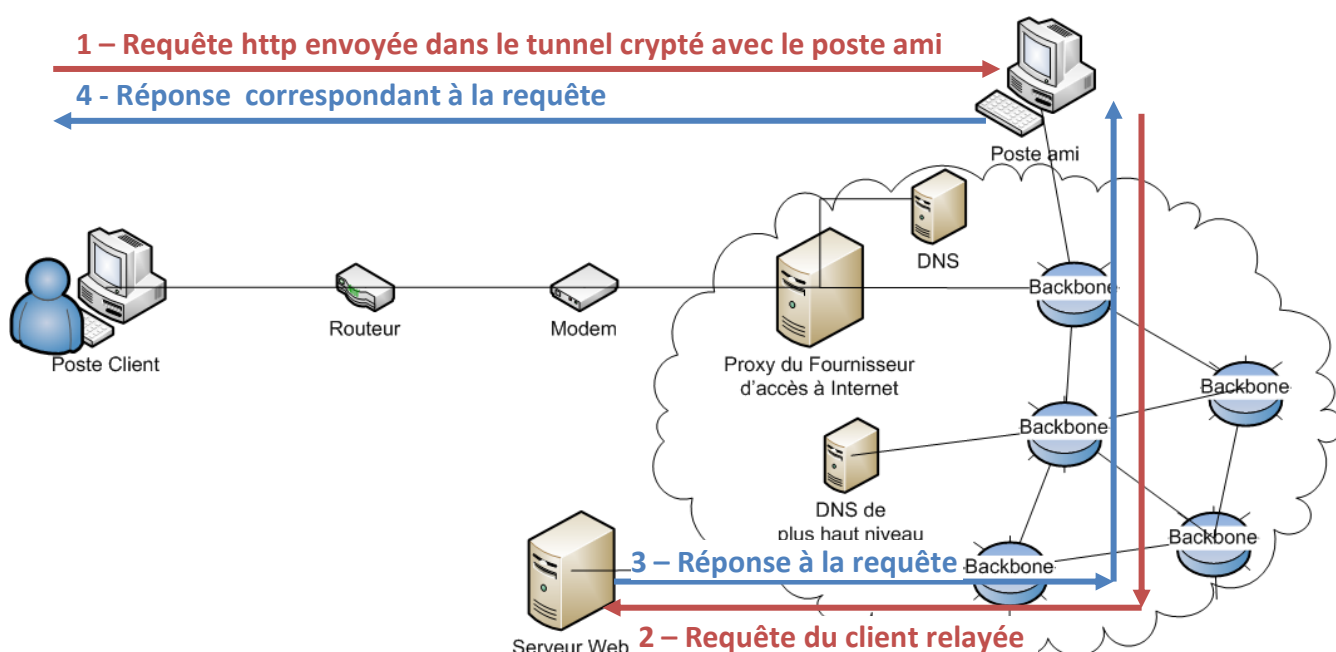
Inconvénients :

- L'utilisateur doit avoir des contacts fiables situés dans une zone non soumise au filtrage.
- Peut difficilement être utilisé dans des points d'accès publics
- Nécessite que le fournisseur d'accès à Internet n'impose pas ses propres *proxys*

3. Le tunneling

a. Fonctionnement

Le principe du tunneling est à peu près le même que celui du proxy. L'utilisateur situé dans un endroit soumis à la censure peut télécharger un logiciel client qui crée un « tunnel » vers un ordinateur d'une zone non filtrée. Les services normaux de l'ordinateur de l'utilisateur sont disponibles, seulement ils fonctionnent au travers d'un tunnel crypté qui passe par un ordinateur ami intermédiaire. Celui-ci transmet ensuite les requêtes de l'utilisateur ainsi que leurs réponses. Les internautes qui ont des contacts dans un pays non filtré peuvent mettre au point des services privés de tunneling. Ceux qui n'ont pas de contacts doivent passer par des services commerciaux de tunneling, souvent payants et disponibles sur abonnement.



Contournement par l'utilisation d'un système de tunneling

Un des avantages de cette technologie est qu'elle permet de faire circuler des informations autres que du simple contenu web. De plus, Il encapsuler un paquet d'informations non cryptées à l'intérieur d'un protocole de cryptage permettant des échanges sécurisés.

b. Limites

Mais attention! Les services gratuits de tunneling incluent souvent de la publicité. Les requêtes pour les publicités sont des requêtes http en clair qui peuvent être interceptées par les autorités. Ils ont alors la possibilité de déterminer si utilisateur a recours à un service de tunneling. En outre, de nombreux services de tunneling reposent sur l'utilisation de serveurs socks² qui ne dissimulent pas les noms de domaines auxquels accède l'utilisateur.

De plus, les applications de tunneling s'adressent davantage à des utilisateurs compétents techniquement et qui ont besoin des services de contournement sécurisés (mais pas anonymes). Elles ne peuvent également pas être utilisées dans des lieux publics (bibliothèques, cybercafés) car elles nécessitent une installation.

c. Exemples

Quelques exemples de services de tunneling

- www.http-tunnel.com
- www.hopster.com
- www.htthost.com

d. Récapitulatif

Avantages :

- Transfert crypté sur le réseau.
- Nombreux protocoles supportés (et pas seulement le trafic Web)
- Il existe des services commerciaux que les utilisateurs peuvent payer s'ils n'ont pas de contacts dans des pays non soumis au filtrage

Inconvénients :

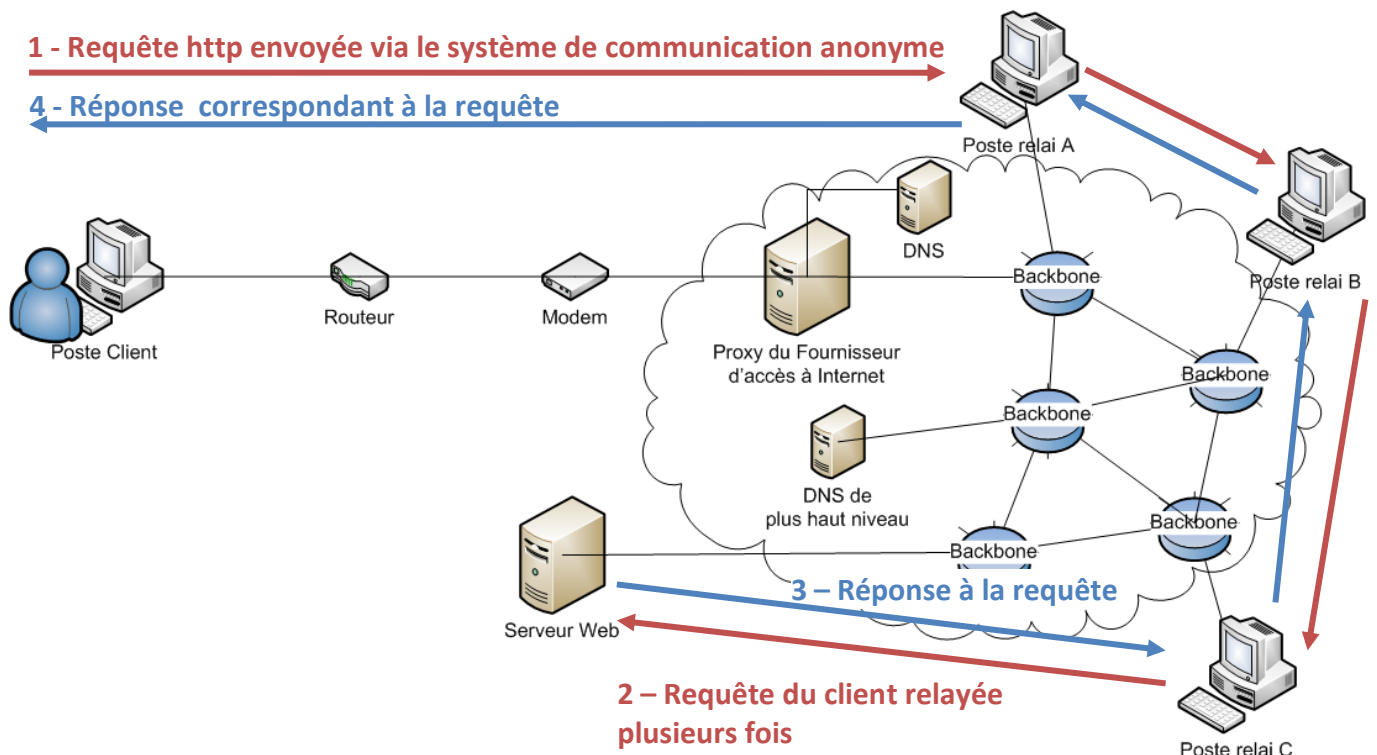
- Les services commerciaux de tunneling sont connus de tous et peuvent être filtrés
- Cette technologie ne peut pas être utilisée à partir de points d'accès publics où les utilisateurs n'ont pas la possibilité d'installer le logiciel, comme les cybercafés ou les bibliothèques
- L'utilisation d'applications de tunneling peut demander plus de compétences techniques que les autres méthodes de contournement

² Serveur *proxy* permettant de faire passer tout type d'informations

4. Les systèmes de communication anonymes

a. Fonctionnement

Le système de communication anonyme fonctionne en fait de la même façon que dans le cas d'un tunneling à quelques différences près : Il n'y a pas un mais plusieurs ordinateurs relais de sorte que le lien soit brouillé quant à l'émetteur de la requête ; et il n'y a pas nécessairement le système de cryptage comme pour le tunnel.



Fonctionnement du système de contournement anonyme

En outre, leurs objectifs sont différents. Les systèmes de communications anonymes veillent essentiellement à ce que la confidentialité de l'utilisateur soit assurée en masquant son identité aux sites qu'il visite. Les systèmes les plus évolués utilisent même différents systèmes de routage pour garantir que l'identité de l'utilisateur est masquée du système de communications anonymes lui-même.

Les systèmes de contournement quant à eux ne se concentrent pas forcément sur l'anonymat. En effet, ils cherchent à fournir à l'utilisateur les moyens d'envoyer et de recevoir des informations sur le Web de la manière la plus sécurisée possible. Le contournement de la censure nécessite une technologie de communication sécurisée, mais il ne garantit pas nécessairement un anonymat complet.

Les systèmes de communications anonymes sont généralement utilisés pour contourner les filtres. L'un des avantages de ces systèmes est qu'ils se basent sur plusieurs réseaux auxquels il est possible de se connecter alternativement pour contourner la censure. Un autre est évidemment de pouvoir surfer sur le Net de façon anonyme.

b. Limites

Par ailleurs, il faut noter que cette technologie peut ralentir de manière significative la connexion de l'utilisateur. Les internautes qui cherchent à contourner la censure s'apercevront également que les autorités en charge du filtrage prennent des mesures pour bloquer l'utilisation des systèmes de communications anonymes. Si ces systèmes passent par un port statique, le logiciel de filtrage peut être configuré pour en bloquer l'accès. Plus le système de communications anonymes est connu et plus le risque qu'il soit bloqué est important. Enfin, dans certains pays où Internet est contrôlé, l'utilisation de tels systèmes peut attirer l'attention sur les utilisateurs [7].

De plus, le logiciel d'anonymisation doit être installé sur l'ordinateur de l'utilisateur et certains nécessitent un certain degré de compétence technique. Il faut donc également disposer d'autorisations suffisantes. Comme pour le tunneling, les personnes qui accèdent à Internet via des terminaux publics, des bibliothèques ou des cybercafés seront très probablement incapables d'utiliser cette technique.

c. Exemples

- **Tor** est un réseau de tunnels virtuels qui permet à des personnes ou des groupes de personnes d'améliorer la confidentialité et la sécurité de leurs communications sur Internet. Tor offre une base pour toute une série d'applications qui permettent de partager des informations sur des réseaux publics sans compromettre la confidentialité des communications. Sur <http://www.torproject.org/index.html.fr>
- **JAP** permet de naviguer sur Internet de façon anonyme. Au lieu de se connecter directement à un serveur Web, les utilisateurs font un détour en se connectant de façon cryptée via plusieurs intermédiaires.
Sur http://anon.inf.tu-dresden.de/index_en.html
- **Freenet** est un logiciel libre qui permet de publier et d'obtenir des informations sur Internet sans craindre la censure. Il se base sur un réseau entièrement décentralisé où ceux qui publient ou utilisent les informations restent complètement anonymes.
Sur <http://freenetproject.org>

d. Récapitulatif

Avantages :

- Les systèmes de communications anonymes peuvent assurer à la fois la sécurité et l'anonymat.
- Nombreux protocoles supportés (et pas seulement le trafic Web)
- La communauté de d'utilisateurs et de développeurs fournit un support technique.

Inconvénients :

- Les systèmes de communications anonymes ne sont pas spécifiquement conçus pour le contournement.
- Ils sont largement connus et peuvent être filtrés.
- Ils ne sont pas utilisables aux points d'accès publics car ils nécessitent l'installation d'un logiciel
- Un certain niveau de compétences techniques est requis.

Conclusion

Cette étude de différentes solutions de contournement nous permet donc de dégager 4 grandes méthodes. Le choix de l'une ou l'autre de ces technologies dépendra des besoins de l'utilisateur en terme de d'anonymat (si l'utilisateur doit se protéger lors d'une tentative de contournement) ; en terme de fonctionnalités (consultation de sites Internet via le protocole http uniquement ou utilisation de services plus larges tel que les services d'e-mail, de transfert de fichiers, d'accès sécurisés). Ce choix se fera aussi en fonction de ses droits sur le poste utilisé (Il aura peu de droits dans une bibliothèque ou un cybercafé mais tout les droits sur un ordinateur personnel) ; de ses connaissances techniques (certaines technologies sont plus complexes à mettre en place) ; et enfin de ses contacts dans une zone non soumise au filtrage (Une personne ayant un contact pourra passer par une technologie de contournement dans un cadre privé alors qu'une personne n'ayant pas de contact sera obligée d'utiliser un service publique et souvent payant).

Pour les personnes dans un pays fortement soumis à la censure et où toute tentative de contournement est punie, il sera indispensable de passer par un système de communication anonyme.

Si la personne souhaite un accès complet à tous les services en ligne (consultation de page web, e-mail, transferts ftp et autres protocoles), il lui faudra obligatoirement avoir le droit d'installer sur son poste un logiciel spécifique, celui qu'il aura choisi pour le contournement, et savoir comment configurer ce logiciel.

Si la personne n'a besoin que d'un accès en consultation, un système de contournement en ligne public lui suffira. Cependant, il n'aura pas la possibilité de s'identifier ce qui exclu donc les *webmails*, les forums, et tous les sites nécessitant une authentification de l'utilisateur.

Pour les personnes ayant des contacts dans des zones non soumises à la censure et un point d'accès privé, les solutions de tunneling ou de *proxy* sont adaptées. L'utilisateur devra choisir entre ses 2 technologies en fonction des failles laissées dans sa zone de censure, il devra les essayer jusqu'à trouver une méthode non bloquée.

S'il en existe une qui fonctionne, l'utilisateur aura alors un accès complet à Internet. Il devra faire attention cependant : il peut être reconnu comme ayant recours a des méthodes de contournement. Il a la possibilité d'utiliser en plus un système de communication anonyme pour parfaire sa sécurité au détriment des performances du réseau.

Pour les personnes qui disposent d'un point d'accès privé mais d'aucun contact à l'étranger, il sera préférable d'utiliser des services commerciaux de tunneling ou de *proxy*. Attention cependant ! Les risques d'interception et de blocage sont beaucoup plus grands que sur des réseaux privés moins « formels ».

Les services gratuits et publics sont dans tous les cas fortement déconseillés en raison des risques encourus et de leur manque de fiabilité.

Pour les personnes n'ayant qu'un accès public et aucun contact, la seule solution reste des systèmes de contournement en ligne. Ceux qui ne sont pas bloqués par le filtrage en place permettront une simple consultation de page Internet.

Au final, des solutions existent et sont utilisées. Seulement, la nécessité d'avoir un point d'accès privé, des connaissances techniques et/ou des contacts à l'étranger peuvent être des contraintes bloquantes pour certaines personnes. L'utilisation de ces technologies peut également être dangereuse si l'utilisateur est intercepté. Selon les pays, les internautes les utilisant risquent des fortes amendes voire l'emprisonnement [8].

Dans tous les cas les mesures de contournement ne sont que des solutions « illégales » mises en place par des groupes de hackers ou par des sociétés commerciales. Le problème de la liberté d'expression ne sera réglé que le jour où des mesures politiques et juridiques seront mises en place. La Chine particulièrement subit des pressions politiques à l'occasion des Jeux Olympiques 2008 quelle doit organiser. Peut-être la liberté d'expression finira t'elle par s'assouplir pour permettre un jour un web International non censuré...

Références bibliographiques

[1] Reporters sans frontières. « La liste des 13 ennemis d'Internet », http://www.rsf.org/article.php3?id_article=19601, 7 novembre 2006

[2] Astrid Girardeau. « Censure et filtrage en forte hausse sur le net », <http://www.ecrans.fr/Censure-et-filtrage-en-forte.html>, 21 mai 2007.

[3] Eric Sautédé. « La censure de YouTube en Chine est une première », 19 mars 2008

[4] Sylvie Kauffmann, Martine Jacot, Brice Pedroletti. « La censure sur Internet : Etats contre cyberdissidents », dans Le Monde du 29/08/2007

[5] Pascale Nivelles. « A Pékin, les JO se rapprochent, pas les libertés », Libération du 11 avril 2008

[6] Nart Villeneuve. « Choisir sa technique pour contourner la censure », http://www.rsf.org/article.php3?id_article=14981, 14 avril 2006

[7] Bennett Haselton. « List of possible weaknesses in systems to circumvent Internet censorship », <http://peacefire.org/circumventor/list-of-possible-weaknesses.html>, 11/7/2002

[8] Sylvie Kauffmann, Martine Jacot, Brice Pedroletti, « La censure sur Internet : Etats contre cyberdissidents », Le Monde du 29/08/2007

Autres ressources en ligne : les sites des auteurs des solutions de contournement

<http://www.torproject.org/index.html.fr>

<http://freenetproject.org/>

http://anon.inf.tu-dresden.de/index_en.html