COMMENT CONTOURNER LA CENSURE SUR INTERNET

Published : 2017-06-21
License : GPLv2+

INTRODUCTION

1. INTRODUCTION

Le 10 décembre 1948, l'adoption de la Déclaration Universelle des Droits de l'Homme par l'Assemblée générale des Nations Unies a marqué le début d'une nouvelle ère. L'intellectuel libanais Charles Habib Malik a décrit cette scène aux délégués comme suit:

> *Chaque membre de l'Organisation des Nations Unies a solennellement promis de respecter et d'observer cette charte des Droits de l'Homme. En revanche, ces droits ne nous avaient jamais été clairement définis dans la déclaration, ni dans quelque autre instrument juridique national. C'est la première fois que ces principes des droits humains et des libertés fondamentales sont énoncés sous la contrainte et de manière précise.* ***Je sais maintenant ce que mon gouvernement s'est engagé à promouvoir, viser et respecter. Je peux m'agiter contre mon gouvernement et, s'il ne parvient pas à respecter son engagement, j'aurai avec moi le monde entier pour me soutenir moralement et je le saurai.***
>
> Un des droits fondamentaux décrit par l'article 19 de la Déclaration Universelle est le droit à la liberté d'expression:
>
> *Toute personne a le droit à la liberté d'opinion et d'expression; ce droit inclut la liberté d'affirmer ses opinions sans compromis,* ***et de chercher, recevoir et transmettre des informations et idées à travers tous les médias et sans tenir compte des frontières.***

Il y a 60 ans, lorsque ces mots ont été écrits, personne n'imaginait la façon dont le phénomène global qu'est Internet étendrait la capacité des gens à chercher, recevoir et transmettre des informations, pas seulement à travers les frontières, mais aussi à une vitesse hallucinante et sous des formes pouvant être copiées, éditées, manipulées, recombinées et partagées avec un petit nombre ou un large public, d'une manière fondamentalement différente des moyens de communication existants en 1948.

PLUS D'INFORMATIONS ET D'AUTANT D'ENDROITS INIMAGINABLES

L'incroyable augmentation, ces dernières années, de ce qui est disponible sur Internet et des lieux où se trouve l'information a eu pour effet de mettre une partie incroyablement vaste du savoir humain et de ses activités à disposition, et à des endroits que nous n'imaginions pas : Dans un hôpital d'un lointain village de montagne, dans la chambre de votre enfant de 12 ans, dans la salle de conférence où vous montrez à vos collègues le design du nouveau produit qui vous donnera de l'avance sur la concurrence, chez votre grand-mère.

Dans tous ces endroits, se connecter au monde ouvre un nombre impressionnant d'opportunités pour améliorer la vie des gens. Si vous attrapez une maladie rare pendant vos vacances, le petit hôpital du village peut vous sauver la vie en envoyant vos analyses à un spécialiste de la capitale, voire même dans un autre pays ; votre enfant de 12 ans peut faire des recherches pour son projet scolaire ou se faire des amis dans d'autres pays ; vous pouvez présenter votre nouveau produit à des responsables de bureaux du monde entier en simultanée, ils peuvent vous aider à l'améliorer ; votre grand-mère peut rapidement vous envoyer par e-mail sa recette spéciale de tarte aux pommes afin que vous ayez le temps de la faire pour le dessert de ce soir.

Mais Internet ne contient pas seulement des informations pertinentes et utiles à l'éducation, l'amitié et la tarte aux pommes. Comme le monde, il est vaste, complexe et souvent effrayant. Il est également accessible à des gens malveillants, avides, sans scrupules, malhonnêtes ou simplement malpolis, tout comme il vous est accessible ainsi qu'à votre enfant de 12 ans et à votre grand-mère.

PERSONNE NE VEUT LAISSER ENTRER

CHEZ SOI LE MONDE ENTIER

Avec le meilleur et le pire de la nature humaine transposés sur Internet et certains types d'escroquerie et de harcèlement rendus plus faciles par la technologie, il n'est pas surprenant que la croissance d'Internet ait été accompagnée de tentatives de contrôle de l'utilisation qui en est faite. Les motivations sont nombreuses, telles que :

- Protéger les enfants de contenus perçus comme inappropriés, ou limiter leur contact avec des gens pouvant leur nuire.
- Réduire le flot d'offres commerciales non désirées dans les e-mails ou sur le web.
- Contrôler la taille du flux de données auquel chaque utilisateur est capable d'accéder en même temps.
- Empêcher les employés de partager des informations considérées comme la propriété de leur employeur, d'utiliser une ressource technique de ce dernier ou leur temps de travail dans le cadre d'activités personnelles.
- Restreindre l'accès à des contenus ou activités en ligne, bannies ou réglementées dans une juridiction spécifique (un pays ou une organisation comme une école) à l'exemple de contenus explicitement sexuels ou violents, des drogues ou de l'alcool, des jeux et de la prostitution, des informations sur des groupes religieux, politiques ou autres groupes et idées réputés dangereux.

Certaines de ces préoccupations impliquent de permettre aux gens de contrôler leur propre expérience d'Internet, par exemple en utilisant des filtres bloquant les spams sur leur propre compte e-mail, mais d'autres préoccupations impliquent de restreindre la manière dont d'autres personnes peuvent utiliser Internet et ce à quoi elles peuvent ou non accéder. Ce dernier cas entraîne d'importants conflits et désaccords lorsque les personnes dont l'accès est restreint ne pensent pas que le blocage soit approprié ou dans leur intérêt.

QUI FILTRE OU BLOQUE INTERNET?

Les personnes ou institutions qui tentent de restreindre l'utilisation d'Internet à certains utilisateurs sont aussi nombreuses et diversifiées que leurs objectifs. Cela inclut les parents, les écoles, les sociétés commerciales, les cybercafés ou les fournisseurs d'accès Internet (FAI), et les gouvernements à différents niveaux.

L'extrémité du spectre du contrôle d'Internet, c'est quand un gouvernement tente de restreindre la possibilité à l'ensemble de sa population d'utiliser Internet pour accéder à toute une catégorie d'information ou de partager librement des informations avec le monde extérieur. Les recherches menées par l'OpenNet Initiative (http://opennet.net) ont montré les différentes manières que les pays utilisent pour filtrer et bloquer l'accès à Internet à leurs citoyens. On y compte des pays qui utilisent des politiques de filtrage invasives, pris en flagrant délit de blocage généralisé des accès aux organisations de défense des droits de l'homme, aux nouvelles, aux blogs et services Web, défiant le *status quo* ou jugés menaçants ou indésirables. D'autres pays bloquent l'accès à certaines catégories de contenus, ou de façon intermittente, vers certains sites Web ou services réseau lors d'évènements stratégiques : élections ou autres manifestations publiques. Même des pays défenseurs de la liberté d'expression essaient quelquefois de limiter ou de surveiller l'utilisation d'Internet en supprimant la pornographie, les contenus qualifiés de « discours haineux », le terrorisme, les autres activités criminelles, les correspondances militaires ou diplomatiques fuitées, ou encore les infractions au copyright.

FILTRER MÈNE À SURVEILLER

Chacun de ces groupes, officiel ou privé, peut aussi utiliser diverses techniques visant à surveiller l'activité en ligne des personnes qui l'inquiètent, pour être sûr que les tentatives de restriction fonctionnent. Ceci va des parents regardant par-dessus l'épaule de leurs enfants ou vérifiant les sites visités depuis leur ordinateur, aux sociétés surveillant les e-mails de leurs employés, en passant par les agences chargées de faire respecter la loi qui demandent des informations aux fournisseurs d'accès Internet (FAI), voire saisissent votre ordinateur comme preuve d'activités " indésirables ".

QUAND LA CENSURE EXISTE-T-ELLE?

Selon qu'on se place du point de vue ce celui qui restreint l'accès à Internet et/ou surveille son utilisation, ou de celui de la personne pour qui cet accès devient limité, presque aucun de ces objectifs, quel que soit la méthode utilisée pour y parvenir, ne peuvent être considérés comme légitimes et nécessaires. Il s'agit d'une censure inacceptable et d'une violation fondamentale des droits de l'homme. Un adolescent dont l'école bloque l'accès à son jeu en ligne favori ou à un réseau social comme Facebook, va trouver sa liberté personnelle limitée tout autant que quelqu'un que son gouvernement interdit de lire un journal en ligne sur l'opposition politique.

QUI BLOQUE MON ACCÈS À INTERNET?

L'identité des acteurs en mesure de restreindre l'accès à Internet sur un ordinateur donné, dans n'importe quel pays donné, dépend de qui a la possibilité de contrôler des parties spécifiques de l'infrastructure technique. Ce contrôle peut être basé sur des relations ou des exigences légalement établies, sur la capacité du gouvernement ou d'autres institutions, de faire pression sur ceux qui détiennent le contrôle légal de l'infrastructure technique pour satisfaire des demandes de blocage, de filtrage ou de collecte d'information. De nombreuses parties de l'infrastructure internationale sur lesquelles s'appuie Internet sont sous le contrôle de gouvernements, ou d'agences contrôlées par des gouvernements, lesquels peuvent effectuer ces restrictions, en accord avec la loi locale ou non. Le filtrage ou le blocage de parties d'Internet peut-être un processus complexe ou très simple, nettement défini ou presque invisible. Certains pays reconnaissent publiquement le blocage, publient leurs critères de blocage et remplacent les sites bloqués par des messages explicatifs. D'autres pays n'ont pas de politique claire et s'appuient parfois sur des interprétations floues ou incertaines pour faire pression sur les FAI afin d'exercer le filtrage. Dans certains cas, le filtrage est déguisé en faille technique et les gouvernements ne prennent pas ouvertement la responsabilité de reconnaître le blocage délibéré d'un site. Les opérateurs réseau, y compris d'un même pays et soumis aux mêmes réglementations, peuvent procéder au filtrage de plusieurs manières, par prudence, ignorance technique ou par compétition commerciale.

À tous les niveaux possibles de filtrage, depuis l'individu jusqu'à l'échelle nationale, les difficultés techniques rencontrées lors du blocage précis de ce qui est considéré comme indésirable peuvent avoir des conséquences inattendues et souvent ridicules. Les filtres parentaux censés bloquer les contenus à caractère sexuel empêchent l'accès à des informations médicales utiles. Les tentatives pour bloquer les spams peuvent supprimer des correspondances professionnelles importantes. Les tentatives pour bloquer l'accès à certains nouveaux sites peuvent aussi couper l'accès à des ressources éducatives.

QUELLES MÉTHODES EXISTENT POUR CONTOURNER LE FILTRAGE?

Tout comme de nombreux individus, des entreprises et gouvernements voient Internet comme une source d'information dangereuse qui doit être contrôlée, de nombreux individus et collectifs travaillent dur pour s'assurer qu'Internet, et les informations qu'on y trouve, sont librement accessibles à toute personne qui le souhaite. Ces personnes ont autant d'intentions différentes que celles qui cherchent à contrôler Internet. Toutefois, pour ceux dont la connexion à Internet est limitée et qui veulent en changer, peu importe que les outils aient été développés par quelqu'un qui voulait discuter avec sa petite amie, écrire un manifeste politique ou envoyer des spams.

Une grande quantité d'énergie, fournie par des groupes commerciaux, des associations à caractère non lucratif et des bénévoles dévoués, vouée à l'élaboration d'outils et de techniques pour contourner la censure sur Internet a permis la création de méthodes de contournement des mesures de filtrage d'Internet. Elles peuvent aller de simples canaux sécurisés à des programmes informatiques complexes. Cependant, elles fonctionnent à peu près toutes de la même manière : Elles indiquent à votre navigateur web de faire un détour par un ordinateur intermédiaire, appelé proxy, qui :

- est situé dans un lieu non soumis à la censure d'Internet ;
- n'a pas été bloqué depuis l'endroit où vous vous trouvez ;
- sait comment récupérer et renvoyer du contenu à des utilisateurs tel que vous.

QUELS SONT LES RISQUES D'UTILISATION DES OUTILS DE CONTOURNEMENT ?

Seul vous, qui espérez contourner les restrictions de votre accès Internet, êtes capable de décider s'il y a des risques notables à accéder à l'information que vous recherchez, mais aussi si le bénéfice est plus important que les risques encourus. Il n'y a peut-être aucune loi qui bannit spécifiquement l'information que vous voulez ou le fait d'y accéder. À l'inverse, le manque de sanctions légales ne signifie pas que cela ne présente aucun risque pour vous, comme le harcèlement, la perte de votre emploi, ou pire.

Les chapitres suivants expliquent comment fonctionne Internet, décrivent différentes formes de censure en ligne, et présentent des outils et techniques variés qui pourraient vous aider à contourner ces limites à la liberté d'expression. Le problème global de la vie privée et de la sécurité sur Internet sera étudié tout au long de ce livre, qui commence par traiter les bases, puis s'intéresse à quelques sujets plus avancés et se termine par une brève section destinée aux webmasters et aux spécialistes des ordinateurs qui souhaitent aider les autres à contourner la censure d'Internet.

2. A PROPOS DE CE GUIDE

Ce guide, « Contourner la censure sur Internet », introduit et explique l'utilisation de quelques logiciels et techniques parmi les plus utilisés pour outrepasser la censure.

Il apporte aussi des informations pour éviter la surveillance et la détection lors du contournement de la censure. Cependant, s'agissant d'un sujet très vaste, nous n'en parlerons que quand il y est directement lié.

Une discussion complète sur les techniques d'anonymat et éviter la détection de contenus ou d'activités est au-delà de la portée de ce livre.

COMMENT ET PAR QUI CE LIVRE A-T-IL ÉTÉ ÉCRIT ?

Le contenu de la première version de ce livre a été, en grande partie, rédigé lors d'un « Book Sprint » en novembre 2008 dans les belles montagnes de l'Etat de New York aux États-Unis. Huit personnes ont travaillé ensemble de manière intensive pendant cinq jours pour le créer.

La nouvelle version du guide que vous lisez en ce moment a été assemblée durant un second « Book Sprint », organisé près de Berlin, en Allemagne, début 2011. Cette fois, 11 personnes ont travaillé ensemble et sans relâche pendant 5 jours.

Ce livre est, bien sûr, un document voué à évoluer et disponible gratuitement sur Internet, où vous pouvez le modifier et l'améliorer.

En plus des contenus écrits durant les deux « Book Sprints », ce manuel contient des contenus issus de publications précédentes. Ceci ajoute les contributions de :

- Ronald Deibert
- Ethan Zuckerman
- Roger Dingledine
- Nart Villeneuve
- Steven Murdoch
- Ross Anderson
- Freerk Ohling
- Frontline Defenders
- Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, et John Palfrey du centre Berkman pour Internet et la société à l'Université d'Harvard

Ces auteurs ont gentiment accepté de nous laisser utiliser leur travail dans un contexte sous licence GPL.

Ce guide a été écrit dans les guides FLOSS. Pour l'enrichir, suivez les étapes suivantes :

1. S'INSCRIRE

Inscrivez-vous sur les guides FLOSS :
http://booki.flossmanuals.net/

2. CONTRIBUEZ !

Choisissez un manuel (http://booki.flossmanuals.net/bypassing-censorship/edit/) et un chapitre sur lequel vous souhaitez travailler.

Pour toute question relative à une contribution, rejoignez-nous sur le salon de discussion indiqué ci-dessous et contactez-nous ! Nous attendons votre contribution avec impatience !

Pour plus d'information sur l'utilisation des guides FLOSS, vous pouvez aussi lire notre guide:
http://en.flossmanuals.net/FLOSSManuals

3. CHAT

C'est une bonne idée de discuter avec nous, cela permet de coordonner toutes les contributions. Nous avons un salon de discussion dédié sur IRC (Internet Chat Relay). Si vous savez comment utiliser IRC, vous pouvez vous connecter grâce aux informations suivantes :
Serveur : irc.freenode.net
Canal : #booksprint

Si vous ne savez pas utiliser IRC, le site web suivant vous donne accès à un logiciel de discussion depuis votre navigateur internet :
http://irc.flossmanuals.net/

De l'aide pour l'utilisation de ce client IRC web est disponible à l'adresse suivante:
http://en.flossmanuals.net/FLOSSManuals/IRC

4. LISTE DE DIFFUSION

Pour discuter de n'importe quel sujet à propos des guides FLOSS, inscrivez-vous sur notre mailing list
: http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net

DÉMARRAGE RAPIDE

3. DÉMARRAGE RAPIDE

3. DÉMARRAGE RAPIDE

Internet est censuré quand les personnes ou groupes de personnes qui contrôlent un réseau empêchent les utilisateurs d'accéder à certains contenus ou services.

La censure sur Internet revêt plusieurs formes. Par exemple, des gouvernements peuvent bloquer les services e-mails habituels pour contraindre les citoyens à utiliser un service de messagerie étatique qui peut être facilement surveillé, filtré ou fermé. Les parents peuvent contrôler le contenu auquel accèdent leurs enfants mineurs. Une université peut empêcher les étudiants d'accéder à Facebook depuis la bibliothèque. Un gérant de cybercafé peut bloquer le partage de fichiers en peer to peer (P2P). Les régimes autoritaires peuvent censurer les rapports sur les atteintes aux droits de l'homme, ou sur les fraudes lors des précédentes élections. Les gens ont des points de vue très variables sur la légitimité de ces formes de censure.

CONTOURNEMENT

Le contournement est l'action de déjouer la censure d'Internet. Il y a bien des moyens de le faire, mais pratiquement tous les outils fonctionnent d'une manière similaire. Ils ordonnent à votre navigateur de passer par un ordinateur intermédiaire, appelé proxy, qui :

- est situé dans un lieu non soumis à la censure d'Internet
- n'a pas été bloqué depuis l'endroit où vous vous trouvez
- sait comment récupérer et renvoyer du contenu à des utilisateurs tels que vous.

SÉCURITÉ ET ANONYMAT

Gardez bien à l'esprit qu'aucun outil n'est la solution idéale pour votre situation. Les différents outils offrent des degrés de sécurité variables, mais la technologie ne peut éliminer les risques physiques que vous prenez en vous opposant au pouvoir en place. Ce livre contient plusieurs chapitres expliquant comment fonctionne Internet, ce qui est important pour comprendre la censure et comment la déjouer sans se mettre en danger.

IL Y A BEAUCOUP DE VARIANTES

Certains outils fonctionnent uniquement avec votre navigateur Web alors que d'autres peuvent être appliqués à plusieurs programmes à la fois. Ces programmes peuvent avoir besoin d'être configurés pour diriger le trafic Internet à travers un proxy. Avec un peu de patience, vous pourrez faire tout ça sans installer aucun programme sur votre ordinateur. Notez bien que les outils qui récupèrent les pages Web pour vous peuvent ne pas afficher les sites correctement.

Certains outils utilisent plus d'un ordinateur intermédiaire afin de cacher vos visites à des services bloqués. Cela aussi cache vos activités aux fournisseurs de ces outils, ce qui peut être important pour votre anonymat. Un outil peut avoir une manière intelligente de se renseigner sur les proxys alternatifs auxquels il peut se connecter, au cas où l'un de ceux que vous utilisez soit lui aussi censuré.

Dans l'idéal, le trafic généré par les requêtes, leur récupération et leur renvoi est chiffré afin de le protéger des regards indiscrets.

Choisir l'outil le plus adapté à votre situation n'est toutefois pratiquement pas la décision la plus importante que vous ferez quand il deviendra difficile d’accéder à ou de produire du contenu face à la censure d'Internet. Même si il est difficile de fournir des conseils concrets sur de telles choses, il est crucial de passer du temps à réfléchir sur le contexte, tel que :

- où, quand et comment vous avez l'intention d'utiliser ces outils.
- qui pourrait vouloir vous empêcher de faire ce que les outils vous permettent de faire.
- avec quelle force ces organisations et ces personnes s'opposent à cette utilisation.
- quelles ressources sont à leur disposition pour les aider à atteindre les objectifs qu'elles visent, jusqu'à et y compris la violence.

ACCÉDER À LA PLUPART DES SITES WEB BLOQUÉS SANS PROGRAMME COMPLÉMENTAIRE

L'outil de contournement le plus basique est le proxy Web. Bien qu'il y ait beaucoup de raisons pour que cela ne soit pas la solution optimale pour vous, c'est souvent un bon point de départ pour un contournement très basique. En admettant qu'elle n'est pas encore bloquée de chez vous, visitez l'adresse suivante : http://sesaweenglishforum.net

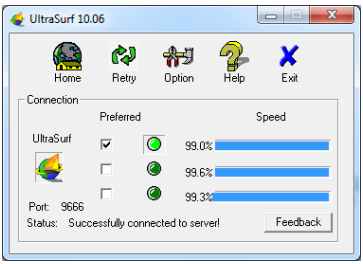
Acceptez les conditions d'utilisation, et entrez l'adresse du site bloqué que vous voulez visiter dans la barre d'adresse bleue :

Appuyez sur Entrée ou cliquez sur GO et, si vous accédez au site demandé, cela fonctionne. Si le lien ci-dessus ne fonctionne pas, vous devrez trouver une autre méthode de contournement. Les chapitres sur les proxys Web et sur Psiphon dans ce livre donnent quelques conseils pour trouver un proxy Web et plein d'autres pour décider si vous devriez vous en servir une fois que vous l'avez trouvé.

Si vous avez besoin d'accéder à toutes les fonctionnalités d'un site Web particulièrement complexe comme Facebook, vous voudrez certainement utiliser un outil simple, installable comme Ultrasurf plutôt qu'un proxy Web. Si vous désirez ou avez besoin d'une solution éprouvée par des tests de sécurité rigoureux dans le but de rester anonyme sans avoir besoin de savoir qui administre le service, vous devriez utiliser Tor. Si vous avez besoin d'accéder via Internet à des services filtrés autres que des sites Web, comme par exemple des plateformes de messagerie instantanées ou des serveurs mails (ceux utilisés par des programmes comme Mozilla Thunderbird ou Microsoft Outlook), vous devriez essayer HotSpot Shield ou d'autres services OpenVPN. Tous ces outils, qui ont leur propre chapitre plus loin dans ce livre, sont décrits brièvement ci-dessous.

ACCÉDER À TOUS LES SITES WEB ET PLATEFORMES BLOQUÉS

Ultrasurf est un outil proxy gratuit pour les systèmes d'exploitation Windows. Il peut être téléchargé ici : http://www.ultrareach.com/, http://www.ultrareach.net/ ou http://www.wujie.net/. Le fichier Zip téléchargé doit être décompressé à l'aide du clic droit, en sélectionnant « Extraire tout... ». Le fichier .exe extrait peut être lancé directement (même d'une clé USB dans un cybercafé) sans installation.



Ultrasurf se connecte automatiquement et lance une nouvelle instance du navigateur Internet Explorer ave lequel vous ouvrirez les sites Web bloqués.

OUTREPASSER LES FILTRES ET RESTER ANONYME SUR LE WEB

Tor est un réseau sophistiqué de serveurs proxys. C'est un programme gratuit et libre, développé principalement pour permettre la navigation Web anonyme. Il s'agit aussi un merveilleux outil pour contourner la censure. Le navigateur Tor Bundle pour Windows, Mac OS X ou GNU/Linux peut être téléchargé depuis https://www.torproject.org/download/download.html.fr. Si le site Web torproject.org est bloqué, vous pouvez trouver d'autres endroits où l'obtenir en tapant "tor mirror" dans votre moteur de recherche préféré ou en envoyant un email à gettor@torproject.org contenant « help » dans le corps du message.

Quand vous cliquez sur le fichier téléchargé, il s'extrait à l'endroit que vous voulez. Cela peut aussi être une clé USB qui pourra être utilisée dans un cybercafé. Vous pouvez lancer Tor en cliquant sur « Démarrer Tor Browser » (attention à bien fermer toutes les instances de Tor ou Firefox qui sont déjà en fonctionnement). Après quelques secondes, Tor lance une version spéciale du navigateur Firefox sur un site Web de test. Si ce message s'inscrit en vert « Congratulations. Your browser is configured to use Tor. » (« Félicitations. Votre navigateur est configuré pour utiliser Tor. »), vous pouvez alors utiliser cette fenêtre pour visiter les sites Web jusqu'alors bloqués.

ENCAPSULEZ TOUT VOTRE TRAFIC INTERNET DANS UN TUNNEL SÉCURISÉ

Si vous voulez accéder à des services Internet autres que le Web, comme les emails, via un client comme Outlook ou Thunderbird, une manière simple et sûre est d'utiliser un VPN (pour Virtual Private Network, soit Réseau privé virtuel). Un VPN va chiffrer dans un canal tout le trafic Internet entre vous et un autre ordinateur, de telle manière que, non seulement les différentes sortes de communication apparaîtront identiques aux oreilles indiscrètes, mais le chiffrement les rendra illisibles à tout le monde sur tout leur trajet. Quand vous vous connectez à un VPN, votre FAI ne verra pas le contenu que vous échangez, mais il sera toutefois capable de voir que vous vous connectez à un VPN. Beaucoup de compagnies internationales utilisent un VPN pour se connecter de manière sécurisé à leurs bureaux distants, la technologie VPN a peu de risque d'être bloquée dans son ensemble.

Hotspot Shield

Une manière simple de débuter avec les VPN est d'utiliser Hotspot Shield. Il s'agit d'une solution VPN gratuite (mais commerciale) disponible pour les systèmes d'exploitation Windows et Mac OS X.

Pour installer Hotspot Shield vous devez télécharger le programme depuis https://www.hotspotshield.com. La taille du fichier est d'environ 6Mo, donc avec une connexion lente, le téléchargement peut prendre 25 minutes ou plus. Pour l'installer, double-cliquez sur le fichier téléchargé et suivez les instructions données par l'assistant d'installation.

Une fois l'installation terminée, démarrez Hotspot Shield en cliquant sur l'icône « Hotspot Shield Launch » sur votre bureau ou par « Programmes > Hotspot Shield ». Une fenêtre de navigation s'ouvrira sur une page de statut montrant les différentes étapes des tentatives de connexion : « Authentification » ou « Assignation de l'adresse IP ». Une fois connecté, Hotspot Shield vous redirigera vers une page de bienvenue. Cliquez sur « Start » pour commencer la navigation.

Pour arrêter Hotspot Shield, faites un clic-droit sur l'icône dans la barre de tâches et sélectionnez « Disconnect/OFF ».

CONTEXTE GÉNÉRAL

4. COMMENT FONCTIONNE LE RÉSEAU ?
5. LE NET ET LA CENSURE
6. CONTOURNEMENT ET SÉCURITÉ

4. COMMENT FONCTIONNE LE RÉSEAU ?

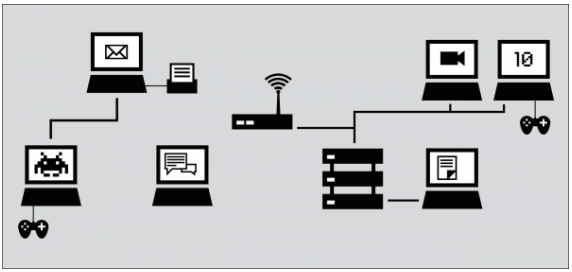
Imaginez un groupe de personnes qui décident de partager des informations disponibles sur leurs ordinateurs en les connectant, et en échangeant ces informations entre tous ces ordinateurs. Le résultat de leurs efforts est un ensemble d'interfaces capables de communiquer les unes avec les autres au travers d'un réseau. Bien entendu, ce réseau a encore plus de valeur et d'utilité s'il est connecté à d'autres réseaux, à d'autres ordinateurs, et, par conséquent, d'autres utilisateurs.

Ce désir simple de vouloir se connecter et partager de l'information de façon électronique se manifeste aujourd'hui sous la forme d'Internet. Alors qu'Internet s'est rapidement développé, la complexité de ses interconnexions a, elle aussi, augmenté. Internet est littéralement bâti sur l'interconnexion d'un très grand nombre de réseaux.

L'application fondamentale d'Internet peut être décrite comme un facilitateur de transfert des informations digitales, depuis leur point de départ jusqu'à leur destination, en utilisant un chemin adapté et un mode de transport approprié.

Les réseaux locaux d'ordinateurs, appelés « LAN » (pour Local Area Network), connectent physiquement un certain nombre d'ordinateurs et autres périphériques entre eux s'ils sont réunis en un même lieu. Les LAN peuvent aussi se connecter à d'autres réseaux grâce à des appareils nommés routeurs qui gèrent les flux d'informations entre les réseaux. Les ordinateurs d'un LAN peuvent communiquer entre eux directement, afin d'échanger des fichiers, de partager des imprimantes, ou de jouer à des jeux en réseau multi-joueurs.

Un LAN serait fonctionnel même si il n'était pas connecté au reste du monde, mais il devient clairement plus utile lorsqu'il l'est.



L'Internet d'aujourd'hui est un réseau mondial décentralisé de réseaux locaux d'ordinateurs, aussi vastes que les réseaux d'universités, d'entreprises, d'opérateurs ou d'hébergeurs de services.

Les organisations qui gèrent les interconnexions entre ces différents réseaux sont appelés Fournisseurs d'Accès à Internet (FAI). Le rôle d'un FAI est de faire parvenir les données à l'endroit approprié, généralement en faisant suivre ces données vers un nouveau routeur (appelé routeur de « Prochain Saut » ou « Next Hop ») plus proche de la destination finale des données. Souvent, ce routeur de « Prochain Saut » appartient à un FAI différent.

Pour ce faire, le FAI doit lui-même obtenir un accès à Internet, depuis un FAI plus important tel qu'un opérateur national (certains pays ont un seul opérateur d'ordre national, probablement l'opérateur historique du pays, ou un opérateur lié au gouvernement, alors que d'autres pays ont plusieurs opérateurs, qui peuvent être des entreprises privées de télécommunication se faisant concurrence). Les FAI nationaux peuvent recevoir leur connexion depuis une des compagnies internationales qui maintiennent et utilisent les serveurs et connexions qui forment ce que l'on appelle souvent une « épine dorsale » (ou « Backbone ») d'Internet.

« L'épine dorsale » est construite à partir des plus importants équipements, installations et infrastructures de réseaux et de leurs interconnexions à l'échelle mondiale, via des câbles de fibres optiques et des satellites. Ces connexions établissent des communications entre les utilisateurs d'Internet dans les différents pays et continents. Les FAI nationaux et internationaux se connectent à cette « épine dorsale » à travers des routeurs connus sous le nom de « passerelles », qui permettent aux réseaux dispersés de communiquer entre eux. Ces passerelles, comme d'autres routeurs, peuvent être des points de contrôle et de surveillance du trafic Internet.

STRUCTURER INTERNET

Les architectes d'Internet admettent généralement qu'il n'y a qu'un seul internet, qu'il est global, et qu'il devrait permettre à n'importe quelle paire d'ordinateurs, situés n'importe où dans le monde de pouvoir communiquer directement l'un avec l'autre, dans la mesure où les propriétaires respectifs de ces ordinateurs le souhaitent.

Dans une note de 1996, Brian Carpenter, alors président du comité pour l'architecture d'Internet (Internet Architecture Board), écrivait:

```
D'une façon très générale, la communauté — de ceux qui élaborent
Internet — croit
que le but est la connectivité… La croissance du réseau semble montrer
qu'elle est
une récompense en soi, bien plus que chaque application individuelle.
```

Il existe encore une communauté majeure des pionniers d'Internet et des utilisateurs de la première heure qui privilégient les idéaux d'inter-connectivité mondiale, de standards ouverts et de libre accès à l'information, bien que ces idéaux entrent souvent en conflit avec les intérêts politiques et économiques et n'influencent pas directement la gestion ni la politique courante de chaque parcelle d'Internet. Les initiateurs d'Internet ont aussi créé, et continuent de créer, des standards conçus pour que d'autres puissent facilement monter leurs propres réseaux, et les connecter entre eux. Comprendre les standards d'Internet permet de mieux comprendre comment Internet fonctionne et comment les sites et services en ligne deviennent ou non accessibles.

STANDARDS DE CONNEXION DES APPAREILS

Aujourd'hui, la plupart des LAN sont construits avec la technologie Ethernet câblée ou sans fil (802.11 ou Wi-Fi). Toutes les interconnexions (de LAN et d'autres interfaces) qui constituent Internet utilisent des standards techniques, dits **protocoles** Internet, afin de permettre aux ordinateurs de communiquer entre eux. Souvent, ces interconnexions utilisent des équipements et installations privées, et sont mises en place en vue de la réalisation d'un profit. Dans certaines juridictions, les connexions internet sont réglementées en détails. Dans d'autres, il y a très peu ou pas de réglementation.

Le standard élémentaire qui unit tous les appareils sur l'Internet global est appelé l'« Internet Protocol » (IP).

STANDARDS D'IDENTIFICATION DES INTERFACES RÉSEAU

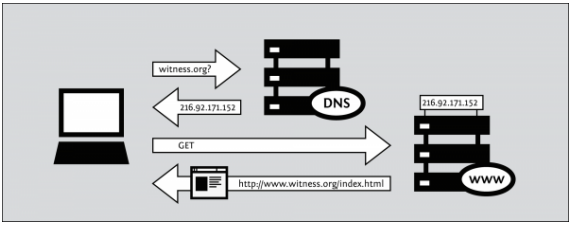
Quand votre ordinateur se connecte à Internet, il lui est normalement assigné une adresse numérique IP. Comme une adresse postale, l'adresse IP identifie de manière unique un seul ordinateur sur Internet. Contrairement à l'adresse postale, cependant, une adresse IP (particulièrement pour un matériel informatique personnel) n'est pas nécessairement liée de façon permanente à un ordinateur en particulier. Ainsi, lorsque votre ordinateur se déconnecte d'Internet et se reconnecte plus tard, il peut recevoir une adresse IP (unique) différente. La version du protocole IP dont l'usage est actuellement prédominant est IPv4. Dans le protocole IPv4, une adresse IP est écrite sous la forme de quatre nombres, compris entre 0 et 255, séparés par des points (par ex. : 207.123.209.9).

NOMS DE DOMAINES ET ADRESSES IP

Tous les serveurs Internet, tels que ceux qui hébergent les sites Web, ont également des adresses IP.

Par exemple, l'adresse IP de www.witness.org est 216.92.171.152. Étant donné que se rappeler d'une adresse IP n'est pas pratique et qu'elle peut changer avec le temps, un système spécifique a été mis en place pour vous permettre d'atteindre plus facilement votre destination sur Internet. Ce système, c'est le DNS (pour « Domain Name System », ou « Système des noms de domaines »), dans lequel un ensemble d'ordinateurs est chargé de fournir à votre ordinateur les adresses IP associées aux « noms » humainement mémorisables.

Par exemple, pour accéder au site de Witness, vous entrerez l'adresse www.witness.org, que l'on appelle également un nom de domaine, au lieu de 216.92.171.152. Votre ordinateur enverra alors un message avec ce nom à un serveur DNS. Une fois que le serveur DNS a traduit le nom de domaine en une adresse IP, il partage cette information avec votre ordinateur. Ce système rend la navigation web et d'autres usages d'internet plus conviviaux pour les humains, et plus protocolaires pour les ordinateurs.



D'un point de vue mathématique, IPv4 permet à un bassin de 4.2 milliards d'ordinateurs différents, d'être connectés à Internet. Il existe aussi une technologie qui permet à de multiples ordinateurs de partager la même adresse IP. Le stock d'adresses disponibles s'est toutefois trouvé plus ou moins épuisé au début de l'année 2011, le protocole IPv6 a donc été conçu. Il offre un répertoire d'adresses uniques beaucoup plus important. Les adresses IPv6 sont beaucoup plus longues, et encore plus difficiles à retenir que les traditionnelles adresses IPv4. Par exemple,
2001:0db8:85a3:0000:0000:8a2e:0370:7334

En 2011, moins d'1% d'internet utilise le protocole IPv6 mais cela risque d'évoluer considérablement dans un avenir proche.

PROTOCOLES D'ENVOI D'INFORMATION VIA LE RÉSEAU

L'information que vous échangez via Internet peut prendre plusieurs formes :

- Un email à votre cousin.
- La photo ou vidéo d'un événement.
- Une base de données d'informations de contact.
- Un fichier contenant des consignes.
- Un document contenant un rapport sur un sujet sensible.
- Un programme informatique qui enseigne une compétence.

Il y a une multitude de programmes Internet adaptés à la manipulation adéquate des divers types d'information en fonction de protocoles spécifiques :

- L'email via SMTP (« Simple Mail Transport Protocol » soit « Protocole simple de transfert de courrier »).
- La messagerie instantanée via XMPP (« eXtensible Messaging and Presence Protocol » soit « Protocole extensible de messagerie et de présence »).
- Le partage de fichiers via FTP (« File Transfert Protocol » ou « Protocole de transfert de fichiers »).
- Le partage de fichiers en peer to peer via BitTorrent.
- Les newsgroups sur le réseau Usenet, via le NNTP (« Network News Transfer Protocol » ou « Protocole réseau de transfert de nouvelles »).
- Une combinaison de plusieurs protocoles : la communication vocale utilisant la VoIP (« Voice overt Internet Protocole » soit « Voix sur IP »), SIP (« Session Initiation Protocol » soit « Protocole d'initiation de session ») et RTP (« Real-time Transport Protocol » ou « Protocole de transfert en temps réel »).

LE WEB

Bien que beaucoup de gens utilisent indifféremment les termes « Internet » et « Web », le Web ne fait réellement référence qu'à une seule façon de communiquer sur Internet. Lorsque vous accédez au Web, vous le faites en ayant recours à un logiciel appelé un navigateur Web, tels que Mozilla Firefox, Google Chrome, Opera, ou Microsoft Internet Explorer. Le protocole qui régit le Web est appelé HTTP (« Hyper-Text Transfert Protocol » ou « Protocole de transfert hypertexte »). Vous avez sans doute entendu parler du HTTPS, la version sécurisée du HTTP, qui utilise un cryptage TLS (« Transport Layer Security » soit « Sécurité de transport par couche »), pour protéger vos communications.

PARCOURS DE VOS INFORMATIONS SUR INTERNET

Suivons l'exemple d'une visite de site web à partir de votre ordinateur personnel.

Connexion à Internet

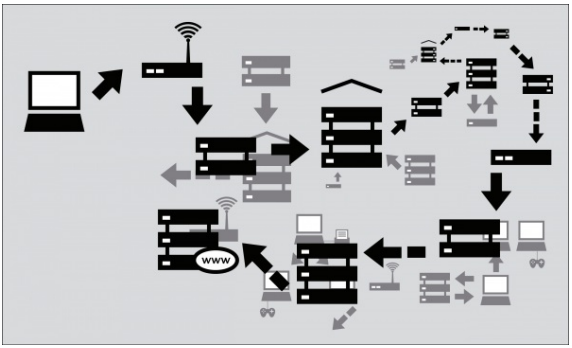
Pour connecter votre ordinateur à Internet, vous aurez besoin d'un équipement supplémentaire, comme un modem ou un routeur, pour vous connecter au réseau de votre FAI. Habituellement, l'ordinateur de l'utilisateur final peut être connecté avec son FAI de plusieurs façons :

- un modem, utilisant les lignes téléphoniques pour envoyer les données sous forme d'appel téléphonique.
- L'ADSL ou le SDSL, un moyen plus rapide et plus efficace pour envoyer des données par lignes téléphoniques sur de courtes distances.
- le modem câble, qui envoie les données par le réseau câblé de la télévision.
- Les câbles en fibre optique, surtout en zones urbaines à forte densité des pays développés.
- Les liaisons sans-fil élargies fixes, surtout en zones rurales.
- les services data par le réseau de téléphonie mobile.

Navigation jusqu'au site web

1. Vous saisissez https://security.ngoinabox.org/. L'ordinateur envoie le nom de domaine « security.ngoinabox.org » à un serveur DNS sélectionné, qui renvoie un message contenant l'adresse IP pour le serveur de « Tactical Tech Security in a Box » (actuellement, 64.150.181.101).
2. Le navigateur envoie une requête de connexion à cette adresse IP.
3. La requête passe à travers une série de routeurs, chacun faisant suivre à un routeur plus proche de la destination de la requête une copie de celle-ci, jusqu'à ce qu'elle atteigne un routeur qui trouve l'ordinateur spécifique désiré.
4. Cet ordinateur vous renvoie l'information voulue, autorisant votre navigateur à envoyer l'URL complet et donc à recevoir les données nécessaires pour afficher la page.

Le message du site web jusqu'à vous voyage à travers d'autres appareils (ordinateurs ou routeurs) : Chacun des appareils situés le long d'un chemin peut être appelé un saut. Le nombre de sauts est le nombre d'ordinateurs ou de routeurs que votre message rencontre le long de son trajet, souvent compris entre 5 et 30.



POURQUOI C'EST IMPORTANT

En temps normal, tous ces processus complexes sont cachés et vous n'avez pas besoin de les comprendre pour trouver l'information que vous recherchez. Cependant, quand des personnes ou des organisations essayent de limiter votre accès à l'information interfèrent avec la bonne marche de ce système, votre capacité à utiliser Internet peut être restreinte. Dans ce cas, bien comprendre ce qu'elles ont fait pour interférer avec votre accès peut devenir très intéressant.

Considérez les pare-feux. Il s'agit d'appareils qui interdisent intentionnellement certains types de communication entre un ordinateur et un autre. Les pare-feux aident un propriétaire de réseau à faire respecter ses politiques concernant quels types de communication et quels usages du réseau il autorise. Au début, l'usage de pare-feux était conçu comme une mesure de sécurité informatique : Ils pouvaient repousser des attaques informatiques à l'encontre d'ordinateurs mal configurés par mégarde et vulnérables. Les pare-feux sont maintenant utilisés pour bien d'autres objectifs et pour faire appliquer des politiques de contrôle bien au-delà du domaine de la sécurité informatique, dont le contrôle des contenus.

Un autre exemple est celui des serveurs DNS, décrits comme aidant à fournir une adresse IP correspondant au nom de domaine demandé. Dans certains cas, ces serveurs peuvent être utilisés comme des mécanismes de censure en empêchant la bonne adresse IP d'être renvoyée, et ainsi bloquant effectivement l'accès à l'information demandée sur ce domaine.

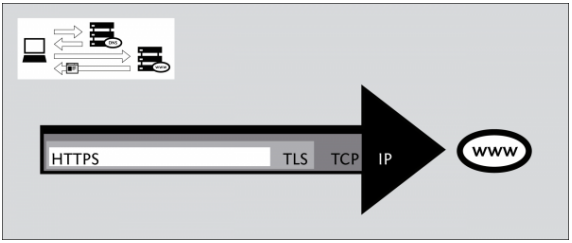
La censure peut avoir lieu à différents points de l'infrastructure d'Internet, couvrant tout le réseau, des domaines et sous domaines, des protocoles individuels, ou un contenu spécifique identifié par un logiciel de filtrage. La meilleure méthode pour éviter la censure dépendra de la méthode spécifique de censure utilisée. Comprendre ces différences vous aidera à choisir les mesures appropriées pour que vous puissiez utiliser Internet efficacement et sûrement.

PORTS ET PROTOCOLES

Pour pouvoir partager des données et des ressources, les ordinateurs ont besoin d'accepter des conventions sur le format et la façon d'échanger l'information. Ces conventions, que nous appelons protocoles, sont parfois comparées à la grammaire des langages humains. L'Internet est basé sur une série de protocoles de ce genre.

Le modèle en couches du réseau

Les protocoles Internet reposent sur d'autres protocoles. Par exemple, quand vous utilisez un navigateur Web pour accéder à un site, le navigateur se base sur le protocole HTTP ou HTTPS pour communiquer avec le serveur Web. Cette communication, à son tour, repose sur d'autres protocoles. Supposons que nous utilisions HTTPS avec un site web donné, pour nous assurer que nous y accédons de façon sécurisé.



Dans l'exemple précédent, le protocole HTTPS repose sur le protocole **TLS** pour chiffrer les communications, afin de les rendre privées et non modifiées lorsqu'elles voyagent sur le réseau. Le protocole TLS, à son tour, repose sur le protocole **TCP**, pour s'assurer que cette information n'est pas accidentellement perdue ou abimée pendant la transmission. Finalement, TCP repose sur le protocole IP, pour s'assurer que les données sont délivrées à la destination voulue.

En utilisant le protocole chiffré HTTPS, votre ordinateur utilise toujours le protocole non chiffré DNS pour récupérer l'adresse IP associée au nom de domaine. Le protocole DNS utilise le protocole **UDP** pour véritablement router la requête au serveur DNS, et UDP repose sur IP pour la transmission effective des données à la destination voulue.

À cause de cette hiérarchie entre les protocoles, on parle souvent des protocoles réseaux comme d'un ensemble de couches. Les protocoles de chaque couche correspondent à un aspect du fonctionnement des communications.

Se servir des ports

Les ordinateurs se connectent entre eux via le protocole TCP mentionné ci-dessus et restent connectés durant un certain temps pour permettre aux protocoles de plus haut niveau d'effectuer leurs tâches. TCP utilise le concept de numéro de **port** pour gérer ces connexions et les distinguer les unes des autres. Les numéros de port permettent aussi à l'ordinateur de décider lequel des logiciels devrait accepter telle requête ou donnée. UDP implémente lui aussi une fonctionnalité similaire.

L'IANA (« Internet Assigned Names Authority » ou « Autorité de distribution des noms sur Internet ») assigne des numéros de port pour divers protocoles de haut niveau utilisés par les services applicatifs. Voici quelques exemples communs de numéros de port standard :

- 20 et 21 FTP (transfert de fichier)
- 22 SSH (accès à distance sécurisé)
- 23 Telnet (accès à distance peu sûr)
- 25 SMTP (transfert d'email)
- 53 DNS (résolution d'un nom d'ordinateur en adresse IP)
- 80 HTTP (navigation Web normale, parfois utilisé par les proxys)
- 110 POP3 (lecture d'email)
- 143 IMAP (envoi et réception d'email)
- 443 HTTPS (connexion Web sécurisée)
- 993 IMAPS (IMAP sécurisé)
- 995 POP3S (POP3 sécurisé)
- 1080 SOCKS (proxy de bas niveau)
- 1194 OpenVPN (réseau privé virtuel)
- 3128 Squid (proxy)
- 8080 Proxy HTTP standard

L'utilisation de ces numéros de port particuliers n'est généralement pas une directive du protocole. En fait, n'importe quel type de données pourrait être envoyé à travers n'importe quel port (et utiliser des ports non standards peut être un moyen de contournement technique utile). Cependant ces numéros sont utilisés par défaut, pour des raisons pratiques. Par exemple, votre navigateur sait que, si vous demandez un site Web sans numéro de port, il devrait automatiquement essayer d'utiliser le port 80. D'autres types de logiciel ont également de tels comportements par défaut de manière à ce que vous puissiez utiliser normalement Internet sans avoir à connaître et vous rappeler des numéros de port associés aux services que vous utilisez.

La cryptographie

La cryptographie est une forme de défense technique contre la surveillance qui utilise des procédés mathématiques sophistiqués pour brouiller les communications et les rendre incompréhensibles à des oreilles indiscrètes. La cryptographie peut également empêcher qu'un opérateur réseau ne modifie les communications, ou au moins rendre de telles modifications détectables. Cela marche généralement comme un tunnel depuis le logiciel que vous utilisez, tel un navigateur, jusqu'à l'autre bout de la connexion, comme un serveur Web.

La cryptographie moderne est connue pour sa grande résistance aux attaques techniques. La grande disponibilité des logiciels de chiffrage donne aux utilisateurs une protection de leur vie privée très résistante aux écoutes. D'un autre côté, le chiffrement peut être contourné par différents moyens, via des **logiciels malveillants** ou, de manière plus générale, lors d'un problème de partage ou d'échange de **clés de chiffrement**, lorsque les utilisateurs ne peuvent pas suivre ou ignorent les procédures nécessaires à l'utilisation sûre de la cryptographie. Par exemple, les logiciels de chiffrement ont généralement besoin d'un moyen de vérifier l'identité de la personne de l'autre côté de la connexion réseau. Sans quoi, la communication serait vulnérable à une attaque « **man-in-the-middle** » (soit « un homme au milieu ») où une tierce personne se fait passer pour le correspondant de chacun pour intercepter les communications. La vérification d'identité est effectuée de différentes manières par différents logiciels, mais ignorer ou contourner cette étape augmente votre vulnérabilité à l'écoute.

Une autre technique de surveillance est **l'analyse de trafic**, où des informations sur les communications sont utilisées pour deviner leur contenu, leur origine ou leur destination, même si le contenu reste incompréhensible au censeur. L'analyse de trafic peut être une technique très efficace et que l’on peut difficilement contrer. Cela concerne en particulier les systèmes d'anonymisation, où les techniques d'analyse de trafic peuvent aider à identifier un participant anonyme. Les systèmes d'anonymisation avancés comme Tor prennent en compte des mesures faites pour réduire l'efficacité de l'analyse de trafic, mais peuvent rester vulnérables selon la puissance du système d'écoute.

5. LE NET ET LA CENSURE

Comprendre comment Internet fonctionne dans la pratique peut aider à associer les sources de censure à des menaces potentielles. Le contrôle et la censure d'Internet peuvent revêtir de nombreuses formes. Un gouvernement national pourrait non seulement bloquer l'accès à du contenu, surveiller le type d'informations consultées, et pourrait punir des utilisateurs pour leurs activités en ligne qu'il jugerait inacceptable. Les gouvernements peuvent soit définir le contenu à bloquer et mettre le filtrage en pratique eux-mêmes, soit créer un cadre légal, ou extra-légal, pour encourager des entreprises indépendantes à mettre en place le blocage et la surveillance.

QUI CONTRÔLE INTERNET ?

L'histoire complète de la gouvernance d'Internet est complexe et politique. Elle est encore débattue actuellement. Les gouvernements ont souvent le pouvoir et les ressources pour mettre en place leur méthode de surveillance et de contrôle favorite, s'ils possèdent et dirigent les infrastructures directement ou par des entreprises de télécommunication privées. Un gouvernement qui veut bloquer l'accès à l'information peut facilement le faire, directement ou indirectement, au niveau de la création de l'information où lors de sa traversée de la frontière.

Les gouvernements ont aussi l'autorité légale pour espionner les citoyens, beaucoup vont même au-delà de ce que la loi autorise en utilisant des méthodes extra-légales pour surveiller et restreindre l'utilisation d'Internet, voire la transformer selon leurs propres règles.

IMPLICATION DES GOUVERNEMENTS

Internet a été développé par des chercheurs financés par le gouvernement américains dans les années 1970. Il s'est progressivement imposé au niveau universitaire, puis aux utilisations personnelle et professionnelle.

De nos jours, une communauté globale travaille à maintenir les standards et partenariats qui ont pour but de parvenir à une connectivité et interopérabilité au niveau mondial, sans aucune distinction géographique.

Cependant, les gouvernements n'ont pas intérêt à suivre les cette ligne de conduite. Certains construisent leur réseau national de télécommunications afin d'avoir des « points centraux » où ils peuvent contrôler l'accès de tout le pays à des services ou sites spécifiques voire, dans certains cas, empêcher l'accès à cette portion d'Internet depuis l'extérieur. D'autres gouvernements ont passé des lois ou opté pour des contrôles informels afin de réguler le comportement des FAI privés en les incitant parfois à participer à la surveillance, au blocage, ou à supprimer l'accès à des éléments particuliers.

Certaines infrastructures d'Internet sont gérées par des gouvernements ou des entreprises en lien avec des gouvernements. Il n'existe aucun organe de gouvernance d'Internet qui soit totalement indépendant. Les gouvernements traitent les affaires de contrôle d'Internet et des infrastructures de télécommunications comme des questions de souveraineté nationale. Nombre d'entre eux se permettent d'interdire ou de bloquer l'accès à certains types de contenus et services jugés offensant ou dangereux.

POURQUOI LES ÉTATS VOUDRAIENT-ILS CONTRÔLER LE NET ?

Bon nombre de gouvernements ont un problème avec le fait qu'Internet n'ait aucune frontière technique, géographique ou politique. Pour l'utilisateur final, sauf à compter les millisecondes, cela ne fait strictement aucune différence qu'un site soit hébergé dans le même pays ou à l'autre bout du monde. Cet état de fait est très alarmant pour les États. La censure sur Internet, inspirée des espoirs de rétablir des frontières géographiques, peut arriver pour beaucoup de raisons.

La classification suivante est adaptée de l'Open Net Initiative http://opennet.net/

- **Les raisons politiques**
  Les gouvernements veulent censurer les points de vue et opinions contraires à celles propres au pays, ce qui inclut des sujets comme les droits de l'homme ou la religion.
- **Les raisons sociales**
  Les gouvernements veulent censurer les pages Web relatives à la pornographie, aux jeux d'argent, à l'alcool, aux drogues, et tout autre sujet qui pourrait sembler choquant pour la population.
- **Les raisons de sécurité nationale**
  Les gouvernements veulent bloquer le contenu associé à des mouvements dissidents, et tout ce qui menace la sécurité nationale.

Afin de s'assurer que les contrôles de l'information sont efficaces, les gouvernements peuvent aussi filtrer les outils qui permettent aux gens de contourner la censure d'Internet. Dans les cas extrêmes, les gouvernements peuvent refuser de fournir un accès à Internet au public, comme en Corée du Nord, où Internet peut être coupé sur tout le territoire pendant des périodes de protestations publiques, comme ce qui est arrivé brièvement au Népal en 2005, en Égypte ou en Libye en 2011.

Le contrôle peut être effectué à la fois sur les fournisseurs d'accès et les fournisseurs de contenu.

- Les gouvernements peuvent soumettre les fournisseurs d'accès à un contrôle strict, afin de réguler et gérer le trafic Internet, et de permettre la surveillance et la gestion des internautes dans le pays. Cela permet également de bloquer le contenu qui vient de l'étranger. N'ayant aucun contrôle sur le fournisseur de contenu Facebook, Le gouvernement pakistanais a demandé aux FAI locaux de bloquer l'accès à Facebook en mai 2010 afin de bloquer l'accès à des caricatures du prophète Mahomet qui ont été rendues disponibles sur le réseau social.
- Les gouvernements peuvent demander à des fournisseur de contenus, comme les éditeurs de sites web présents dans le pays, les webmasters ou les moteurs de recherches, de bloquer et d'interdire l'accès à certains types de contenus et de services jugés offensants ou dangereux. On a, entre autres, demandé à des filières locales de Google d'enlever du contenu controversé dans plusieurs pays (comme la Chine, avant mars 2010, quand Google a redirigés ses activités de moteur de recherche vers Google Hong Kong)

SUIS-JE BLOQUÉ OU FILTRÉ ?

En général, il est difficile de déterminer si quelqu'un essaie de vous empêcher d'accéder à un site Web ou d'envoyer des informations à d'autres personnes. Quand vous essayez d'accéder à un site bloqué, vous pouvez voir un message d'erreur conventionnel ou rien du tout. Le comportement apparent peut ressembler à une indisponibilité technique. Le gouvernement ou le FAI peut même nier qu'une censure est en place et aller jusqu'à mettre en cause le site web (étranger).

Plusieurs organisations, et notablement l'OpenNet Initiative, utilisent des logiciels pour tester l'accès à Internet dans divers pays et pour étudier comment l'accès peut être compromis par les différents acteurs. Ce peut être une tâche difficile, voire dangereuse, selon les autorités concernées.

Dans certains pays, il n'y a aucun doute que le gouvernement bloque des pans d'Internet. En Arabie Saoudite, par exemple, tenter d'accéder à du contenu sexuellement explicite renvoie à un message du gouvernement expliquant la raison du blocage du site.

Dans les pays qui bloquent sans avertissement, un des signes les plus communs de la censure est qu'un nombre important de sites avec un contenu de même nature est apparemment inaccessibles pour des raisons techniques, ou semblent être hors ligne (par exemple, des erreurs « Page introuvable », ou des connexions qui échouent souvent). Une autre indication possible est que les moteurs de recherche renvoient des résultats hors sujet, voire à rien sur certains thèmes.

Le filtrage ou le blocage est également effectué par d'autres entités que les gouvernements. Les parents peuvent filtrer les informations qu'atteignent leurs enfants. Beaucoup d'organisations, depuis les écoles jusqu'aux entreprises, restreignent l'accès à Internet afin d'empêcher les utilisateurs d'avoir des communications non contrôlées, d'utiliser des heures de travail, ou du matériel de l'entreprise pour des raisons personnelles, d'atteindre au copyright, ou encore d'utiliser trop de ressources réseau.

Beaucoup de gouvernements ont les ressources et la capacité légale pour contrôler des parties importantes de l'infrastructure réseau d'un pays. Si le gouvernement est votre adversaire, gardez à l'esprit que toute l'infrastructure des communications, de l'Internet aux lignes mobiles et fixes, peut être contrôlée.

CONTEXTE GÉOGRAPHIQUE

Des utilisateurs, à des endroits différents, peuvent avoir des expériences très variées de contrôle des contenus présents sur Internet.

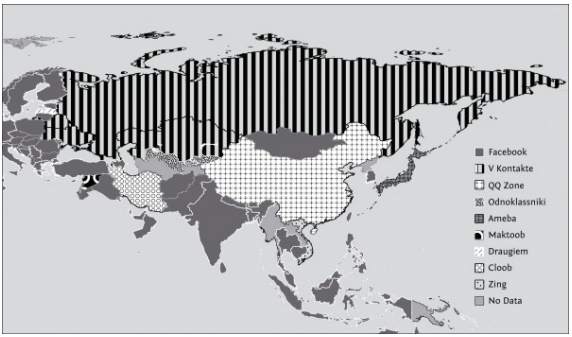
- À certains endroits, votre gouvernement est peut-être légalement empêché de filtrer ou a pu décider de ne pas filtrer le contenu. Vous êtes peut-être contrôlé par votre FAI pour que vos informations soient vendues à des publicitaires. Le gouvernement a peut-être demandé aux FAI d'installer des infrastructures de contrôle (mais pas de filtrage) dans leur réseau. Le gouvernement a peut-être effectué une demande de votre historique et logs de messagerie instantanée, ou a peut-être stocké ces informations pour une utilisation postérieure. Dans cette situation, il fera en sorte de ne pas attirer l'attention. Vous faites aussi face à des menaces d'acteurs non gouvernementaux, comme des criminels qui attaquent des sites web, ou volent des informations bancaires personnelles.
- À certains endroits, les FAI vont peut-être utiliser des moyens techniques pour bloquer des sites ou services, mais le gouvernement ne semblera pas tenter de tracer ou de réprimer les tentatives d'accès, et ne semblera pas agir de manière coordonnée dans une stratégie de contrôle du contenu d'Internet.
- À certains endroits, vous pouvez accéder à des services locaux qui sont des équivalents viables de services étrangers. Ces services sont gérés par votre FAI ou des agents gouvernementaux. Vous êtes peut-être libre de poster des informations sensibles, mais elles seront supprimées. Si ça se passe trop souvent, cependant, la répression deviendra peut-être plus dure. Les restrictions vont peut-être devenir évidentes seulement durant des évènements avec des répercussions politiques.
- À certains endroits, votre gouvernement va peut-être filtrer la plupart des sites étrangers, et plus particulièrement les sites d'informations. Il exerce un contrôle serré sur les FAI pour bloquer les contenus et conserver les traces des créateurs de contenu. Si vous utilisez un réseau social, l'infiltration pourra être envisagée. Le gouvernement peut encourager vos voisins à vous espionner.

CONTEXTE PERSONNEL

Les gouvernements ont un ensemble de motivations pour contrôler et restreindre différents types d'activités des utilisateurs d'Internet de leur pays.

- Activitstes : Vous voulez peut-être améliorer votre gouvernement ou vous en voulez un nouveau. Peut-être que vous voulez réformer une partie précise de votre société, ou agir pour les droits de minorités. Peut-être que vous voulez dénoncer des problèmes environnementaux, des abus, de la fraude, ou corruption, à votre travail. Votre gouvernement et vos employeurs s'y opposeront à tout moment, mais ils fourniront plus d'efforts pour vous contrôler si des manifestations sont envisagées bientôt.
- Blogueurs : Vous voulez peut-être écrire à propos de votre vie quotidienne, mais certaines personnes sont réduites au silence à cause de leur appartenance ethnique ou de leur genre. Peu importe ce que vous avez à dire, vous n'êtes pas supposé le dire. Vous pouvez être dans un pays avec principalement des utilisateurs non limités, mais vos opinions ne sont pas populaires dans votre communauté. Vous préférez peut-être l'anonymat ou le besoin de vous mettre en relation avec un groupe de support.
- Journalistes : vous avez peut-être certaines préoccupations similaires à celles des activistes et des blogueurs. Le crime organisé, la corruption, et les violences gouvernementales sont des sujets dangereux à traiter. Vous voulez peut-être vous protéger ainsi que vos sources d'information.
- Lecteurs : vous n'êtes peut-être pas actifs politiquement, mais le contenu est tellement censuré que vous avez besoin d'outils de contournement pour obtenir des nouvelles, du divertissement, des sciences, ou de l'industrie. Vous voulez peut-être également lire une BD en ligne ou consulter les nouvelles d'autres pays. Votre gouvernement vous laissera peut-être faire jusqu'à ce qu'ils aient d'autres raisons de vous contrôler.

La ressource la plus couramment bloquée sur Internet était, jusqu'à aujourd'hui, les contenus sexuellement explicites. Maintenant, ce sont les réseaux sociaux. La popularité internationale croissante de ces sites a transformé des millions d'internautes à travers le monde en victimes potentielles de la censure. Certains réseaux sociaux sont populaires à une échelle mondiale, comme Facebook, MySpace ou Linkedin, tandis que d'autres ont un grand nombre d'utilisateurs dans un pays ou une région précise : QQ (Qzone) en Chine, Cloob en Iran, vKontakte en Russie, Hi5 au Pérou et en Colombie, Odnoklassniki dans les pays du Commonwealth, Orkut en Inde et au Brésil, Zing au Vietnam, Maktoob en Syrie, Ameba et Mixi au Japon, Bebo au Royaume-Uni, ainsi de suite.



COMMENT LA CENSURE FONCTIONNE ?

[Cette partie est adaptée *d'Access Denied*, Chapitre 3, par Steven J. Murdoch et Ross Anderson].

Les techniques décrites dans ce chapitre sont quelques-unes des méthodes employées par les censeurs qui tentent d'empêcher des internautes d'accéder à des services ou contenus particuliers. Les opérateurs réseau peuvent filtrer ou manipuler le trafic Internet en tout point du réseau, grâce à une grande variété de technologies, avec des degrés variables de précision et de personnalisation. Ces opérations impliquent en général l'utilisation de logiciels pour observer ce que les utilisateurs essaient de faire et pour interférer de manière sélective avec les activités que l'opérateur réseau considère comme interdites dans sa politique de sécurité. Un filtrage peut ainsi être mis en œuvre et appliqué par un État, par un FAI, local ou national, ou même par l'administrateur d'un réseau local Des filtres logiciels peuvent être installés directement sur des ordinateurs personnels.

Les objectifs conduisant au déploiement d'un système de filtrage varient suivant les motivations de l'organisation qui l'emploi. Il peut s'agir de rendre un site Web particulier (ou une page Web donnée) inaccessible à ceux qui souhaitent le voir, de le rendre peu fiable, ou de dissuader les utilisateurs d'y accéder. Le choix du mécanisme de filtrage va aussi dépendre des possibilités de l'organisation qui réclame le filtrage, de son influence et son degré d'écoute, des personnes qu'elle veut voir se conformer à ses souhaits, et de la quantité d'argent qu'elle est prête à dépenser pour ce faire. D'autres considérations portent sur le taux d'erreur acceptable, le fait de savoir si l'existence du filtrage devrait être connue ou cachée, et de son degré de fiabilité (aussi bien à l'égard des utilisateurs lambda que de ceux qui souhaitent le contourner).

Nous allons décrire plusieurs techniques permettant de bloquer un contenu donné une fois qu'une liste de ressources à bloquer est établie. L'élaboration de cette liste est un défi considérable aussi bien qu'une faiblesse dans les systèmes déployés. Non seulement, la quantité énorme de sites Web existant rend difficile la création d'une liste exhaustive des contenus interdits, mais lorsque les contenus se déplacent et que les sites Web changent d'adresse IP, la tenue à jour de cette liste réclame des efforts considérables. Qui plus est, si l'administrateur d'un site souhaite lutter contre le blocage, le site peut être déplacé plus rapidement qu'il n'aurait été autrement. Nous allons tout d'abord décrire les mesures techniques utilisées contre les utilisateurs finaux, puis exposer brièvement les mesures utilisées contre les éditeurs et hébergeurs, ainsi que les méthodes d'intimidation non-techniques. Veuillez noter que cette liste n'est pas exhaustive, et que plusieurs de ces techniques peuvent être utilisées en même temps dans un cas donné.

MESURES TECHNIQUES DIRIGÉES CONTRE LES UTILISATEURS FINAUX

Sur les réseaux de communication modernes tels qu'Internet, la censure et la surveillance des communications et des activités des populations sont, en pratique, intimement liées. La plupart des FAI dans le monde surveillent certains aspects des communications de leurs clients pour des usages de taxation ou de lutte contre des abus tels que le spam. Les FAI enregistrent souvent les noms des comptes des utilisateurs associés aux adresses IP. À moins que les utilisateurs n'emploient des technologies de protection de leur vie privée pour l'empêcher, il est techniquement possible au FAI d'enregistrer toute les informations qui circulent sur son réseau, y compris le contenu exact des communications des utilisateurs.

Cette surveillance est également un prérequis pour la mise en œuvre d'une censure du réseau par des mesures techniques. Un FAI qui essaie de censurer les communications que ses utilisateurs veulent transmettre doit être à même de lire ces communications pour déterminer lesquelles violent ses règles. Il en découle que le cœur de l'approche visant à réduire la censure sur Internet réside dans la dissimulation au FAI du contenu détaillé de ses communications, aussi bien à un niveau individuel que par l'encouragement de la diffusion de technologies de protection de la vie privée qui empêchent la surveillance.

Cela signifie que les contre-mesures techniques à la censure du réseau reposent souvent sur l'usage d'un masquage ou d'un chiffrement, autant que possible, de façon à rendre impossible à connaître, le contenu transféré au FAI.

Cette section explique certaines des techniques spécifiques utilisées par les censeurs pour bloquer des contenus et empêcher l'accès par des moyens techniques.

Le filtrage par URL

Un moyen pour les pays et autres institutions pour bloquer l'accès à des informations sur le Web est d'empêcher l'accès en se basant sur **l'URL** entière ou sur une portion. Les censeurs d'Internet veulent souvent bloquer certains **noms de domaines** dans leur intégralité, parce qu'ils interdisent le contenu de ces domaines. Une des façons les plus simples de bloquer des sites Web est de bloquer tout le nom de domaine. Parfois, les autorités sont plus sélectives, et ne bloquent que certains **sous-domaines** du domaine, en laissant le reste accessible. C'est le cas au Vietnam, où le gouvernement bloque certaines sections des sites, comme la version en vietnamien de la BBC et de Radio Free Asia, mais censurent peu les contenus écrits en anglais.

Les censeurs, par exemple, pourraient filtrer seulement le sous-domaine news.bbc.co.uk, tout en laissant bbc.co.uk et www.bbc.co.uk non filtrés. De même, ils pourraient vouloir filtrer les pages contenant certains types de contenu tout en autorisant l'accès au reste du domaine hébergeant ces pages. Une approche du filtrage est de chercher un nom de répertoire, comme « worldservice » pour bloquer seulement le service d'information en langues étrangères de la BBC bbc.co.uk/worldservice mais pas le site web anglais dans son ensemble. Les censeurs peuvent parfois même bloquer certains pages d'après leurs noms, ou chercher des termes dans les requêtes, qui suggèrent un contenu offensant ou indésirable.

Le filtrage par URL peut être effectué localement, par l'utilisation de logiciels spéciaux installés sur l'ordinateur dont vous vous servez. Par exemple, les ordinateurs d'un cybercafé pourraient tous utiliser un logiciel de filtrage qui bloque l'accès à certains sites.

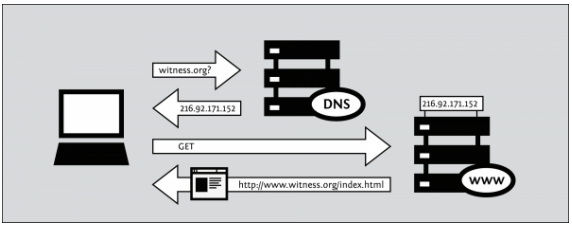
Le filtrage par URL peut aussi être effectué en un point central du réseau, comme un **serveur proxy**. Un réseau peut être configuré pour ne pas laisser les utilisateurs se connecter directement aux sites web mais plutôt les forcer, ou du moins les encourager, à passer par ce serveur proxy.

Les serveurs proxy sont utilisés pour relayer les requêtes et stocker temporairement dans une mémoire cache les pages Web qu'ils récupèrent pour les fournir à plusieurs utilisateurs. Cela réduit la fréquence à laquelle un FAI doit récupérer une page Web populaire, économisant ainsi des ressources et améliorant le temps de réponse.

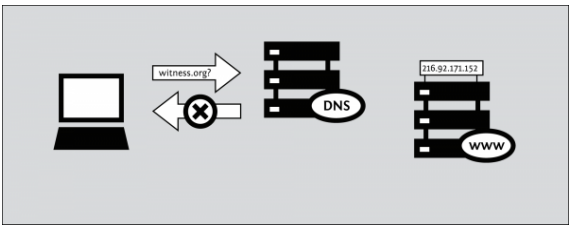
Cependant, s'il améliore la performance, un proxy HTTP peut aussi bloquer des sites Web. Le proxy décide si les requêtes pour les pages doivent être transmises et, si c'est le cas, envoie les requêtes vers les serveurs Web où se trouvent les contenus cherchés. Puisque l'intégralité du contenu de la requête est lisible, des pages Web individuelles peuvent être filtrées d'après le nom de la page, ou son contenu final. Si une page est bloquée, le proxy pourrait retourner une explication précise de la raison, ou bien prétendre que la page n'existe pas ou retourner une erreur.

Filtrage DNS et usurpation

Quand vous saisissez une adresse URL dans un navigateur Web, la première action du navigateur est de demander à un serveur **DNS**, dont l'adresse numérique est connue, de chercher le nom de domaine référencé dans l'URL et de fournir l'adresse IP correspondante.



Si le serveur DNS est configuré pour bloquer l'accès, il consulte une **liste noire** des noms de domaines bannis. Lorsque le navigateur demande l'adresse IP de l'un des domaines figurant sur la liste noire, le serveur DNS donne une réponse fausse ou ne répond pas du tout.



Lorsque le serveur DNS donne une réponse incompréhensible, ou ne répond pas du tout, l'ordinateur demandeur ne peut pas obtenir l'adresse IP exacte du service qu'il cherche à contacter. Sans cette adresse IP, l'ordinateur ne peut pas continuer, et il affiche un message d'erreur. Comme le navigateur ne peut pas connaître l'adresse IP exacte du site Web, il ne peut pas contacter le site pour lui demander une page. Le résultat est que tous les services dépendant d'un nom de domaine particulier, par exemple toutes les pages d'un serveur Web, sont indisponibles. Dans ce cas, un blocage délibéré peut apparaitre de façon erronée comme un problème technique ou une erreur aléatoire.

De façon similaire, un censeur peut forcer un enregistrement DNS à pointer vers une adresse IP incorrecte, redirigeant de ce fait les internautes vers un autre site Web. Cette technique est nommée « **DNS spoofing** », soit « **usurpation DNS** », et les censeurs peuvent l'utiliser pour usurper l'identité d'un serveur et afficher des sites Web forgés, ou re-router le trafic des utilisateurs vers un serveur illégitime capable d'intercepter leurs données. Sur certains réseaux, la réponse fausse conduit à un serveur Web différent qui explique clairement la nature du blocage qui vient de se produire. Cette technique est utilisée par les censeurs qui ne cherchent pas à cacher qu'ils ont mis en place une censure et qui souhaitent que les utilisateurs ne soient pas perturbés par ce qui vient de leur arriver.

Filtrage par IP

Quand des données sont envoyées à travers Internet, elles sont groupées en petites unités, appelées **paquets**. Un paquet contient les données à transmettre ainsi que des informations sur le moyen de le transmettre, comme les adresses IP de l'ordinateur d'où il vient et de celui auquel il est destiné. Les **routeurs** sont des ordinateurs qui relaient les paquets sur le chemin de l'expéditeur au destinataire, en choisissant l'étape suivante. Si les censeurs veulent empêcher les utilisateurs d'accéder à certains serveurs, ils peuvent configurer les routeurs qu'ils contrôlent afin que ceux-ci jettent, ignorent et abandonnent, les données destinées aux adresses IP filtrées, voire retourner un message d'erreur à celles-ci. Le filtrage basé uniquement sur l'adresse IP bloque tous les serveurs fournis par un serveur donné, par exemple à la fois les sites Web et les serveurs d'e-mails. Puisque seule l'adresse IP est vérifiée, les **noms de domaines** qui partagent la même adresse IP sont tous bloqués, même si un seul devait être bloqué originellement.

Filtrage par mots-clefs

Le filtrage par adresse IP ne peut bloquer les communications qu'en se basant sur la source et sur la destination des paquets, pas sur ce qu'ils contiennent. Ce peut être un problème pour le censeur s'il est impossible d'établir une liste complète des adresses IP offrant un contenu interdit, ou si une adresse IP contient suffisamment de contenu autorisé pour qu'il semble injuste de bloquer la totalité des communications avec elle.

Un contrôle plus fin est possible : le contenu des paquets peut être inspecté à la recherche de mots-clefs bannis. Comme les routeurs réseaux n'examinent normalement pas tout le contenu du paquet, un dispositif supplémentaire est nécessaire. Le processus de contrôle du contenu du paquet est souvent appelé DPI (« **Deep Packet Inspection** » ou « **Inspection des paquets en profondeur** »).

Une communication où serait identifié du contenu prohibé pourrait être coupée en bloquant les paquets directement où en créant un message pour dire aux deux interlocuteurs que l'autre a terminé la conversation. Les dispositifs qui réalisent toutes ces fonctions de censures, et davantage, sont déjà disponibles sur le marché. Le censeur peut aussi utiliser un proxy HTTP obligatoire, comme décrit précédemment.

La gestion de flux

La gestion de flux est une technique utilisée par les gestionnaires d'un réseau pour lui permettre de fonctionner de façon fluide en priorisant certains types de paquets et en retardant d'autres types de paquets correspondant à certains critères. La gestion de flux est relativement similaire au contrôle du trafic routier. En général, tous les véhicules (les paquets) ont la même priorité, mais certains véhicules sont temporairement mis en attente par des contrôleurs de trafic ou par des feux, pour éviter des embouteillages à certains endroits. Dans le même temps, certains véhicules (pompiers, ambulances) peuvent avoir besoin d'atteindre leur destination plus vite, et reçoivent une priorité par rapport aux autres véhicules, qui sont retardés. Une logique similaire est applicable aux paquets qui nécessitent une **latence faible** pour des performances optimales, comme **la voix sur IP, ou VoIP**.

La gestion de flux peut également être utilisée par des gouvernements ou d'autres entités pour retarder les paquets porteurs d'informations spécifiques. Si les censeurs veulent restreindre l'accès à certains services, ils peuvent aisément identifier les paquets liés à ces services et accroitre leur latence en leur donnant une priorité faible. Cela conduit les utilisateurs à l'impression trompeuse que le site visité est lent ou peu fiable, ou cela peut tout simplement rendre le site défavorisé d'usage peu agréable comparé à d'autres sites. Cette technique est parfois utilisée contre des réseaux de partage de fichiers en peer to peer (P2P), comme **Bittorrent**, par des FAI qui défavorisent le partage de fichiers.

Le blocage de port

Filtrer individuellement des numéros de port restreint l'accès à des services particuliers sur un serveur, comme le Web ou l'e-mail. Les services les plus répandus sur Internet ont des numéros de port caractéristiques. La relation entre les services et les numéros de port est normalisé par l'IANA, mais il n'y a pas d'obligation. Ces recommandations permettent aux routeurs de deviner à quel service un paquet est destiné. Ainsi, pour bloquer seulement le trafic Web d'un site, un censeur pourrait ne bloquer que le port 80, parce que c'est celui généralement utilisé pour accéder au Web.

L'accès aux ports peut être contrôlé par l'administrateur du réseau ou de l'organisation où se trouve l'ordinateur que vous utilisez, qu'il s'agisse d'une entreprise ou d'un cybercafé, par le FAI qui vous connecte à Internet, ou par une autre entité, comme par exemple un organe de censure gouvernemental qui a accès aux connexions disponibles chez le FAI. Des ports peuvent également être bloqués pour d'autres raisons que la censure de contenu : Réduire les spams, décourager certains usages du réseau comme l'échange de fichiers peer-to-peer, la messagerie instantanée, ou les jeux en réseau.

Si un port est bloqué, tout le trafic sur ce port devient inaccessible. Les censeurs bloquent souvent les ports 1080, 3128 et 8080 parce que sont les ports de proxy les plus communs. Si c'est le cas, vous ne pourrez pas utiliser de proxy qui utilise un de ces ports. vous devrez recourir à une autre technique de contournement ou bien trouver ou créer des proxys qui écoutent sur un port inhabituel.

Par exemple, dans une université, seuls les ports 22 (SSH), 110 (POP3), 143 (IMAP), 993 (IMAP sécurisé), 995 (POP3 sécurisé) et 5190 (messagerie instantanée ICQ) peuvent être ouverts pour des connexions vers l'extérieur, forçant les internautes à utiliser des techniques de contournement ou à accéder aux autres services Internet par des ports non-standard.

Coupure d'Internet

La coupure complète d'Internet est un exemple de censure extrême, perpétrée par des États en réponse à des événements politiques et/ou sociaux brûlants. Toutefois, la rupture complète des communications du réseau, aussi bien domestiques qu'internationales, requiert un travail intense, puisqu'il est nécessaire de couper non seulement les protocoles qui connectent le pays au réseau international, mais aussi les protocoles qui connectent les FAI entre eux et avec leurs abonnés. Des pays ont déjà complètement coupé l'accès à Internet (le Nepal en 2005, la Birmanie en 2007, l'Égypte, la Libye et la Syrie en 2011) comme moyen de réprimer une agitation politique. Ces coupures ont duré de quelques heures à plusieurs semaines, bien que quelques personnes aient réussi à se connecter, en RTC par l'intermédiaire d'un FAI étranger, ou en utilisant des accès de téléphonie mobile ou un lien satellitaire.

La rupture des connexions internationales, de ce fait, ne détruit pas nécessairement la connexion entre les FAI domestiques, ou la communication entre différents utilisateurs d'un même FAI. Des étapes supplémentaires sont à réaliser pour isoler complètement les utilisateurs d'un réseau interne. Pour cette raison, il est plus difficile de rompre la connexion locale dans les pays comptant plusieurs FAI.

ATTAQUER LES ÉDITEURS

Les censeurs peuvent également essayer de supprimer le contenu et les services à leur source en s'attaquant à la capacité de l'éditeur à publier ou à héberger l'information. Ceci peut être accompli de plusieurs façons.

Restrictions légales

Parfois, les autorités peuvent induire les opérateurs de services à censurer ou à collaborer avec la censure. Certains hébergeurs de blogs ou fournisseurs d'e-mail, par exemple, peuvent décider de filtrer certains mots-clés sur leurs serveurs, peut-être à la demande de gouvernements. Dans ce cas, il y a peu d'espoir qu'une quelconque technique de contournement puisse contrer la censure de ces services. Nous concevons généralement le contournement comme un effort pour atteindre les services réseau désirés situés ailleurs, comme un autre pays ou une autre juridiction.

Déni de service

Là où l'organisation déployant un système de filtrage n'a pas l'autorité ni l'accès à l'infrastructure réseau pour ajouter des mécanismes de blocage conventionnels, des sites Web peuvent être rendus inaccessibles en surchargeant le serveur ou la connexion réseau. Cette technique connue sous le nom d'attaque DoS, « Denial-of-Service », soit « Déni de service », peut être mise en œuvre depuis un unique ordinateur disposant d'une connexion réseau très rapide. Plus classiquement, le contrôle d'un grand nombre d'ordinateurs est pris pour organiser une attaque DoS distribuée (DDoS).

Désenregistrement de nom de domaine

Comme expliqué précédemment, la première étape d'une requête Web est de contacter le serveur DNS local pour trouver l'adresse IP de l'emplacement cherché. Enregistrer tous les noms de domaine existant serait infaisable donc on utilise à la place des « résolveurs récursifs » qui conservent des adresses vers d'autres serveurs DNS qui ont plus de chance de connaître la réponse. Ces serveurs dirigeront le résolveur récursif vers les DNS suivants, jusqu'à un serveur « autorité » qui peut retourner la réponse.

Le DNS est organisé de manière hiérarchisée, avec des domaines de premier niveau, régionaux, comme « .uk » et « .de », génériques comme « .org » et « .com ». Les serveurs responsables de ces domaines délèguent la gestion des sous-domaines comme « example.com » à d'autres serveurs DNS, et y redirigent les requêtes concernant ces domaines. Ainsi, si le serveur DNS de premier niveau désenregistre un nom de domaine, les résolveurs récursifs seront incapables de trouver l'adresse IP et rendront le site inaccessible.

Les domaines de premiers niveaux géographiques sont habituellement gérés par le gouvernement du pays en question, ou par une institution associée. Donc si un site est enregistré dans le domaine d'un pays qui interdit le contenu hébergé, il court le risque d'être désenregistré.

Saisie de serveur

Les serveurs hébergeant du contenu sont nécessairement localisés quelque part, tout comme l'administrateur qui les gère. Si ces endroits sont sous le contrôle légal ou extra-légal de quelqu'un opposé au contenu hébergé, le serveur peut être déconnecté, ou les administrateurs contraints de le désactiver.

INTIMIDATION DES UTILISATEURS

Les censeurs peuvent aussi essayer de décourager les utilisateurs de ne serait-ce qu'essayer d'accéder au contenu banni de plusieurs manières.

Surveillance

Les mécanismes ci-dessus empêchent d'accéder à un contenu banni, mais ils sont à la fois grossiers et faillibles. Une autre approche, qui peut être appliquée en parallèle au filtrage, est de surveiller les sites Web visités. Si un accès à un contenu prohibé est détecté (ou une tentative d'y accéder), alors des mesures légales (ou extra-légales) pourraient être utilisées comme représailles.

Si la répréhension est connue, elle pourrait décourager d'autres de tenter d'accéder aux contenus bannis, y compris si les mesures techniques pour empêcher l'accès sont insuffisantes. Dans certains endroits, les censeurs essaient de créer l'impression que leurs agents sont partout et que tout le monde est surveillé en permanence, que ce soit le cas ou non.

Techniques sociales

Des techniques sociales sont souvent utilisées pour décourager les utilisateurs d'accéder à un contenu inapproprié. Les familles peuvent placer l'ordinateur dans le salon, où l'écran est visible de toutes les personnes présentes, plutôt que dans un lieu privé : c'est un moyen modéré de décourager les enfants d'accéder à des sites qui ne leur sont pas adaptés. Un bibliothécaire peut orienter les ordinateurs de façon que leurs écrans soient visibles depuis son bureau. Un cybercafé peut avoir une caméra de vidéosurveillance. Il pourrait y avoir une réglementation locale imposant de telles caméras, et obligeant les utilisateurs à s'enregistrer au moyen d'une carte nationale d'identité comportant une photographie.

Vol et destruction des infrastructures de communication

Les censeurs ont la possibilité d'interdire certains types de technologies de communication dans leur ensemble à certains endroits. Dans ce cas, ils peuvent ostensiblement confisquer, chercher et détruire du matériel du système de communication interdit dans le but de faire passer le message que cette utilisation ne sera pas tolérée.

6. CONTOURNEMENT ET SÉCURITÉ

Le type de sécurité dont vous avez besoin dépend de vos activités et de leurs conséquences. Certaines mesures devraient être pratiquées par tous, que l'on se sente menacé ou pas. Certaines pratiques de prudence en ligne, requièrent plus d'efforts, mais sont nécessaires à cause de restrictions sévères de l'accès à Internet. Vous pouvez être confronté à des attaques issues de technologies rapidement mises en œuvre et déployées, à des vieilles technologies, à de l'espionnage, ou bien d'une combinaison des trois. Ces facteurs peuvent changer souvent.

QUELQUES BONNES PRATIQUES DE SÉCURITÉ

Il y a des mesures que chaque utilisateur d'ordinateur devrait prendre pour assurer sa sécurité : Protéger les informations relatives à son réseau d'activistes ou garder secret son numéro de carte de crédit. Cela dit, certains des outils dont vous avez besoin sont les mêmes.

Méfiez-vous des programmes qui vous promettent une sécurité parfaite : La sécurité en ligne est une combinaison de bons logiciels et de comportements humains. La question de savoir ce qui devrait rester hors ligne, à qui faire confiance, et autres questions de sécurité ne peut être résolue seulement par la technologie. Privilégiez des programmes qui ont été audités ou listent les risques sur leur site Web.

Maintenez votre système à jour : les développeurs de systèmes d'exploitation fournissent des mises à jour que vous devriez installer régulièrement. Elles peuvent être automatiques, à la demande en saisissant une commande ou en ajustant un paramètre de votre système. Certaines de ces mises à jour permettent à votre système d'être plus efficace et plus facile à utiliser, d'autres corrigent des failles de sécurité. Les attaquants sont rapidement au courant de ces failles, quelquefois avant même qu'elles soient corrigées. Il est donc crucial de les corriger au plus vite.

Si vous utilisez encore Microsoft Windows, utilisez un anti-virus et maintenez votre système à jour. Un programme malveillant appelé « malware » est un logiciel écrit pour voler des informations, ou utiliser votre ordinateur. Les virus et les programmes malveillants peuvent obtenir un accès à votre système, faire des modifications et se rendre invisibles. Ils peuvent vous être envoyés dans un e-mail, se trouver dans une page Web que vous visitez, ou faire partie d'un fichier qui ne semble pas suspect. Les éditeurs de logiciels antivirus cherchent constamment les nouvelles menaces et les ajoutent à la liste des choses que votre ordinateur bloquera. Pour permettre au logiciel de détecter ces nouvelles menaces, vous devez installer les mises à jour dès qu'elles sont disponibles.

Utilisez des mots de passe sûrs : aucun système à saisie de mot de passe ne peut résister à la menace d'une attaque brute, mais vous pouvez améliorer votre sécurité en les rendant plus difficiles à deviner. Utilisez des combinaisons de lettres, chiffres, signes de ponctuations. Combinez minuscules et majuscules. Ne vous servez pas de dates anniversaires, de numéros de téléphone, ou de mots qui puissent être devinés en cherchant des informations publiques vous concernant.

Utilisez des logiciels libres ou open-source « Free Open-Source Software » (FOSS). Les logiciels open-source sont distribués comme des produits à la fois fonctionnels ou à améliorer aux utilisateurs et programmeurs. Cela assure plusieurs avantages en termes de sécurité par rapport aux logiciels propriétaires (par opposition à open-source) et commerciaux, qui peuvent n'être disponibles dans votre pays que par des canaux illégaux à cause des restrictions et frais d'export. Vous pourriez ne pas être en mesure de télécharger les mises à jour officielles pour une version piratée. Avec les logiciels libres, vous n'avez pas besoin de chercher une version sans virus ni failles de sécurité sur des sites suspects. Chaque version officielle sera librement accessible depuis le site des auteurs. Si des failles de sécurité apparaissent, elles peuvent être détectées par des bénévoles ou des utilisateurs concernés. Une communauté de programmeurs travaillera à l'élaboration d'une solution, souvent très rapidement.

Utilisez des logiciels qui ne font pas le lien entre qui vous êtes et où vous êtes. Tout ordinateur connecté à Internet possède une adresse IP. Celle-ci peut être utilisée pour déterminer votre position physique, simplement en la recopiant dans un site public de « WhoIs ». Les proxys, VPN et Tor redirigent votre trafic via trois ordinateurs disséminés dans le monde. Si vous vous servez d'un unique proxy, sachez que, tout comme un FAI, son fournisseur peut voir tout votre trafic. Vous pouvez lui faire confiance, plus qu'à votre FAI, mais les mêmes avertissements s'appliquent à n'importe quel moyen de connexion. Consultez la section sur les proxys, Tor et les VPN pour en savoir plus sur les risques.

Démarrez l'ordinateur sur des CD et des clés USB. Si vous utilisez un ordinateur public ou un ordinateur sur lequel vous ne voulez pas laisser de trace, utilisez une version de GNU/Linux que vous pouvez lancer depuis un média amovible. Un Live CD ou une clé USB de démarrage peuvent servir à utiliser un ordinateur sans avoir à installer quoi que ce soit.

Utilisez des applications portables : il y a aussi des versions portables des logiciels de contournement qui fonctionnent sous Windows depuis une clé USB.

Restez à jour : les efforts investis pour vous trouver peuvent changer. Une technologie qui fonctionne un jour peut arrêter de fonctionner ou ne plus être sûre le jour suivant. Même si vous n'en avez pas besoin maintenant, sachez où trouver des informations. Si le fournisseur du logiciel que vous utilisez offre un support technique, assurez-vous d'en savoir assez à ce propos avant que leurs sites Web ne soient bloqués.

UN ACCÈS SÉCURISÉ AUX RÉSEAUX SOCIAUX

Dans le contexte de sociétés fermés et de gouvernements répressifs, la surveillance devient une menace majeure pour les utilisateurs de sites de réseaux sociaux, tout particulièrement s'ils utilisent ces services pour coordonner des activités citoyennes, ou pour s'engager dans l'activisme en ligne ou bien le journalisme citoyen.

Un problème central avec les plateformes de réseaux sociaux est la quantité de données privées que vous partagez à votre sujet, vos activités et vos contacts, et qui y a accès. Comme ces technologies évoluent et l'accès aux réseaux sociaux se fait de plus en plus via des téléphones portables, la révélation de la géolocalisation des utilisateurs à un instant donné devient aussi une menace significative.

Dans cette optique, certaines précautions deviennent encore plus importantes. Vous devriez :

- Ajuster vos paramètres de confidentialité sur la plateforme du réseau social.
- Savoir exactement quelles sont les informations que vous partagez et avec qui.
- Comprendre les paramètres de géolocalisation par défaut, et de les ajuster si besoin.
- Accepter dans votre réseau seulement les gens que vous connaissez vraiment et à qui vous faites confiance.
- Accepter dans votre réseau les gens qui seront suffisamment attentifs pour protéger les informations privées que vous partagez avec eux, ou apprenez-leur à se protéger.
- Savoir que même les personnes les plus attentives de votre réseau peuvent donner des informations si elles sont menacées par votre adversaire. Pensez donc à limiter le nombre de gens et les informations qui leurs sont accessibles.
- Savoir qu'accéder à votre plateforme de réseau social depuis un outil de contournement ne vous protégera pas automatiquement de la plupart des menaces qui pèsent sur votre vie privée.

Pour en savoir plus, lisez cet article de la Privacy Rights Clearinghouse : *« Social Networking Privacy : How to be Safe, Secure and Social »* http://www.privacyrights.org/social-networking-privacy/#general-tips [NdT : lien en anglais]

Comment accéder à un réseau social quand il est filtré ?

Utiliser HTTPS pour accéder aux sites Web est important. Si votre plateforme de réseau social propose un accès en HTTPS, vous devriez vous y connecter que par ce biais et, si possible, le choisir par défaut. Par exemple, sur Facebook, vous pouvez modifier « Compte > Paramètres du compte > Sécurité du compte > Utiliser une connexion sécurisée (https) pour Facebook lorsque c'est possible » afin de vous connecter par défaut en HTTPS à votre compte Facebook. Dans certains lieux, l'utilisation de la connexion HTTPS peut aussi vous permettre d'accéder à un service autrement inaccessible. Par exemple, http://twitter.com/ a été bloqué en Birmanie alors que https://twitter.com/ reste accessible.

Si vous voulez protéger votre anonymat et votre vie privée lorsque vous contournez le filtrage imposé sur votre service de réseau social, un tunnel SSH ou un VPN vous donneront de meilleures garanties qu'un proxy Web, en particulier contre le risque de révélation de l'adresse IP. L'utilisation d'un réseau anonymisé tel que Tor peut se révéler insuffisante, parce que les plateformes de réseaux sociaux rendent aisée la révélation d'informations permettant l'identification et exposant des détails de vos contacts et relations.

UTILISATION PLUS SÛRE DES ORDINATEURS PARTAGÉS

Une proportion significative de la population, surtout dans les pays en voie de développement, n'a pas d'accès Internet à domicile. Cela peut-être dû à son coût, au manque d'équipement en ordinateurs personnels, ou à des problèmes dans les infrastructures de communication ou du réseau électrique.

Pour cette partie de la population, le seul moyen abordable et commode existant d'accéder à Internet est de recourir à des lieux où les ordinateurs sont partagés entre plusieurs personnes. On peut citer les cybercafés, les Télécentres, les stations de travail, les écoles et les bibliothèques.

Avantages potentiels des ordinateurs publics

Accéder à Internet depuis un ordinateur public offre certains avantages :

- Vous pouvez obtenir des conseils et de l'assistance technique des autres utilisateurs ou de l'équipe technique sur la façon de contourner le filtrage.
- Les outils de contournement peuvent être déjà installés et configurés.
- D'autres utilisateurs peuvent partager avec vous des informations, hors ligne, à l'abri de la censure.
- Si vous n'êtes pas un utilisateur régulier d'un équipement informatique, si vous ne fournissez pas des documents d'identité à l'opérateur, et si vous ne vous connectez pas en ligne avec votre véritable nom ou ne divulguez pas d'informations véridiques, il est difficile de vous identifier en se basant sur votre activité en ligne.

Principaux risques d’utilisation ordinateurs publics

Le fait que vous accédiez à Internet dans un espace public ne vous rend pas anonyme et ne vous protège pas. C'est même bien souvent l'exact opposé. Parmi les principales menaces :

- Le propriétaire de l'ordinateur, ou même une personne qui a utilisé l'ordinateur avant vous, peut facilement programmer l'ordinateur pour espionner ce que vous faites, par exemple enregistrer tous vos mots de passe. L'ordinateur peut aussi être programmé pour contourner ou annuler les protections des logiciels de sécurité et de confidentialité que vous utilisez.
- Dans certains pays tels la Birmanie et Cuba, les clients des cybercafés sont obligés de montrer leur carte d'identité ou passeport avant d'utiliser le service. Cette information d'identité peut être enregistrée et classée avec l'historique de navigation des clients.
- Chaque donnée que vous laissez sur l'ordinateur que vous avez utilisé peut être journalisée (historique de navigation, cookies, fichiers téléchargés, etc...)
- Les logiciels ou matériels de journalisation de la frappe clavier installés sur l'ordinateur du client peuvent enregistrer chaque caractère saisi pendant votre session, comme votre mot de passe, avant même que cette information soit envoyé sur Internet. Au Vietnam, un clavier virtuel apparemment inoffensif, pour taper des caractères vietnamiens, a été utilisé par le gouvernement pour surveiller l'activité des utilisateurs de cybercafés et d'autres accès publics.
- Votre session peut être enregistrée par un logiciel spécial qui réalise des captures d'écrans à intervalles réguliers, ou bien surveillée par caméra CCTV, ou bien simplement par une personne telle que le responsable du cybercafé qui regarde par-dessus votre épaule.

Ordinateurs publics et censure

En plus de la surveillance, les utilisateurs des ordinateurs publics se voient souvent offrir un accès limité à Internet et doivent faire face à des obstacles supplémentaires pour utiliser leur solution de contournement favorite.

- Dans certains pays, comme la Birmanie, les propriétaires de cybercafés doivent disposer des affiches sur la censure du Web et sont responsables du respect des lois de censure au sein de leur entreprise. Des filtrages supplémentaires peuvent être mis en place par les gestionnaires de cybercafé (contrôle et filtrage côté client), pour compléter le filtrage fait au niveau des FAI ou au niveau national.
- Les utilisateurs peuvent être incités par les restrictions présentes à éviter de visiter certains sites Web par peur de la répression, renforçant ainsi la censure.
- Les ordinateurs sont souvent configurés pour empêcher les utilisateurs d'installer un quelconque logiciel, y compris les logiciels de contournement, ou de brancher un appareil sur le port USB (comme des clés USB). À Cuba, les autorités ont commencé à déployer un logiciel de contrôle pour les cybercafés, AvilaLink, qui empêche les utilisateurs d'installer ou d'exécuter certains logiciels ou de lancer des applications depuis une clé USB.
- L'ordinateur peut être configuré pour empêcher les internautes d'utiliser un autre navigateur qu'Internet Explorer, afin d'éviter l'utilisation d'extensions pour navigateurs comme Mozilla Firefox ou Google Chrome dédiées à la vie privée ou au contournement.
-

Meilleures pratiques de la sécurité et du contournement

Selon l'environnement dans lequel vous vous servez d'un ordinateur public, vous pouvez essayer ce qui suit :

- Identifiez les mesures de surveillances mises en place d'après la liste précédemment énumérée (CCTV, surveillance humaine, keyloggers, etc.) et adaptez votre comportement.
- Exécutez des logiciels de contournement depuis une clé USB.
- Utilisez un système d'exploitation que vous contrôlez grâce à un Live CD.
- Changez régulièrement de cybercafé si vous craignez la surveillance récurrente, cantonnez-vous au même si vous pensez qu'il est sûr.
- Amenez votre propre ordinateur portable au cybercafé et utilisez-le à la place des ordinateurs publics.

CONFIDENTIALITÉ ET HTTPS

Certains réseaux filtrés utilisent en priorité, voire exclusivement, du filtrage par mots-clefs, plutôt que de bloquer des sites en particulier. Des réseaux peuvent bloquer toute communication utilisant des mots-clefs considérés comme sensibles d'un point de vue politique, religieux ou culturel. Ce blocage peut-être ostensible ou déguisé en erreur technique. Par exemple, certains réseaux font apparaître une erreur lorsque vous cherchez quelque chose et que l'opérateur du réseau pense que cela est indésirable. Ainsi, il y a moins de chances que les utilisateurs dénoncent une censure.

Si le contenu des communications n'est pas chiffré, il sera visible par l'équipement réseau du FAI comme les routeurs et les pare-feux, où la censure et la surveillance à base de mots-clefs peuvent être mises en place. Cacher le contenu des communications à l'aide du chiffrement rend la tâche de la censure bien plus difficile, parce que l'équipement réseau ne peut plus distinguer les communications qui contiennent les mots-clefs interdits des autres.

Utiliser le chiffrement pour garder les communications confidentielles évite aussi que les équipements réseau ne journalisent les communications pour les analyser et cibler des individus d'après les faits qu'ils ont lu ou écrit.

Qu'est-ce que le HTTPS ?

Le HTTPS est une version sécurisée du protocole HTTP utilisée pour accéder aux sites Web. Il fournit une mise à jour de sécurité pour l'accès aux sites Web en utilisant le chiffrement pour empêcher l'écoute et l'usurpation des contenus de vos communications. Utiliser HTTPS pour accéder à un site peut empêcher l'opérateur réseau de savoir quelle partie du site vous utilisez ou quelles informations vous envoyez et recevez. Le support du HTTPS est déjà assuré dans tous les navigateurs Web connus, donc pas besoin de logiciel pour l'utiliser.

Habituellement, si un site propose l'HTTPS, vous pouvez accéder à la version sécurisée du site en commençant l'URL par https:// à la place de http://. Vous pouvez aussi savoir si vous utilisez la version sécurisée du site en regardant si l'adresse affichée dans la barre de navigation de votre navigateur Web commence par https://.

Tous les sites n'ont pas de version HTTPS. Peut-être moins de 10% des sites web en proposent une. En revanche, les sites le faisant comprennent la plupart des sites les plus utilisés. Un site Web n'est disponible en HTTPS que si le propriétaire du serveur le configure pour. Les experts en sécurité exhortent régulièrement les sites Web de le faire, et le support de HTTPS croît régulièrement.

Si vous essayez d'accéder à un site via HTTPS et recevez une erreur, ça ne veut pas toujours dire que votre réseau bloque le site. Ce peut être simplement que le site n'est pas disponible en HTTPS (à qui que ce soit). Cependant, certains types de messages d'erreurs peuvent montrer que quelqu'un bloque de manière active le site ou usurpe la connexion, en particulier si le site est censé être disponible en HTTPS.

Exemples de sites proposant le HTTPS

Voici quelques exemples de sites célèbres qui proposent le HTTPS. Dans certains cas, son utilisation est optionnelle, non obligatoire, et vous devez donc choisir explicitement la version sécurisée du site afin d'en bénéficier.

Nom du site	Version HTTP	Version HTTPS
Facebook	http://www.facebook.com/	https://www.facebook.com/
Gmail	http://mail.google.com/	https://mail.google.com/
Google Search	http://www.google.com/	https://encrypted.google.com/
Twitter	http://twitter.com/	https://twitter.com/
Wikipedia	http://en.wikipedia.org/	https://secure.wikimedia.org/wikipedia/en/wiki/
Windows Live Mail (MSN Hotmail)	http://mail.live.com/ http://www.hotmail.com/	https://mail.live.com/

Si vous faites une recherche Google depuis https://encrypted.google.com/ plutôt que depuis http://www.google.com/ ; votre opérateur réseau ne sera pas capable de connaître les termes de votre recherche. Il ne pourra donc pas bloquer les recherches « inappropriées » (mais l'opérateur réseau pourrait décider de bloquer encrypted.google.com en entier). De même, si vous utilisez Twitter à travers de https://twitter.com/ plutôt que de http://twitter.com/ ; l'opérateur réseau ne pourrait pas voir les tweets que vous lisez, les tags que vous consultez, ou ce que vous y postez, ni avec quel compte vous vous connectez (mais l'opérateur réseau peut décider de bloquer les accès à twitter.com en HTTPS).

HTTPS et SSL

HTTPS utilise un protocole de sécurité nommé TLS pour « Transport Layer Security » ou SSL pour « Secure Sockets Layer ». Vous pouvez entendre des gens parler d'un site qui « utilise SSL » ou que c'est un « site SSL ». Dans le contexte d'un site Web, cela signifie que le site est disponible en HTTPS.

Utiliser HTTPS en plus d'une technique de contournement

Les techniques de contournement qui utilisent le chiffrement ne se substituent pas à l'utilisation de HTTPS, parce que le rôle de ce chiffrement est différent.
Pour de nombreuses techniques, dont les VPN, proxys et Tor, il est toujours possible et pertinent d'utiliser des adresses HTTPS quand vous accédez à un site bloqué. Cela assure une plus grande sécurité et empêche le fournisseur de l'outil de contournement lui-même de savoir ce que vous faites. Ce peut être important même si vous lui faites confiance, parce que celui-ci (ou le réseau dont il se sert) pourrait être infiltré ou subir des pressions.

Certains développeurs de techniques de contournement comme Tor exhortent avec virulence les utilisateurs à toujours utiliser HTTPS, pour être sûrs que les relais eux-mêmes ne puissent pas les espionner. Vous pouvez en lire plus sur ce problème sur https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext [NdT: en anglais]. Utiliser le HTTPS dès que possible est une bonne habitude à prendre, même lorsqu'on utilise déjà d'autres techniques de contournement.

Trucs et astuces d'utilisation de HTTPS

Si vous aimez enregistrer les sites que vous visitez régulièrement dans vos marques-pages afin de ne pas avoir à taper à nouveau l'adresse complète, souvenez-vous d'enregistrer la version sécurisée.

Dans Mozilla Firefox, vous pouvez installer l'extension « HTTPS Everywhere » pour activer automatiquement HTTPS quand vous visitez un site connu pour le proposer. L'extension est disponible à cette adresse https://www.eff.org/https-everywhere/.

Ne pas utiliser HTTPS, les risques

Quand vous n'utilisez pas HTTPS, un opérateur réseau, comme votre FAI ou l'opérateur d'un pare-feu national, peut enregistrer tout ce que vous faites ainsi que le contenu de certaines pages auxquelles vous accédez. Ils peuvent utiliser cette information pour bloquer certains pages ou créer des documents pouvant être utilisés contre vous plus tard. Ils peuvent aussi modifier le contenu de pages Web pour supprimer certaines informations et insérer des logiciels malveillants pour vous espionner ou infecter votre ordinateur. Dans de nombreux cas, d'autres utilisateurs du même réseau peuvent aussi faire ces choses sans être l'opérateur officiel du réseau.

En 2010, certains de ces problèmes ont été amplifiés par un programme appelé « Firesheep », qui permet aux utilisateurs d'un réseau de prendre le contrôle des comptes sociaux des autres utilisateurs extrêmement facilement. Firesheep fonctionnait parce que, au moment où il a été créé, ces sites de réseaux sociaux ne proposaient généralement pas le HTTPS, ou de manière limitée pour protéger uniquement certaines parties du site. Cette démonstration a fortement attiré l'attention des média, et amené davantage de sites à demander l'utilisation de HTTPS, ou du moins à offrir un accès HTTPS optionnel. Cela a aussi permis à des personnes sans connaissances techniques d'usurper le compte d'autres personnes.

En janvier 2011, durant une période de troubles politiques en Tunisie, le gouvernement a commencé à intercepter les connections des utilisateurs de Facebook pour voler leurs mots de passe. Ce fut fait en modifiant la page de connexion de Facebook et en ajoutant de manière invisible un logiciel qui envoyait des informations de connexion aux autorités. De telles modifications sont techniquement simples à effectuer et pourrait être faites par tout opérateur réseau à tout moment. Pour autant que l'on sache, les utilisateurs tunisiens de Facebook qui utilisaient HTTPS étaient complétement protégés.

Risques d'utilisation de HTTPS

Quand c'est possible, utiliser HTTPS est presque toujours plus sûr qu'utiliser HTTP. Même si quelque chose se passe mal, cela ne devrait pas rendre vos communications plus faciles à espionner ou filtrer. Essayez d'utiliser HTTPS là où vous pouvez a du sens mais sachez qu'en principe, le chiffrement peut être légalement restreint dans certains pays. Le HTTPS ne fournit pas toutefois une protection complète dans certains cas.

Les avertissements de certificat

Parfois, quand vous essayez d'accéder à un site en HTTPS, votre navigateur Web affichera un message décrivant un problème avec le certificat numérique du site. Le certificat est utilisé pour assurer la sécurité de la connexion. Ces avertissements sont là pour vous protéger des attaques, ne les ignorez pas. Si vous les ignorez ou les contournez, vous serez peut-être en mesure d'utiliser le site mais limiterez la capacité de HTTPS à protéger vos communications. Dans ce cas, l'accès au site ne sera pas plus sécurisé que par une connexion HTTP ordinaire.

Si vous êtes confronté à un avertissement de certificat, vous devriez le rapporter par e-mail au webmaster du site auquel vous tentez d'accéder, afin qu'il corrige le problème.

Si vous utilisez un site en HTTPS monté par une personne, comme certains proxys Web, vous pourriez recevoir une erreur de certificat parce que celui-ci est auto-signé, signifiant que le navigateur n'a pas de moyen de déterminer si la communication est sur écoute. Pour certains de ces sites, vous n'aurez pas d'autre alternative que d'accepter le certificat auto-signé si vous voulez y accéder. Cependant, vous devriez essayer de vous assurer par un autre moyen, comme l'e-mail ou la messagerie instantanée, que le certificat est celui attendu, ou regarder si c'est toujours le même lorsque vous utilisez une autre connexion à Internet depuis un autre ordinateur.

Le contenu mélangé

Une page Web est généralement composée de nombreux éléments différents, qui peuvent se trouver à différents endroits et être récupérés séparément les uns des autres. Parfois un site utilisera le HTTPS pour certains éléments de la page Web mais seulement du HTTP pour les autres. Par exemple, un site pourrait ne permettre qu'un accès HTTP pour accéder à certaines images. En février 2011, le site sécurisé de Wikipédia rencontra ce problème. Le texte des pages pouvait être récupéré en HTTPS alors que toutes les images étaient récupérées en http : Les images pouvaient ainsi être identifiées et bloquées, ou utilisées pour déterminer quelle page Wikipédia l'utilisateur lisait.

Redirection vers la version HTTP d'un site

Certains sites utilisent HTTPS de manière limitée et forcent les utilisateurs à retourner à un accès HTTP même après une connexion en HTTPS. Par exemple, certains sites utilisent HTTPS pour les pages de connexion, où les utilisateurs entrent leurs identifiants de compte, mais le HTTP pour les autres pages, une fois l'utilisateur connecté. Ce genre de connexion rend les utilisateurs vulnérables à la surveillance. Vous devriez y faire attention. Si vous êtes redirigé vers une page non sécurisé durant votre navigation sur un site, vous n'avez plus la protection du HTTPS.

Réseaux et pare-feux bloquant HTTPS

À cause de la manière dont HTTPS fait entrave à la surveillance et au blocage, certains réseaux bloquent complétement HTTPS pour l'accès à certains sites, ou mêmes bloquent l'utilisation de HTTPS complétement. Dans ce cas, vous pouvez être contraint d'utiliser la version non sécurisée de ces sites. Vous pourriez vous retrouver incapable d'accéder à un site à cause du blocage de HTTPS. Si vous utilisez HTTPS Everywhere, ou certains logiciels similaires, vous ne pourrez pas utiliser certains sites parce qu'ils ne permettent pas la connexion non sécurisée.

Si votre réseau bloque le HTTPS, vous devez comprendre que l'opérateur réseau peut voir et enregistrer toutes vos activités de navigation. Dans ce cas, vous devriez essayer d'autres techniques de contournement, en particulier celles qui offrent d'autres formes de chiffrement, comme les VPN et les proxys SSH.

Utilisation de HTTPS depuis un ordinateur non sûr

Le HTTPS ne protège que le contenu de vos communications lorsqu'elles transitent sur Internet. Il ne protège pas votre ordinateur ni les contenus affichés sur votre écran ou ceux de votre disque dur. Si l'ordinateur que vous utilisez est public ou, d'une quelconque manière non sûr, il pourrait contenir un logiciel de contrôle, d'espionnage ou de censure qui enregistre ou bloque certains mots-clés sensibles. Dans ce cas, la protection offerte par HTTPS pourrait se révéler moins efficace, puisque le contrôle et la censure viendraient de l'ordinateur lui-même, plutôt que d'un pare-feu du réseau.

Vulnérabilité du système de certificats de HTTPS

Le système de certificats par autorité de HTTPS utilisé pour sécuriser les connexions, PKI pour « Public Key Infrastructure » (« Infrastructure à clé publique »), a certaines vulnérabilités. Ainsi, un agresseur compétent ayant à sa disposition les ressources adéquates pourrait faire en sorte que votre navigateur n'affiche pas d'avertissement lors d'une attaque. On ne sait pas encore clairement si cela s'est déjà produit quelque part. Ce n'est pas une raison pour se passer de HTTPS puisque, même dans le pire des cas, une connexion HTTPS n'est pas moins sûr qu'une connexion HTTP.

TECHNIQUES BASIQUES

7. TRUCS ET ASTUCES
8. SOYEZ CRÉATIF
9. LES PROXYS WEB
10. PSIPHON
11. SABZPROXY

7. TRUCS ET ASTUCES

Il existe un certain nombre de techniques pour contourner le filtrage Internet. Si votre objectif est seulement d'afficher des pages ou utiliser des services en ligne bloqués où vous vous trouvez, et que vous ne vous souciez pas du fait que votre contournement soit détecté ou observé, ces techniques pourraient vous suffire :

- Utiliser HTTPS
- Utiliser des noms de domaines ou URL alternatifs pour afficher le contenu bloqué.
- Utiliser des sites tiers pour afficher le contenu bloqué.
- Passer par des passerelles d'e-mail, pour recevoir les pages bloquées.

UTILISER HTTPS

HTTPS est la version sécurisée du protocole HTTP utilisé pour accéder aux sites web.

Dans certains pays, et si le site que vous souhaitez visiter a activé HTTPS, tapez simplement l'adresse (URL) en commençant par https:// à la place de http:// peut vous permettre d'accéder au site, même si l'adresse http:// est bloquée.

Par exemple, http://twitter.com/ a été bloqué en Birmanie, alors que https://twitter.com/ était accessible.

Pour plus de détails sur cette technique, lisez le chapitre « Confidentialité et HTTPS », et le chapitre « HTTPS Everywhere ».

DES NOMS DE DOMAINES ET DES URL ALTERNATIVES

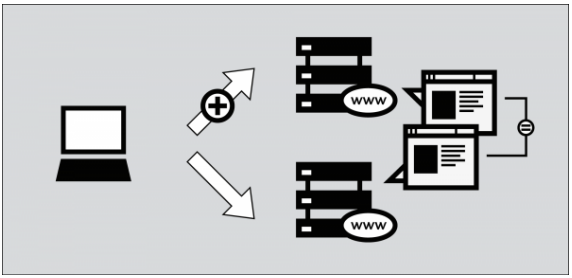
L'un des moyens les plus courants pour censurer un site Web consiste à bloquer l'accès à son nom de domaine, par exemple « news.bbc.co.uk ». Cependant, les sites restent souvent accessibles par d'autres noms de domaine. Par exemple : « newsrss.bbc.co.uk ». Si un nom de domaine est bloqué, essayez de découvrir si le contenu est disponible avec un autre nom de domaine.

Vous pouvez également essayer d'accéder aux versions spéciales que certains sites web proposent pour les smartphones. Il s'agit souvent des mêmes URL, au début desquelles on ajoute "m" ou "mobile", par exemple :

- http://m.google.com/mail (Gmail)
- http://mobile.twitter.com
- http://m.facebook.com ou http://touch.facebook.com
- http://m.flickr.com
- http://m.spiegel.de
- http://m.hushmail.com

UTILISER DES SITES TIERS

Il y a de nombreuses manières d'accéder au contenu d'une page web en passant par un site tiers plutôt que par le site source.



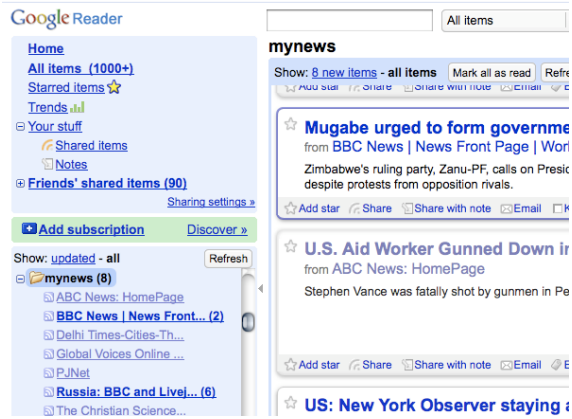
Les pages en cache

De nombreux moteurs de recherche conservent des copies de pages web précédemment indexées, que l'on appelle les pages en cache. Lorsque vous recherchez un site web, cherchez le petit lien « En cache » à coté de vos résultats de recherche. Dans la mesure où vous récupérez une copie de la page bloquée depuis les serveurs du moteur de recherche, et non pas depuis le site, il se peut que vous puissiez accéder au contenu bloqué. Certains pays ont cependant entrepris de bloquer également les services de cache.

Agrégateurs RSS

Les agrégateurs RSS pour « Really Simple Syndication, » comprenez « Syndication vraiment simple, » sont des sites Web qui vous permettent de vous abonner et de lire les flux RSS, qui sont constitués des actualités ou autres contenus proposés par les sites que vous avez choisi. Pour en savoir davantage sur leur utilisation, consultez http://rssexplained.blogspot.com. Un agrégateur RSS se connecte aux sites, télécharge les flux que vous avez sélectionnés, et les affiche. C'est l'agrégateur RSS qui se connecte aux sites Web, pas vous. Vous pourrez donc peut-être accéder de cette manière au contenu des sites bloqués. Cette technique n'est valable que pour les sites Web qui offrent un flux RSS de leur contenu, bien entendu, tels que les weblogs et les sites d'information. Il y a de nombreux agrégateurs RSS en ligne gratuits comme Google Reader http://reader.google.com, Bloglines http://www.bloglines.com ou FriendFeed http://friendfeed.com.

Ci-dessous, un exemple d'affichage de liens par Google Reader :



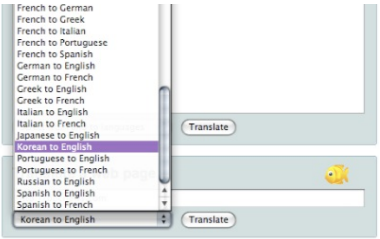
Traducteurs

Il existe de nombreux traducteurs linguistiques en ligne, souvent fournis par les moteurs de recherche. Si vous consultez un site Web par l'intermédiaire d'un service de traduction, c'est ce service qui accède au site, pas vous. Cela vous permet de lire du contenu bloqué traduit dans de nombreux langages différents.
Vous pouvez utiliser le service de traduction pour contourner le blocage, même si vous n'avez pas besoin de traduire le texte. Vous le faites en choisissant comme langage source un langage qui n'apparaît pas sur la page Web originale vers un langage quelconque. Par exemple, pour utiliser un tel service afin de voir un site Web en anglais, choisissez la traduction du chinois en anglais. Le service de traduction ne traduira que les sections en chinois, s'il y en a, et laisse inchangées les sections en langue anglaise qui constituent le reste de la page.

Parmi les services de traduction les plus connus, on trouve Babelfish http://babelfish.yahoo.com et Google Traduction http://translate.google.com.

L'exemple ci-dessous illustre les trois étapes nécessaires pour consulter une page dans Babelfish. D'abord, renseignez l'URL de la page Web que vous voulez visiter :

Choisissez ensuite le langage dans lequel vous souhaiter lire le site Web. Dans cet exemple nous disons à Babelfish de traduire du coréen en anglais. Puisqu'il n'y a pas de coréen dans le texte d'origine, la page restera identique.



Une fois le langage choisi, cliquez sur « Translate » et la page s'affiche.

Bien sûr, il faut que le site de traduction lui-même soit accessible, ce qui n'est pas toujours le cas, car les autorités qui exercent le blocage connaissent l'utilisation possible des outils de traduction pour le contournement. D'après http://www.herdict.org, le site http://translate.google.com n'est pas accessible en Arabie Saoudite.

Les filtres à faible bande passante

Il s'agit de services Web conçus pour rendre la navigation Web plus facile dans les endroits où les vitesses de connexion sont restreintes. Ils suppriment ou réduisent les images, enlève les publicités, et compressent le site Web pour faire en sorte qu'il soit plus léger et se télécharge plus rapidement.

Comme pour les services d'agrégation ou de traduction, vous pouvez aussi utiliser les filtres à faible bande passante pour contourner le blocage de sites en les consultants depuis ce service plutôt que depuis votre ordinateur. Un filtre à faible bande passante utile est disponible à cette adresse http://loband.org.

Les archives du Web

Le site archive.org « Wayback Engine » sur http://www.archive.org/web/web.php permet aux utilisateurs de voir des versions archivées de page Web. Des millions de sites Web et les données associées (images, code source, documents, etc.) sont sauvegardées dans une immense banque de données.

Tous les sites Web ne sont pas disponibles cependant, certains propriétaires de sites Web choisissent d'en exclure leur site et les sauvegardes prennent longtemps avant d'être ajoutées.

UTILISER LES SERVICES D'E-MAIL

Les services d'e-mail et de webmail peuvent être utilisés pour partager des documents avec des groupes d'amis ou de collègues, et même naviguer sur le Web.

Accéder aux pages Web via l'e-mail

À l'instar des filtres à faible bande passante, il existe des services destinés aux connexions Internet lentes ou instables qui permettent de demander une page Web par e-mail. Ces services envoient une réponse e-mail contenant la page Web demandée dans le corps du message ou bien comme pièce jointe. Ils peuvent être assez inconfortables à utiliser, puisqu'il faut envoyer une requête séparée pour chaque page Web et attendre la réponse. Dans certaines situations, ils peuvent être très efficaces pour atteindre des pages Web bloquées, tout spécialement en accédant à un service de webmail sécurisé.

Web2mail

L'un de ces services est web2mail, http://web2mail.com/. Pour l'utiliser, envoyez un e-mail à www@web2mail.com contenant l'adresse URL de la page Web que vous voulez consulter dans l'objet du message. Vous pouvez aussi effectuer des recherches Web simple en indiquant les termes dans le sujet. Par exemple, vous pouvez chercher des outils pour le contournement de la censure en tapant : « rechercher outils contournement censure » dans l'objet de l'e-mail puis en l'envoyant à www@web2mail.com.

EmailTheWeb

Un autre service du même genre, EmailTheWeb, http://www.emailtheweb.com, permet d'envoyer une page Web à n'importe qui, y compris vous-même. Pour envoyer une page par e-mail, vous devrez vous inscrire sur le site ou bien utiliser votre compte GMail. Le service gratuit vous permet d'envoyer jusqu'à 25 pages par jour.
Vous trouverez davantage d'information et de support sur ce sujet sur la liste de diffusion ACCMAIL. Pour vous y enregistrer, envoyez un e-mail contenant « SUBSCRIBE ACCMAIL » dans le corps du message à listserv@listserv.aol.com.

RSS vers e-mail

Certaines plateformes offrent un service similaire au Web vers e-mail, mais avec les flux RSS plutôt que des pages Web. Voici une liste non exhaustive :

- https://www.feedmyinbox.com
- http://www.myrssalerts.com
- http://www.feedmailer.net
- http://blogtrottr.com

FoE

Le service FoE, pour « Feed over Email, » comprenez Transmission par e-mail, est un autre projet du même genre. Créé par Sho Sing Ho, du Broadcasting Board of Governors, il est toujours en cours de développement à l'heure où ces lignes sont écrites. La progression du projet peut être suivie ici : http://code.google.com/p/foe-project.

Sabznameh

Si vous cherchez à accéder aux informations persanes censurées depuis l'intérieur des frontières de l'Iran, vous devriez vous intéresser à Sabznameh. Cette plateforme robuste et évolutive de « Feeds over Email » permet à des lecteurs de nouvelles indépendantes permettant d'accéder par e-mail aux contenus bloqués.

Le moyen le plus simple d'accéder à Sabznameh est d'envoyer un e-mail vide (sans sujet ni corps) à help@sabznameh.com. Ainsi vous pouvez vous enregistrer même sans avoir accès à http://sabznameh.com. Vous recevrez en réponse un e-mail qui vous guidera étape par étape pour vous enregistrer à une ou plusieurs des publications disponibles.

Utiliser un webmail pour partager des documents

Si vous essayez de partager des documents en ligne, mais voulez contrôler qui y a accès, vous pouvez les conserver dans un espace privé qui ne sera visible qu'à ceux connaissant le bon mot de passe. Un moyen simple de partager des documents parmi des petits groupes d'amis ou de collègues est d'utiliser un compte de webmail comme Gmail, https://mail.google.com, et de partager les identifiants avec les personnes à qui vous voulez donner accès aux documents. La plupart des fournisseurs de webmail sont gratuits, il est facile de changer régulièrement de compte, rendant plus difficile pour quelqu'un d'extérieur au groupe, de tracer ce que vous faites. Vous trouverez une liste de webmails gratuit ici : http://www.emailaddresses.com/email_web.htm.

LES RISQUES ET LES AVANTAGES

Ces techniques simples sont rapides et faciles à utiliser. Vous pouvez les essayer avec un effort minimal. Beaucoup d'entre elles fonctionnent dans bien des situations. Cependant, elles sont aussi faciles à détecter et à bloquer. Puisque la plupart n'enregistrent ni ne cachent vos communications, elles sont aussi vulnérables aux contrôles et blocages par mots-clefs.

8. SOYEZ CRÉATIF

Si votre fournisseur d'accès à Internet (FAI) censure l'accès à certains sites Web ou services, vous pouvez utiliser les outils présentés dans les autres chapitres de ce livre. Vous pouvez aussi imaginer de nouveaux moyens pour accéder librement à une information, comme suit :

UTILISER DES FAI ALTERNATIFS

Parfois la régulation du filtrage n'est pas appliquée de façon uniforme et cohérente par tous les FAI. Les gros fournisseurs, avec un grand nombre d'abonnés, tout comme les entreprises de télécommunication nationalisées, sont soumis à un contrôle plus fort et à une répression plus importante que les start-ups. En 2002, le gouvernement allemand a adopté une loi régulant Internet qui ne s'appliquait aux FAI que dans un Land. Les utilisateurs ont pu contourner la règlementation en s'abonnant à un FAI disposant d'une étendue nationale aux installations situées dans d'autres régions du pays. De la même façon, une loi Allemande, imposée en 2010, ne devait ne concerner que les FAI ayant plus de 10 000 abonnés (pour éviter une fuite de la liste noire). Elle était facilement contournable si l'on s'abonnait à de petits FAI locaux. Pendant la révolution égyptienne de 2011, il a été dit que Noor DSL était le dernier FAI à obéir à l'ordre d'éteindre Internet à cause de sa part de marché relativement faible (8%) et l'importance de ses clients. Parmi eux, la bourse égyptienne, la banque nationale d'Égypte et Coca-Cola.

Les FAI alternatifs peuvent aussi être trouvés à l'étranger et quelques entreprises ont même renoncé à faire payer un abonnement aux utilisateurs résidant dans un pays où il y a de graves troubles politiques. Pendant les révoltes de 2011 en Lybie et en Égypte, plusieurs citoyens ont mis à disposition des informations sur la situation politique et sociale de leurs pays respectifs en connectant leur modem bas débit à des FAI étrangers, ou en utilisant des techniques de communication alternatives comme le satellite, la transmission radio par paquets ou les connexions non filtrées de multinationales ou d'ambassades.

LES RÉSEAUX MOBILES

Les réseaux mobiles sont des moyens de plus en plus populaires pour disséminer et accéder à l'information non censurée, en partie par le fort taux de pénétration dans les pays où le coût d'un ordinateur ou d'une connexion à Internet personnelle est prohibitif. Beaucoup de fournisseurs de solutions mobiles ne sont pas des FAI, leurs réseaux ne sont pas concernés de la même façon par les restrictions. Cependant, ces réseaux sont habituellement plus faciles à contrôler et fréquemment sujet à une surveillance étendue.

Des activistes, dans différents pays, ont utilisé leurs téléphones et des logiciels open-source gratuits comme FrontlineSMS (http://www.frontlinesms.com) pour gérer des campagnes basées sur les SMS et leur permettre l'accès à des services de microblogging comme Twitter. Un ordinateur faisant tourner FrontlineSMS et étant connecté à Internet peut servir de plateforme à d'autres utilisateurs pour poster de l'information sur Internet à l'aide de leurs téléphones mobiles.

Les réseaux mobiles peuvent aussi être utilisés par des périphériques alternatifs. Le Kindle 3G, un lecteur de livres numériques d'Amazon, par exemple, est vendu avec un abonnement mobile international gratuit, qui permet l'accès gratuit à Wikipedia à travers les réseaux mobiles dans plus de 100 pays.

NE PAS UTILISER INTERNET

Parfois, l'accès à Internet est complètement restreint et les activistes sont obligés d'utiliser des moyens alternatifs pour distribuer et accéder à une information non censurée. En 1989, bien avant la généralisation d'Internet, des étudiants de l'Université du Michigan ont acheté un fax pour envoyer des résumés des médias internationaux aux universités, aux entités gouvernementales, aux hôpitaux et aux principales entreprises en Chine pour offrir une alternative aux rapports gouvernementaux à propos des événements de la place Tiananmen.

Si votre accès à internet est restreint, prenez en compte la possibilité d'échanger des informations en peer to peer à travers des moyens alternatifs. L'infrarouge (IrDA) et le bluetooth sont disponibles sur beaucoup de téléphones récents et peuvent être utilisés pour transférer des données sur de courtes distances. D'autres projets, comme la « Pirate Box » (http://wiki.daviddarts.com/PirateBox), utilisent le Wi-Fi et des logiciels open-source gratuits pour créer des périphériques de partage de fichiers mobiles. Dans les pays où Internet a un faible taux de pénétration, comme Cuba. Les clés USB sont aussi de plus en plus utilisées par les gens qui veulent distribuer une information non censurée. Parmi d'autres technologies utilisées par les activistes pendant les événements politiques de 2011 en Libye et en Égypte, on relevait le fax, le speak2tweet (une plateforme lancée par Google et Twitter qui met à disposition des numéros de téléphones pour tweeter par l'intermédiaire d'un répondeur téléphonique) et les SMS.

UTILISER DES TECHNOLOGIES TRÈS VIEILLES OU TRÈS RÉCENTES

Souvent, une censure utilise les techniques de filtrage et de surveillance sur les protocoles et services Internet standards. Essayez d'utiliser des technologies très vieilles ou très récentes qui ne sont ni bloquées ni surveillées. Avant l'avènement des logiciels de messagerie instantanée (Windows Live Messenger, AIM, etc.), les communications de groupes utilisaient IRC (Internet Chat Relay), un protocole qui permet l'échange de messages texte en temps réel sur Internet. Même s'il est moins populaire que ses successeurs, IRC existe toujours et est toujours utilisé à grande échelle par une grosse communauté d'internautes. Un BBS (Bulletin Board System) est un ordinateur exécutant un logiciel qui permet aux utilisateurs de se connecter, d'envoyer et de télécharger des logiciels ou tout autre forme de données, lire des actualités et échanger des messages avec d'autres utilisateurs. À l'origine, les utilisateurs devaient appeler un numéro de téléphone en utilisant leur modem pour accéder à ces systèmes mais, depuis les années 1990, plusieurs BBS ont aussi autorisé l'accès avec des protocoles Internet textuels interactifs comme Telnet ou SSH.

Les nouvelles technologies profitent aussi des mêmes bénéfices que les vieilles, puisqu'elles sont utilisées par un nombre limité d'utilisateurs et sont donc moins soumis à la censure. Le nouveau protocole Internet IPv6, par exemple, est déjà déployé par certains FAI dans certains pays et n'est généralement pas filtré.

USAGES ALTERNATIF DES SERVICES WEB

Beaucoup d'internautes dont la connexion est censurée ont commencé à utiliser les services Web d'une façon différente que celle pour laquelle ils avaient été prévus à l'origine. Par exemple, les utilisateurs se sont servi de systèmes de discussion de certains jeux vidéo pour échanger sur des questions sensibles, ce qui aurait été détecté sur un système de discussion classique. Une autre technique est de partager un seul compte mail et de sauvegarder la discussion dans le dossier « Brouillons », ce qui évite d'envoyer des e-mails via Internet.

Les services de sauvegarde en ligne, comme Dropbox.com ou Spideroak.com, ont été utilisés par des activistes pour distribuer et partager des documents ainsi que d'autres types de données.

Les services destinés à la traduction, au cache ou à la mise en page ont été utilisés comme des proxys simples pour contourner la censure sur Internet. Les exemples les plus connus sont Google Traduction, Google cache et Archive.org. De plus, il existe plusieurs applications originales comme Browsershots.org (qui effectue des captures d'écran des sites Web), PDFMyURL.com (qui permet de créer une version PDF d'un site Web), URL2PNG.com (permettant de créer des documents facilement lisibles sur les liseuses électroniques de document comme le Nook et le Kindle).

TOUT CANAL PEUT ÊTRE UN CANAL DE CONTOURNEMENT

Si vous disposez d'un quelconque moyen de communication avec une personne ou un ordinateur coopératif échappant à la censure que vous subissez, vous devriez être en mesure d'utiliser ce canal comme moyen de contournement de la censure. Les gens ont déjà utilisé le salon de discussion d'un jeu vidéo pour outrepasser une censure car les censeurs ne pensaient pas à surveiller ou à bloquer l'accès à des jeux vidéo populaires. Dans les jeux qui permettent de créer des objets virtuels sophistiqués, les joueurs ont eu l'idée de créer virtuellement des ordinateurs, des écrans de télévision et d'autres types de périphériques qui leur permettent d'accéder à une ressource normalement censurée.

Les gens ont aussi eu l'idée de dissimuler de l'information au sein de profils sur les réseaux sociaux. Par exemple, une personne peut déposer, d'une façon déguisée, l'adresse d'un site Web auquel il souhaite accéder sur son profil d'un réseau social. Un ami, avec un accès à Internet non-censuré, peut capturer le contenu du site demandé dans un fichier image et le déposer sur un profil différent. Ce procédé peut être automatisé par un logiciel ce qui permet de le rendre rapide et automatique, au lieu d'avoir besoin d'une personne physique pour le faire.

Avec l'aide de la programmation, même un canal ne supportant qu'une faible quantité d'information numérique ou textuelle, en réception ou en émission, peut être converti en un proxy Web (quand un canal cache entièrement l'existence d'un type de communication, il est appelé canal couvert). Par exemple, les développeurs ont créé de des applications proxy de type IP sur DNS ou HTTP sur DNS pour contourner des pare-feux en utilisant le protocole DNS (Domain Name System). Un exemple de logiciel est « Iodine » disponible sur http://code.kryo.se/iodine. Vous pouvez aussi lire la documentation d'un logiciel équivalent sur http://en.cship.org/wiki/DNS_tunnel et http://www.dnstunnel.de. Avec ces logiciels, une requête pour accéder à quelque chose est déguisée comme une demande de résolution d'un grand nombre de domaines sans relation avec celui demandé. Le contenu de l'information demandée est déguisé comme contenu des réponses à ces requêtes. Beaucoup de pare-feux ne sont pas configurés pour bloquer ce genre de communications puisque le système DNS n'a jamais été conçu pour permettre une communication avec l'utilisateur final mais pour fonctionner comme dictionnaire d'information à propos des adresses des domaines.

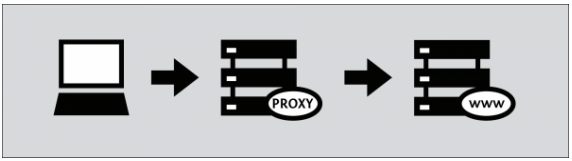
Beaucoup d'applications intelligentes qui utilisent les canaux couverts de contournement sont possibles et c'est un domaine de recherche et de discussion permanente. Pour être pleinement fonctionnelles, celles-ci requièrent un serveur dédié hébergé quelque part ailleurs et le logiciel doit être disponible des deux côtés du canal et installé par des utilisateurs compétents.

9. LES PROXYS WEB

Un proxy vous permet de récupérer un site Web ou un autre contenu via Internet même quand l'accès direct à la ressource est bloqué là où vous vous trouvez. Différents types de proxys existent :

- Les proxys Web, qui requièrent simplement de connaître l'adresse du site Web. Son adresse URL peut être de la forme : http://www.example.com/cgi-bin/nph-proxy.cgi.
- Les proxys HTTP, qui impliquent que vous ou une composante logicielle modifie la configuration de votre navigateur. Les proxys HTTP ne fonctionnent que pour les contenus Web. Vous obtiendrez sans doutes les informations sur un proxy sous cette forme : « proxy.example.com:3128 » ou « 192.168.0.1:8080 ».
- Les proxys SOCKS, qui demandent également une configuration du navigateur. Ils fonctionnent pour beaucoup de services Web, depuis l'e-mail aux messageries instantanées. Les informations sur un proxy SOCKS sont de la même forme que celles d'un proxy HTTP.

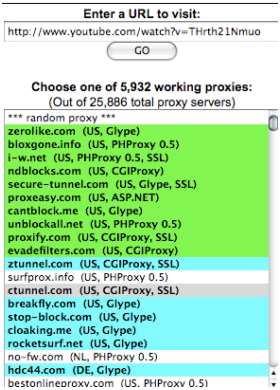
Un proxy Web fonctionne comme un navigateur intégré à une page Web. Il consiste généralement en un petit formulaire où vous pouvez saisir l'adresse URL de la page Web à laquelle vous souhaitez accéder. Le proxy affiche alors la page, sans que vous n'ayez à vous connecter.



Quand vous utilisez un proxy Web, vous n'avez pas à installer un logiciel ou changer la configuration de l'ordinateur, ce qui signifie que vous pouvez vous en servir depuis n'importe quel ordinateur, y compris dans un cybercafé. Entrez simplement l'adresse du proxy Web pour accéder à la page où vous pourrez saisir l'adresse de la page à laquelle vous voulez accéder.
Lorsque vous accéder à une page par l'intermédiaire d'un proxy Web, vous devriez pouvoir utiliser les boutons « Précédent » et « Suivant » de votre navigateur ainsi qu'utiliser les liens et formulaires dans le site tout en continuant à utiliser le proxy. En effet, le proxy modifie tous les liens de la page afin qu'ils disent désormais à votre navigateur de demander les URL au proxy. Étant donnée la complexité des sites Web actuels, cela peut cependant être une tâche difficile. Ainsi, vous pourriez tomber sur des pages, liens ou formulaires coupant à travers la connexion du proxy. Quand cela se produit, vous pourrez normalement voir que le formulaire du proxy aura disparu de la fenêtre de navigation.

COMMENT TROUVER UN PROXY WEB ?

Vous pouvez trouver des URL de proxy Web sur des sites comme http://www.proxy.org, en vous inscrivant à une liste de diffusion comme http://www.peacefire.org/circumventor, en suivant un flux Twitter spécifique à votre pays, ou simplement en cherchant « proxy Web gratuit » dans un moteur de recherche. Le site proxy.org liste des milliers de proxys Web gratuits :



Entre autres, les plateformes de proxy Web comprennent CGIProxy, PHProxy, Zelune, Glype, Psiphon et Piciade. Comme évoqué précédemment, ce ne sont pas des logiciels que vous installez sur votre ordinateur. Ce sont des logiciels serveur que quelqu'un d'autre doit installer sur un ordinateur connecté à un ordinateur non soumis au filtrage. Toutes ces plateformes fournissent les mêmes fonctionnalités de base, mais elles ont des apparences différentes et chacune a ses forces et ses faiblesses. Certaines sont meilleures pour certaines choses, comme le streaming vidéo, ou l'affichage précis de sites Web complexes.

Certains proxys Web sont privés. Ils ne sont généralement accessibles qu'à un petit nombre d'utilisateurs connus de la personne proposant le proxy, ou des clients qui paient pour le service. Les proxys Web privés ont leurs avantages :

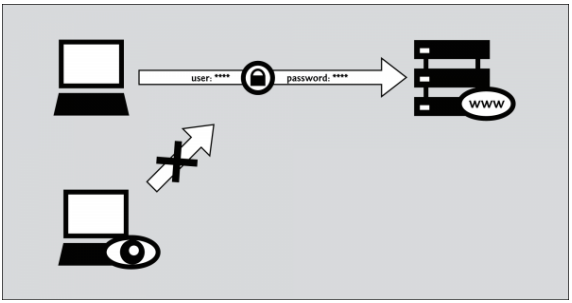
- plus de chances de rester inconnus et donc accessibles.
- moins de trafic et sont donc plus rapides.
- plus de fiabilité, si l'accès est sécurisé et ils sont gérés par quelqu'un que vous connaissez.

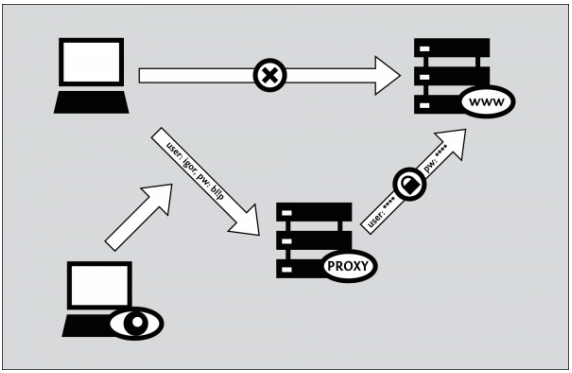
L'accès peut-être restreint par une demande de nom d'utilisateur et de mot de passe, ou simplement en n'apparaissant pas dans les listes publiques mentionnées ci-dessus.

Les proxys Web sont faciles à utiliser, mais ils ont des inconvénients importants par rapport aux autres outils de contournement. Aussi, ils sont souvent utilisés comme un moyen temporaire pour apprendre à utiliser des outils plus avancés, qui doivent souvent être téléchargés sur des sites Web filtrés. L'accès à un proxy Web peut aussi être utile le temps de réparer ou de remplacer un outil qui a cessé de fonctionner.

PROBLÈMES DE COMPATIBILITÉ DES PROXYS WEB

Les proxys Web ne fonctionnent que pour le trafic Web. Ils ne peuvent donc pas être utilisés pour d'autres services Internet comme l'e-mail ou la messagerie instantanée. Beaucoup sont également incompatibles avec des sites Web complexes comme Facebook, les sites de streaming tels Youtube, ainsi que les sites sécurisés en HTTPS. Ce dernier point signifie que bien des proxys Web seront incapables de vous permettre d'accéder aux formulaires de connexion de sites, tel un webmail. Pire, certains proxys Web ne disposent pas de HTTPS. Si vous utilisez un proxy de ce genre pour accéder à un site normalement sécurisé, vous pourriez exposer des informations sensibles, comme votre mot de passe.





Nous parlerons d'avantage des problèmes de sécurité de ce genre ci-dessous.

À l'exception notable d'HTTPS, la plupart des problèmes de compatibilité peuvent être résolus en utilisant la version « mobile » ou en « HTML simple » des sites Web, lorsqu'elle est disponible. Malheureusement, seuls peu de sites offrent ce genre d'interface simplifiée, et encore moins avec un accès à toutes les fonctionnalités. Si un site Web propose une version mobile, son URL commence souvent par un « m » en lieu et place de « www ». Par exemple : https://m.facebook.com, http://m.gmail.com, ou https://m.youtube.com. Vous pouvez parfois trouver un lien pour la version mobile ou en HTML simple d'un site dans le pied-de-page.

RISQUES DE SÉCURITÉ RELATIFS AUX PROXYS WEB

Gardez en tête que certains des risques sont associés à l'utilisation de proxys Web, en particulier ceux gérés par des gens ou des organisations que vous ne connaissez pas. Si vous utilisez un proxy Web simplement pour lire une page comme http://www.bbc.co.uk, vos seuls vrais problèmes sont qu'une personne puisse apprendre :

- que vous avez eu accès à des informations censurées.
- Quel proxy vous avez utilisé pour ce faire.

Si votre proxy Web fonctionne correctement, et si vous y accéder avec HTTPS, ces informations ne devraient pouvoir être connues que par l'administrateur du proxy lui-même. Cependant, si vous utilisez une connexion HTTP non sécurisée, si votre proxy fonctionne mal, ou est mal conçu, ces informations seront révélées à quiconque contrôle votre connexion à Internet. Les proxys Web chiffrés ne fonctionne pas du tout dans certains pays, parce qu'ils ne permettent pas de contourner les filtres utilisant la censure par mots-clefs plutôt que le blocage par URL ou par adresse IP.

Pour certains, les risques ci-dessus ne sont pas un gros problème. En revanche, ils pourraient devenir très sérieux si vous avez l'intention d'utiliser un proxy Web pour accéder à certains sites de contenus tels que ceux :

- Qui vous demandent des identifiants de connexion.
- A travers lesquels vous accédez à des informations sensibles.
- Sur lesquelles vous voulez créer ou partager du contenu.
- commerciaux ou de banques.
- en HTTPS.

Dans ce genre de situations, proscrivez l'utilisation de proxys Web non sécurisés ou qui ne sont pas dignes de confiance. Vous devriez toujours éviter d'utiliser les proxys Web dans ce cas. Bien qu'il n'y ait pas de garantie qu'un outil plus « avancé » sera plus sécurisé, les obstacles rencontrés par les logiciels de contournement à installer pour garder vos communications privées sont généralement moins complexes que ceux auxquels font face les proxys Web.

L'obscurcissement n'est pas du cryptage

Certains proxys Web, en particulier ceux qui ne supportent pas le HTTPS, utilisent des systèmes de codage simple pour contourner les filtres par domaines ou par mots-clefs peu efficaces. Un système comme ROT-13, remplace chaque caractère par celui qui le précède de 13 places dans l'alphabet latin (voir http://www.rot13.com pour tester vous-même). En utilisant ROT-13, « http://www.bbc.co.uk » devient « uggc://jjj.oop.pb.hx ». Les concepteurs de proxys ont trouvé cette astuce très utile car cette URL est envoyée par le navigateur au proxy Web et peut donc être interceptée par un filtre par mots-clefs. Pourtant, les systèmes d'encodage ne sont pas très fiables puisque rien n'empêcher d'ajouter « jjj.oop.pb.hx » à la liste des mots-clefs filtrés, voire même « uggc:// » pour bloquer ce type de proxy.

Ce qu'il faut retenir de l'encodage des caractères est qu'il ne protège pas votre anonymat des observateurs tiers, qui peuvent toujours lister les sites que vous visitez. Et, même s'il est appliqué à tout le texte des pages que vous consultez et au contenu que vous envoyez plutôt que simplement aux URL, il n'assure toujours pas votre confidentialité. Si cela vous inquiète, n'utilisez que les proxys Web qui supportent le HTTPS.

N'oubliez pas, l'administrateur du proxy peut tout voir.

Les conseils du paragraphe ci-dessus soulignent l'importance de HTTPS, aussi bien sur le site censuré que sur le proxy lui-même, lorsque vous échangez des informations sensibles. Cependant, il est important de noter que, même lorsque vous accéder à un site sécurisé à travers un proxy sécurisé, vous vous en remettez complètement à ceux qui administrent le proxy Web, puisque la personne ou l'organisation peut lire tout le trafic que vous envoyez ou recevez. Cela comprend tous les mots de passe que vous pourriez avoir à saisir pour accéder à un site donné.

Même l'outil de contournement le plus avancé, qui devra être installé sur l'ordinateur, doit reposer sur un proxy d'un genre ou d'un autre pour contourner les filtres Web. Quoi qu'il en soit, tous les outils réputés de ce genre sont conçu de manière à protéger le contenu du trafic Web en HTTPS, y compris des sites de contournement. Malheureusement, ce n'est pas le cas des proxy Web, qui doivent reposer sur la bonne vieille confiance, confiance qui dépend non seulement de la volonté de l'administrateur du service à protéger vos intérêts, mais aussi sur sa politique de journalisation, sur ses compétences techniques, et l'environnement légal et réglementaire où il opère.

RISQUES LIÉS À L'ANONYMAT VIA LES PROXYS WEB

Les outils créés pour contourner le filtrage n'offrent pas nécessairement l'anonymat, y compris ceux contenant le mot « Anonymizer » dans leur nom ! En général, l'anonymat est une propriété beaucoup plus évasive de la sécurité que la simple confidentialité (empêcher les écoutes). Et, comme décrit plus haut, afin de vous assurer même une confidentialité basique à travers un proxy Web, vous devez au minimum :

- Vous connecter au proxy en HTTPS.
- Accéder à la version HTTPS du site via le proxy.
- faire confiance à la volonté, à la politique et aux compétences logicielles et techniques de l'administrateur du proxy.
- prendre en compte tous les avertissements du navigateur, comme expliqué dans le chapitre sur le HTTPS.

Toutes ces conditions sont aussi des prérequis pour l'anonymat, quel que soit son degré. Si un tiers peut lire le contenu de votre trafic, il peut facilement associer votre adresse IP à la liste des sites Web que vous visitez. C'est le cas même si vous utilisez un pseudonyme pour vous connecter ou envoyer des messages (à l'opposé, aucun outil ne vous protégera si donnez votre véritable identité).

Publicités, virus et logiciels malveillants

Certaines des personnes qui mettent en place des proxys Web le font pour gagner de l'argent. Ce peut être simplement en vendant de la publicité qui s'affiche ouvertement sur les pages consultées via le proxy.

Ou alors, un administrateur malveillant pourrait essayer d'infecter les ordinateurs de ses utilisateurs. Ce sont des « drive-by-downloads », qui peuvent infester vos ordinateur dans le but d'envoyer des courriers publicitaires ou de les utiliser à des fins illégales.

La chose la plus importante que vous puissiez faire pour vous protéger contre les virus et logiciels malveillants est de garder vos logiciels à jour, en particulier votre système d'exploitation et votre antivirus. Vous pouvez aussi bloquer les publicités en utilisant AdBlockPlus (http://www.adblockplus.org) et certains contenus malveillants avec NoScript (http://noscript.net), deux extensions pour le navigateur Mozilla Firefox. Vous trouverez plus d'informations pour éviter ces risques sur le site StopBadware Web (http://www.stopbadware.org [NdT: en anglais]).

Les cookies et les scripts

Il y a aussi des risques associés à l'utilisation des cookies et des scripts à l'intérieur des pages. La plupart des proxys Web peuvent être configurés pour retirer les cookies et les scripts, mais certains sites tels que les plateformes de réseau sociaux ou de vidéos comme Facebook et Youtube, en ont besoin pour fonctionner correctement. Les sites web et les publicitaires, peuvent utiliser ces mécanismes logiciel pour vous pister, même lorsque vous utiliser des proxys, afin de relier entre elles les différentes activités en ligne d'une même personne.

Certains cookies peuvent rester enregistrés sur votre ordinateur même après un redémarrage. Aussi, n'autoriser que certains cookies est une bonne idée. Par exemple, dans Mozilla Firefox, vous pouvez indiquer à votre navigateur de ne garder les cookies que pour la session (jusqu'à la fermeture du programme). Vous pouvez faire de même avec l'historique. Généralement parlant, cependant, les proxys Web restent très limités dans votre capacité à protéger votre identité face aux sites Web auxquels vous accédez. Si vous souhaiter garantir votre sécurité contre ce type de traçage, vous devriez être très précautionneux lors de la configuration de votre navigateur et du proxy, ou bien utiliser un autre outil de contournement.

Aider les autres

Si vous êtes dans un pays avec un accès à Internet non restreint et que vous désirez aider les autres à contourner la censure, vous pouvez installer un proxy Web sur votre propre site web ou sur votre ordinateur personnel, ce qui est expliqué dans la section « Aider les autres » de ce livre.

10. PSIPHON

Psiphon est une plateforme de proxy Web open-source qui a un peu évolué au cours des dernières années. Différent des autres logiciels de proxy comme CGIProxy et Glype, surtout via sa configuration sur le serveur.
En général, Psiphon :

- est accessible en HTTPS.
- supporte l'accès aux sites HTTPS.
- dispose d'une compatibilité proche de la perfection avec des sites Web complexes comme Youtube.
- peut demander l'identification avec nom d'utilisateur et mot de passe.
- permet d'enregistrer une adresse e-mail pour recevoir les URL de nouveaux proxys, fournies par l'administrateur dans le cas où celui-ci serait bloqué.
- permet d'inviter d'autres personnes (dans le cas de l'identification).

La version actuelle du logiciel serveur Psiphon tourne seulement sur GNU/Linux, et est plus difficile à installer et administrer que la plupart des autres proxys. Il facilite des opérations de large ampleur, en tant que service de contournement résistant au blocage, pour ceux qui manquent de compétences pour utiliser des outils plus avancés.

HISTOIRE DE PSIPHON

Psiphon 1, la première version du proxy Web, était conçue pour tourner sur Windows et permettre à un utilisateur non-expert d'un pays sans filtrage de fournir des services de contournement simples à certaines personnes des pays le subissant. Facile à installer, facile à utiliser, elle proposait partiellement le HTTPS, ce qui la rendait plus sécurisée que la plupart de ses concurrents. Il demandait aussi aux utilisateurs de se connecter, ce qui évitait l'afflux et réduisait la probabilité que ces petits serveurs ne soient ciblés par la censure. Psiphon 1 n'est plus maintenu ni supporté par l'organisation qui l'a développé.

Psiphon fut complétement réécrit pour la version 2, avec pour objectif la performance, la sécurité, la compatibilité et l'adaptabilité dans le contexte d'un modèle centralisé. Ces objectifs ont été atteints avec plus au moins de succès. À l'origine, les utilisateurs Psiphon 2 devaient s'enregistrer sur un certain nœud privé avec un nom d'utilisateur et un mot de passe. Psiphon Inc. donna aux premiers utilisateurs de chaque région des privilèges supplémentaires qui leur permettaient d'inviter d'autres personnes à accéder aux proxys. Les premiers proxys de Psiphon 2 demandaient aussi à ignorer l'avertissement « Certificat non valide » du navigateur parce que, bien que le HTTPS soit disponible, les administrateurs n'avaient pas pu ou pas voulu acheter de certificat signé. Tous les nœuds privés de Psiphon déployés par la société elle-même ont maintenant des certificats signés et ne devraient plus déclencher d'avertissement de la part du navigateur. Évidemment, ce n'est pas le cas des installations tierces du logiciel Psiphon. Finalement, tous ses utilisateurs ont maintenant le droit d'envoyer un certain nombre d'invitations.

Les nœuds publics de Psiphon 2 mis en place par la suite ne demandent pas d'identification. Un nœud public charge automatiquement une page d'accueil et utilise une langue donnée, mais peut être utilisé pour naviguer ailleurs et échapper à la censure. Les nœuds publics comprennent un lien qui permet aux utilisateurs de créer un compte et, éventuellement, d'enregistrer une adresse e-mail. Cela permet aux administrateurs du proxy d'envoyer une nouvelle URL aux utilisateurs pour lesquels les nœuds sont bloqués depuis leur pays. En général, on s'attend à ce que les nœuds publics soient bloqués et remplacés plus souvent que les nœuds privés. Tout comme les nouveaux nœuds privés, les nœuds publics sont sécurisés à l'aide de HTTPS et ceux mis en place par Psiphon Inc. utilisent des certificats signés valides.

COMMENT ACCÉDER À UN NOEUD

PSIPHON ?

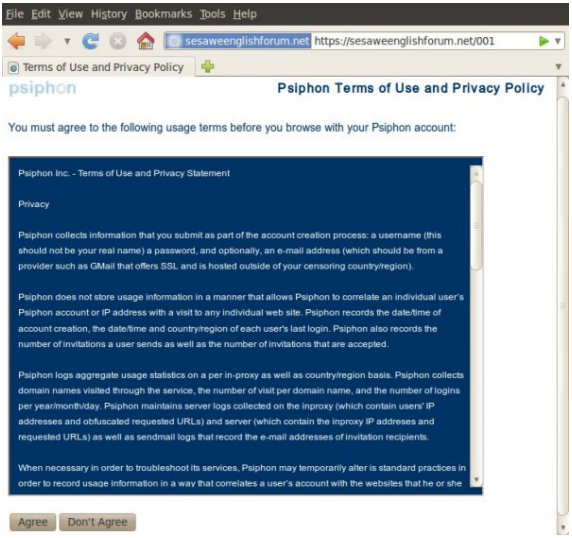
Psiphon Inc. n'a pas de manière centralisée pour distribuer les nœuds publics, aussi appelés nœuds right2know, tout en limitant et en contrôlant le blocage de ses proxys. Un nœud public en anglais, dédié au forum de support pour le contournement de Seawave est accessible via http://sesaweenglishforum.net. D'autres nœuds publics sont distribués de manière privée (via des listes de diffusion, des flux Twitter, des émissions radios, etc.) par les créateurs de contenus qui forment la base des clients de Psiphon.

Les nœuds privés de Psiphon fonctionnent différemment. Même s'il était possible d'imprimer un lien d'invitation dans ce livre, ce serait malavisé, puisque le principe des nœuds privés est de limiter leur croissance et de conserver un semblant de la confiance entre individus d'un même réseau social entre ses utilisateurs. Après tout, une invitation envoyée à un ne serait-ce qu'un délateur serait suffisante pour que l'adresse IP du nœud se retrouve filtrée par le pays. Pire, si cette invitation est acceptée, l'informateur pourrait aussi connaître l'adresse URL du proxy envoyée par les administrateurs du système. Si vous recevez une invitation, elle contiendra un lien ressemblant à celui-ci https://privatenode.info/w.php?p=A9EE04A3. Il vous permettra de créer un compte et d'enregistrer votre adresse e-mail. Pour ce, suivez les instructions du paragraphe « Créer un compte » ci-dessous.

Après l'avoir créé, vous n'aurez plus besoin du lien d'invitation. À la place, vous vous connecterez via une URL plus facile à retenir comme https://privatenode.info/harpo.

UTILISER UN NOEUD PUBLIC PSIPHON

La première fois que vous vous connectez à un nœud public Psiphon, vous verrez les conditions d'utilisation et la politique de confidentialité. Lisez-les avec précaution, car elles contiennent des conseils de sécurité important comme des informations sur la manière dont l'administrateur du proxy gère vos données. Pour utiliser le proxy, vous devez les accepter.

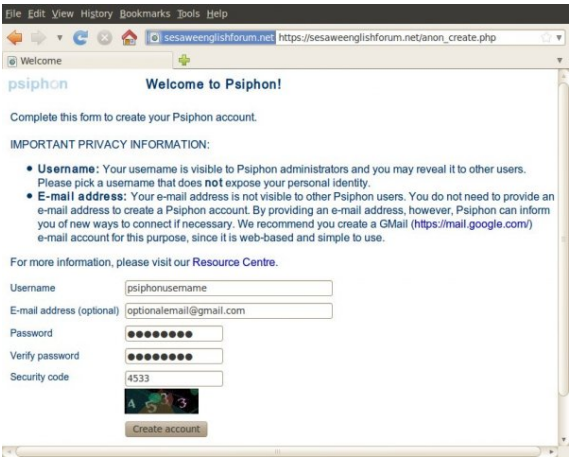


Ensuite, Psiphon chargera la page d'accueil par défaut associée au nœud, comme illustré plus bas. Vous pouvez suivre les liens affichés sur la page — ils vous feront passer automatiquement par le proxy — ou bien visiter d'autres sites Web à l'aide de la barre d'adresse bleue, appelée « BlueBar », en haut de la page.

CRÉER UN COMPTE

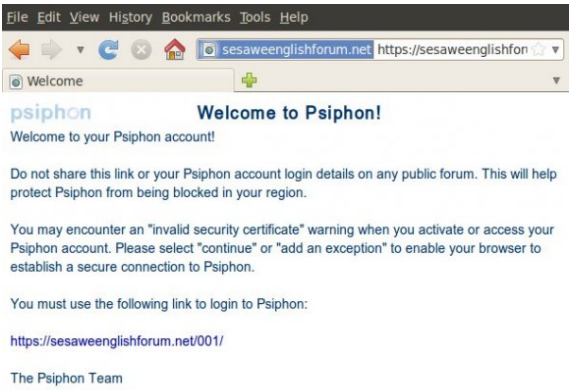
Tant que vous vous souvenez ou avez en marque-page l'URL d'un nœud public non cloqué, vous pouvez vous en servir pour accéder à des sites Web filtrés. Créer un compte vous permet de modifier certaines préférences, comme la langue du proxy ou la page d'accueil par défaut. Ainsi, vous enregistrez une adresse e-mail afin que l'administrateur du nœud puisse vous envoyer l'URL d'un nouveau proxy si le nœud se retrouve bloqué. Pour ce faire, cliquez sur le lien « Create account » dans la Bluebar.

Si vous recevez une invitation à un nœud privé Psiphon, les étapes nécessaires à la création d'un compte sont les mêmes que ce qui suit.



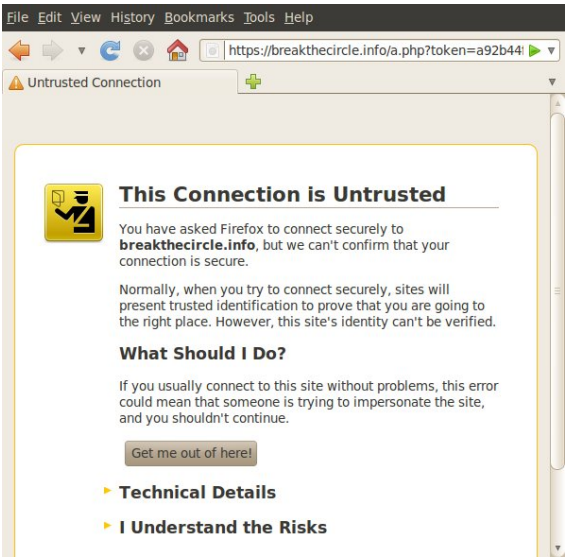
Lorsque vous remplissez le formulaire d'inscription, vous devriez choisir un nom d'utilisateur qui ne soit pas relié à votre véritable identité via les services d'e-mail, de réseaux sociaux, ou d'autres plateformes du genre. Les mêmes considérations sont à envisager concernant l'adresse e-mail, si vous décidez d'en inscrire une. Seuls certains utilisateurs du proxy peuvent voir votre nom d'utilisateur et votre adresse mais ils sont enregistrés quelque part en base de données et visible par les administrateurs de Psiphon. Si vous choisissez d'enregistrer une adresse e-mail, il vaut mieux que vous y accédez via une connexion HTTPS.

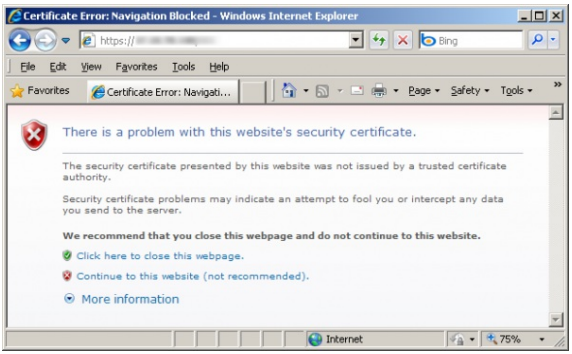
Voici des webmail supportant le HTTPS: https://mail.google.com, https://www.hushmail.com et https://mail.riseup.net. Pour éviter la création automatisée de comptes Psiphon, vous devez lire les nombres affichées dans l'image et les recopier dans le dernier champ. Une fois la manipulation terminée, cliquez sur « Create account ».



Vous devriez voir un message confirmant la création de votre compte. Vous pouvez désormais utiliser l'adresse URL affichée dans la page pour vous connecter au nœud Psiphon. Remarquez que le préfixe est en HTTPS et qu'il contient un court suffixe (« /001 » dans l'image ci-dessus). Vous pouvez imprimer cette page d'accueil ou enregistrer l'URL dans vos marques-pages, ne confondez pas avec la page d'accueil. Bien sûr, vous aurez aussi besoin du nom d'utilisateur et du mot de passe choisis dans les étapes précédentes.

La page d'accueil peut aussi proposer des conseils, comme illustré précédemment, à propos des avertissements de certificat et de la nécessité de les accepter pour utiliser Psiphon. Ces informations sont en fait périmées et vous ne devriez pas vous en formaliser. Au contraire, si vous rencontrez un avertissement de ce genre lorsque vous vous connectez, vous devriez y faire très attention. Si cela arrive, vous devriez fermer votre navigateur et consulter info@psiphon.ca ou english@seawave.net pour des conseils supplémentaires.





INVITER D'AUTRES PERSONNES

Si vous utilisez un compte pour vous connecter à votre proxy Psiphon, vous aurez peut-être la possibilité d'inviter d'autres personnes. Pour lutter contre le blocage, vous obtiendrez des jetons d'invitation lentement, et le nombre d'invitations que vous pouvez avoir à la fois est limité. Évidemment, si votre proxy est un nœud public, vous pouvez simplement envoyer l'adresse URL du proxy à d'autres personnes. Cependant, après un blocage, si vous recevez le message de migration à l'adresse e-mail que vous avez renseignez, vous découvrirez que votre compte a été déplacé vers un nœud privé. Vous ne devriez jamais partager l'URL d'un nœud privé, sauf à travers le mécanisme d'invitation prévu par Psiphon.

Une fois que vous avez obtenu au moins une invitation, vous verrez un lien dans la Bluebar du genre: « Invite (1 remaining) » comme montré ci-dessous.

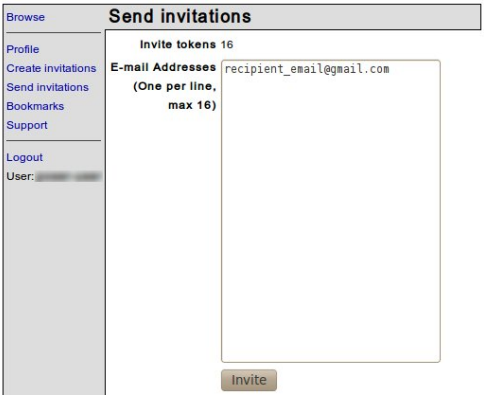
Il y a deux manières d'inviter quelqu'un sur un proxy Psiphon :

- La fonction « Send invitations » envoie automatiquement les liens à un ou plusieurs destinataires. Les messages d'invitation viendront de Psiphon, pas de votre compte.
- La fonction « Create invitations » génère un ou plusieurs liens d'invitation que vous pourrez distribuer par vous-même.

Si vous cliquez sur le lien dans la Bluebar, vous serez envoyé vers l'écran « Send invitations ». Pour obtenir un lien sans qu'il ne soit envoyé, accéder à votre profil puis cliquez sur « Create invitations ».

Envoyer une invitation

Cliquez sur « Invite » dans la Bluebar ou « Send invitations » dans votre profil. Entrez une adresse e-mail pour chaque personne à qui vous voulez envoyer une invitation — une adresse par ligne — et cliquez sur « Invite ».



Vous verrez un message indiquant qu'un ou plusieurs messages ont été mis en attente, ce qui signifie que Psiphon enverra vos liens d'invitations dans les prochaines minutes.

Rappelez-vous que vous ne devez inviter dans les nœuds privés seulement des gens que vous connaissez.

Créer une invitation

Cliquez sur « Create invitations » dans votre profil. Choisissez le nombre de liens d'invitations que vous voulez générer et cliquez sur « Invite ».

Vous pouvez distribuer ces liens d'invitations par tous les moyens à votre disposition, mais :

- une invitation ne peut être utilisée qu'une seule fois.
- pour les nœuds privés, n'affichez pas les liens publiquement, pour éviter d'exposer l'adresse du proxy.
- pour les nœuds privés, vous ne devriez inviter que des gens que vous connaissez.

REPORTER UN SITE WEB CASSÉ

Certains sites Web qui reposent sur des scripts inclus dans la page et des technologies Web complexes comme Flash et AJAX peuvent ne pas s'afficher correctement à travers Psiphon. Dans le but d'améliorer la compatibilité de Psiphon avec de tels sites, les développeurs ont besoin de savoir lesquels posent problème. Si vous trouvez un tel site Web, vous pouvez le rapporter facilement en cliquant sur le lien « Broken page » dans la Bluebar. Si vous donnez une brève description du problème dans le champ approprié, cela permettra à l'équipe de développement de Psiphon de comprendre l'erreur pour les aider à trouver une solution. Quand vous aurez fini, cliquez sur « Submit » et votre message sera envoyé aux développeurs.


Create new ticket
Browse
Create new ticket
Profile
Create invitations
Send invitations
Bookmarks
Support
Logout
User:
Submit
Cancel
Subject
Broken page
Description
http://www.facebook.com/?_fb_noscript=1
I can log in, but some features don't to work properly. For example, I can't seem to send friend requests. (The mobile site appears to work, though!)
Submit
Cancel

11. SABZPROXY

SabzProxy, *proxy vert* en persan, est un proxy Web distribué gratuitement par l'équipe de Sabznameh.com. Il est basé sur le code de PHProxy, qui n'est plus maintenu depuis 2007. Pour des informations plus poussée sur le concept de proxy Web, référez-vous au chapitre précédent.

La principale amélioration apportée par SabzProxy au code de PHProxy est l'encodage des URL, qui rend SabzProxy plus difficile à détecter. PHProxy a toutefois une empreinte facile à prévoir, ce qui a engendré son blocage dans plusieurs pays, dont l'Iran. Seul le DPI permettrait de détecter et bloquer SabzProxy.

SabzProxy est en persan mais fonctionne dans n'importe quelle langue. Bien des gens dans bien des pays s'en servent pour mettre en place leur propre proxy Web public.

INFORMATIONS GÉNÉRALES

Système d'exploitation supporté	
Langue	Persian
Site Web	http://www.sabzproxy.com
Support	E-mail: sabzproxy@gmail.com

COMMENT ACCÉDER À SABZPROXY ?

SabzProxy est un proxy Web distribué. Cela signifie qu'il n'y a ni serveur central de SabzProxy, ni entité commerciale destinée à créer et diffuser les serveurs. Il compte plutôt sur sa communauté et ses utilisateurs pour l'installation et le partage de nouveau nœuds dans leurs réseaux. Vous pouvez accéder à de tels nœuds par différents forums, par réseau, et vous êtes invité à les partager avec vos amis lorsque vous en trouvez un.

Le forum d'aide au contournement de Seawave fait tourner sa propre instance, disponible à cette adresse : http://kahkeshan-e-sabz.info/home (connectez-vous avec: flossmanuals / flossmanuals).

Si vous possédez un espace de stockage Web et voulez créer et partager votre propre instance SabzProxy avec vos amis et votre famille, consultez le chapitre sur l'installation de SabzProxy dans la section « Aider les autres » de ce livre.

COMMENT ÇA MARCHE ?

Voici un exemple montrant comment SabzProxy fonctionne :

1. Accédez à l'instance SabzProxy avec votre navigateur.
2. Entrez l'adresse de la page Web censurée à laquelle vous voulez accéder dans le champ adapté : par exemple, http://www.bbc.co.uk/persian.
3. Cliquez sur « Go » ou « Enter ».

Le site Web apparaît dans la fenêtre du navigateur.

Vous pouvez voir la barre verte de SabzProxy ainsi que le site Web de la BBC en persan en-dessous.

Pour continuer à surfer, vous pouvez soit :

- suivre un lien de la page, qui vous fera passer par le proxy.
- spécifier une nouvelle URL dans le champ en haut de la page.

OPTIONS AVANCÉES

Habituellement, vous pouvez laisser les options par défaut. Quoi qu'il en soit, vous avez la possibilité de choisir entre plusieurs options avancées :

- **Include mini URL-form on every page » / « آدرس فرم »**
  Cochez cette option si vous voulez que les pages affichées contiennent un champ URL sans avoir à retourner à l'accueil de SabzProxy. Vous pouvez décocher cette option si vous avez un petit écran ou voulez plus d'espace pour les pages.
- **Remove client-side scripting / « ها حذف اسکریپت » (i.e., JavaScript)**
  Cochez cette option si vous voulez retirer les scripts des pages Web. Parfois, Javascript peut poser des problèmes indésirables, en affichant des publicités en ligne ou en traçant votre identité. Utiliser les versions simplifiées ou mobiles des sites Web complexes, comme les services de webmail ou les plateformes sociales, peut vous aider à vous passer de Javascript.
- **Allow cookies to be stored / « کوکی ها قبول کردن »**
  Les cookies sont de petits fichiers textes souvent enregistrés lorsque vous naviguez sur le Web. Ils sont nécessaires pour les sites Web demandant une identification mais sont aussi utilisés pour vous tracer. Si vous activez cette option, chaque cookie sera stocké longtemps. Si vous voulez activer cookies seulement pour la session, choisissez plutôt l'option « Store cookies for this session only ».
- **Show images on browsed pages / « عکسها نمایش »**
  Si vous utilisez une connexion à Internet lente, vous devriez désactiver cette option afin que les pages soient plus légères et rapides à charger.
- **Show actual referring Web site / « مسیرها نمایش »**
  Par défaut, votre navigateur prévient tous les sites Web de la page d'où vous venez, celle où vous avez cliqué sur le lien qui vous a amené à consulter le site Web. Cela est enregistré dans les journaux du site Web et analysé automatiquement. Pour améliorer votre confidentialité, vous pouvez décocher cette option.
- **Strip meta information tags from pages / « هاي متا حذف تگ »**
  Les balises meta sont des informations supplémentaires que les sites Web fournissent et qui sont utilisées par les clients logiciels. Ces informations peuvent comprendre le nom de l'auteur, une description du contenu du site, ou des mots-clefs pour les moteurs de recherche. Les systèmes de filtrage peuvent se baser sur ces balises. Vous devriez laisser cette option cochée afin d'éviter d'offrir ces informations aux filtres.
- **Strip page title / « صفحات حذف عنوان »**
  SabzProxy supprime, grâce à cette option, le titre des pages Web que vous voyez normalement dans la barre de titre de votre navigateur. Cela peut être utile, par exemple pour cacher le nom du site que vous visitez aux gens vous entourant, lorsque votre navigateur se trouve minimisé dans la barre des tâches.
- **Store cookies for this session only / « موقت کوکي ها »**
  Cette option permet de n'activer les cookies que pour la session de navigation courante, ce qui peut permettre de limiter le traçage qu'ils permettent.

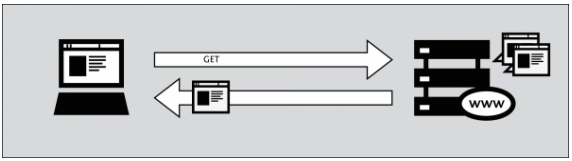
FIREFOX ET SES EXTENSIONS

12. INTRODUCTION À FIREFOX
13. NOSCRIPT ET ADBLOCK
14. HTTPS EVERYWHERE
15. RÉGLAGES PROXY ET FOXYPROXY

12. INTRODUCTION À FIREFOX

Notre hypothèse est que vous ne seriez pas en train de lire ce chapitre si vous ne saviez pas ce qu'est un navigateur Internet. Cependant, si vous ne le savez pas, un navigateur est le logiciel que vous utilisez pour visiter des sites web sur Internet.

Dans un chapitre précédent, nous avions expliqué que l'Internet est un gigantesque réseau d'ordinateurs, tous reliés les uns aux autres. Certains de ces ordinateurs sont des « serveurs web », soit des ordinateurs hébergeant un site web. Si vous voulez visiter ces sites à partir d'un ordinateur ou d'un appareil mobile, vous avez besoin d'un moyen de surfer et de les afficher. C'est ce que fait un navigateur.



L'un des navigateurs les plus populaires est Firefox, un navigateur open source libre, créé par la fondation Mozilla en 2003. Firefox fonctionne sur tous les principaux systèmes d'exploitation, Windows, MacOS et Linux. Il a été traduit dans plus de 75 langues. Cerise sur le gâteau, il est complètement gratuit.

OÙ OBTENIR FIREFOX

Si vous voulez installer Firefox, vous pouvez trouver les fichiers d'installation ici :

https://www.mozilla.com/firefox/

Lorsque vous visitez ce site, le fichier d'installation approprié pour votre système d'exploitation (Windows/Mac/Linux) vous sera automatiquement proposé. Pour plus d'informations sur la façon d'installer Firefox sur chacun de ces systèmes d'exploitation, vous pouvez voir le manuel FLOSS de Firefox : http://en.flossmanuals.net/firefox

QU'EST-CE QU'UN ADD-ON FIREFOX ?

Lorsque vous téléchargez et installez Firefox pour la première fois, il peut gérer immédiatement les tâches de base d'un navigateur. Vous pouvez également ajouter des fonctionnalités supplémentaires ou changer la façon dont se comporte Firefox en installant des *add-on*, des petits ajouts pour étendre le pouvoir de Firefox. Il y a plusieurs sortes d'add-on :

- des extensions qui fournissent des fonctionnalités supplémentaires au navigateur.
- des thèmes qui changent l'apparence de Firefox.
- des plugins qui permettent à Firefox de manipuler des choses qu'il ne supporte pas nativement (pour les animations Flash, les applications Java, etc.)

La variété des add-on disponibles est énorme. Vous pouvez ajouter des dictionnaires pour des langues différentes, suivre les conditions météorologiques dans d'autres pays, obtenir des suggestions de sites Web similaires à celui que vous consultez actuellement, et beaucoup d'autres choses.

Firefox garde une liste à jour des add-on sur son site (https://addons.mozilla.org/firefox), ou vous pouvez les consultez par catégorie à http://addons.mozilla.org/firefox/browse.

Avant d'installer un add-on, garder à l'esprit qu'il peut lire beaucoup d'informations à partir de votre navigateur donc il est très important de choisir des add-on de sources fiables. Sinon, un add-on installé, pourrait partager des informations vous concernant à votre insu, tenir un registre des sites que vous avez visité, ou même endommager votre ordinateur.

Nous vous recommandons de ne jamais installer un add-on pour Firefox sauf s'il est disponible à partir de la page Firefox sur les add-on. Vous ne devriez également jamais installer Firefox si vous n'obtenez pas les fichiers d'installation d'une source fiable. Il est important de noter que l'utilisation de Firefox chez quelqu'un d'autre ou sur dans un cyber café augmente votre vulnérabilité potentielle.

Dans les trois chapitres suivants, nous examinerons certains add-on qui sont particulièrement pertinents pour faire face à la censure sur Internet.

13. NOSCRIPT ET ADBLOCK

Bien qu'aucun outil ne puisse vous protéger complètement de toutes les menaces à votre confidentialité et votre sécurité, les extensions Firefox décrites dans ce chapitre peuvent réduire sensiblement votre exposition aux plus communes, et améliorer vos chances de rester anonyme.

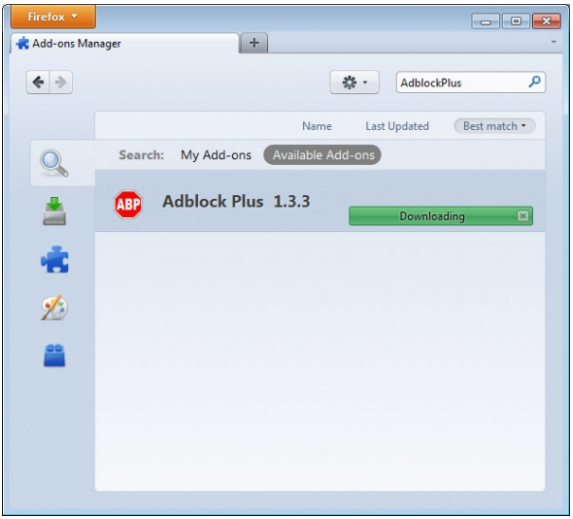
ADBLOCK PLUS

Adblock Plus, http://www.adblockplus.org, scanne les pages Web à la recherche de publicités et de contenus pouvant vous chercher, puis les bloque. AdBlock Plus se base sur des listes de filtrage tenues par des bénévoles pour se tenir au courant des dernières mises à jour.

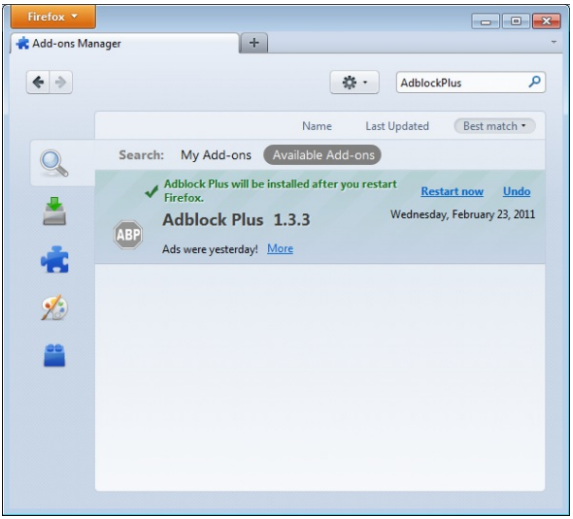
Commencer à utiliser AdBlock Plus

Une fois Firefox installé :

1. téléchargez la dernière version d'AdBlock Plus sur http://adblockplus.org/en/installation#release ou cherchez l'extension dans le gestionnaire de Firefox (Firefox > Modules complémentaires).
2. Confirmez que vous voulez installer AdBlock Plus en cliquant sur « install now ».

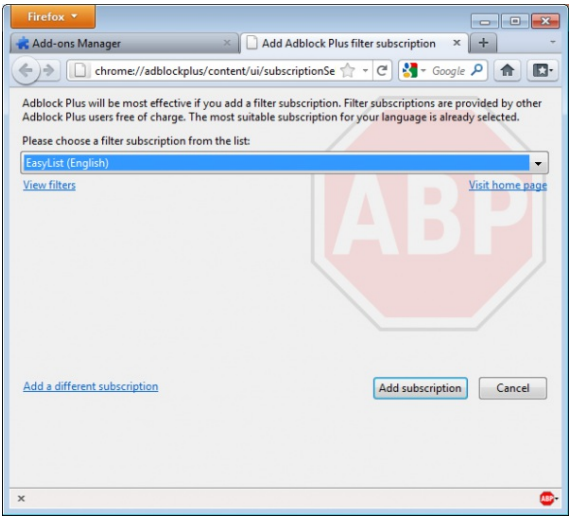


3. Après avoir installé AdBlock Plus, Firefox vous demandera de redémarrer.



Choisir un abonnement à un filtre

AdBlock Plus en lui-même ne fait rien. Il voit chaque élément du site Web commencer à se charger, mais il ne sait pas lesquels bloquer. C'est ce à quoi servent les filtres. Après le redémarrage, AdBlock Plus vous demandera de vous abonner à un filtre (gratuitement).



Quel filtre choisir ? AdBlock Plus en propose quelques-uns dans le menu déroulant et vous devriez vous renseigner quant à l'efficacité de chacun. Un bon filtre pour commencer à protéger votre confidentialité est EasyList (http://easylist.adblockplus.org/en).

Aussi tentant que cela puisse paraître, n'ajoutez pas tous les abonnements que vous trouvez, puisque certains peuvent se superposer et provoquer de comportement inattendus. EasyList (visant les sites en anglais) fonctionne bien avec les autres extensions EasyList (dédiées à d'autres régions, comme RuAdList, ou thèmes, comme EasyPrivacy). En revanche, il entre en conflit avec la liste Fanboy (aussi pour les sites anglais).

Vous pouvez à tout moment changer vos abonnements dans les préférences. Pour y accédez, cliquez sur l'icône de AdBlock Plus puis « Préférences ». Pour enregistrer vos changements, cliquez sur « OK ».

Créer des filtres personnalisés

AdBlock Plus vous permet aussi de créer vos propres filtres, si vous le souhaitez. Rendez-vous dans les préférences et cliquez sur « Ajouter un filtre » dans le coin inférieur gauche. Les filtres personnalisés ne se substituent pas à l'avantage que procurent les sites tels que EasyList, mais ils peuvent être utiles pour bloquer certains contenus non gérés par les listes publiques. Par exemple, si vous voulez empêcher l'accès à Facebook depuis d'autres sites Web, vous pouvez ajouter ce filtre :

```
||facebook.*$domain=~facebook.com|~127.0.0.1
```

La première partie « ||facebook.* » demande de bloquer tout ce qui vient du domaine de Facebook. La seconde partie « $domain=~facebook.com|~127.0.0.1 » désactive ce filtre pour les requêtes venant de vous ou de Facebook quand vous naviguez sur le site.

Vous trouverez un guide sur la création de filtres ici : http://adblockplus.org/en/filters.

Activer et désactiver AdBlock Plus pour des éléments ou sites Web

Vous pouvez accéder à la liste des éléments identifiés par AdBlock

Plus en cliquant sur l'icône « APB »  et en choisissant « Ouvrir la liste des éléments filtrables », ou bien en appuyant simultanément sur Ctrl, Shift et sur V. Un panneau s'ouvre au bas de votre navigateur et vous permet d'activer ou désactiver chaque élément au cas-par-cas. Autrement, vous pouvez désactiver AdBlock Plus pour un domaine ou une page donné en cliquant sur l'icône et en choisissant « Désactiver pour [nom de domaine] » ou « Désactiver seulement pour cette page ».

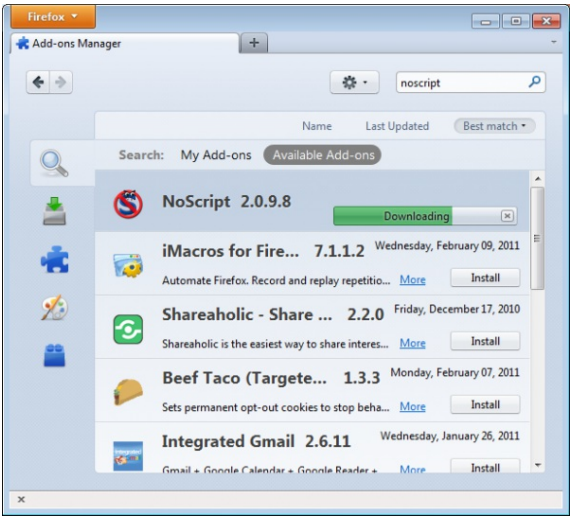
NOSCRIPT

L'extension NoScript protège votre navigateur en bloquant tous les éléments Javascript, Java ainsi que d'autres exécutables contenus dans les sites Web. Pour dire à NoScript d'autoriser certains sites, vous devez les ajouter à une liste blanche. Cela peut sembler fastidieux, mais le blocage de NoScript est très efficace contre des menaces comme XSS « Cross Site Scripting » quand un code malveillant est appelé depuis un autre site, ou le clickjacking, un élément sur lequel vous cliquez révèle vos informations et peut prendre le contrôle de votre ordinateur. Pour obtenir NoScript, allez sur http://addons.mozilla.org ou http://noscript.net/getit.

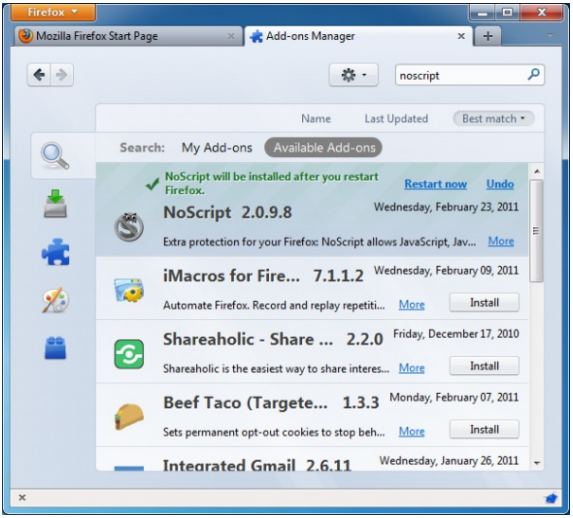
La manière dont NoScript vous protège peut altérer l'apparence et les fonctionnalités de certains pages Web sûres. Heureusement, vous pouvez modifier manuellement comment NoScript doit fonctionner sur ces pages. c'est à vous de trouver le bon équilibre entre confort et sécurité.

Démarrer avec NoScript

1. Allez sur la page de téléchargement http://noscript.net/getit et cliquez sur le bouton vert « INSTALL ».
2. Confirmez l'installation en cliquant sur "Install Now".



3. Redémarrez votre navigateur lorsque celui-ci vous le demande.



Les notifications NoScript et l'autorisation de sites Web

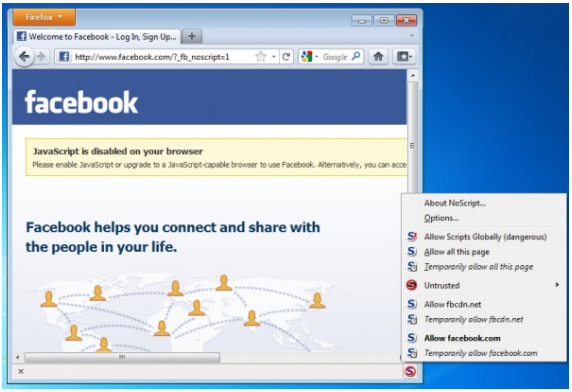
Après le redémarrage, vous verrez une icône NoScript dans le coin inférieur droit de votre navigateur, dans la barre d'état, ou bien à côté de la barre d'adresse, indiquant le niveau actuel d'autorisation que la page Web a d'exécuter des programmes.

- Protection maximale : les scripts sont bloqués pour le site actuel et les pages qu'il charge. Même si certains scripts se trouvent dans votre liste blanche, ils ne seront pas exécutés (les fichiers externes ne sont pas activés).
- Protection forte : le site ne peut toujours pas exécuter de scripts, mais les fichiers externes sont autorisés. Dans ce cas, du code peut s'exécuter, mais la page a peu de chances de fonctionner correctement. Elle ne peut pas appeler ses propres scripts.
- Permissions restreintes : les scripts sont autorisés pour la page actuelle, mais les fichiers et scripts externes ne sont pas autorisés. Cela arrive quand le site Web appelle d'autres pages ou des éléments de scripts hébergées ailleurs.
- Confiance relative : tous les scripts sont autorisés, mais certains contenus importés (comme les iframes) sont bloqués.
- Protection sélective : les scripts sont autorisés pour certaines URL. Les autres sont considérés comme non fiables.
- Tous les sites sont autorisés dans la page actuelle.
- Les scripts sont autorisés de manière globale, mais le contenu considéré comme non fiable n'est pas chargé.

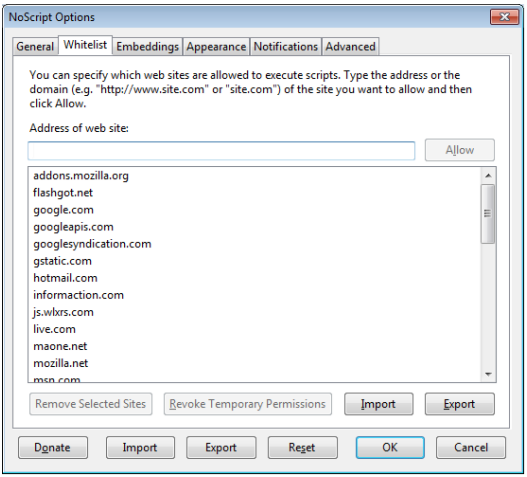
Pour ajouter un site auquel vous faites confiance dans la liste blanche, cliquez sur l'icône de NoScript et choisissez :

- « Autoriser [nom de domaine] » pour autoriser les scripts hébergés sur le domaine
- « Autoriser toute la page » pour autoriser l'exécution de tous les scripts — y compris ceux hébergés ailleurs.

Par ailleurs, vous pouvez ajouter des noms de domaines directement à la liste blanche en modifier les options de NoScript (cliquer sur l'icône puis « Options ») dans l'onglet « Liste blanche ».



Vous pouvez aussi utiliser « Autoriser [nom de domaine] temporairement » ou « Autoriser cette page temporairement » pour n'autoriser le chargement du contenu que pour la session de navigation. Cela peut être utile pour les gens qui n'ont l'intention de visiter un site qu'une fois et veulent limiter la taille de leur liste blanche.



Marquer le contenu comme non fiable

Si vous voulez empêcher définitivement les scripts de certains sites Web de se charger, vous pouvez les marquer comme non fiables. Cliquez sur l'icône de NoScript, ouvrez le menu « Non fiable » et choisissez le domaine à marquer comme non fiable. NoScript se souviendra de ce choix, même si l'option « Autoriser Javascript globalement » est activée.

14. HTTPS EVERYWHERE

HTTPS Everywhere est un add-on pour Firefox produit en collaboration par The Tor Project https://www.torproject.org et Electronic Frontier Foundation https://eff.org/.

La plupart des sites sur le Web supportent le chiffrement des données via le protocole HTTPS, mais n'en facilitent pas l'utilisation, par exemple en vous connectant par défaut en HTTP, même si le protocole HTTPS est disponible. Autre exemple, en fournissant sur les pages chiffrées des liens qui vont vous rediriger vers la version non chiffrée du site. De cette manière, les données telles que les noms d'utilisateur et les mots de passe envoyés et reçus par ces sites sont transférés en clair et sont facilement lisibles par un tiers.

L'extension HTTPS Everywhere résout ces problèmes en réécrivant toutes les requêtes à ces sites en HTTPS. Même si cette extension est appelée « HTTPS Everywhere », elle active simplement HTTPS sur une liste particulière de sites qui ont choisi de supporter ce protocole. Elle ne peut en aucun cas rendre votre connexion à un site sécurisée si le site en question ne supporte pas le protocole HTTPS.

La plupart de ces sites incluent un grand nombre de contenus, comme des images ou des icônes, provenant de domaines tiers qui ne sont pas accessibles via HTTPS. Comme toujours, si l'icône indiquant le chiffrement de la connexion apparait comme cassée, ou arbore un point d'exclamation, vous demeurez vulnérables à certaines attaques utilisant des techniques actives ou de l'analyse de trafic. Néanmoins, les efforts nécessaires pour surveiller votre activité devraient être augmentés.

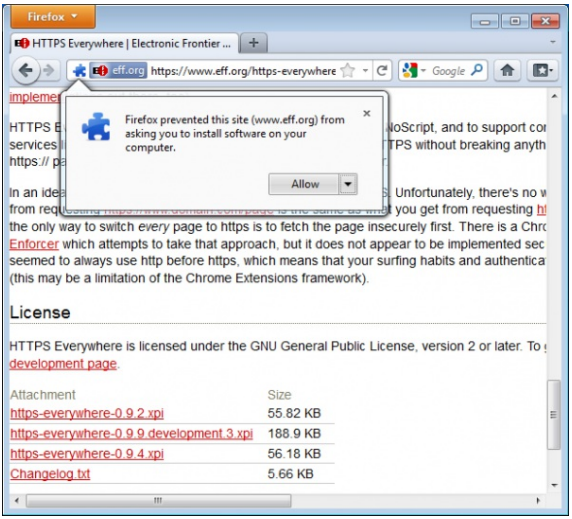
Certains sites, comme Gmail, proposent un support HTTPS automatique, mais l'utilisation de HTTPS Everywhere vous protègera aussi des attaques de type SSL-stripping, via lesquelles un attaquant peut cacher la version HTTPS du site aux yeux de votre ordinateur si vous commencez par vous connecter à sa version HTTP.

Des informations complémentaires à ce sujet sont disponibles à l'adresse : https://www.eff.org/https-everywhere.

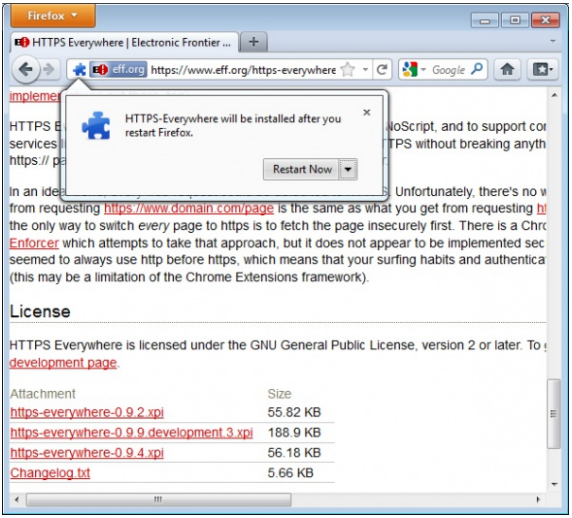
INSTALLATION

Tout d'abord, téléchargez l'extension HTTPS Everywhere sur le site officiel : https://www.eff.org/https-everywhere. Sélectionnez la dernière version.

Dans notre exemple, c'est la version 0.9.4 de HTTPS Everywhere qui est utilisée. Il est probable qu'une version plus récente soit désormais disponible.

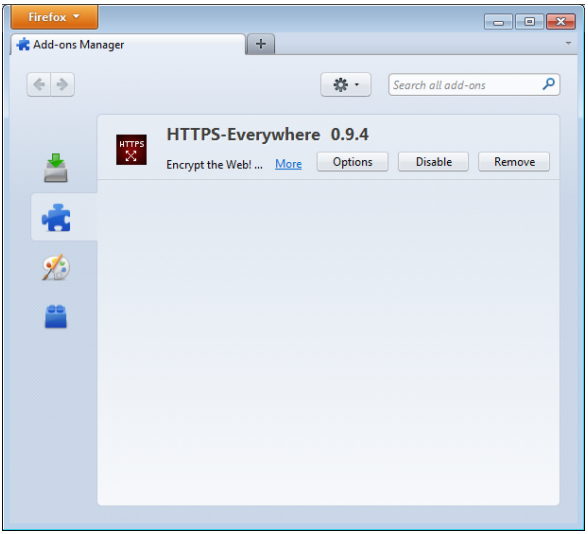


Cliquez sur « Autoriser ». Vous devrez ensuite redémarrer Firefox en cliquant sur le bouton « Redémarrez maintenant ». HTTPS Everywhere est désormais installé.

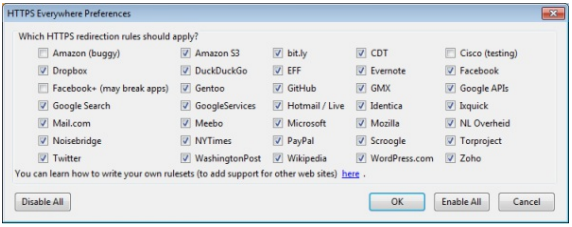


CONFIGURATION

Pour accéder au panneau de configuration de HTTPS Everywhere dans Firefox 4 (Linux), cliquez sur le menu Firefox en haut à gauche de votre écran et sélectionnez « Modules complémentaires ». Sous un système d'exploitation différent ou dans une autre version de Firefox, ce menu peut être situé à un emplacement différent.



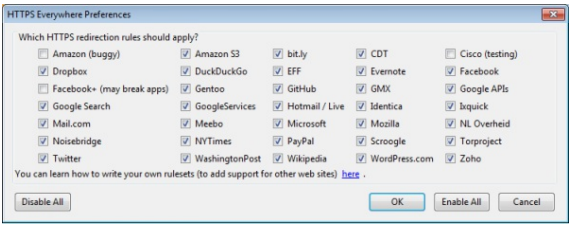
Cliquez sur le bouton « Options ».



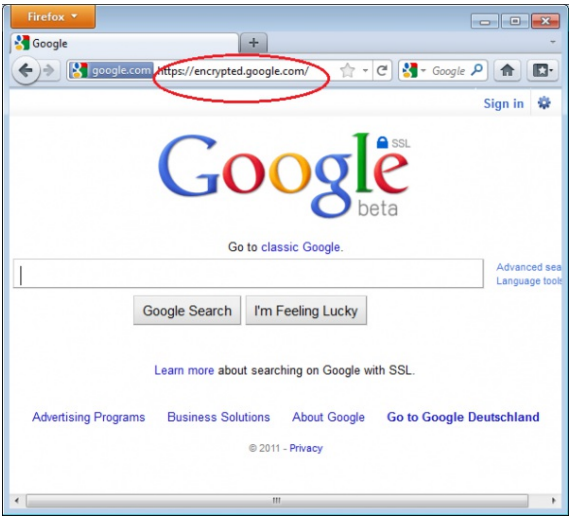
Une liste de tous les sites supportés où le protocole HTTPS est disponible va s'afficher. Si une règle de redirection particulière vous pose problème, vous pouvez la désactiver ici. Dans ce cas, HTTPS Everywhere ne modifiera plus la façon dont vous vous connecterez à ce site particulier.

UTILISATION

Une fois activé et configuré, HTTPS Everywhere est transparent à l'utilisation. Essayez de taper une adresse HTTP non sécurisée, par exemple, http://www.google.com.



Press Enter. You will be automatically redirected to the secure HTTPS encrypted Web site (in this example: https://encrypted.google.com). No other action is needed.



Si le réseau bloque HTTPS

Votre administrateur réseau peut décider de bloquer les versions sécurisées des sites Web de façon à augmenter sa capacité à espionner ce que vous faites. Dans de tels cas, HTTPS Everywhere peut vous empêcher d'accéder à ces sites puisque elle force votre navigateur à utiliser la version protégée de ces sites et jamais la version non protégée. Nous avons entendu parler du réseau Wifi d'un aéroport où toute les connections via HTTP était permises, mais pas les connexions en HTTPS. Peut-être que les administrateurs du réseau étaient intéressés par la surveillance de ce que faisaient les utilisateurs. Dans cet aéroport, les utilisateurs de HTTPS Everywhere n'avaient plus la possibilité d'utiliser certains sites à moins de désactiver temporairement HTTPS Everywhere.

Dans ce cas de figure, vous devriez choisir d'utiliser HTTPS Everywhere en collaboration avec une technologie de contournement telle que Tor ou un VPN afin de contourner le blocage des accès sécurisés aux sites Web.

Ajouter le support d'autres sites dans HTTPS Everywhere

Vous pouvez ajouter vos propres règles à l'extension HTTPS Everywhere pour vos sites Web favoris. Vous trouverez comment faire ceci à l'adresse : https://www.eff.org/https-everywhere/rulesets. L'avantage de procéder ainsi consiste en l'apprentissage de HTTPS Everywhere afin de s'assurer que votre accès à ces sites est sécurisé. Toutefois, HTTPS Everywhere ne vous permettra pas d'accéder à des sites de manière sécurisée si l'administrateur du site n'a pas choisi d'en permettre l'accès de cette manière. Si un site ne supporte pas le protocole HTTPS, il n'y a aucun intérêt à ajouter une règle pour ce site.

Si vous vous occupez d'un site Web et que vous avez fait en sorte que sa version HTTPS soit disponible, une bonne idée serait d'en proposer l'ajout dans la prochaine version de HTTPS Everywhere.

15. RÉGLAGES PROXY ET FOXYPROXY

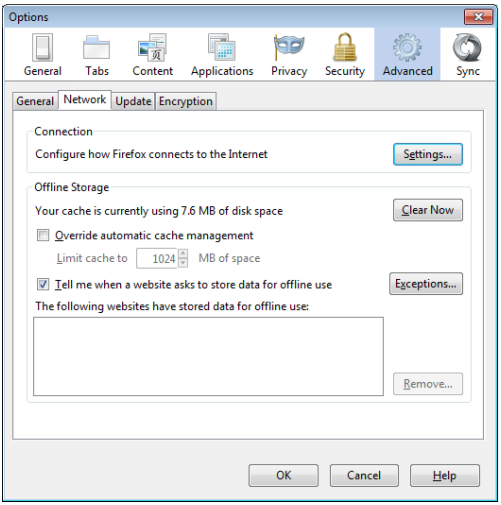
Un serveur proxy vous autorise à joindre un site Web ou une adresse Internet même si l'accès direct est bloqué dans votre pays ou par votre FAI. Il existe de nombreux types de proxys :

- Des proxys Web, qui nécessitent seulement de connaître l'adresse du site. Une URL de proxy Web ressemble à http://www.example.com/cgi-bin/nph-proxy.cgi.
- Des proxys HTTP, qui nécessitent de modifier les réglages de votre navigateur. Ils fonctionnent uniquement pour du contenu Web. Vous pouvez obtenir l'information d'un proxy HTTP dans le format « proxy.example.com:3128 » ou « 192.168.0.1:8080 ».
- Des proxys SOCKS, qui nécessitent également une modification des réglages de votre navigateur. Les proxys SOCKS fonctionnent pour beaucoup d'applications Internet différentes, incluant des outils email et messagerie instantanée. L'information d'un proxy SOCKS ressemble exactement à l'information d'un proxy HTTP.

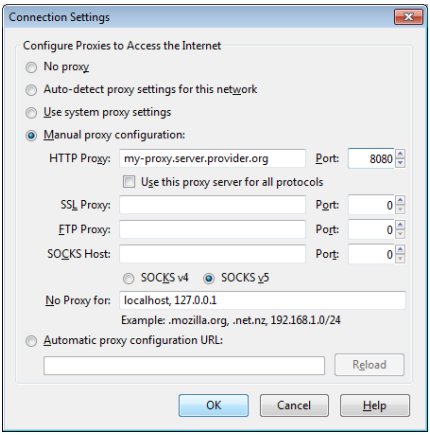
Vous pouvez utiliser un proxy Web directement sans aucune modification en tapant l'URL. Cependant, les proxys HTTP et SOCKS doivent être configurés depuis votre navigateur Web.

CONFIGURATION PAR DÉFAUT D'UN PROXY FIREFOX

Dans Firefox 4 (Linux), vous accédez à l'écran de configuration en cliquant dans le menu Firefox. Choisissez « Édition » puis sélectionnez « Préférences ». Dans la fenêtre pop-up, choisissez l'icône « Avancé » puis l'onglet « Réseau ». Vous devriez voir cette fenêtre :



Choisissez « Paramètres », cliquez sur « Configuration manuelle du proxy » et entrez les informations dur serveur proxy que vous souhaitez utiliser. Rappelez-vous bien que les proxys HTTP et SOCKS fonctionnent différemment : Les informations doivent être entrées dans les champs correspondants. S'il y a une colonne (:) dans les informations du proxy, il s'agit du séparateur entre l'adresse proxy et le numéro de port. Votre écran devrait ressembler à ça :



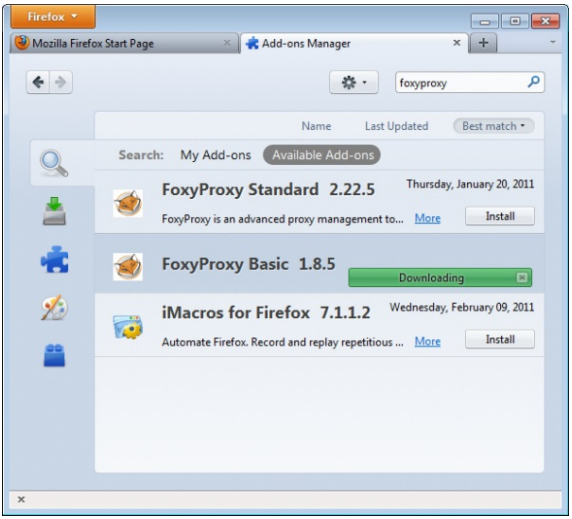
Après avoir cliqué sur « OK », vous devez sauvegarder votre configuration, votre navigateur Web vous connectera automatiquement à travers le proxy lors des prochaines connections. Si vous obtenez un message d'erreur tel que « le serveur proxy refuse les connections » ou « impossible de détecter le serveur proxy » c'est qu'il y a un problème de configuration. Dans ce cas, répétez les étapes précédentes et sélectionnez « Pas de proxy » dans le dernier écran pour le désactiver.

FOXYPROXY

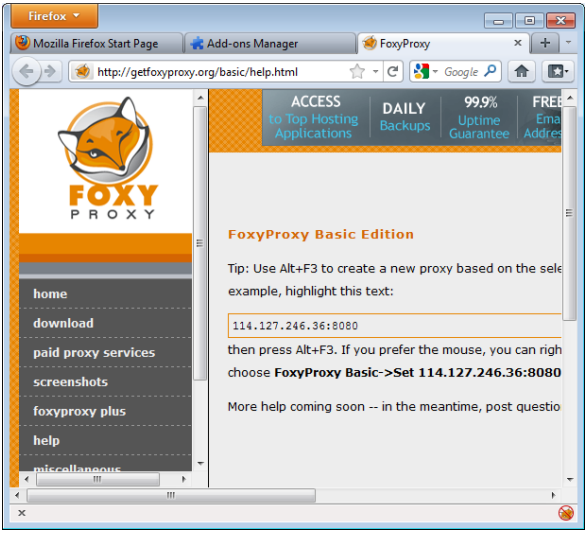
FoxyProxy est une extension gratuite pour Mozilla Firefox qui permet de gérer plus facilement des serveurs proxy multiples et d'en changer rapidement. Pour les détails, visitez http://getfoxyproxy.org/.

Installation

Ouvrez un nouvel onglet dans Firefox (version 4) et tapez « about:addons » dans la barre d'adresse, puis appuyez sur la touche « Entrée ». Dans le champ de recherche en haut à droite, tapez le nom de l'extension que vous voulez installer (ici, « FoxyProxy »). Deux versions de FoxyProxy apparaîtront dans les résultats: « Standard » et « Basic ». Pour connaître les différences, rendez-vous à cette adresse http://getfoxyproxy.org/downloads.html#editions. Vous pouvez vous contenter de la version « basic ». Une fois que vous avez choisi, cliquez sur le bouton « Installer » à droite correspondant.

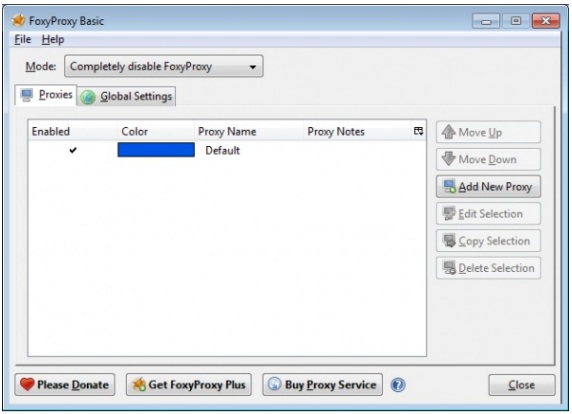


Après l'installation, Firefox demandera à redémarrer. Suite au redémarrage, un onglet s'ouvrira sur le site de FoxyProxy et vous verrez apparaître l'icône de l'extension dans votre interface.

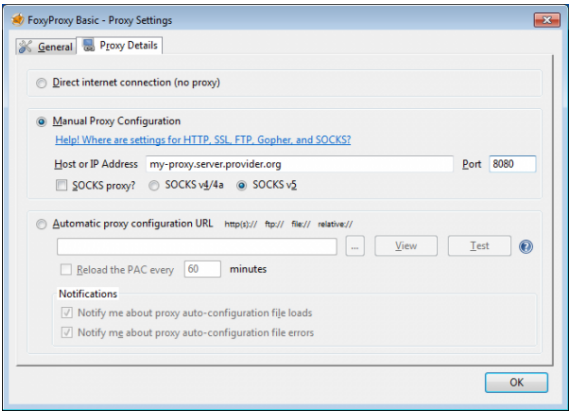


Configuration

Afin que FoxyProxy fonctionne, il a besoin de savoir quelles configurations de proxy il doit utiliser. Cliquez simplement sur l'icône de l'extension. Voici à quoi la fenêtre devrait ressembler :



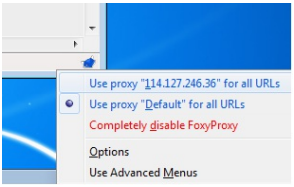
Vous devez alors ajouter un proxy en cliquant sur « Ajouter un nouveau proxy ». Dans la fenêtre qui s'ouvre, vous renseignez alors la configuration du proxy de la même manière que dans la configuration de Mozilla Firefox.



Dans l'onglet « Informations », choisissez l'option « Configuration manuelle du proxy » puis entrez l'adresse IP et le port à utiliser. Si tel est le cas, cochez la case « Proxy SOCKS ? ». Enfin, cliquez sur « OK ». Vous pouvez ajouter d'autres proxys en répétant ces opérations.

Utilisation

Vous pouvez basculer sur un autre de votre proxys (ou choisir de ne plus utiliser) en faisant un clic droit sur l'icône de FoxyProxy.



Faites simplement un clic gauche pour choisir l'option appropriée.

OUTILS

16. INTRODUCTION

L'idée de base pour contourner la censure sur Internet consiste à faire transiter les requêtes par un serveur tiers qui n'est pas bloqué et qui est connecté à l'Internet grâce à une connexion non filtrée. Ce chapitre présente certains des outils qui permettent d'utiliser ce type de serveur pour déjouer le blocage, le filtrage et la surveillance sur l'Internet. Le choix de l'outil susceptible de réaliser le mieux vos objectifs doit se fonder sur une évaluation préalable du type de contenu auquel vous voulez accéder, des ressources disponibles et des risques encourus.

Les outils destinés à déjouer le blocage, le filtrage et la surveillance sur l'Internet sont conçus pour faire face à différents obstacles et menaces. Ils permettent de :

- **Contourner la censure :** possibilité de lire ou publier un contenu, d'envoyer ou recevoir des informations, ou de communiquer avec des personnes en particulier, des sites ou des services en contournant les tentatives faites pour vous en empêcher. Et cela, sur le même mode que l'option cache de Google ou un agrégateur RSS qui peut être utilisé pour accéder indirectement à un site web bloqué.
- **Empêcher l'écoute :** préserver le caractère privé des communications, afin que personne ne voit ou n'entende le contenu de votre communication (même s'ils arrivaient à voir avec qui vous communiquez). Les outils destinés à tenter de contourner la censure sans empêcher l'écoute restent malgré tout vulnérables à la censure au moyen du filtrage par détection de mots-clés qui bloque toutes les communications contenant certains mots interdits. Par exemple, diverses formes de cryptage, comme HTTPS ou SSH, rendent les informations illisibles pour toute autre personne que l'expéditeur ou le destinataire. Des oreilles indiscrètes verront quel utilisateur se connecte à quel serveur Web, mais ne verront du contenu qu'une suite de lettres sans aucun sens.
- **Conserver l'anonymat :** la capacité de communiquer de manière à ce que personne ne se connecte[1] aux informations ou aux personnes avec qui vous vous connectez – pas plus votre fournisseur d'accès Internet que les sites ou les personnes avec lesquels vous communiquez. De nombreux serveurs et outils proxys n'offrent parfait ni même aucun anonymat : l'opérateur proxy peut observer le trafic entrant et sortant du proxy et déterminer sans difficulté qui envoie les informations, quand et à quelle fréquence ; un observateur mal intentionné à un bout ou à l'autre de la connexion est en mesure de recueillir les mêmes informations. Des outils comme le logiciel Tor sont conçus pour rendre la tâche difficile aux cyber-attaquants qui veulent recueillir ce type d'informations sur les utilisateurs en limitant la quantité d'informations qui peut se trouver sur un nœud du réseau concernant l'identité de l'utilisateur ou le lieu où il se trouve.
- **Dissimuler ce que vous faites :** camoufler les communications que vous envoyez de manière à ce que la personne qui vous espionne ne puisse deviner que vous êtes en train d'essayer de contourner la censure. Par exemple, la stéganographie, qui consiste à dissimuler les messages textuels dans un fichier image ordinaire, permet carrément de cacher le fait que vous utilisez un outil de contournement. Utiliser un réseau avec divers types d'utilisateurs signifie qu'un adversaire ne peut deviner ce que vous faites grâce au choix de logiciel que vous avez fait. Ce procédé est particulièrement efficace lorsque d'autres personnes utilisent le même système pour accéder à un contenu qui ne soulève pas de problème de censure.

Certains outils protègent vos communications d'une de ces manières uniquement. Par exemple, de nombreux proxy peuvent contourner la censure mais n'empêchent pas l'écoute. Il est important de comprendre que si vous souhaitez atteindre votre but, il vous faudra disposer d'un assortiment d'outils.

Chaque type de protection convient à des personnes différentes dans des situations différentes. Lorsque vous choisissez un outil de contournement de la censure sur l'Internet, vous devez garder à l'esprit le type de protection dont vous avez besoin et savoir si l'ensemble d'outils particuliers que vous utilisez vous fournit ce type de protection. Par exemple, que se passera-t-il si quelqu'un détecte que vous tentez de contourner un système de censure ? Accéder à un site est-il votre priorité ou tenez-vous en même temps à rester anonyme pendant votre tentative ?

Il est parfois possible d'utiliser un même outil pour déjouer la censure et protéger son anonymat, mais la procédure est différente pour chacun. Par exemple, le logiciel Tor sert habituellement pour les deux, mais les utilisateurs de Tor ne procéderont pas de la même manière selon leur priorité. Si c'est pour préserver son anonymat, il est important d'utiliser le navigateur Internet associé à Tor, puisqu'il a été modifié pour empêcher la divulgation de votre véritable identité.

AVERTISSEMENT IMPORTANT

La plupart des outils de contournement de la censure arrivent à être détectés par les opérateurs de réseaux ou les instances gouvernementales qui en font l'effort, du fait que le trafic qu'ils génèrent peut révéler des caractéristiques particulières. Cela vaut assurément pour les méthodes de contournement qui n'utilisent pas le cryptage, mais c'est également valable pour les méthodes qui le font. Il est très difficile de tenir secret le fait que vous utilisez une technologie pour contourner le filtrage, en particulier si vous utilisez une technique assez connue ou si vous continuez à utiliser le même service ou la même méthode pendant longtemps. Il y a également des moyens de découvrir votre comportement ne s'appuyant pas sur une technologie : observation en personne, surveillance ou de nombreuses formes de collecte d'informations classiques effectuée par des personnes.

Nous ne pouvons pas prodiguer de conseils spécifiques relatifs à l'analyse de menaces ou au choix d'outils pour contrer ces menaces. Les risques diffèrent selon la situation et le pays et varient fréquemment. Il faut toujours s'attendre à ce que ceux qui tentent de limiter les communications ou activités poursuivent leurs efforts pour améliorer leurs méthodes.

Si vous agissez de telle manière que vous vous mettez en danger à l'endroit où vous êtes, vous devez évaluer par vous-même le degré de sécurité dans lequel vous vous trouvez et (si possible) consulter des experts.

- Le plus souvent, vous devrez dépendre d'un service fourni par des personnes que vous ne connaissez pas. Vous devrez être conscient qu'elles peuvent avoir accès à des informations relatives à votre lieu d'origine aux sites que vous visitez et même aux mots de passe que vous saisissez sur des sites web non cryptés. Même si vous connaissez la personne et que vous lui faites confiance, étant donné qu'elle utilise un proxy à saut unique ou un RPV, elle peut être piratée ou contrainte de compromettre la confidentialité de vos informations.
- N'oubliez pas que les promesses d'anonymat et de sécurité faites par différents systèmes peuvent s'avérer inexactes. Recherchez une source indépendante les confirmant. Les outils open source peuvent être évalués par des amis calés en technologie. Vous pouvez trouver des bénévoles qui trouveront et corrigeront les failles de sécurité de logiciels open source. Cela est difficile avec des logiciels privés.
- Vous devrez sans doute être discipliné et respecter soigneusement certaines procédures et pratiques de sécurité. Négligez ces procédures peut considérablement réduire les dispositifs de sécurité dont vous disposez. Il est risqué de penser trouver une solution « en un clic » en matière d'anonymat ou de sécurité. Par exemple, il ne suffit pas de faire passer votre trafic par un proxy ou bien Tor. Procéder absolument à un cryptage, assurez la protection de votre ordinateur et éviter de divulguer votre identité dans le contenu que vous publiez.
- Soyez conscient que des personnes (ou des gouvernements) peuvent créer des pièges – de faux sites web et proxys présentés comme offrant une communication sécurisée ou le moyen de contourner la censure mais qui en fait s'emparent des communications à l'insu des utilisateurs.
- Il arrive même parfois qu'un "Policeware" soit installé sur l'ordinateur de l'utilisateur – soit à distance soit directement – et comme un logiciel malveillant, il contrôle toutes les activités dans l'ordinateur même quand celui-ci n'est pas connecté à Internet et annihile la plupart des autres mesures de sécurité préventive. Soyez attentif aux menaces non techniques. Que se passe-t-il si quelqu'un vole votre ordinateur ou téléphone portable ou celui de votre meilleure amie ? si un employé d'un cybercafé regarde par dessus votre épaule ou braque un appareil photo sur votre écran ou votre clavier ? si quelqu'un s'assied devant un ordinateur dans un cybercafé à la place quittée par votre amie parti en oubliant de fermer sa session et que cette personne vous envoie un message en se faisant passer pour elle ? Et si quelqu'un faisant partie de votre réseau social est arrêté et contraint de dévoiler des mots de passe ?
- Soyez conscient des conséquences possibles dans le cas où des lois ou règlementations restreignent ou interdisent les documents auxquels vous voulez accéder ou les activités que vous entreprenez.

Pour en savoir plus sur la sécurité numérique et la protection de la vie privée, voir :

http://www.frontlinedefenders.org/manual/en/esecman/intro.html
http://security.ngoinabox.org/html/en/index.html

[1] In English here, it doesn't seem right : "so that no one can connect you to the information or people you are connecting with"

17. FREEGATE

Freegate est un outil de proxy pour les utilisateurs de Windows, développé à la base par DIT-INC pour contourner la censure en Chine et en Iran.

INFORMATIONS GÉNÉRALES

Système d'exploitation supporté	
Langues	English, Chinese, Persian, Spanish
Site Web	http://www.dit-inc.us/freegate
Support	Forum: http://www.dit-inc.us/support

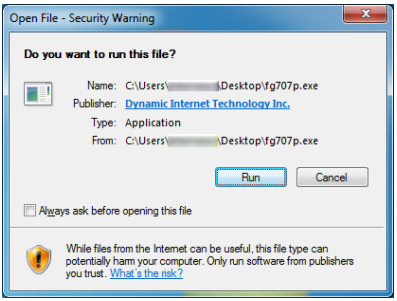
OBTENIR FREEGATE

Téléchargez le logiciel gratuitement à cette adresse http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/Freegate.shtml.

Vous obtiendrez un fichier à l'extension .zip, que vous devrez commencer par extraire. Double-cliquez sur le fichier téléchargé et choisissez « Extraire tout », puis cliquez sur le bouton « Extraire ». Le fichier ainsi obtenu fait environ 1.5 Mo. Le nom du fichier exécutable devrait ressembler à une courte série de lettres et de chiffres (par exemple « fg707.exe »).

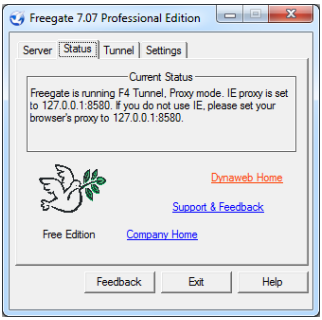
INSTALLATION

Quand vous lancez l'application pour la première fois, vous verrez peut-être un avertissement de sécurité. Vous pouvez l'accepter en décochant la case « Always ask before opening this file ».



LANCER FREEGATE

L'application devrait se lancer et se connecter automatiquement à un serveur.



Quand le tunnel sécurisé est lancé avec succès, vous verrez la fenêtre de statut de Freegate et une nouvelle instance d'Internet Explorer s'ouvrira automatiquement avec l'adresse http://dongtaiwang.com/loc/phome.php?v7.07&l=409, selon la version et le langage. C'est la confirmation que vous utilisez bien Freegate correctement à travers un tunnel chiffré.

Si tout s'est bien passé, vous pouvez commencer à naviguer normalement en utilisant la fenêtre d'Internet Explorer ouverte automatiquement pour contourner la censure d'Internet.

Si vous voulez utiliser une autre application avec FreeGate (par exemple le navigateur web Firefox ou le client de messagerie Pidgin), vous devrez les configurer pour utiliser Freegate comme serveur proxy. L'IP est 127.0.0.1 et le port est 8580.

Dans l'onglet Settings de Freegate, vous pouvez choisir votre langage entre l'anglais, le chinois traditionnel, le chinois simplifié, le perse, et l'espagnol. Dans l'onglet Status, vous pouvez tracer votre trafic en téléchargement/upload à travers le réseau Freegate. L'onglet Server vous permet de choisir entre plusieurs serveurs, dont un pourrait être plus rapide que votre connexion actuelle.

18. SIMURGH

Simurgh, « phoenix » en Persan ? est un proxy super léger. Il peut être exécuté sans aucune installation préalable ou des droits administrateurs sur l'ordinateur. Vous pouvez le copier sur votre clé USB et l'utiliser sur un ordinateur partagé, par exemple dans un cybercafé.

INFORMATIONS GÉNÉRALES

Système d'exploitation supporté	
Langue	English
Site Web	https://simurghesabz.net
Support	E-mail: info@simurghesabz.net

TÉLÉCHARGEMENT SIMURGH

Pour utiliser le service Simurgh, téléchargez l'outil gratuitement à partir de https://simurghesabz.net.

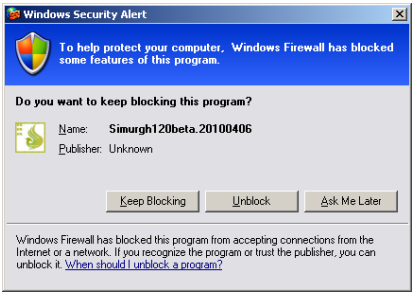
Il est disponible pour toute version de Microsoft Windows. La taille du fichier est inférieure à 1 MO, il peut donc être téléchargé, même sur une lente connexion Internet dans un délai raisonnable.

UTILISER SIMURGH

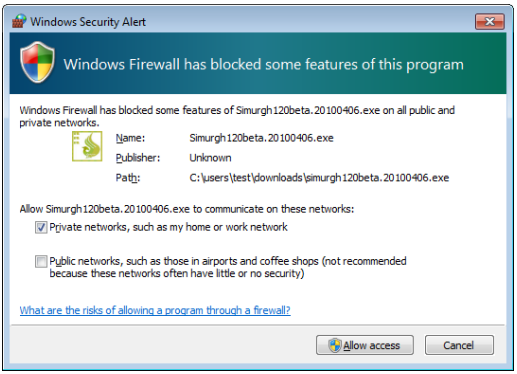
Pour lancer Simurgh, cliquez sur le fichier que vous avez téléchargé. Par défaut, les fichiers téléchargés avec Microsoft Internet Explorer sont situés sur votre bureau et les fichiers téléchargés avec Mozilla Firefox sont situés dans « Mes documents » puis dans « Téléchargements ».

Notez que lorsque vous exécutez Simurgh pour la première fois, vous pouvez rencontrer une alerte de sécurité Windows. Elle demande si vous souhaitez continuer à bloquer Simurgh : Il est très important que vous sélectionnez " »Débloquer » ou « Autorisez l'accès » (selon votre version de Microsoft Windows)

Vous pouvez voir cet avertissement pop-up :



Ou celui-ci :

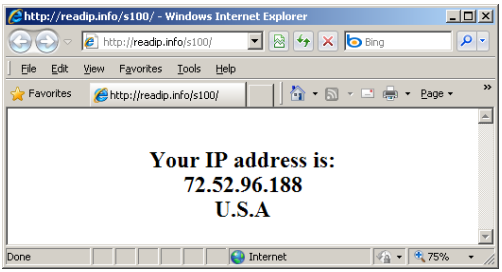


Après avoir démarré avec succès Simurgh, cliquez sur Démarrer pour créer une connexion sécurisée.

Lorsque le bouton Démarrer se change avec un bouton Stop, Simurgh a réussi à se connecter à ses serveurs.

Assurez-vous que vous êtes connecté au serveur de Simurgh

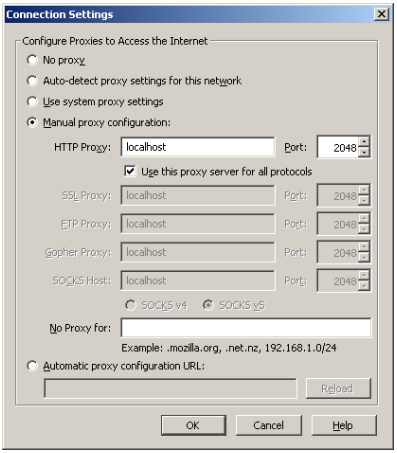
Maintenant une nouvelle fenêtre de votre navigateur Internet Explorer s'ouvre avec une page de test. Si vous voyez votre connexion provient d'un autre pays, comme les USA, cela confirme que Simurgh a réussi à modifié les paramètres de votre navigateur et vous pouvez automatiquement surfer sur la connexion sécurisée Simurgh.



Vous pouvez également utiliser le site internet http://www.geoiptool.com pour vérifier d'où votre connexion semble provenir. Si le site indique votre position très loin (dans un autre pays comme les USA), vous utilisez la connexion sécurisée Simurgh.

UTILISER SIMURGH AVEC MOZILLA FIREFOX

Afin d'utiliser un autre navigateur comme Mozilla Firefox, vous devez le configurer pour utiliser le HTTP proxy "localhost" avec le port 2048. Dans Firefox, vous pouvez trouver les paramètres du proxy via le menu Outils > Options > Réseau > Paramètres. Dans le champ de la fenêtre « Paramètres de connexion », sélectionnez « Configuration manuelle du Proxy » et entrez "localhost" (sans les guillemets) ainsi que le proxy HTTP et le port 2048, comme le montre l'imprime-écran ci-dessous. Pour accepter les nouveaux paramètres, cliquez sur OK.



19. ULTRASURF

****
Attention ! Ce logiciel est dangereux !
Pour plus de renseignements, vous pouvez lire cet article :
http://reflets.info/syrie-ultrasurf-ou-comment-le-gouvernement-syrien-piege-ses-opposants-avec-un-malware/
Merci de relayer cette information.
****

UltraSurf, du développeur UltraReach Corp Internet, est un proxy conçu pour aider les utilisateurs d'Internet Chinois à contourner leur censure. Il peut également fonctionner pour les utilisateurs dans d'autres pays.

INFORMATIONS GÉNÉRALES

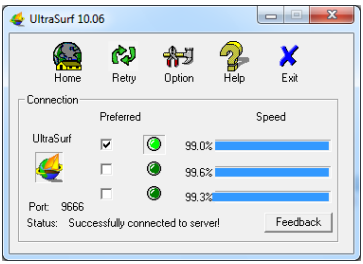
Système d'exploitation supporté	
Langues	Anglais
Site Web	http://www.ultrareach.com
Support	FAQ : http://www.ultrareach.com/usercenter_en.htm

OBTENIR ULTRASURF

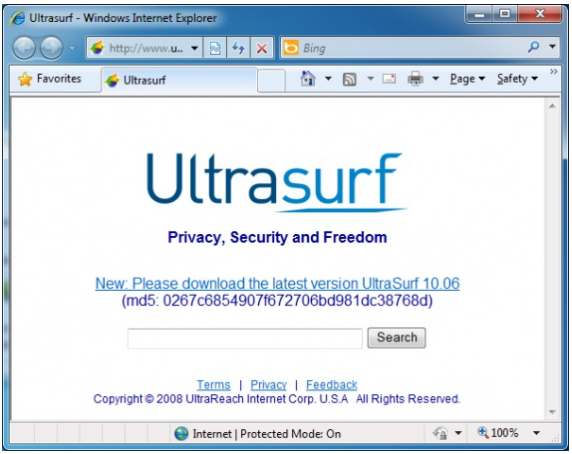
Vous pouvez télécharger gratuitement le logiciel, pour Windows uniquement, à cette adresse http://www.ultrareach.com ou sur http://www.ultrareach.net ou enfin sur http://www.wukie.net. La dernière page est en chinois, mais le téléchargement est facile à trouver et il est en anglais.

INSTALLATION ET UTILISATION D'ULTRASURF

Une fois téléchargé, le fichier « u1006.zip » (selon le numéro de la version), vous pouvez facilement l'extraire avec un clique-droit en sélectionnant « Extraire Tout ». Double-cliquez sur la nouvelle icone « u1006 » pour lancer l'application.



UltraSurf ouvrira automatiquement Internet Explorer et affichera la page de recherche http://www.ultrareach.com/search.htm. Vous pouvez maintenant commencer à naviguer grâce à l'instance d'Internet Explorer qu'a lancé UltraSurf.



Si vous souhaitez utiliser une autre application avec UltraSurf telle que le navigateur Firefox ou le client de messagerie instantanée Pidgin, vous devez alors les configurer pour utiliser le client UltraSurf comme un serveur proxy : l'IP est 127.0.0.1 (votre PC, aussi connu comme « localhost ») et le port 9666.

Vous pouvez ouvrir le Guide de l'utilisateur d'UltraSurf en cliquant sur « Aide » dans la fenêtre principale d'UltraSurf.

Infos sur l'UltraSurf chinois (wujie) :
http://www.internetfreedom.org/UltraSurf

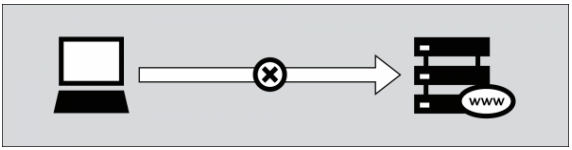
Guide de l'utilisateur chinois : http://www.wujie.net/userguide.htm

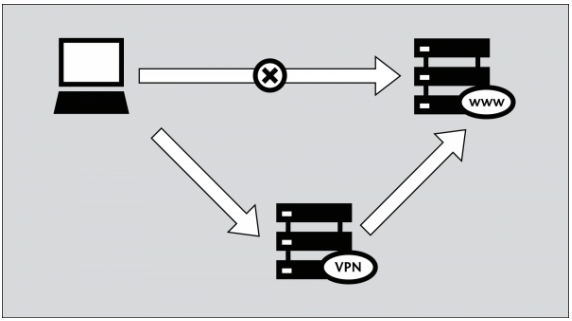
20. SERVICES VPN

Un VPN, comprenez un réseau virtuel privé, chiffre et encapsule tout trafic Internet entre vous et un autre ordinateur. Cet ordinateur peut appartenir à un service commercial de VPN, votre société, ou un contact de confiance.

Parce que les services VPN encapsulent tout trafic Internet, ils peuvent être utilisés pour envoyer un e-mail, de la messagerie instantanée, de voix sur IP (VoIP) et tout autre service Internet et de navigation Web, faisant que tout ce qui voyage à travers le tunnel soit illisible tout le long du chemin.

Si l'encapsulation se termine dans une zone où Internet est restreint, cela peut être une méthode efficace de contournement, vu que l'entité/serveur de filtrage ne voit que les données chiffrées, et n'a aucun moyen de savoir quelle donnée transite. Cela a également l'effet de rendre vos différents types de trafic imperméables aux yeux indiscrets.





Depuis que beaucoup d'entreprises internationales utilisent la technologie VPN pour permettre aux employés qui ont besoin d'accéder à des données financières sensibles ou d'autres informations depuis leur domicile ou à distance sur Internet, elle est moins susceptible d'être bloquée que les technologies utilisées uniquement pour des raisons de contournement.

Il est important de noter que la donnée est chiffrée jusqu'au bout du tunnel et qu'ensuite elle voyage jusqu'à sa destination finale de manière non-chiffrée. Si, par exemple, vous établissez un tunnel à un fournisseur VPN commercial, et qu'ensuite vous sollicitez la page Web http://news.bbc.co.uk à travers le tunnel, la donnée sera chiffrée depuis votre ordinateur jusqu'à l'ordinateur du fournisseur VPN, mais de là il sera non-chiffré jusqu'au serveur géré par la BBC, comme un trafic internet normal. Cela veut dire que le fournisseur VPN, la BBC et quiconque contrôle le système entre ces deux serveurs sera, en théorie, capable de voir quelle donnée vous avez envoyé ou demandé.

UTILISER UN SERVICE VPN

Un service VPN peut ou ne peut pas requérir d'installation logicielle côté client (beaucoup d'entre eux se basent sur le support existant dans Windows, Mac OS ou GNU/Linux et donc se passent de logiciel supplémentaire).

Utiliser un service VPN vous oblige à faire confiance aux propriétaires du service, mais cela vous fournit une méthode simple et pratique pour contourner le filtrage d'Internet, gratuitement ou moyennant une contribution mensuelle généralement comprise entre 5 et 10 dollars US en fonction du service. Les services gratuits sont souvent rétribués soit par la publicité soit par une limite de bande passante ou/et par un trafic maximum autorisé sur une période donnée.

Services VPN populaires :

- Hotspot Shield, https://hotspotshield.com
  Selon un rapport du Berkman Center datant de 2010, Hotspot Shield est incontestablement le service VPN le plus populaire. Pour plus de détails sur comment obtenir et utiliser Hotspot Shield, lisez le chapitre qui lui est consacré dans ce guide.
- UltraVPN : http://www.ultravpn.fr
- FreeVPN : http://www.thefreevpn.com
- CyberGhost : http://cyberghostvpn.com
- Air VPN : https://airvpn.org
  AirVPN offre des comptes gratuits sans restriction de bande passante, de trafic et sans publicité pour les militants par simple requête.
- Vpnod : http://www.vpnod.com
- VpnSteel : http://www.vpnsteel.com
- Loki Network Project : http://www.projectloki.com
- ItsHidden : http://itshidden.com

Les exemples de services VPN payants incluent Anonymizer, GhostSurf, XeroBank, HotSpotVPN, WiTopia, VPN Swiss, Steganos, Hamachi LogMeIn, Relakks, Skydur, iPig, iVPN.net, FindNot, Dold, UnblockVPN and SecureIX.

Une liste de fournisseurs VPN gratuits et payants, avec leur coût mensuel et leurs caractéristiques techniques est disponible à cette adresse http://en.cship.org/wiki/VPN.

VPN STANDARDS ET CRYPTAGE

Il y a de nombreuses normes différentes pour configurer des réseaux VPN, incluant IPSec, SSL/TLS et PPTP, qui varient en termes de complexité, de niveaux de sécurité fournis, et de systèmes d'exploitation sur lesquels ils sont disponibles. Il existe de nombreuses utilisations différentes de chaque norme logicielle qui possèdent diverses autres fonctionnalités.

- Alors que le PPTP est connu pour utiliser un chiffrage plus faible que IPSec ou SSL/TLS, il peut s'avérer utile pour contourner un blocage Internet, et le logiciel client est parfaitement intégré dans la plupart des versions de Microsoft Windows.
- Les systèmes VPN basé sur le SSL/TLS sont relativement faciles à configurer, et fournissent un niveau de sécurité solide.
- IPSec fonctionne au niveau d'Internet, responsable du transfert des paquets dans l'architecture Internet, tandis que les autres fonctionnent au niveau de l'application. Cela rend IPSec plus flexible, car il peut être utilisé pour protéger tous les hauts niveaux de protocoles mais est également difficile à configurer.

CONFIGURER VOTRE PROPRE SERVICE VPN

Comme alternative aux services VPN commerciaux payants, les utilisateurs ayant des contacts dans des zones non-restreintes peuvent leur demander de télécharger et d'installer des logiciels qui permettent de configurer un service VPN privé. Cela requiert un plus haut degré de connaissances techniques mais a l'avantage d'être gratuit et sans restriction. Le caractère personnel d'une telle configuration permet également qu'elle soit moins sujette au blocage qu'un service commercial disponible depuis longtemps. Un des programmes open source les plus utilisés disponible pour configurer ce genre de VPN privé est OpenVPN (http://openvpn.net), qui peut être installé sur Linux, MacOS, Windows et de nombreux autres systèmes d'exploitation.

Pour Comprendre comment configurer un système OpenVPN, lisez le chapitre qui lui est consacré dans ce guide.

AVANTAGES

Un VPN fournit un transfert chiffré de vos données, ce qui en fait un des moyens les plus sûrs de contourner la censure d'Internet. Une fois configuré, il est simple et transparent à l'usage.

Les VPN sont plus adaptés à des utilisateurs expérimentés qui ont besoin de moyens de contournement sécurisés plutôt que simplement du trafic web et qui ont accès à l'Internet depuis leur propre ordinateur sur lesquels ils peuvent installer des logiciels supplémentaires. Les VPN sont une excellent ressource pour les utilisateurs situés dans des lieux censurés qui n'ont pas de contacts de confiance dans des zones non-censurées. La technologie VPN est une application commerciale ordinaire qui n'est pas vraiment susceptible d'être bloquée.

INCOVÉNIENTS ET RISQUES

Certains VPN, principalement les gratuits, sont publics et peuvent être filtrés. Ils ne peuvent normalement pas être utilisés depuis un accès public sur lequel les utilisateurs ne peuvent pas installer de logiciels tels que dans les cybercafés ou les bibliothèques. L'utilisation d'un VPN nécessite un plus haut niveau technique que les autres méthodes de contournement.

Un opérateur réseau peut détecter si un VPN est utilisé et peut déterminer qui en est le fournisseur. L'opérateur réseau ne devrait pas être capable de voir les communications envoyées à travers le VPN à moins qu’il ne soit pas correctement configuré.

L'opérateur VPN, semblable à un opérateur proxy, peut voir ce que vous faites à moins d'utiliser des moyens de chiffrement supplémentaires dans vos communications, tels que HTTPS pour le trafic Web. Sans chiffrement supplémentaire, vous devez faire confiance à l'opérateur VPN de ne pas abuser de ses accès.

21. VPN SUR UBUNTU

Si vous utilisez Ubuntu comme système d'exploitation, vous pouvez vous connecter à un VPN en utilisant l'application NetworkManager et le client libre OpenVPN.

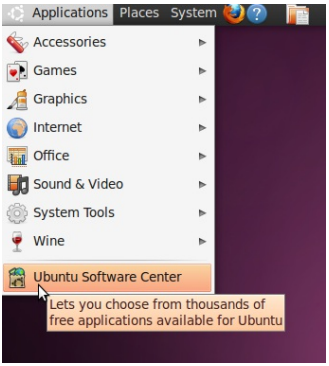
OpenVPN vous permet de vous connecter à des réseaux VPN utilisant diverses méthodes d'authentification. Pour notre exemple, nous allons apprendre comment se connecter à un serveur VPN en utilisant AirVPN, un service gratuit. La méthode de configuration pour OpenVPN sur Ubuntu est la même quelque soit le service VPN que vous utilisiez.

Installer OpenVPN pour NetworkManager

NetworkManager, un utilitaire vous permettant d'ouvrir ou de fermer votre connexion VPN, est inclus dans Ubuntu par défaut. Vous pouvez le trouver dans la zone de notification de votre écran, juste à côté de l'horloge.

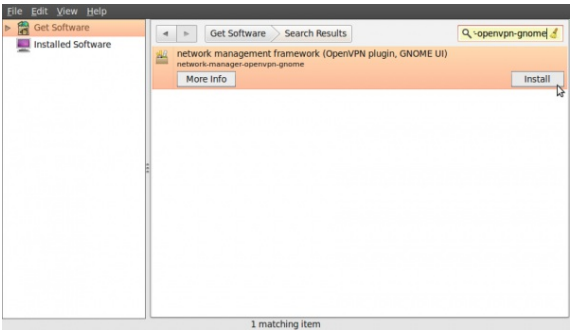
Ensuite, ajoutons une extension OpenVPN qui va travailler avec NetworkManager, en utilisant la Logithèque Ubuntu.

1. Ouvrez la Logithèque Ubuntu dans le menu Applications situé en haut à gauche de votre écran.

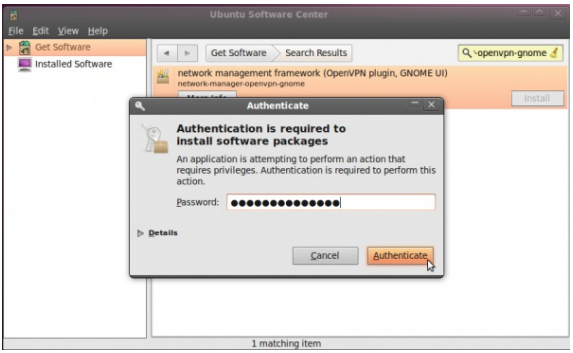


2. La Logithèque Ubuntu vous permet de chercher, installer et désinstaller des logiciels sur votre ordinateur. Cliquez sur la zone de recherche en haut à droite de la fenêtre.

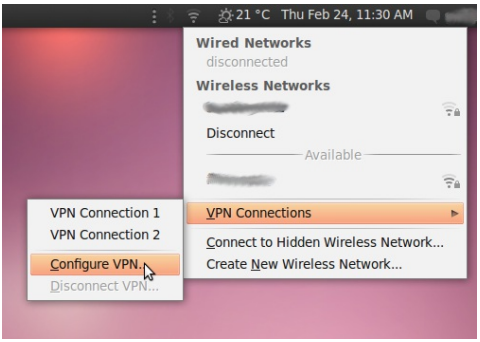
3. Dans la zone de recherche, tapez « network-manager-openvpn-gnome » (l'extension pour NetworkManager qui va activer OpenVPN). Ce paquet inclut tous les fichiers dont vous avez besoin pour établir une connexion VPN, y compris le client OpenVPN. Cliquez sur installer.



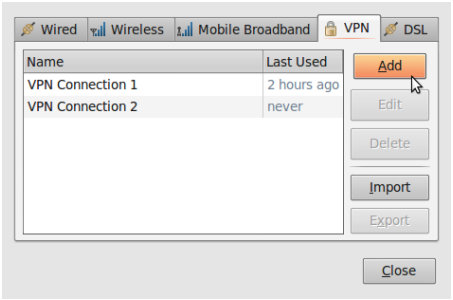
4. Il est possible qu'Ubuntu vous demande des droits supplémentaires pour installer le logiciel. Dans ce cas, tapez votre mot de passe et cliquez sur « S'authentifier ». Une fois que le paquet est installé, vous pouvez fermer la fenêtre de la Logithèque.



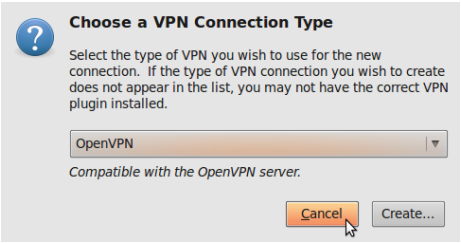
5. Pour vérifier que le client OpenVPN est correctement installé, cliquez sur l'icône du Gestionnaire de Réseau à gauche de l'horloge du système et sélectionnez « Connexion VPN > Configurer un VPN ».



6. Cliquez sur « Ajouter » sous l'onglet VPN.



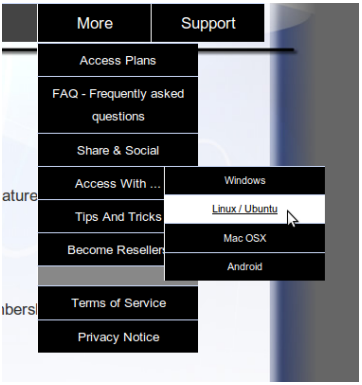
7. Si vous voyez une option OpenVPN, vous avez correctement installé le client OpenVPN dans Ubuntu. Cliquez sur « Annuler » et fermez le Gestionnaire de Réseau.



Obtenir un compte AirVPN

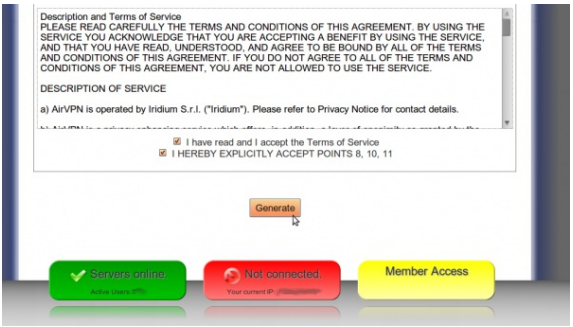
AirVPN, http://www.airvpn.org, est un service gratuit mais vous devrez vous enregistrer sur leur site web pour télécharger les fichiers de configuration pour votre connexion VPN.

1. Allez sur https://airvpn.org/?option=com_user&view=register et créez un compte gratuit. Assurez-vous d'avoir un mot de passe solide, vu que ce sera le mot de passe pour votre accès VPN. Pour des indications sur les mots de passe solides, lisez le chapitre « Menaces et assomption de menaces » dans ce livre.
2. Sur le site d'AirVPN, dans le menu de navigation, sélectionnez « More > Acces with... > Linux/Ubuntu ».

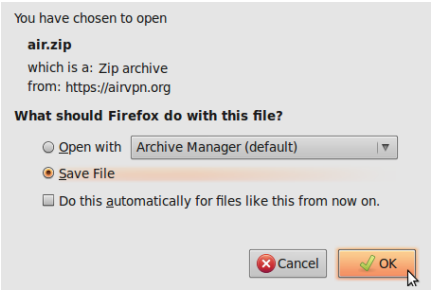


3. Cliquez sur « Access without our client ». On vous demandera le même mot de passe et nom d'utilisateur que ceux que vous avez utilisé pour vous enregistrer.

4. Sélectionnez le mode VPN que vous souhaitez configurer dans NetworkManager, dans notre exemple nous utilisons « Free - TCP – 53, » et laissez le reste des options telles quelles. Assurez-vous que vous avez bien validé les Conditions d'utilisation en bas de la page, et cliquez sur « Generate ».



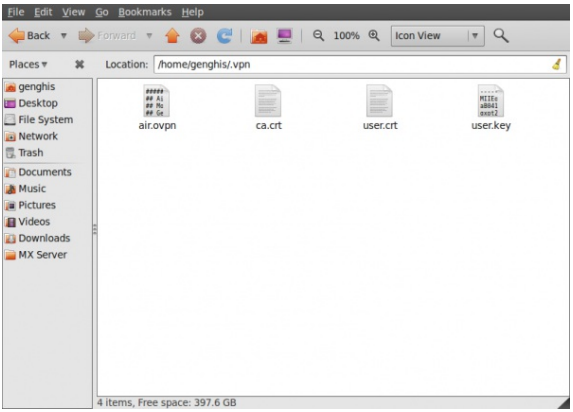
5. Une fenêtre de pop-up vous préviendra que le fichier air.zip est prêt au téléchargement. Il contient les fichiers de configuration et certificats dont vous aurez besoin pour vous connecter au VPN. Cliquez sur « OK ».



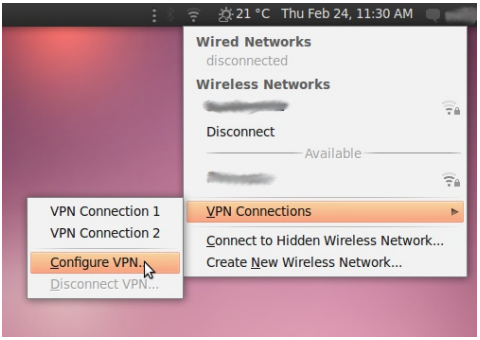
Configurer AirVPN dans NetworkManager

Vous pouvez maintenant configurer NetworkManager pour vous connecter au service AirVPN.

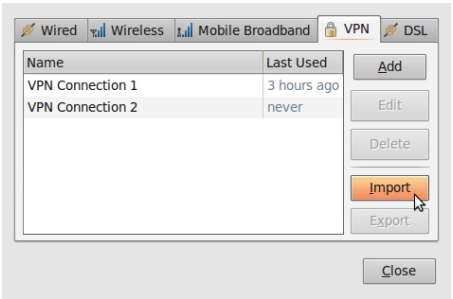
1. Décompressez le fichier que vous avez téléchargé dans un dossier de votre disque dur, par exemple : /home/nomutilisateur/.vpn. Vous devriez avoir 4 fichiers. Le fichier « air.ovpn » est le fichier de configuration que vous devez importer dans NetworkManager.



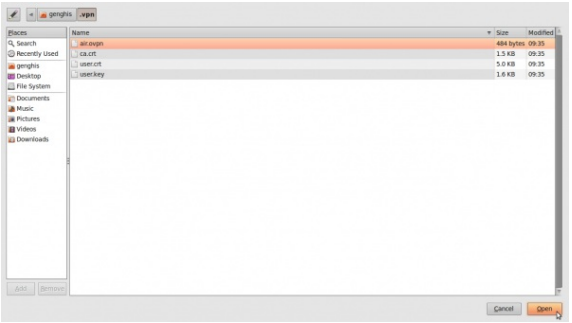
2. Pour importer le fichier de configuration, ouvrez NetworkManager et allez dans « Connexions VPN > Configurer le VPN ».



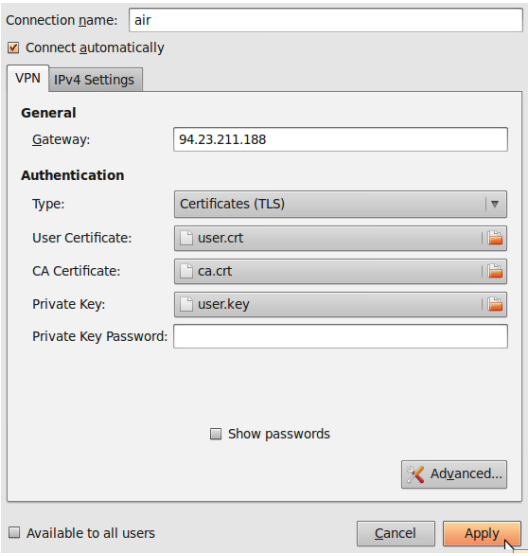
3. Dans l'onglet VPN, cliquez sur « Importer ».



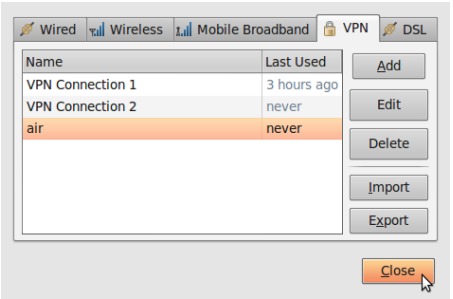
4. Trouvez le fichier air.ovpn que vous venez de décompresser. Cliquez sur « Ouvrir ».



5. Une nouvelle fenêtre va s'ouvrir, ne touchez à rien et cliquez sur « Appliquer ».



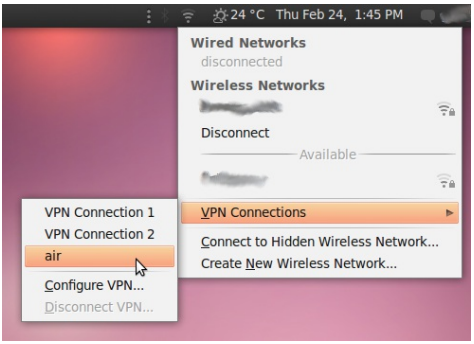
6. Félicitations ! Votre connexion VPN est prête à être utilisée et devrais apparaître dans la liste des connexions de l'onglet VPN. Vous pouvez maintenant fermer NetworkManager.



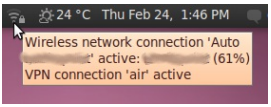
Utiliser votre nouvelle connexion VPN

Maintenant que vous avez configuré NetworkManager pour qu'il se connecte à un service VPN en utilisant le client OpenVPN, vous pouvez utiliser votre connexion pour contourner la censure. Suivez ces étapes :

1. Dans le menu NetworkManager, sélectionnez votre nouvelle connexion dans « Connexions VPN ».

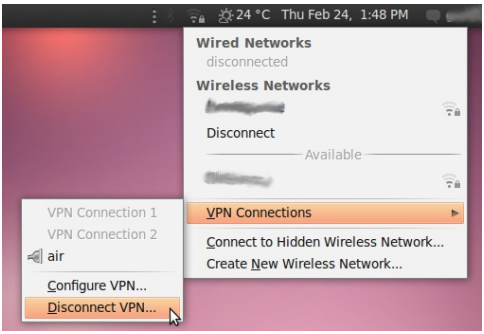


2. Attendez que la connexion VPN s'établisse. Une fois connecté, un petit cadenas devrait apparaître juste en dessous de votre icône NetworkManager, ce qui indique que vous utilisez une connexion sécurisée. Déplacez votre curseur sur l'icône pour confirmer que la connexion est active.



3. Vous pouvez tester le statut de votre connexion en visitant http://www.ipchicken.com. Ce testeur d'IP gratuit devrait confirmer que vous utilisez un serveur airvpn.org.

4. Pour vous déconnecter de votre VPN, sélectionnez « Connexions VPN > Déconnecter le VPN » dans le menu NetworkManager. Vous utilisez maintenant une connexion normale (filtrée) à nouveau.


24 °C Thu Feb 24, 1:48 PM
Wired Networks
disconnected
Wireless Networks
Disconnect
Available
VPN Connections
Connect to Hidden Wireless Network...
Create New Wireless Network...
VPN Connection 1
VPN Connection 2
air
Configure VPN...
Disconnect VPN...

22. HOTSPOT SHIELD

Hotspot Shield est une solution VPN gratuite, mais commerciale, tournant sous Microsoft Windows et Mac OS et qui permet d'accéder à Internet en évitant la censure grâce à un tunnel sécurisé : Elle utilise votre connexion à Internet habituelle, même si elle est censurée.
Puisque Hotspot Shield chiffre toutes vos communications, les logiciels de surveillance utilisés par les censeurs ne peuvent pas voir les sites que vous visitez.

INFORMATIONS GÉNÉRALES

Système d'exploitation supporté	
Langues	Anglais
Site Web	https://www.hotspotshield.com
Support	FAQ : https://www.anchorfree.com/support/hotspot-shield.html E-mail : support@anchorfree.com

OBTENIR HOTSPOT SHIELD

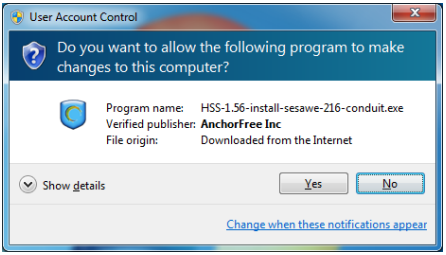
Téléchargez le logiciel sur https://www.hotspotshield.com. Le fichier fait environ 6Mo, le téléchargement peut donc durer 25 minutes ou plus sur une connexion bas-débit. S'il est interdit depuis votre connexion, envoyez un e-mail à hss-sesawe@anchorfree.com avec un des mots suivants dans le sujet de votre message : « hss », « sesawe », « hotspot » ou « shield ». Vous recevrez dans votre boîte de réception le fichier d'installation en pièce jointe.

Attention, si vous utilisez l'extension Firefox NoScript et qu'elle est activée, vous rencontrerez des problèmes lors de l'utilisation de Hotspot Shield. Chaque adresse utilisée par Hotspot Shield dit être inscrite dans la liste blanche ou autorisez les scripts globalement quand vous utilisez Hotspot Shield.

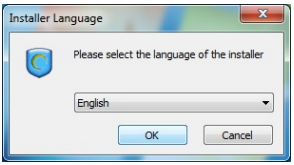
Installer Hostpot Shield

1. Une fois le téléchargement réussi, cherchez le fichier téléchargé sur votre ordinateur et lancez l'installation en double cliquant l'icône.

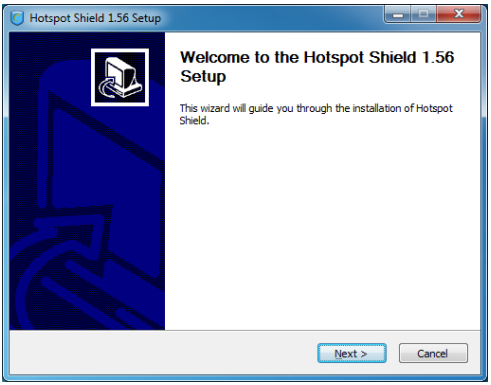
2. Windows peut vous demander l'autorisation d'installer le logiciel. Choisissez « Oui ».



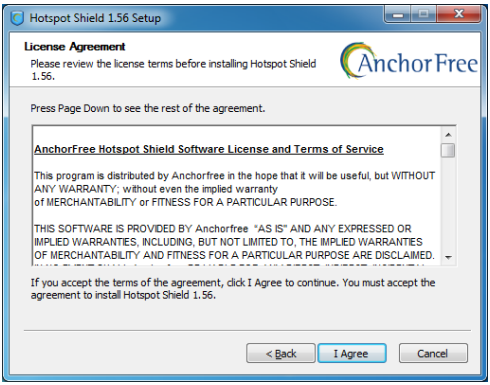
3. Sélectionnez la langue d'installation depuis le menu déroulant.



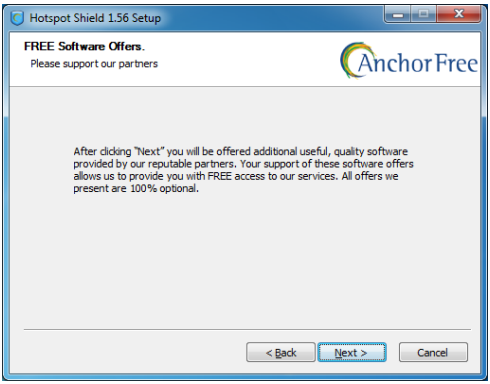
4. Après avoir sélectionné la langue, vous verrez un écran de bienvenue. Cliquez sur « Suivant ».



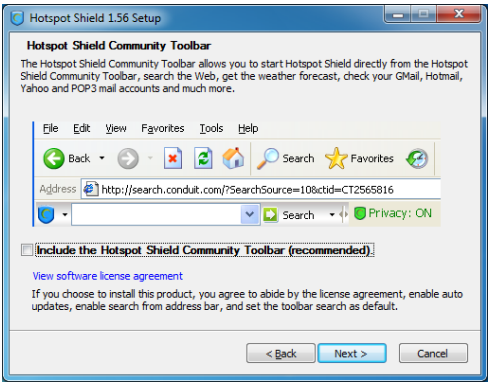
5. Acceptez les termes de la licence en cliquant sur « J'accepte ».



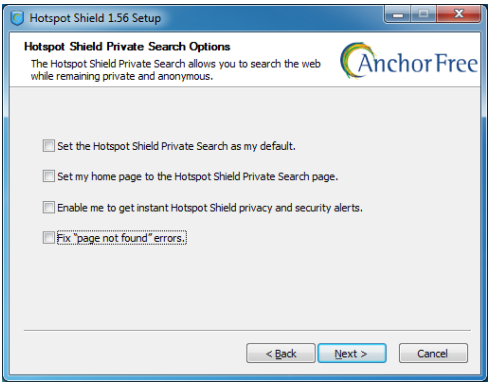
6. Vous verrez une liste de logiciels optionnels que vous pouvez installer. Cliquez sur « Suivant ».



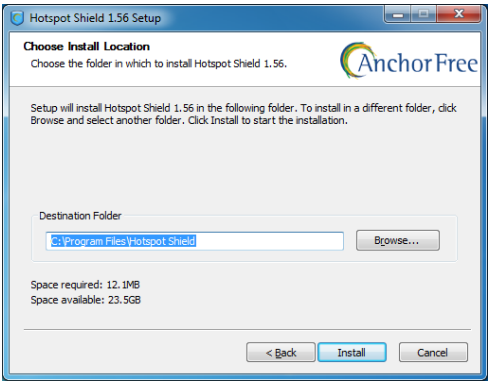
7. Sur l'écran qui suit, vous pouvez décocher la case vous proposant l'installation de la barre d'outils communautaire Hotspot Shield. Cette option n'est pas nécessaire à son bon fonctionnement.



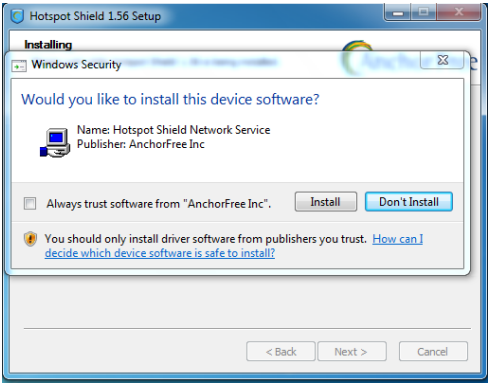
8. D'autres options vous seront proposées sur l'écran suivant. Elles sont facultatives et n'ont pas besoin d'être installées pour utiliser Hotspot Shield.



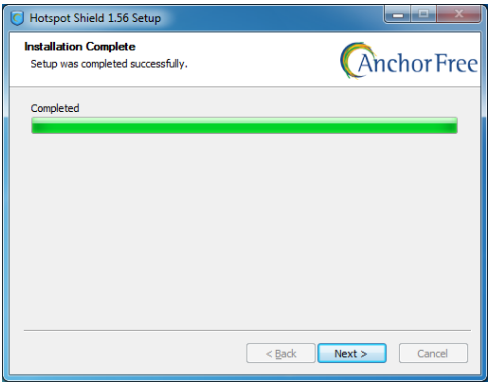
9. Sélectionnez le répertoire du disque dur dans lequel vous souhaitez installer Hotspot Shield.



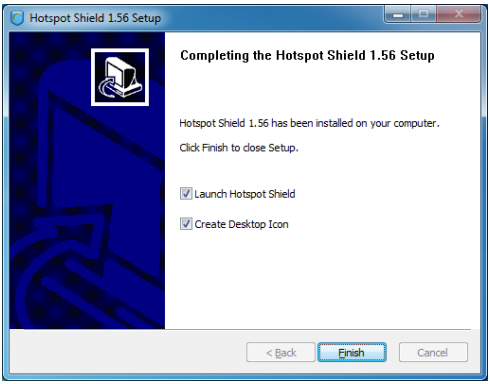
10. Windows peut vous demander des autorisations lors de l'installation des différents composants de Hotspot Shield. Vous pouvez, en toute sérénité, cliquer sur « Installer » à chaque fois.



11. Quand l'installation est terminée, cliquez sur « Suivant ».



12. Vous pouvez lancer Hotspot Shield immédiatement, l'installation terminée et créer une icône sur votre bureau. Adaptez les préférences puis cliquez sur « Terminer ».

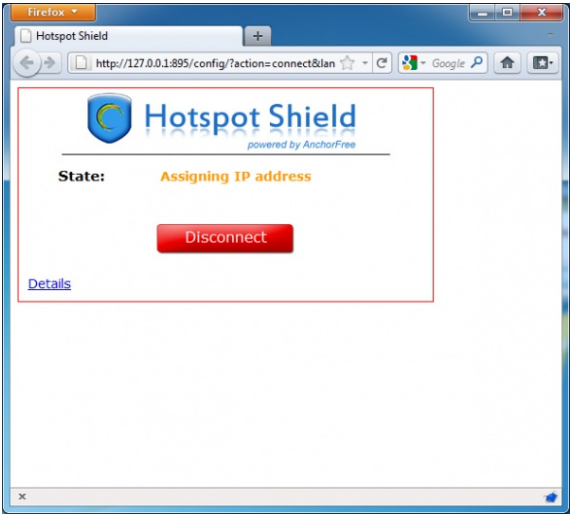


Hotspot Shield est maintenant installé sur votre ordinateur.

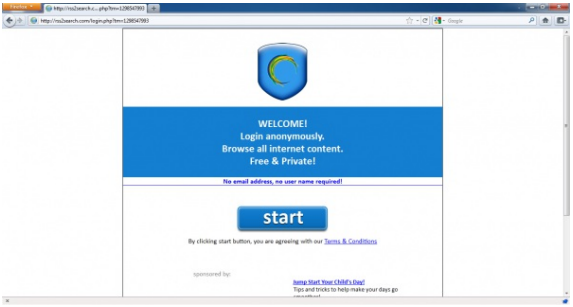
Se connecter au service Hotspot Shield

1. Cliquez sur l'icône de Hotspot Shield sur votre bureau ou depuis le menu « Programmes > Hotspot Shield ».

   PNG - 2.3 kb
2. Une fois que vous avez lancé Hotspot Shield, une fenêtre de navigateur Web s'ouvre sur une page récapitulant l'état de toutes les étapes nécessaires pour la connexion au service comme « Authentification » et « Assignation d'adresse IP ».

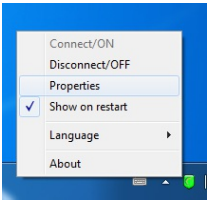


3. Une fois connecté, Hotspot Shield vous redirigera vers une page d'accueil. Cliquez sur « Démarrer » pour commencer à naviguer.



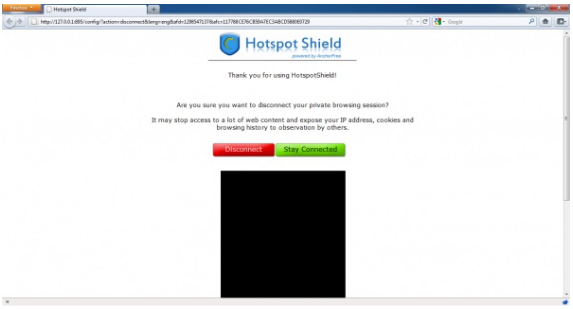
4. Remarque: après avoir cliqué sur « Démarrer », Hotspot Shield doit vous rediriger vers une page de publicité comme celle présente ci-dessous. Vous pouvez fermer cet onglet et commencer à naviguer comme d'habitude. Vous pouvez vérifier que vous êtes bien connecté au service Hotspot Shield en regardant l'icône verte de Hotspot Shield dans la barre des tâches (à côté de l'horloge).

5. Pour vérifier l'état de votre connexion, faites un clic droit sur l'icône de Hotspot Shield dans la barre des tâches et choisissez « Propriétés ».

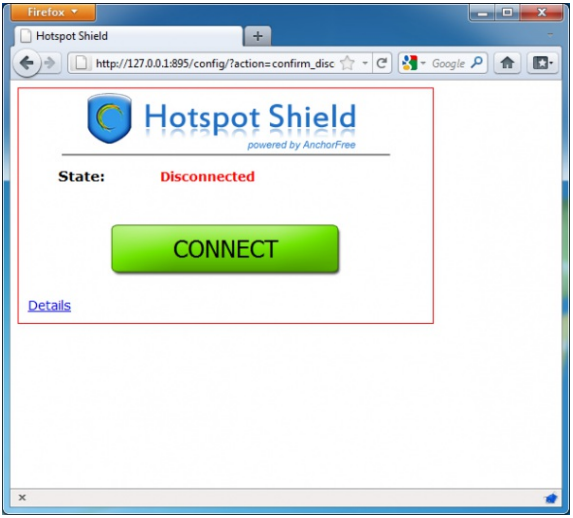


Se déconnecter du service Hotspot Shield

1. Pour vous déconnecter du service, effectuez un clic droit l'icône de Hotspot Shield dans la barre des tâches (voir l'image ci-dessous) et choisissez « Se déconnecter/OFF ».
2. Hotspot vous demandera de confirmer votre demande de déconnexion. Cliquez sur « Se déconnecter ».



3. Une fenêtre d'état doit apparaître et vous confirmer que vous êtes bien déconnecté et donc que vous naviguez sur votre connexion habituelle (celle qui est filtrée). Cliquez sur « Se connecter » pour contourner la censure à nouveau.



23. ALKASIR

Alkasir est un outil client/serveur innovant qui facilite l'analyse, le traçage, et le contournement du filtrage de sites web. Principalement utilisé au Moyen-Orient, Il peut être utilisé ailleurs.

Alkasir utilise un logiciel client dédié utilisant des serveurs proxy. Sa fonctionnalité innovante est de conserver une liste des sites bloqués à jour en récupérant des mises à jour semi-automatiques. Il permet de reporter de nouveaux sites bloqués à travers la communauté d'utilisateurs.

INFORMATIONS GÉNÉRALES

Systèmes d'exploitation supportés	
Langues	Anglais et Arabe
Site Web	https://alkasir.com
Support	Aide https://alkasir.com/help FAQ : https://alkasir.com/faq Contact : https://alkasir.com/contact

COMMENT FONCTIONNE ALKASIR ?

Alkasir a implémenté deux fonctionnalités innovantes et complémentaires. Il est conçu comme un navigateur web (basé sur mozilla firefox) avec un proxy HTTP intégré préconfiguré et une liste intelligente d'adresses bloquées.

CONTOURNER LA CENSURE D'INTERNET

L'innovation d'Alkasir est qu'il se base sur sa liste d'adresses bloquées et son proxy intégré pour atteindre ces adresses bloquées. On accède aux adresses non bloquées directement, sans passer par le proxy. Utiliser le proxy HTTP uniquement quand il est nécessaire permet d'optimiser l'utilisation de la bande passante et d'accéder aux pages non bloquées plus rapidement (vu que les pages auxquelles on accède directement se chargent plus vite).

GARDER LA LISTE D'ADRESSES BLOQUÉES À JOUR

À chaque fois qu'un utilisateur suspecte qu'une adresse est bloquée, il peut le reporter dans l'interface du logiciel. Alkasir vérifie le rapport, puis demande à la personne gérant le pays (un être humain) d'autoriser l'ajout à la base pour conserver la liste à jour et éviter le contenu indésirable d'y entrer, comme la pornographie.

Un seul « contenu bloqué » (un site web bloqué dans un certain pays) dépend souvent de plus d'une adresse. Quand Alkasir détecte une adresse bloquée dans un certain pays, il vérifie lesquelles des adresses référencées sur la page sont également bloquées. De cette façon, Alkasir construit sa liste de contenus bloqués à travers une méthode d'aspiration de site à un niveau.

Enfin, si un utilisateur d'Alkasir n'arrive pas à charger une adresse avec une requête directe (i.e. pas à travers le proxy), le client le remarque et vérifie si l'adresse est nouvelle (pas déjà dans la liste). Si elle l'est, il l'ajoute automatiquement.

La liste des sites bloqués est disponible à cette adresse : https://alkasir.com/map.

Pour résumer, la liste de sites bloqués d'Alkasir est enrichie en permanence par tous ses utilisateurs, via des rapports humains ou automatiques, et le navigateur s'appuie là-dessus pour optimiser la réactivité globale en redirigeant seulement les adresses bloquées dans le proxy.

OBTENIR ALKASIR

Vous pouvez télécharger Alkasir directement depuis le site web, ou le recevoir via e-mail.

TÉLÉCHARGER ALKASIR DEPUIS LE SITE WEB

Vous pouvez télécharger Alkasir depuis le site officiel : https://alkasir.com.

En fonction de votre système d'exploitation et des programmes que vous avez, vous pouvez choisir une des versions suivantes :

- Si vous avez Windows Vista ou Windows 7 et avez firefox, vous avez seulement besoin du « Alkasir installation package » qui requiert 3 Mo d'espace libre.
- Si ce n'est pas le cas, vous devez télécharger « Alkasir complete installation package » qui requiert 41.04 Mo.
  Si vous ne pouvez pas ou voulez pas installer Alkasir de manière permanente sur l'ordinateur que vous utilisez, par exemple dans un cybercafé ou une bibliothèque, vous pouvez télécharger une des deux versions USB :
- Alkasir USB sans Mozilla : sans installation, portable, mais nécessite mozilla firefox, 4 Mo.
- Alkasir USB avec le navigateur Mozilla : pas d'installation, portable, 12 Mo.

Notez que les deux versions ont besoin du framework .Net installé, ce qui est le cas de base sur Windows vista et Windows 7.
Vous pouvez également créer un compte pour recevoir régulièrement des mises à jour et des informations d'Alkasir par e-mail. Elles sortent régulièrement, donc assurez-vous d'avoir la dernière version depuis le site web.

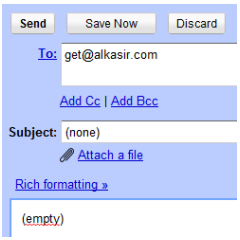
RECEVOIR ALKASIR PAR E-MAIL

Si le site d'Alkasir est bloqué dans votre pays, vous pouvez obtenir le fichier d'installation via un email automatique. Envoyez juste un email vide à l'adresse get@alkasir.com pour demander le fichier d'installation en pièce jointe.
{image}
Vous recevrez un e-mail avec le logiciel joint et des instructions sur comment installer alkasir sur votre ordinateur.

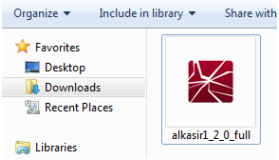
Si vous ne recevez pas le logiciel après quelques minutes, il se peut que vous ayez à ajouter get@alkasir.com à votre liste blanche pour que l'email ne soit pas considéré comme du spam.

INSTALLATION ALKASIR

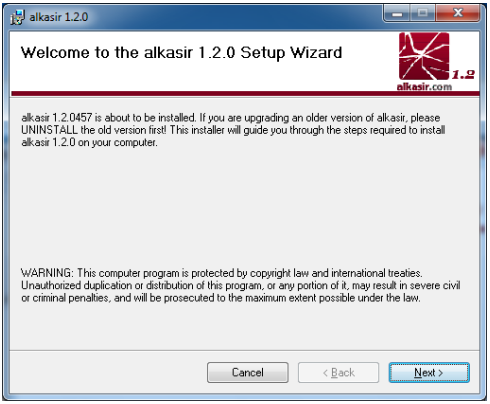
Une fois que vous avez téléchargé le fichier d'installation, double-cliquez sur l'icône.



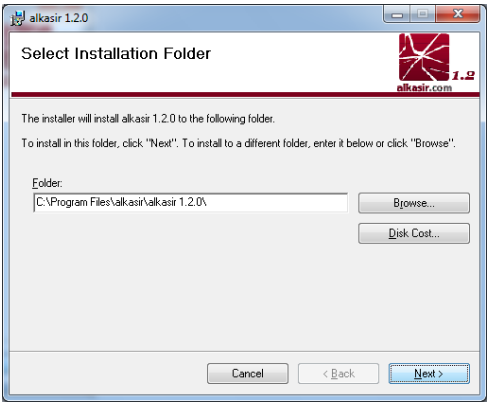
Vous aurez peut-être un avertissement de sécurité. Cliquez sur « Lancer » ou « Accepter ».



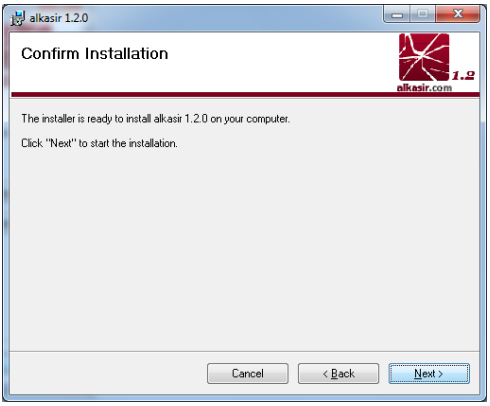
Suivez l'assistant d'installation en cliquant sur le bouton « Suivant ».



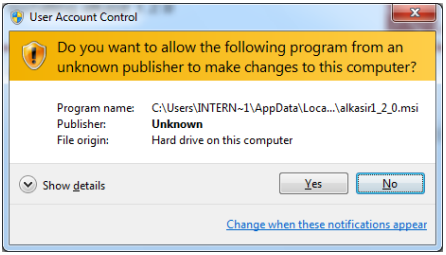
Vous pouvez le dossier d'installation (mais ce n'est pas recommandé).



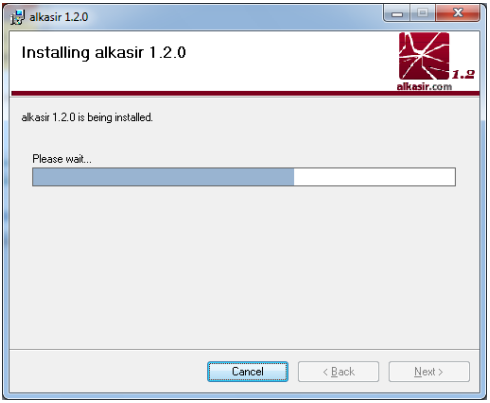
Quand vous êtes prêt, cliquez sur « Suivant ».

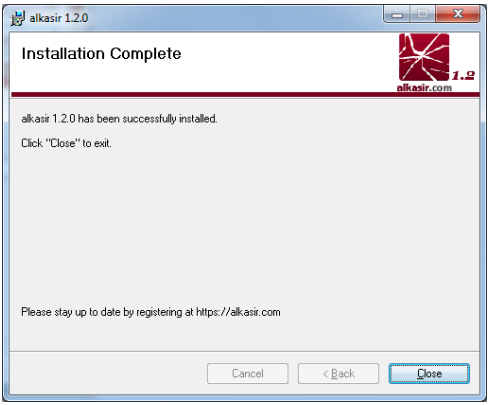


Confirmez l'avertissement de sécurité affiché au-dessus en cliquant « Oui ».



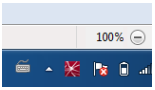
Quand l'installation est finie, cliquez sur « Fermer ».



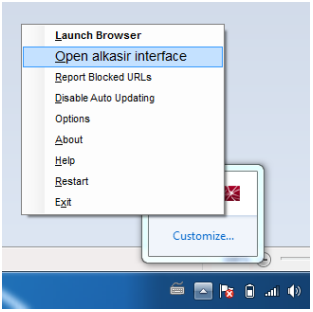


UTILISER ALKASIR

Alkasir devrait se lancer automatiquement dès que Windows se lance. Assurez-vous que le logiciel est bien lancé en vérifiant que l'icône Alkasir est affichée dans votre barre des tâches, à côté de l'horloge.



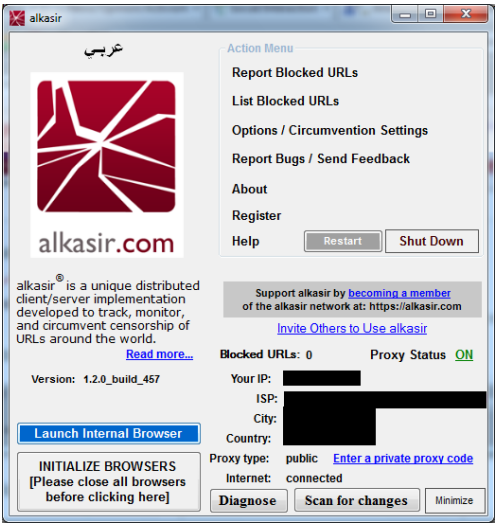
Un clic droit sur l'icône affiche le menu de configuration.



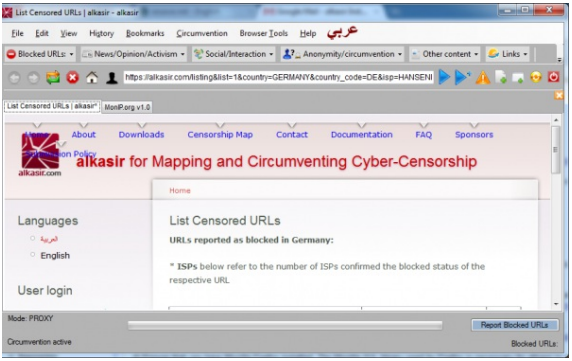
- Lancer le navigateur
- Ouvrir l'interface d'alkasir
- Signaler une adresse bloquée

L'interface principale d'alkasir rassemble toutes les fonctionnalités du logiciel. Vous pouvez effectuer les actions suivantes :

- Lancer, arrêter, et relancer le logiciel
- Lancer le navigateur Alkasir
- S'enregistrer ou se connecter sur http://alkasir.com
- Obtenir des mises à jour pour votre version d'alkasir



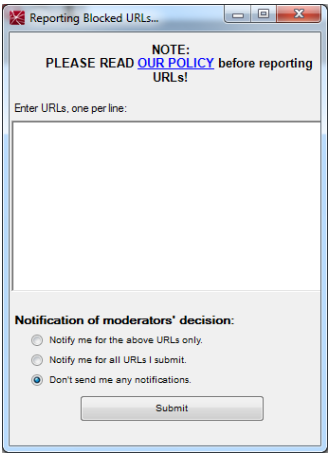
Pour commencer, lancez le navigateur alkasir.



L'interface graphique du navigateur est très similaire à celle de Mozilla Firefox, vu qu'elle utilise la même base. Notez les fonctionnalités spécifiques :

- Un bouton pour avoir une traduction arabe complète
- Un bouton « report blocked url », à utiliser quand vous essayez d'aller sur un site qui a l'air d'être bloqué. Ce bouton est affiché à côté de la barre d'adresse et de la barre de statut.
- Une icône Alkasir pour aller à l'interface principale.

Vous pouvez aussi trouver d'autres menus pour intégrer votre navigateur alkasir avec votre compte.
Il est possible d'activer ou désactiver les mises à jour automatiques pour le logiciel, la liste des proxys, et la liste des sites bloqués.
Si vous arrivez à une page d'erreur qui pourrait révéler un site bloqué (comme un Acces Denied ou connexion Timeout Error), vous pouvez envoyer cette adresse à la liste d'alkasir en cliquant sur le bouton « Report Blocked URL ». Vous pouvez choisir d'être informé de la décision du modérateur sur l'entrée de cette adresse dans la liste (cette décision est basée sur la politique d'alkasir).



PLUS D'INFORMATIONS

Visitez https://alkasir.com pour :

- Une documentation plus fournie sur le logiciel : https://alkasir.com/help
- Une liste des questions les plus fréquemment posées (FAQ) : https://alkasir.com/faq

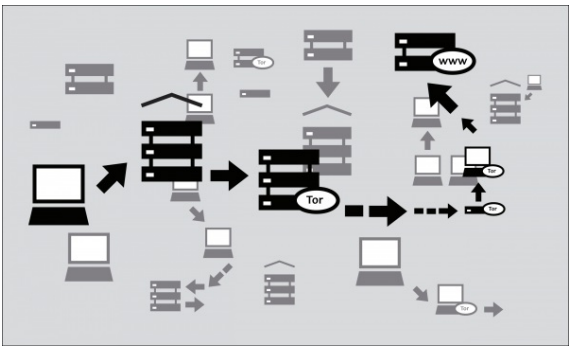
24. TOR : LE ROUTAGE EN OIGNON

Tor (le Routage en oignon) est un réseau très perfectionné de serveurs proxys.

INFORMATIONS GÉNÉRALES

Système d'exploitation supporté	
Langues	13 langues
Site Web	https://www.torproject.org
Support	Liste de diffusion : https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-talk/td>

Quand vous utilisez Tor pour accéder à un site web, vos communications sont acheminées de façon aléatoire, via un réseau de proxys indépendants et bénévoles. Tout le trafic entre les serveurs Tor (ou relais) est crypté, et chacun des relais ne connaît que l'adresse IP de deux autres – celui qui le précède immédiatement et celui qui le suit immédiatement dans la chaîne.



Ceci a pour but d'empêcher d'établir tout lien. Tor rend la tâche très difficile dans les cas suivants :

- que votre fournisseur d'accès ou tout autre observateur local sache à quel site web vous voulez accéder ou quelle information vous envoyez.
- que le site web connaisse votre identité (du moins votre adresse IP).
- qu'un quelconque des relais indépendants connaisse votre identité, puisse vous localiser ou savoir où vous allez, que ce soit directement en ayant votre adresse IP ou en arrivant à déduire ces informations à partir de vos habitudes de navigation grâce à une observation régulière de votre trafic.

DE QUOI AI-JE BESOIN POUR UTILISER LE RÉSEAU TOR ?

Pour se connecter à l'Internet par le réseau Tor, et l'utiliser pour préserver son anonymat, la confidentialité de sa vie privée et contourner la censure, vous devez installer sur votre ordinateur le logiciel client Tor. Il est également possible d'exécuter une version portable du programme à partir d'une clé USB ou tout autre périphérique externe.

Tor est compatible avec la plupart des versions de Windows, Mac OS X et GNU/Linux.

AVEC QUELS LOGICIELS EST-IL COMPATIBLE ?

Tor utilise une interface proxy SOCKS pour se connecter aux applications, donc toute application compatible avec SOCKS (versions 4, 4a et 5) peut voir son trafic rendu anonyme grâce à Tor, notamment :

- la plupart des navigateurs Web.
- de nombreux clients de messagerie instantanée et de réseaux IRC.
- des clients SSH.
- des clients emails.

Si vous avez installé Tor à partir de Vidalia Bundle, Tor Browser Bundle ou Tor IM Browser Bundle, Tor aura également configuré une application proxy HTTP comme frontal pour le réseau Tor. Ceci permettra à d'autres applications non compatibles avec SOCKS de fonctionner avec Tor.

Si Tor vous intéresse principalement pour surfer sur le Web et chatter, vous trouverez plus facile d'utiliser Tor Browser Bundle ou Tor IM Browser qui vous proposeront des solutions préconfigurées et prêtes à l'emploi. Tor Browser Bundle comprend également un Torbutton, qui améliore la protection de la vie privée quand on utilise Tor avec un navigateur Web. Les deux versions de Tor sont téléchargeables à partir de https://www.torproject.org/projects/torbrowser.

AVANTAGES ET RISQUES

Tor peut s'avérer un outil très efficace pour le contournement de la censure et la protection de votre identité. Le cryptage avec Tor dissimule le contenu de vos communications au regard de votre opérateur local de réseau, l'empêche de voir avec qui vous communiquez et quels sites Web vous regardez. S'il est utilisé correctement, il offre une protection de l'anonymat largement supérieure à celle d'un proxy unique.

Toutefois :

- Tor est vulnérable au blocage. La plupart des nœuds de Tor figurent dans un annuaire public ; il est donc facile pour des opérateurs de réseau d'avoir accès à cette liste et d'ajouter les adresses IP de ces nœuds à un filtre. (Une façon de tenter d'éviter ce type de blocage est d'utiliser l'un des divers ponts Tor, ce sont les nœuds d'entrée de Tor qui ne sont pas affichés publiquement, précisément pour éviter le blocage).
- Certains programmes que vous pourriez utiliser avec Tor posent des problèmes et peuvent donc compromettre l'anonymat. Tor Browser Bundle inclut une version de Firefox où Torbutton est installé. Torbutton désactive certains plugins et modifie l'empreinte de votre navigateur de façon à ce qu'elle ressemble à n'importe quel utilisateur de Torbutton. Tor ne vous protégera pas si vous ne configurez pas vos applications pour qu'elles passent par Tor. Certains plugins et scripts ne tiennent pas compte des paramètres du proxy local et peuvent dévoiler votre adresse IP.
- Si vous n'utilisez pas de cryptage supplémentaire pour protéger vos communications, vos données seront décryptées en arrivant au dernier nœud de Tor de la chaîne (appelé nœud de sortie). Autrement dit, vos données seront potentiellement visibles par le propriétaire du dernier nœud Tor ou le FAI entre ce nœud et le site web que vous voulez consulter.

Les développeurs de Tor ont beaucoup réfléchi à ces risques et d'autres et avertissent l'utilisateur sur trois points :

1. Tor ne vous protège pas si vous ne l'utilisez pas correctement. Vous pourrez lire la liste des avertissements ici : https://www.torproject.org/download/download.html.en#warning; suivez ensuite soigneusement les instructions de votre plateforme : https://www.torproject.org/documentation.html.en#RunningTo
2. Même si vous configurez et utilisez Tor correctement, des attaques potentielles demeurent, qui pourraient compromettre la capacité de Tor à vous protéger : https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#Whatattacksremainagainstonionrouting
3. Aucun système d'anonymat n'est parfait dans l'état actuel des choses, et Tor ne fait pas exception à la règle : vous ne pouvez compter uniquement sur le réseau Tor actuel si vous souhaitez bénéficier d'un anonymat sans faille.

UTILISER LE PACK DE NAVIGATION TOR (TOR BROWSER BUNDLE)

Avec le Tor Browser Bundle, vous pouvez utiliser Tor sous Windows, OS X ou GNU/Linux sans avoir besoin de configurer un navigateur Web. Mieux encore, c'est également une application portable qui peut être exécutée à partir d'une clé USB, ce qui vous permet de le transporter vers n'importe quel ordinateur sans avoir besoin de l'installer sur le disque dur de cet ordinateur.

TÉLÉCHARGEMENT DU PACK DE NAVIGATION

Le Tor Browser Bundle est téléchargeable à partir du site Web torproject.org, en un seul fichier ou bien en version « split » composée de plusieurs fichiers. Si votre connexion Internet est lente et peu fiable, la version split aura de meilleures chances de fonctionner que le téléchargement d'un unique très gros fichier.

Si le site Web torproject.org est filtré là où vous vous trouvez, saisissez les mots clés "tor mirrors" dans votre moteur de recherche favori ; les résultats de votre requête comprendront probablement d'autres adresses à partir desquelles télécharger le Tor Browser Bundle.

Obtenir Tor par email : adresser un email à gettor@torproject.org en mettant "help" dans le corps du message, et vous recevrez des instructions sur la manière dont le robot autorépondeur peut vous envoyer le logiciel Tor.

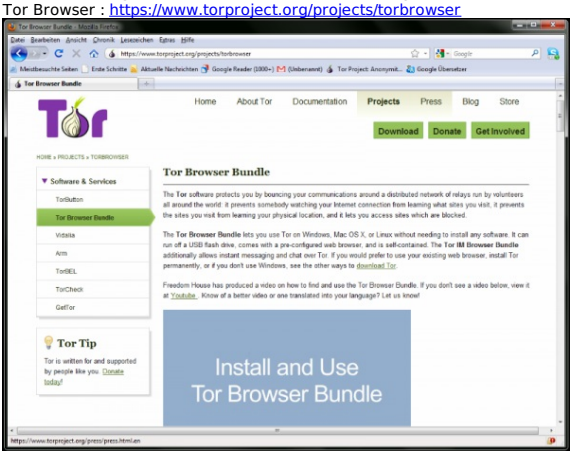
Attention : Lorsque vous téléchargez le Tor Browser Bundle (version classique ou version split), vérifiez les signatures des fichiers, surtout si vous téléchargez des fichiers à partir d'un site miroir. Cette mesure permet de vérifier que les fichiers n'ont pas été altérés. Pour en savoir plus sur les fichiers signatures et la manière de les vérifier, lire https://www.torproject.org/docs/verifying-signature.

Vous pouvez télécharger le logiciel GnuPG nécessaire pour vérifier la signature ici : http://www.gnupg.org/download/index.en.html#auto-ref-2.

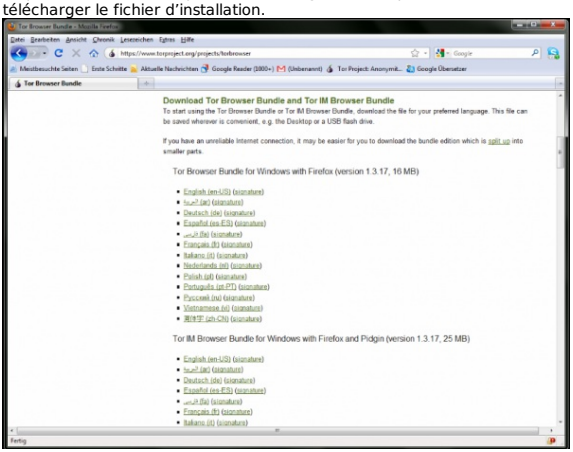
Les instructions ci-dessous correspondent à l'installation de Tor Browser sur Microsoft Windows. Si vous utilisez un système d'exploitation différent, recherchez sur le site Web de Tor les liens et instruction pour le téléchargement.

Installation à partir d'un fichier unique

1. Dans votre navigateur Web, entrez l'URL de téléchargement de Tor Browser : https://www.torproject.org/projects/torbrowser

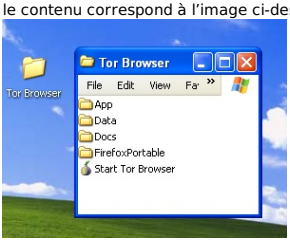


2. Cliquer sur le lien correspondant à la langue choisie pour télécharger le fichier d'installation.



3. Double-cliquez sur le fichier .exe que vous avez téléchargé. Une fenêtre « fichier autoextractible 7-zip » apparaîtra.

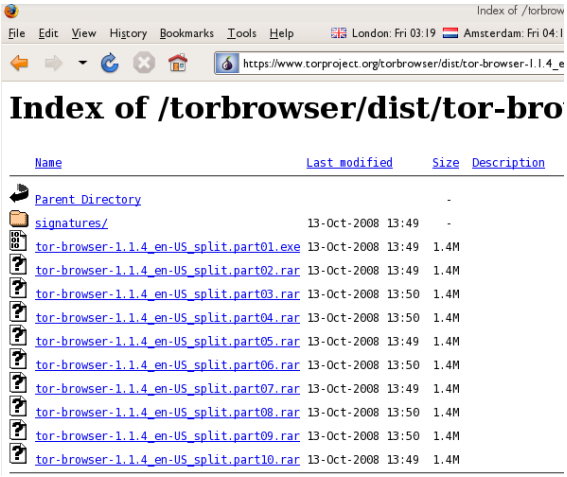
1. Choisissez un dossier vers lequel extraire les fichiers et cliquez sur « Extraire ».
   Remarque : vous pouvez choisir d'extraire les fichiers directement vers la clé USB si vous voulez utiliser Tor Browser sur différents ordinateurs (par exemple, des ordinateurs dans des cybercafés).
2. Quand l'extraction est achevée, ouvrez le dossier et vérifiez que le contenu correspond à l'image ci-dessous :



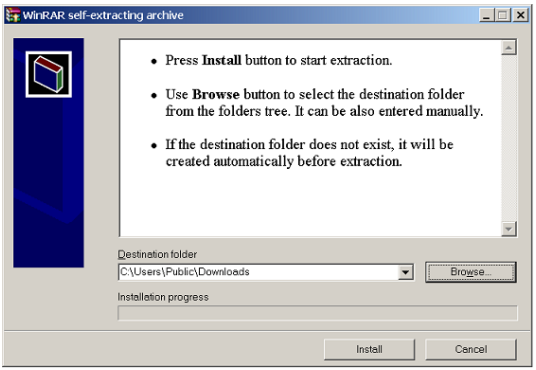
3. Pour nettoyer, supprimer le fichier.exe que vous avez téléchargé à l'origine.

Installation à partir de la version split

1. Dans votre navigateur Web, entrez l'URL de la version split de Tor Browser Bundle (https://www.torproject.org/projects/torbrowser-split.html.en), puis cliquez sur le lien correspondant à la langue choisie pour aller sur une page ressemblant à la page en anglais ci-dessous :



2. Cliquez sur chaque fichier pour le télécharger (l'un avec une terminaison en .exe et neuf autres avec une terminaison en .rar), l'un après l'autre, et sauvegardez-les tous dans un dossier sur votre disque dur.
3. Double-cliquez la première partie (le fichier dont le nom se termine en .exe). Cela lance un programme servant à réunir toutes les parties.



4. Choisissez un dossier où vous voulez installer les fichiers et cliquez sur « Installez ». Le programme affiche des messages sur la progression de l'installation, puis se ferme.
5. Quand l'extraction est achevée, ouvrez le dossier et vérifiez que le contenu correspond à l'image ci-dessous :

6. Pour nettoyer, supprimer tous les fichiers que vous avez téléchargé à l'origine.

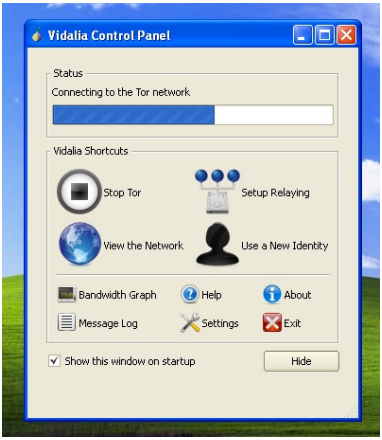
UTILISER TOR BROWSER

Avant de commencer :

Fermez Tor. Si Tor est déjà installé sur votre ordinateur, assurez-vous qu'il n'est pas en cours d'exécution.

Lancez Tor Browser :

Dans le dossier Tor Browser, double-cliquez sur « Démarrer Tor Browser ». Le panneau de contrôle Tor (Vidalia) s'ouvre et Tor commence à se connecter au réseau Tor.



Quand la connexion est établie, Firefox se connecte automatiquement à la page TorCheck puis confirme que votre navigateur est configuré pour utiliser Tor. Cela peut prendre un moment, selon la qualité de votre connexion Internet.

Si vous êtes connecté au réseau Tor, une icône en forme d'oignon vert apparaît dans la barre d'état système au coin inférieur droit de votre écran :

NAVIGATION À L'AIDE DE TOR BROWSER

Essayer de visiter quelques sites Web et de voir s'ils s'affichent. Les sites sont susceptibles de se charger plus lentement que la normale car votre connexion est acheminée à travers plusieurs relais.

SI CELA NE FONCTIONNE PAS

Si l'oignon dans le panneau de contrôle Vidalia ne devient jamais vert ou si Firefox est ouvert, mais affiche une page où vous lisez : « Désolé. Vous n'utilisez pas Tor actuellement », comme dans l'image ci-dessous, c'est en effet le cas.

Si vous lisez ce message, fermez Firefox et Tor Browser, puis répétez les procédures ci-dessus. Vous pouvez effectuer à tout moment cette vérification pour être sûr que vous êtes en train d'utiliser Tor en allant sur https://check.torproject.org/.

Si Tor Browser ne fonctionne pas au bout de deux ou trois tentatives, il est possible que Tor soit bloqué en partie par votre FAI ; il faut alors essayer d'utiliser la fonction pont de Tor – voir la section ci-dessous « Utiliser Tor avec des ponts ».

UTILISER TOR IM BROWSER BUNDLE

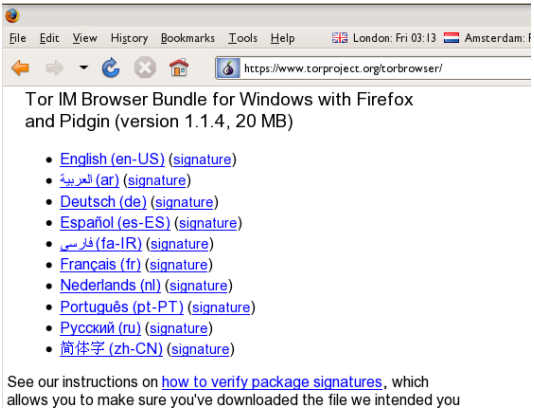
Le Tor IM Browser Bundle est semblable au Tor Browser Bundle, mais il comprend l'accès au client de messagerie instantanée multi-protocole Pidgin, qui vous permet de chatter de manière cryptée à partir de votre protocole de messagerie instantanée comme ICQ, MSN Messenger, Yahoo ! Messenger ou QQ qui peuvent être filtrés.

pidgin_en

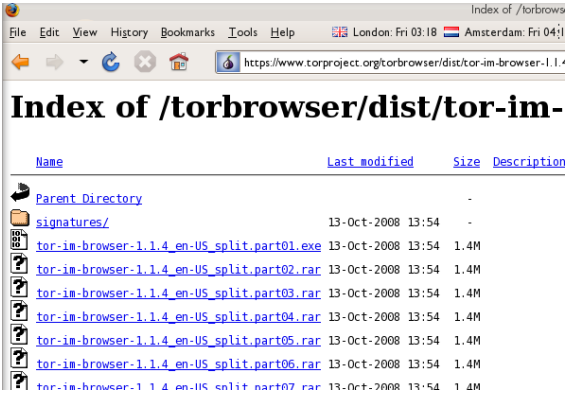
Pour en savoir plus sur Pidgin : http://www.pidgin.im

TÉLÉCHARGER TOR IM BROWSERBUNDLE

Vous pouvez télécharger le Tor IM Browser Bundle directement à partir du site Web de Tor avec ce lien : https://www.torproject.org/projects/torbrowser



Si votre connexion Internet est lente ou peu fiable, vous pouvez également obtenir une version split sur le site Web torproject.org avec ce lien : https://www.torproject.org/projects/torbrowser-split.html.en



AUTO-EXTRAIRE L'ARCHIVE

Pour démarrer, double-cliquez sur le fichier .exe que vous venez de télécharger.

C'est normalement la fenêtre ci-dessous qui s'affichera :

Choisissez un dossier vers le quel vous voulez extraire les fichiers. Dans le doute, conserver l'emplacement par défaut. Puis cliquez sur « Extraire ».

Remarque : vous pouvez choisir d'extraire les fichiers directement vers la clé USB si vous voulez utiliser Tor Browser sur différents ordinateurs (par exemple, des ordinateurs dans des cybercafés).

Quand l'extraction est achevée, ouvrez le nouveau dossier créé et vérifiez que le contenu correspond à l'image ci-dessous (vous y trouverez le dossier PidginPortable) :

Vous pouvez maintenant supprimer en toute sécurité le fichier .exe que vous aviez téléchargé (ou tous les fichiers .rar et .exe si vous avez utilisé la version split)

UTILISER TOR IM BROWSER BUNDLE

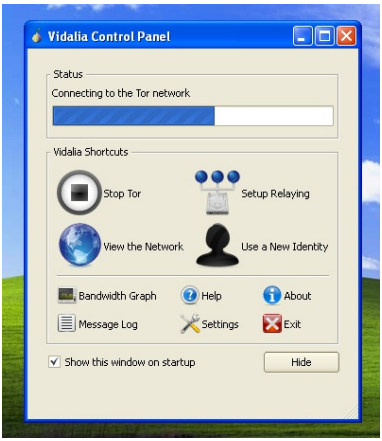
Avant de commencer :

Fermez Firefox. Si le navigateur Firefox est installé sur votre ordinateur, assurez-vous qu'il n'est pas lancé.

Fermez Tor. Si Tor est installé sur votre ordinateur, assurez-vous qu'il n'est pas lancé.

Lancer Tor IM Browser :

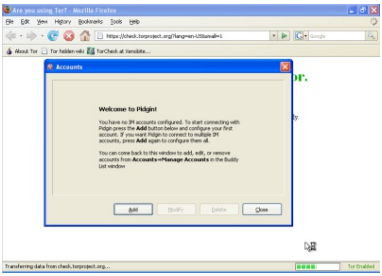
Dans le dossier Tor Browser, double-cliquez sur « Démarrer Tor Browser ». Le panneau de contrôle de Tor (Vidalia) s'ouvre et Tor se connecte au réseau Tor.



Quand une connexion est établie :

Une fenêtre Firefox s'affiche et se connecte à la page TorCheck, où doit figurer l'oignon vert qui confirme que votre navigateur est configuré pour utiliser Tor.

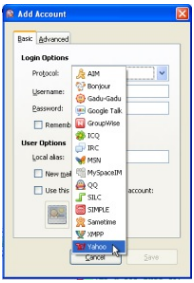
Une fenêtre de l'assistant Pidgin (ci-dessous) s'affiche et vous invite à configurer les paramètres de votre compte de Messagerie Instantanée dans Pidgin.



Vous verrez également apparaître l'icône de Tor (un oignon vert si vous êtes connecté) et l'icône de Pidgin dans la barre d'état système au coin inférieur droit de votre écran

CONFIGURER VOTRE COMPTE DE MESSAGERIE INSTANTANÉE DANS PIDGIN

Vous pouvez configurer votre compte de messagerie instantanée dans la fenêtre de Pidgin. Pidgin est compatible avec la plupart des principaux services de messagerie instantanée (AIM, MSN, Yahoo !, Google Talk, Jabber, XMPP, ICQ, etc.).



Pour en savoir plus sur le mode d'emploi de Pidgin, voir :
http://developer.pidgin.im/wiki/Using%20Pidgin#GSoCMentoring.Evaluations

SI CELA NE FONCTIONNE PAS

Si l'oignon du Panneau de contrôle Vidalia ne devient pas vert ou si Firefox s'ouvre, mais affiche une page où vous lisez : « Désolé, vous n'utilisez pas Tor actuellement », vous devez alors :

- Quitter Vidalia et Pidgin (voir les détails ci-dessous).
- Relancer Tor IM Browser en suivant les étapes ci-dessous ("Utiliser Tor IM Browser Bundle").
- Si Tor Browser ne fonctionne toujours pas au bout de deux ou trois tentatives, il est possible que Tor soit bloqué en partie par votre FAI. Se référer à la section ci-dessous « Utiliser Tor avec des ponts ».

QUITTER TOR IM BROWSER

Pour quitter Tor IM Browser :

- Quittez Vidalia en faisant un clic droit sur l'icône de l'oignon dans votre barre de tâches et choisissez "Quitter" dans le menu contextuel de Vidalia.
- Quittez Vidalia en faisant un clic droit sur l'icône de l'oignon dans votre barre de tâches et choisissez "Quitter" dans le menu contextuel de Pidgin.
- Quand l'icône de Vidalia et l'icône de Pidgin disparaissent de la barre de tâches de Windows au coin inférieur droit de votre écran, c'est que Tor IM Browser est fermé.

UTILISER LES PONTS DE TOR

Quittez Si vous soupçonnez que votre accès au réseau Tor est bloqué, vous pouvez vous servir de l'option pont de Tor. Cette fonction a été spécialement créée pour aider les gens à utiliser Tor à partir des emplacements où l'accès au réseau Tor est bloqué. (Pour utiliser un pont, il faut que vous ayez déjà téléchargé et installé avec succès le logiciel Tor.)

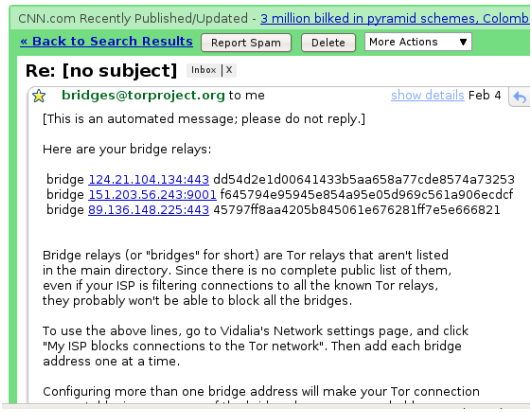
QU'EST-CE QU'UN PONT ?

Les relais-ponts (ou ponts en abrégé) sont des relais de Tor qui ne figurent pas dans le principal annuaire public de Tor, ceci intentionnellement, afin de mettre un terme au blocage de ces relais. Même si votre FAI filtre les connexions à tous les relais de Tor connus du public, il se pourrait qu'il ne réussisse pas à bloquer tous les ponts.

OÙ TROUVER CES PONTS ?

Pour se servir d'un pont, vous devez en localiser un et ajouter ses informations dans vos paramètres réseau. Pour avoir quelques ponts, il suffit d'accéder à l'aide de votre navigateur Web à https://bridges.torproject.org/. Si ce site Web est bloqué ou que vous ayez besoin de plus de ponts, envoyez un email à partir d'un compte Gmail à bridges@torproject.org en indiquant dans le corps de votre message « get bridges » (sans guillemets).

Quasi instantanément, vous recevrez une réponse contenant des informations sur quelques ponts :



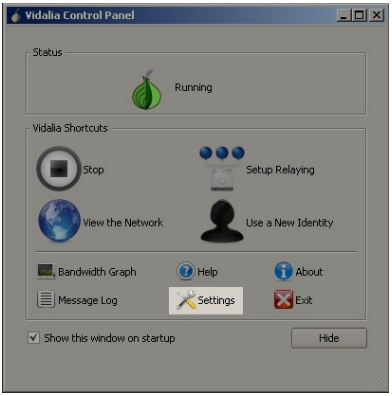
Points très importants :

1. Vous devez impérativement utiliser un compte Gmail pour envoyer votre requête. Si torproject.org acceptait les requêtes provenant d'autres comptes de messagerie, un cyber-attaquant pourrait aisément créer de multiples adresses email et connaître rapidement tous les ponts. Si vous ne possédez pas encore de compte Gmail, cela ne vous prendra que quelques minutes pour en créer un.
2. Si votre connexion Internet est lente, vous pouvez utiliser l'URL https://mail.google.com/mail/h/ pour avoir un accès direct à la version HTML de Gmail.

ACTIVER LE BRIDGING ET ENTRER LES INFORMATIONS SUR LE PONT

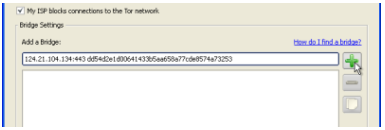
Après avoir obtenu des adresses de relais-ponts, vous devez configurer Tor avec l'adresse de pont Tor de votre choix :

1. Ouvrez le panneau de contrôle de Tor (Vidalia).

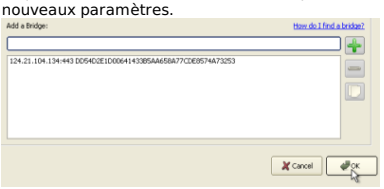


2. Cliquez sur « Paramètres ». Une fenêtre « Paramètres » s'ouvrira.

3. Cliquez sur « Réseau ».
4. Sélectionnez « Mon pare-feu ne me permet de me connecter qu'à certains ports » et « Mon FAI bloque les connexions au réseau Tor ».
5. Entrez les informations relatives à l'URL du pont que vous avez reçues par email dans le champ « Ajouter un pont ».
6. Cliquez sur le + en vert placé sur le côté droit du champ « Ajouter un pont ». L'URL est ajoutée dans la boite ci-dessous :



7. Cliquez sur « OK » en bas de la fenêtre pour valider vos nouveaux paramètres.



8. Dans le panneau de contrôle de Tor, arrêtez et redémarrez Tor pour utiliser vos nouveaux paramètres.

Remarque :

Ajoutez autant d'adresses de ponts que possible. Des ponts supplémentaires augmentent la fiabilité. Un seul pont suffit pour atteindre le réseau Tor, mais si vous n'en avez qu'un et qu'il se fait bloquer ou cesse de fonctionner, vous serez coupé du réseau Tor tant que vous n'aurez pas ajouté de nouveaux ponts.

Pour ajouter plus de ponts dans vos paramètres réseau, répétez l'opération ci-dessus avec les informations correspondant aux ponts supplémentaires obtenues dans le message e-mail reçu de bridges@torproject.org

25. JONDO

Jondo a fait ses débuts en tant que projet universitaire allemand, appelé Java Anon Proxy (JAP), comprenez Proxy Anonyme Java. Il est devenu un outil d'anonymisation solide, comme Tor, qui transfère le trafic à travers plusieurs serveurs indépendants.

Contrairement à Tor, le réseau JonDo mélange des serveurs maintenus par des volontaires avec d'autres maintenus par une entreprise affiliée. Cette disposition donne aux utilisateurs un choix de débit : de 30-50 Ko/s, environ la vitesse d'un modèle RTC, accessible gratuitement, à 660 Ko/s en accès payant. Pour une comparaison plus détaillée et une liste des prix, voyez https://anonymous-proxy-servers.net/en/payment.html.

INFORMATIONS GÉNÉRALES

Systèmes d'exploitation supportés	
Langues	Anglais, Allemand, tchèque, Néerlandais, Français, et Russe
Site Web	http://www.jondos.de
Support	Forum : https://anonymous-proxy-servers.net/forum Wiki : https://anonymous-proxy-servers.net/wiki Formulaire de contact : https://anonymous-proxy-servers.net/bin/contact.pl?

INSTALLATION

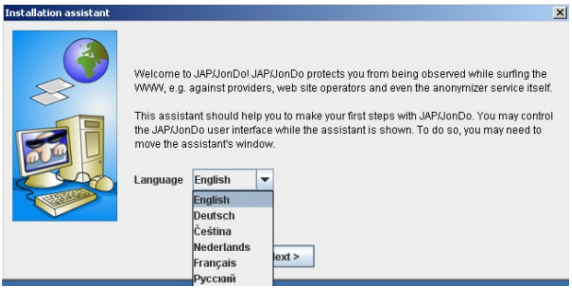
Pour utiliser le réseau JonDo, appelé JonDonym, vous devez télécharger le client JonDo pour votre système d'exploitation sur https://anonymous-proxy-servers.net/en/jondo.html. Des versions sont disponibles pour Linux (environ 9Mio), Mac OS X (environ 17 Mio) et Windows (environ 35 Mio).

Une fois que vous avez téléchargé le client, installez-le comme vous installeriez n'importe quel logiciel de votre système. On vous demandera peut-être si vous souhaitez l'installer sur votre PC ou si vous souhaiter créer une version portable. Dans notre exemple, nous envisageons une installation sur PC.

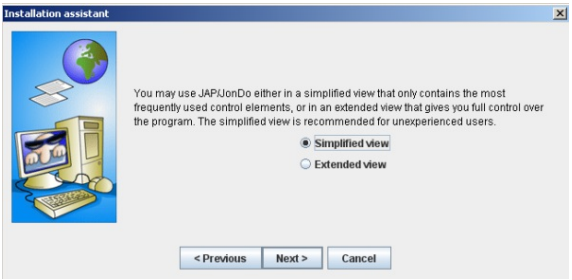
Les utilisateurs de windows peuvent également installer le navigateur JonDoFox, dont nous parlons plus bas.

CONFIGURATION ET UTILISATION

Quand vous lancez JonDo pour la première fois, vous pouvez choisir le langage que vous voulez.

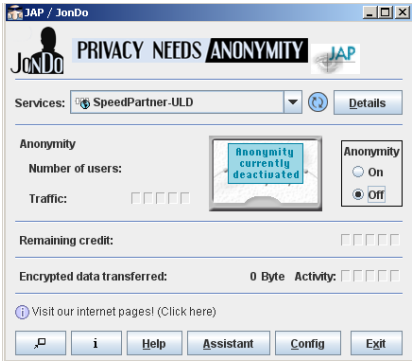


Choisissez ensuite le niveau de détail que vous voulez voir quand vous utilisez le service. Les utilisateurs de base devraient choisir « Vue simplifiée ».

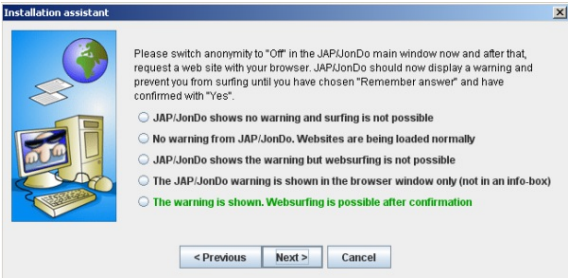


Sur l'écran suivant, l'assistant d'installation vous demande de choisir le navigateur qui utilisera le proxy JonDo. Cliquez sur le nom de votre navigateur, et suivez les instructions.

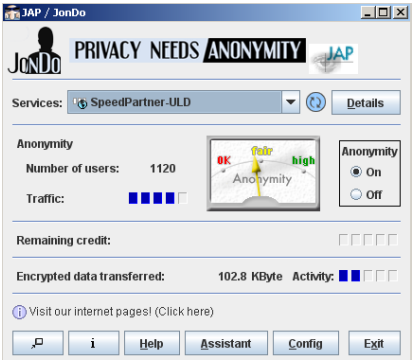
JonDo vous demande enfin de tester votre configuration. Dans le panneau de contrôle, réglez « anonymat » à Off et essayez ensuite d'ouvrir un site via le navigateur que vous venez de configurer.



Si JonDo vous affiche un avertissement et que vous devez cliquer sur « Oui » pour accéder au site, tout est configuré correctement et vous pouvez choisir « L'avertissement est affiché. La navigation est possible après confirmation ». Si une autre description vous correspond, choisissez-la, et l'assistant vous donnera plus d'informations sur la résolution de votre problème.

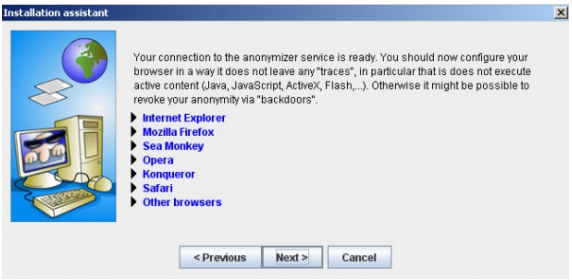


Maintenant, passez à la seconde étape pour vous assurer que la configuration est correcte : réglez l'anonymat sur « On » dans le panneau de contrôle et ouvrez un site aléatoire avec le navigateur que vous avez configuré.

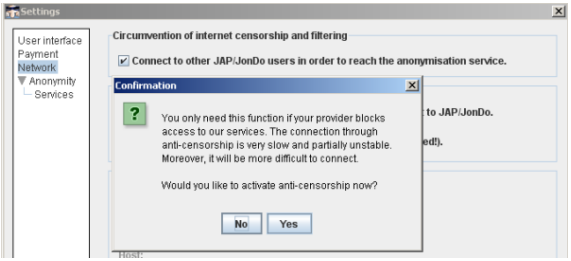


Si le site se charge, tout va bien et vous pouvez cliquer sur « Connexion établie, la navigation fonctionne ». Si une autre description vous correspond, choisissez-la, et l'assistant vous donnera plus d'informations sur la résolution de votre problème.

Vous avez configuré avec succès votre navigateur pour qu'il se connecte au réseau JonDo. Maintenant, vous devez également configurer votre navigateur pour qu'il ne fasse pas fuiter d'informations par accident. Cliquez sur le nom de votre navigateur pour lancer le processus.



Si les serveurs JonDo standards sont déjà bloqués dans votre pays, vous devriez essayer l'option anti-censure. Cliquez sur « Configurer » dans le panneau de contrôle et sélectionnez l'onglet « Réseau ». Cliquez sur « Se connecter à d'autres utilisateurs de JAP/JonDO afin d'atteindre le service d'anonymisation ». Lisez l'avertissement et confirmez en cliquant sur « Oui ».



Afin d'être sûr que vous avez configuré votre navigateur correctement, visitez http://what-is-my-ip-address.anonymous-proxy-servers.net qui vous avertira d'un problème éventuel.

JONDOFOX

Pour plus de sécurité, l'équipe JonDoNym fournit une version modifiée du navigateur Firefox appelée JonDoFox. Comme le paquetage incluant Tor, il empêche la fuite d'informations supplémentaires pendant l'utilisation de l'anonymiseur.

Vous pouvez le télécharger à l'adresse https://anonymous-proxy-servers.net/en/jondofox.html.

26. YOUR-FREEDOM

Your-freedom est un proxy commercial proposant un service gratuit, bien que plus lent.

Leur logiciel est disponible sous Microsoft Windows, Linux et Mac OS, et vous connecte à une trentaine de serveurs, dans une dizaine de pays. Your-Freedom propose aussi des services avancés, comme OpenVPN et des proxys SOCKS, qui en font un outil relativement sophistiqué pour contourner la censure.

INFORMATIONS GÉNÉRALES

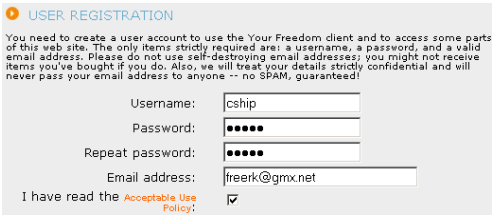
Systèmes d'exploitation supportés	
Langues	20 langues
Site Web	https://www.your-freedom.net
Support	Forum : https://www.your-freedom.net/index.php?id=2 Guide d'utilisation : https://www.your-freedom.net/ems-dist/Your%20Freedom%20User%20Guide.pdf

INTRODUCTION À L'UTILISATION DE YOUR-FREEDOM

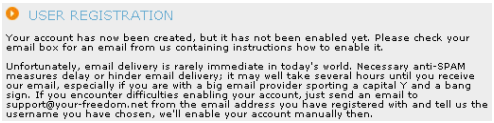
Dans un premier temps, téléchargez l'outil gratuitement sur https://www.your-freedom.net/index.php?id=downloads. Si Java est déjà installé, vous pouvez télécharger la petite version qui pèse environ 2 Mb. Pour le vérifier, vous pouvez visite http://www.java.com/en/download/testjava.jsp. Si vous n'avez pas encore Java, téléchargez l'installeur complet qui pèse environ 12 Mb. Tous les fichiers sont également disponibles sur http://mediafire.com/yourfreedom.

Si vous vivez dans un pays où le gouvernement censure l'accès à Internet, vous devez pouvoir utiliser Your-Freedom avec le compte Sesawe (Nom d'utilisateur: sesawe, Mot de passe: sesawe). Si cela ne fonctionne pas, vous devez vous enregistrer. Pour commencer, créez un compte gratuit sur le site https://www.your-freedom.net/index.php?id=170&L=0.

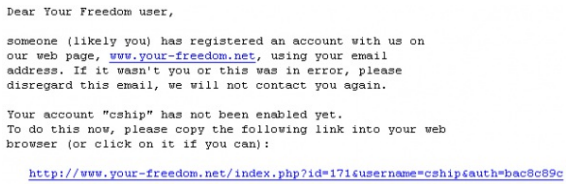
Cliquez sur le lien « First visit ? Click here to register » (Première visite ? Cliquez ici pour vous enregistrer) sous les deux champs d'authentification.



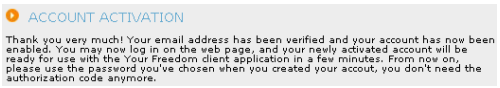
Sur la page suivante, entrez les informations demandées. Nom d'utilisateur, mot de passe adresse e-mail sont les seules informations obligatoires. Les autres sont optionnelles.



Vous verrez alors un message disant que vous enregistrement est presque fini et que dans quelques secondes, vous allez recevoir un e-mail à l'adresse fournie.



Cliquez sur le second lien (le plus long) pour confirmer votre enregistrement.

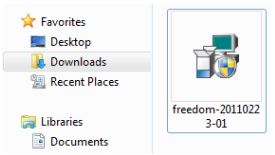


Quand vous verrez l'écran « Thank you », votre compte sera activé.

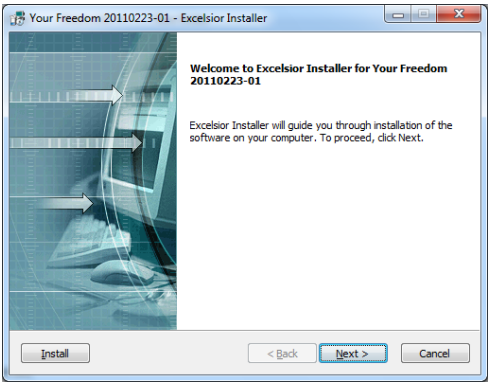
INSTALLATION

Les instructions suivantes et les captures d'écran ont été réalisées sous Windows, mais toutes les étapes et les configurations sont très similaires sur les autres systèmes d'exploitation.

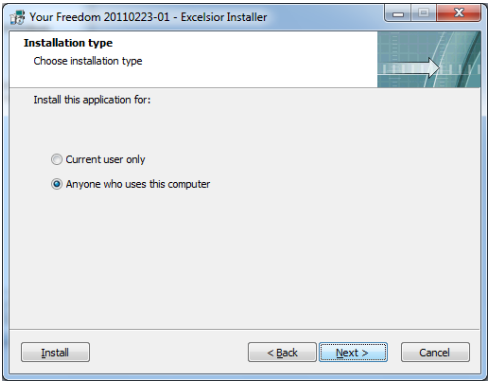
Maintenant vous êtes prêts à installer Your-Freedom.



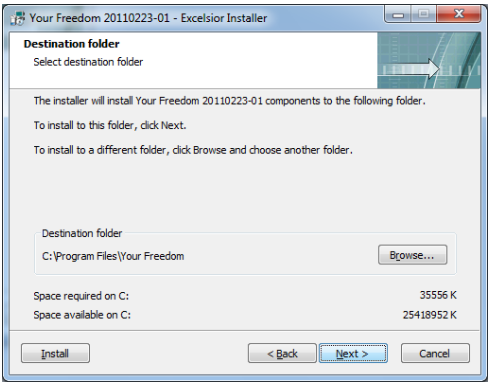
Cliquez sur le fichier téléchargé. Le nom du fichier peut varier selon les versions.



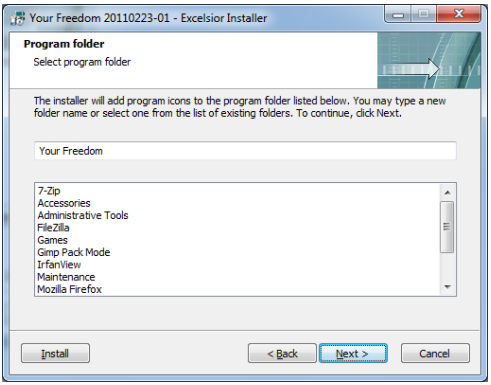
Cliquez sur Suivant sur le premier écran.



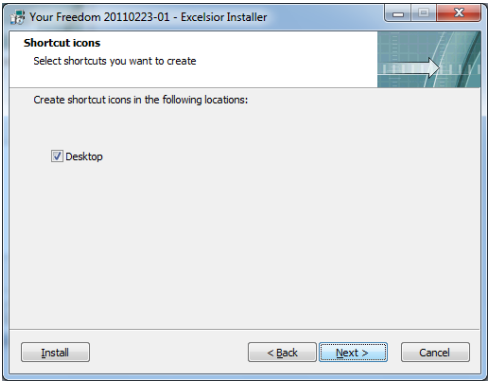
Sur l'écran suivant, vous pouvez choisir si le programme doit être utilisable uniquement pour votre utilisateur ou s'il doit l'être pour tous (recommandé). Cliquez sur Suivant.



Choisissez le répertoire dans lequel installer Your-Freedom. La plupart des utilisateurs peuvent accepter la sélection par défaut. Cliquez sur Suivant.

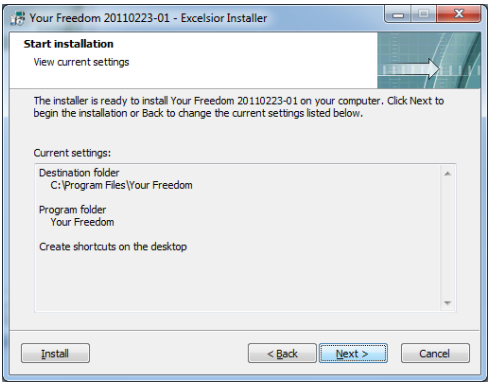


Sur l'écran suivant de l'installeur, vous pouvez choisir le nom qui sera utilisé pour le répertoire du programme. Vous pouvez laisser le réglage par défaut et cliquer sur Suivant.

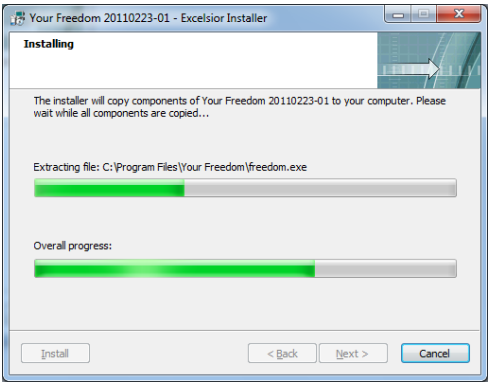


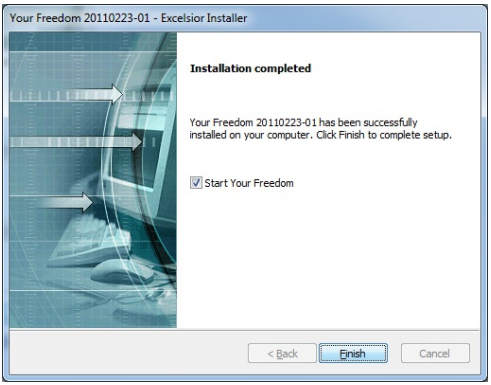
Choisissez si vous voulez créer une icône sur le bureau. Puis cliquez sur Suivant.

Maintenant vous pouvez voir un résumé des décisions que vous avez pris. Confirmez en cliquant sur Suivant ou retournez en arrière si vous avez besoin de modifier quelque chose.



L'installation est maintenant en cours. Cela peut prendre quelques minutes en fonction de votre ordinateur.





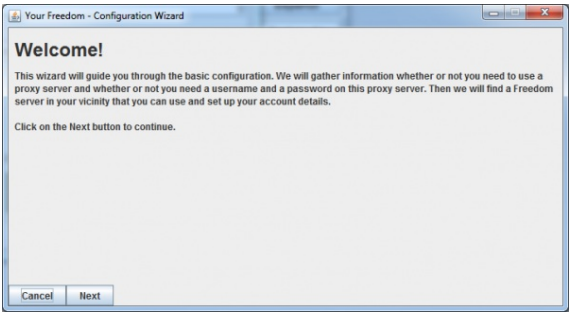
L'installation est terminée. Quittez le programme d'installation en cliquant sur « Terminer ».

CONFIGURATION

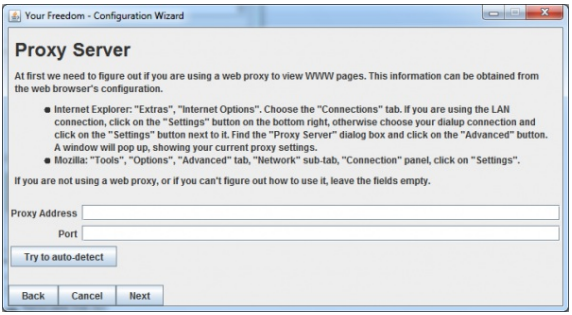
Your-Freedom va démarrer automatiquement. Quand vous lancerez Your-Freedom dans le futur, cliquez sur son icône (la porte) sur votre bureau.

Quand vous démarrez Your-Freedom pour la première fois, vous devez le configurer.

La première étape est de choisir la langue. Cliquez sur celle que vous souhaitez. Vous pourrez en changer plus tard.

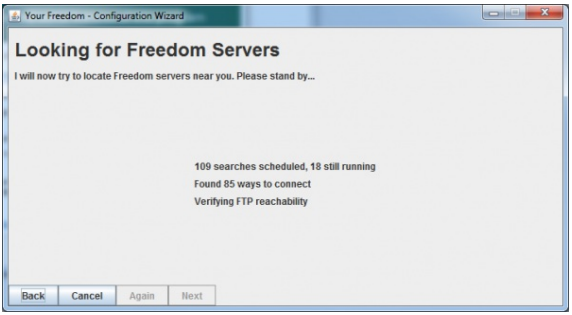


Juste après le premier lancement, vous devriez voir le panneau d'aide à la configuration. Cliquez sur suivant.



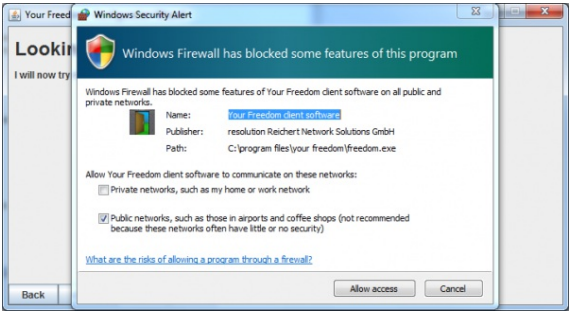
Dans l'écran Serveur Proxy, le programme détecte automatiquement les informations sur un serveur mandataire que vous puissiez l'utiliser. Cliquez sur Suivant.

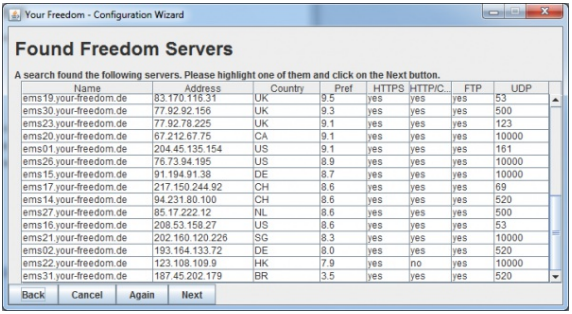
Dans l'écran de sélection de protocoles, vous devez laisser la valeur par défaut et cliquer sur Suivant.



Maintenant, l'aide à la configuration de Your-Freedom va faire quelques tests pour trouver des serveurs, vérifier le type de votre connexion et votre filtrage. Cela peut prendre quelques minutes.

Vous pourrez avoir un avertissement concernant votre pare-feu (ici, pour l'exemple, celui de Windows 7). Vous pouvez autoriser l'accès à Your-Freedom.

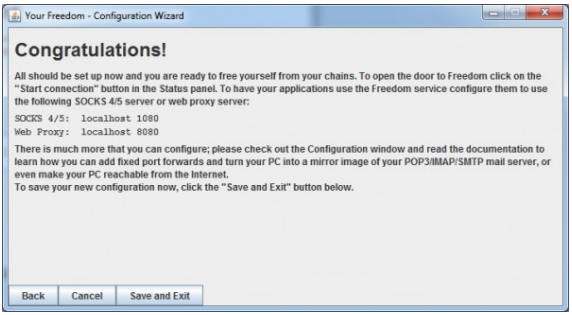




Quand l'aide à la configuration est prête, vous verrez l'écran des serveurs auxquels vous pouvez vous connecter. Choisissez en un, et cliquez sur Suivant.

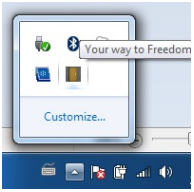
Entrez les informations du compte que vous avez créé au préalable. Si vous n'en avez pas, vous pouvez en créer un gratuitement en envoyant une demande par mail à english@sesawe.net.

Cliquez sur Suivant.

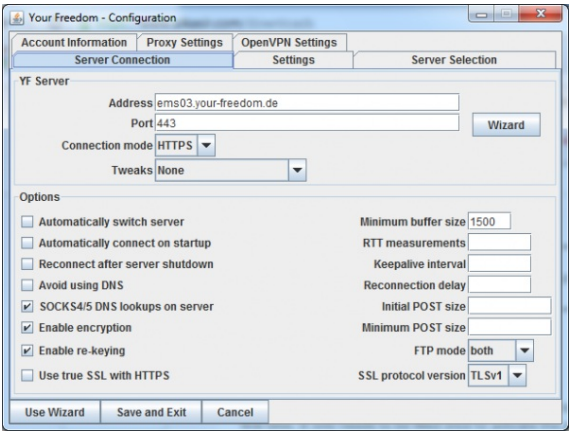


Quand vous verrez l'écran de félicitations, la configuration sera finie. Cliquez sur « Sauvegarder » et « Quitter ».

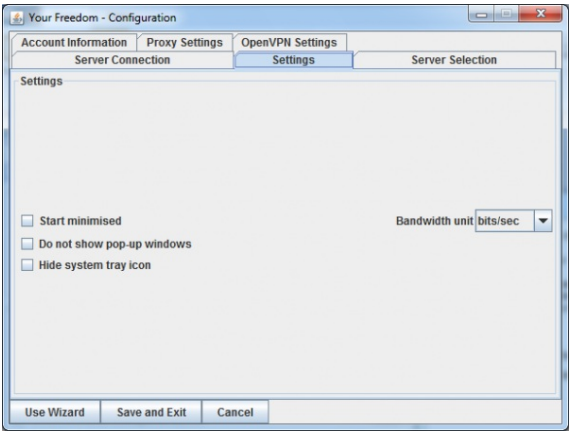
Your-Freedom est maintenant lancé sur votre ordinateur et vous pouvez voir une icône dans la barre de tâches.



Pour plus de sécurité et mieux contourner les filtres, vous pouvez copier la configuration de la capture d'écran ci-dessous en cliquant sur Configuration dans la fenêtre principale de Your-Freedom. Puis cliquez sur « Sauvegarder » et « Quitter ».



Your-Freedom est maintenant connecté à un serveur et fourni un proxy local que vous utilisez avec vos applications favorites, telles qu'Internet Explorer ou Firefox. Pour les configurer automatiquement, cliquez sur l'onglet Applications dans la fenêtre principale de Your-Freedom, sélectionnez les logiciels que vous voulez utiliser et cliquez sur OK. Your-Freedom va automatiquement configurer ces logiciels pour qu'ils se connectent à Internet en passant par le tunnel chiffré fourni par Your-Freedom.



Pour être sûr que vous utilisez Your-Freedom, allez sur le site https://www.your-freedom.net et vérifiez la section sur la gauche. Si le pays détecté n'est pas celui où vous êtes, vous utilisez avec succès le tunnel d'accès chiffré à Internet de Your-Freedom.

TECHNIQUES AVANCÉES

27. NOMS DE DOMAINES ET DNS
28. PROXYS HTTP
29. LA LIGNE DE COMMANDE
30. OPENVPN
31. TUNNELS SSH
32. PROXY SOCKS

27. NOMS DE DOMAINES ET DNS

Si vous avez conclus, suspecté ou ouï dire que la technique utilisée pour censurer votre réseau est basée sur le filtrage ou l'usurpation de DNS, vous devriez considérer ces techniques.

UTILISER DES SERVEURS OU DES NOMS DE DOMAINES ALTERNATIFS

un serveur DNS traduit une adresse Internet humainement compréhensible, le nom de domaine, telle que google.com en une adresse IP, telle que 72.14.207.19, qui identifie le ou les serveur(s) spécifique(s) associé(s) à ce nom. Ce service est le plus souvent accessible à travers des serveurs DNS gérés par votre fournisseur d'accès à Internet (FAI). Un blocage DNS simple est mis en œuvre en donnant une réponse invalide ou incorrecte à une requête DNS, dans le but d'empêcher les utilisateurs de trouver les serveurs qu'ils recherchent. Cette méthode est très facile à mettre en place du côté du censeur, c'est donc très largement utilisé. Gardez à l'esprit que souvent différentes méthodes de censure sont combinées, le blocage de DNS peut donc ne pas être le seul problème.

Vous pouvez potentiellement contourner ce type de censure de deux manières : en changeant les réglages DNS de votre ordinateur pour utiliser des serveurs DNS alternatifs, ou en modifiant votre fichier hosts (fichier ou figurent des associations statiques nom/IP).

SERVEURS DNS ALTERNATIFS

Vous pouvez court-circuiter les serveurs DNS de votre FAI local, en utilisant d'autres serveurs. Cela vous permet de trouver les adresses des domaines qu'il pourrait bloquer. Il y a nombre de services DNS gratuits, accessible (presque) partout que vous pouvez essayer. OpenDNS https://www.opendns.com fournit un tel service et héberge aussi des guides sur comment changer le serveur DNS que votre ordinateur utilise (https://www.opendns.com/smb/start/computer). Il y a aussi une liste mise à jour de serveurs DNS accessibles dans le monde entier sur ce site : http://www.dnsserverlist.org.

Voici une liste de services DNS accessibles publiquement, via le wiki d'Internet Censorship sur http://en.cship.org/wiki/DNS. Quelques un de ces services peuvent bloquer un nombre limité de sites. Consulter le site du fournisseur pour en savoir plus sur leur politique.)

Serveurs DNS accessibles publiquement :

Publicly-available DNS servers

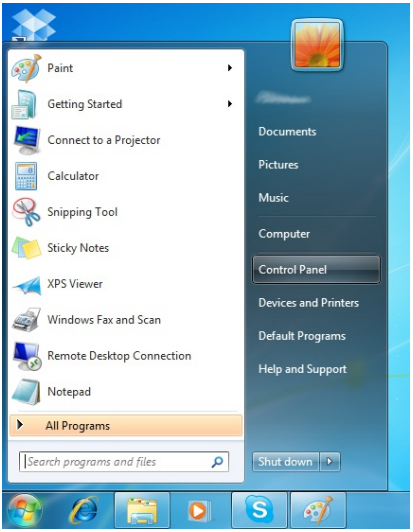
Address	**Fournisseur**
8.8.8.8	Google
8.8.4.4	Google
208.67.222.222	OpenDNS
208.67.220.220	OpenDNS
216.146.35.35	DynDNS
216.146.36.36	DynDNS
74.50.55.161	Visizone
74.50.55.162	Visizone
198.153.192.1	NortonDNS
198.153.194.1	NortonDNS
156.154.70.1	DNS Advantage
156.154.71.1	DNS Advantage
205.210.42.205	DNSResolvers

64.68.200.200	DNSResolvers
4.2.2.2	Level 3
141.1.1.1	Cable & Wireless

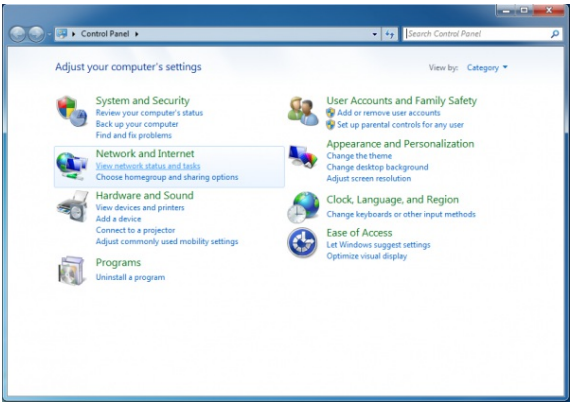
Une fois que vous avez choisi un serveur DNS à utiliser, vous devez saisir votre sélection dans vos options de DNS de votre système d'exploitation.

Changer ses options de DNS sous Windows

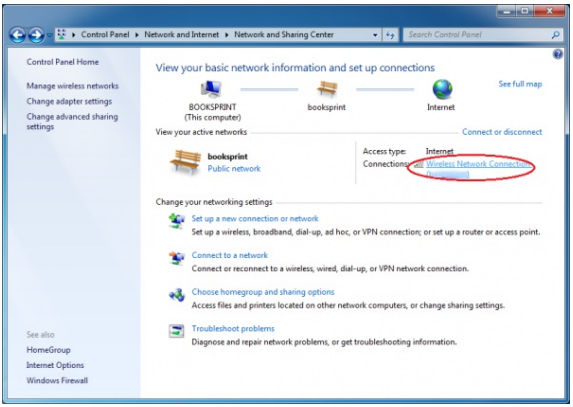
1. Ouvrez votre panneau de configuration, dans le menu Démarrer.



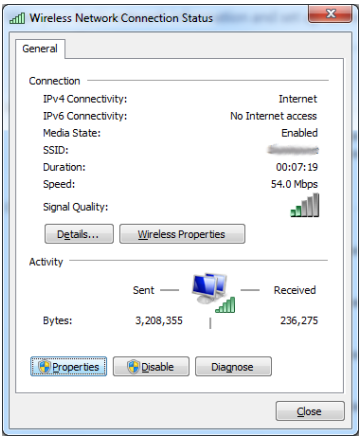
2. Dans Réseau et Internet, cliquez sur « Voir le statut du réseau et statistiques ».



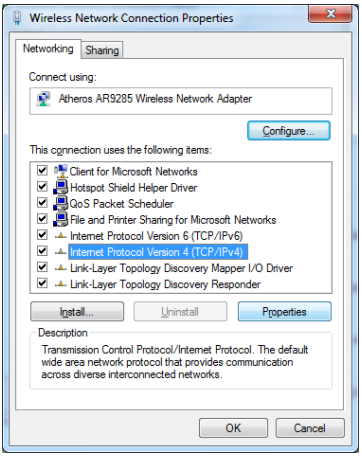
3. Cliquez sur votre connexion sans fil dans le côté droit de votre fenêtre. LA CONNECTION N'EST PAS FORCEMENT WIFI...



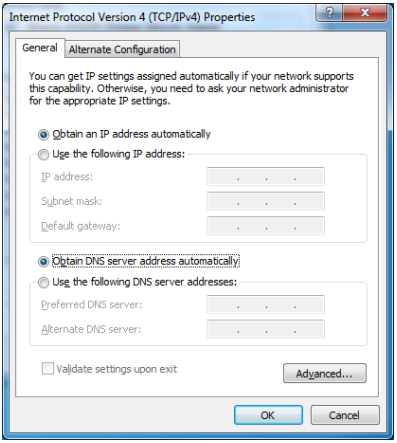
4. La fenêtre Statut de la connexion sans fil va s'ouvrir. Cliquez sur « Propriétés ».



5. Dans la fenêtre Propriétés de la connexion sans fil sélectionnez Internet Protocol Version 4 (TCP/IPv4), et cliquez sur « Propriétés ».



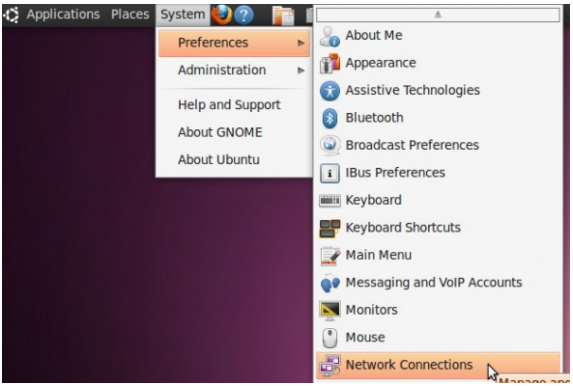
6. Vous devriez maintenant être sur la fenêtre Propriétés TCP/IPv4, où vous allez pouvoir spécifier votre adresse DNS alternative (par exemple : Google Public DNS).



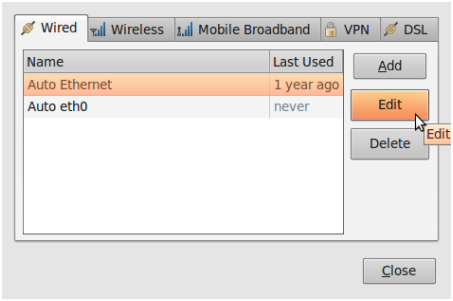
7. En bas de la fenêtre, cliquez sur « Utiliser cette adresse de serveur DNS » et complétez les champs avec l'adresse IP de votre serveur DNS alternatif préféré. Quand vous avez fini, cliquez sur OK. Par défaut, le premier serveur DNS sera utilisé. Le serveur DNS alternatif peut être d'un autre fournisseur.

Changez vos préférences DNS sous Ubuntu

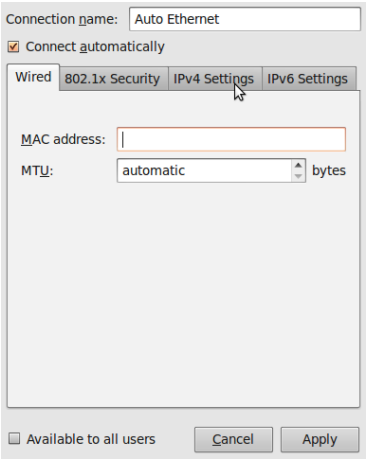
1. Dans le menu Système, allez dans « Préférences > Connexions réseau ».



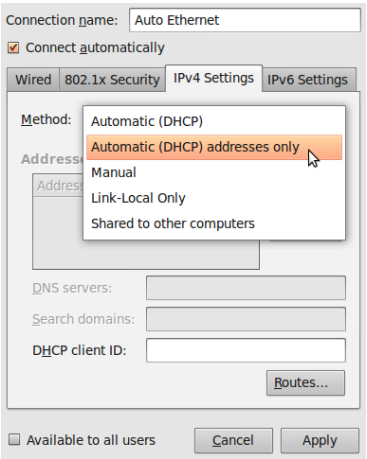
2. Sélectionnez la connexion pour laquelle vous voulez configurer le serveur DNS de Google. Si vous voulez changer les préférences pour une connexion éthernet (filaire), sélectionnez l'onglet Filaire, et sélectionnez ensuite votre interface réseau dans la liste. Si vous voulez changer les préférences pour une connexion sans fil à la place, sélectionnez l'onglet « Sans fil », puis sélectionnez le réseau sans fil approprié.



3. Cliquez sur « Editer », une fenêtre va apparaître, sélectionnez l'onglet Préférences IPv4.

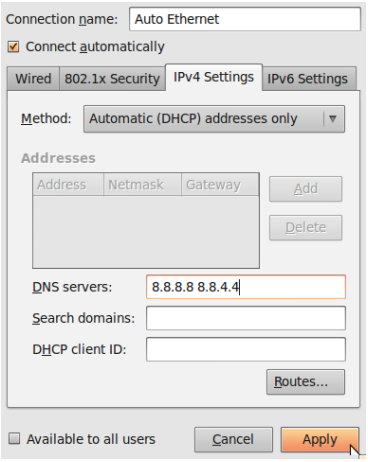


4. Si la méthode sélectionnée est Automatique (DHCP), ouvrez le menu déroulant et sélectionnez « Adresses automatiques uniquement (DHCP) » à la place. Si la méthode est une autre, ne la changez pas.



5. Dans le champ serveurs DNS, entrez les informations IP de votre serveur DNS alternatif, séparé d'un espace. Par exemple, si vous voulez ajouter le DNS Google, écrivez : 8.8.8.8 8.8.4.4

6. Cliquez sur « Appliquer » pour sauvegarder les changements. SI l'on vous demande un mot de passe, ou une confirmation, saisissez le mot de passe, ou confirmez que vous souhaitez effectuer ces changements.



7. Répetez les étapes 1-6 pour chaque connexion réseau que vous souhaitez modifier.

EDITER VOTRE FICHIER HOSTS

Si vous connaissez l'adresse IP d'un site web particulier, ou d'un service Internet bloqué par les serveurs DNS de votre FAI, vous pouvez lister ce site dans les fichiers hôtes :

208.80.152.134 secure.wikimedia.org

Chacune des lignes contient une adresses IP, puis un espace et enfin un nom. Vous pouvez ajouter n'importe quel nombre de sites à votre fichier hosts. Notez que si vous utilisez une mauvaise adresse pour un site, cela peut vous empêcher d'accéder à un site par son nom jusqu'à ce que vous le répariez ou l'enleviez de la liste.

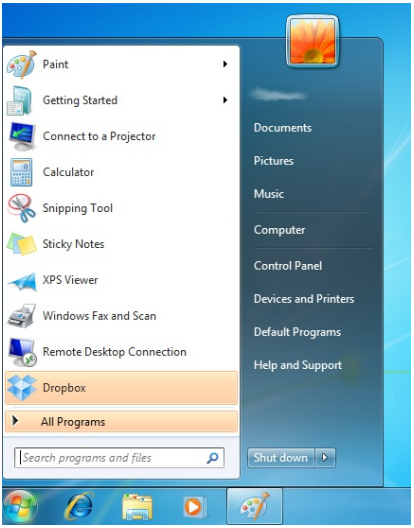
Si vous ne pouvez pas trouver l'adresse IP d'un site à cause de la censure des serveurs DNS de votre FAI, il y a des centaines de services qui vous aideront à faire une recherche DNS non censurée. Par exemple, vous pouvez utiliser n'importe lequel des outils présents sur http://www.dnsstuff.com/tools.

Vous pouvez aussi penser à utiliser les outils de http://www.traceroute.org, outils de diagnostic réseau sophistiqués et fournis par divers FAI. Ils étaient originalement plutôt utilisés pour diagnostiquer des pannes accidentelles de réseau qu'une censure. Ils peuvent aussi inclure la capacité de rechercher l'adresse IP d'un serveur particulier.

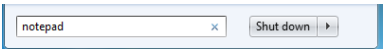
Modifier votre fichier hosts sous Windows Vista/7

Vous utiliserez un simple éditeur de texte, tel que le Bloc-Notes, pour éditer votre fichier hosts. Dans Windows Vista et 7, votre fichier hosts est habituellement situé dans C:\Windows\system32\drivers\etc\hosts.

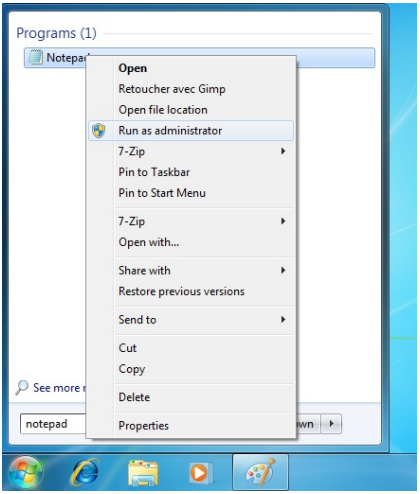
1. Cliquez sur « Démarrer ».



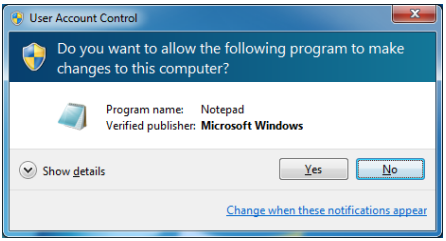
2. Saisissez « notepad » dans la barre de recherche.



3. Une fois que vous avez trouvé le programme, faites un clic-droit et sélectionnez « Exécuter en tant qu'administrateur ».

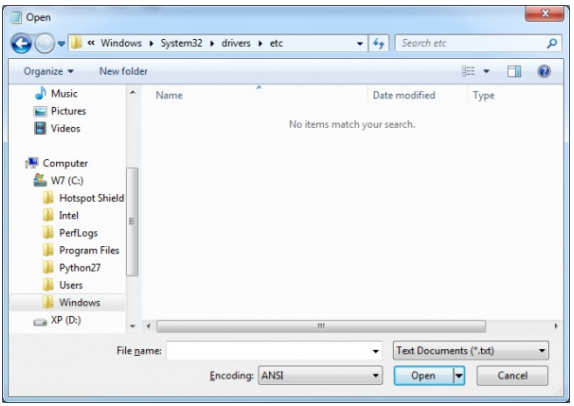


4. Windows vous demandera votre permission pour modifier les fichiers. Cliquez sur « Oui ».

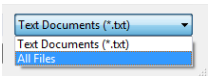


5. Dans le menu Fichier, sélectionnez « Ouvrir ».

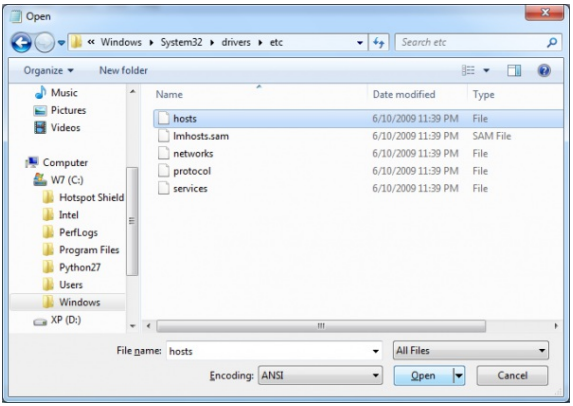
6. Naviguez jusqu'à C:\Windows\system32\drivers\etc\. Vous pouvez remarquer que ce dossier semble initialement vide.



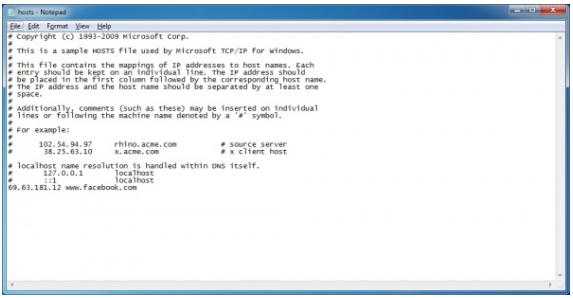
7. Dans le bouton droit de la barre de saisie, sélectionnez Tous les fichiers.



8. Sélectionnez le fichier « hosts » et cliquez sur « Ouvrir ».



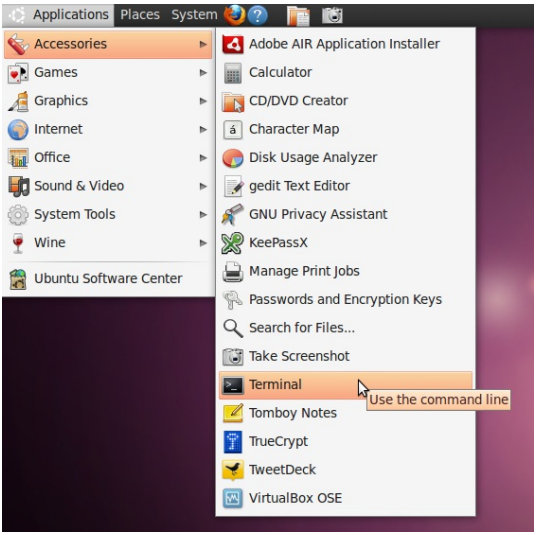
9. Ajoutez, par exemple, la ligne « 69.63.181.12 www.facebook.com » à la fin du fichier et sauvegardez le en pressant Ctrl+S ou en sélectionnant « Fichier > Enregister ».



Modifier votre fichier Hosts sous Ubuntu

Dans Ubuntu, votre fichier hosts est localisé dans /etc/hosts. Pour le modifier, vous devrez avoir quelques connaissances en lignes de commandes. Référez-vous au chapitre « Les lignes de commandes » pour un bref tutorial sur cette fonction.

1. Ouvrez le Terminal via « Acessoires > Terminal » dans votre menu Applications.

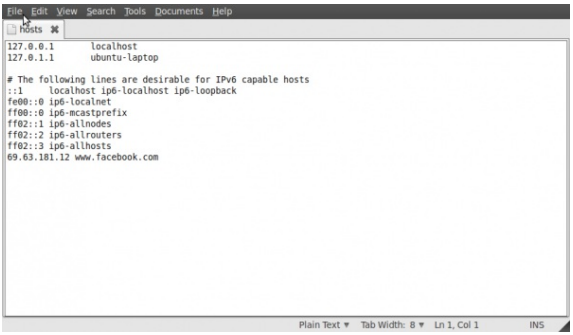


2. Utilisez les commandes suivantes pour ajouter automatiquement une ligne au fichier hosts :

   echo 69.63.181.12 www.facebook.com | sudo tee -a /etc/hosts
3. On peut vous demander votre mot de passe pour modifier le fichier. Une fois autorisé, la commande ajoutera « 69.63.181.12 www.facebook.com" à la dernière ligne du fichier hosts.

4. Optionnel : Si vous vous sentez plus à l'aise dans une interface graphique, ouvrez le Terminal et utilisez la commande suivante pour lancer un éditeur de texte :

   sudo gedit /etc/hosts
5. On peut vous demander votre mot de passe pour modifier le fichier. Une fois que la fenêtre s'est ouverte, ajoutez simplement la ligne « 69.63.181.12 www.facebook.com » à la fin du fichier et sauvegardez le en pressant « Ctrl+S » ou en sélectionnant Fichier > Enregistrer.


File Edit View Search Tools Documents Help
hosts
127.0.0.1 localhost
127.0.1.1 ubuntu-laptop
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
69.63.181.12 www.facebook.com
Plain Text Tab Width: 8 Ln 1, Col 1 INS

28. PROXYS HTTP

Les logiciels appelés applications proxy permettent à un ordinateur de procéder à des requêtes sur Internet à partir d'un autre ordinateur. Le type le plus commun d'applications proxy sont les proxys HTTP, qui manipulent des requêtes pour des sites Web, et les proxys SOCKS, qui manipulent des requêtes de connections d'un grand nombre d'applications. Dans ce chapitre, nous allons nous intéresser aux proxys HTTP et à leur fonctionnement.

LES BONS ET LES MAUVAIS PROXYS

Les applications proxy peuvent être utilisées par les opérateurs réseau pour censurer Internet ou pour contrôler ce que les utilisateurs font. Les applications proxy sont aussi un outil pour les utilisateurs qui font face à une censure et/ou à des restrictions du réseau.

Proxys restrictifs

Un opérateur réseau peut forcer les utilisateurs à accéder à Internet, ou du moins à des pages Web, seulement à travers un certain proxy. Il peut le programmer pour garder une trace de ce à quoi les utilisateurs accèdent et aussi refuser l'accès à certains sites ou services (blocage d'IP ou de ports). Dans ce cas, l'opérateur réseau peut utiliser un pare-feu pour bloquer les connections qui ne passent pas par ce proxy restrictif. Cette configuration est quelques fois un proxyforcé, car les utilisateurs sont forcés de l'utiliser.

Proxys de contournement

Une application proxy peut aussi être utile contre des restrictions. Si vous pouvez communiquer avec un ordinateur se situant dans un endroit non restreint qui fait fonctionner une application proxy, vous pouvez bénéficier de sa connectivité non restreinte. Quelques fois, un proxy est publiquement disponible à l'usage : il s’agit d’un proxy ouvert. Beaucoup des proxys ouverts sont bloqués dans les pays restreignant l'accès à Internet si les personnes administrant le réseau les connaissent.

OÙ TROUVER UNE APPLICATION PROXY

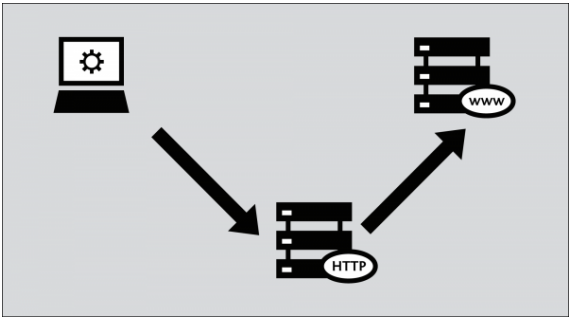
Il y a beaucoup de sites Web avec des listes d'applications proxy ouvertes. Une vue d'ensemble de tels sites est disponible sur http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists.

Beaucoup d'applications proxy ouvertes n'existent uniquement que pour quelques heures, il est donc important d'avoir un proxy à partir d'une liste qui a été récemment mise à jour.

RÉGLAGES DU PROXY HTTP

Pour utiliser une application proxy, vous devez configurer les préférences de proxy de votre système d'exploitation, ou au sein d'applications individuelles. Une fois que vous avez sélectionné un proxy dans les préférences proxy d'une application, celle-ci essaie de l'utiliser pour tout son accès à Internet.

Soyez sûrs que vous prenez bien note des préférences originelles de façon à ce que vous puissiez les restaurer. Si le proxy devient indisponible ou inatteignable pour quelque raison que ce soit, le logiciel qui est programmé pour l'utiliser cesse généralement de fonctionner. Dans ce cas, vous pourriez avoir besoin de restaurer les préférences originelles. Sous Mac OS X et quelques distributions Linux, ces préférences peuvent être configurées dans le système d'exploitation, et sera automatiquement appliqué à des applications telles que les navigateurs Internet ou les services de messagerie instantanée. Sous Windows et certaines autres distributions Linux, il n'y a pas d'endroit général où configurer les préférences de proxy, et chaque application doit être configurée manuellement. Gardez à l'esprit que, même si les préférences de proxy sont configurées dans un endroit général, il n'y a pas de garantie que les logiciels vont supporter ces préférences. Vérifiez les préférences de proxy de chaque logiciel. Normalement, seuls les navigateurs Internet peuvent directement utiliser un proxy HTTP.



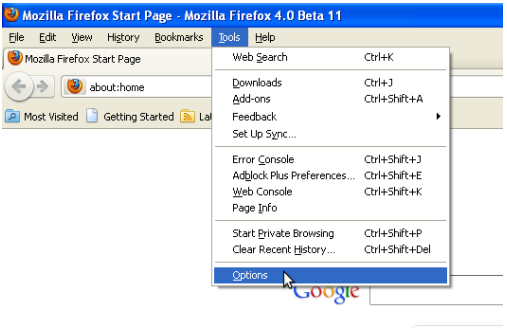
Les étapes ci-dessous décrivent comment configurer Microsoft Internet Explorer, Mozilla FireFox, Google Chrome et le client de messagerie instantanée gratuit et open source, Pidgin, pour utiliser un proxy. Si vous utilisez Firefox pour la navigation Internet, cela peut être plus simple d'utiliser le logiciel FoxyProxy, une alternative aux étapes ci-dessous. Si vous utilisez Tor, il est plus sûr d'utiliser le logiciel TorButton, fourni comme partie du téléchargement Tor Bundle, pour configurer votre navigateur pour l’utiliser.

Alors que les clients de messagerie e-mail tels que Microsoft Outlook et Mozilla Thunderbird peuvent être aussi configurés pour utiliser des proxys HTTP, le trafic actuel d'e-mails en envoyant et en allant chercher les e-mails utilise d'autres protocoles tels que POP3, IMAP et SMTP. Ce trafic ne passera pas à travers un proxy HTTP.

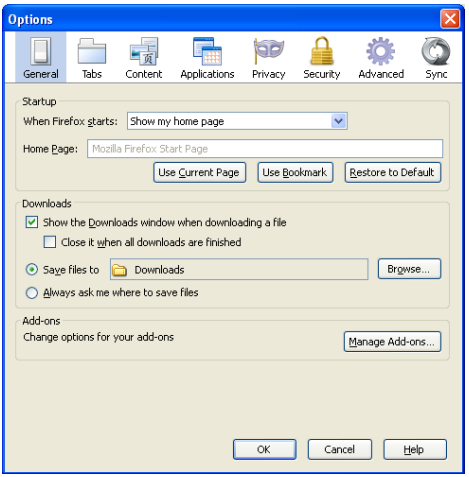
Mozilla Firefox

Pour configurer Firefox pour utiliser un proxy http :

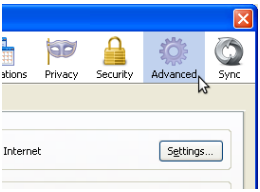
1. Sélectionnez « Outils > Options ».



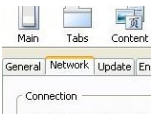
2. La fenêtre Options apparait :



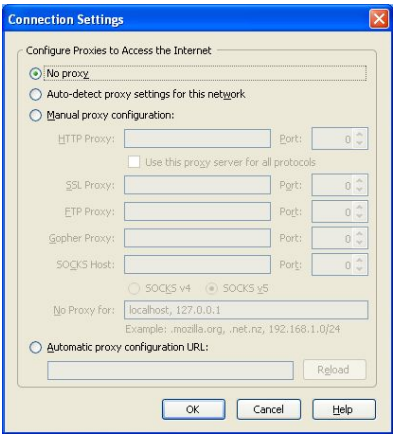
3. Dans la barre d'outils en haut de la fenêtre, cliquez sur « Avancés » :



4. Cliquez sur l'onglet « Réseau ».

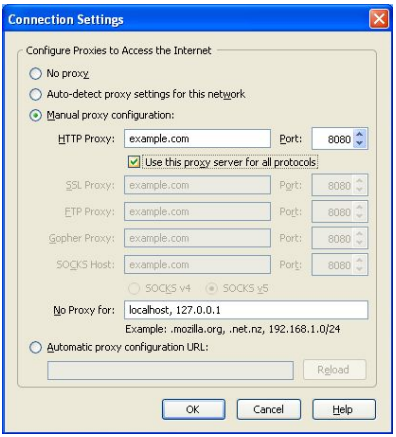


5. Cliquez sur « Préférences », Firefox affiche la fenêtre Préférences de connexion.



6. Sélectionnez « Configuration manuelle du proxy ». Les champs situés en dessous deviennent disponibles.

7. Saisissez l'adresse du proxy HTTP et son numéro de port et cliquez sur « OK ».



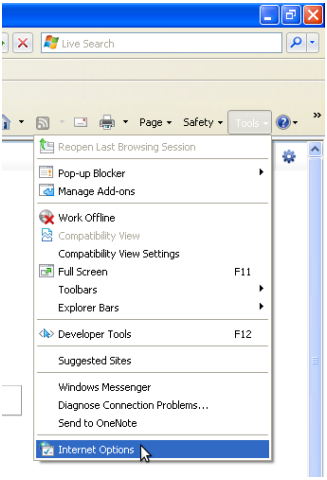
Si vous cliquez sur « Utiliser ce serveur proxy pour tous les protocoles », Firefox essayera d'envoyer les trafics HTTPS (HTTP sécurisé) et FTP à travers ce proxy. Cela peut ne pas fonctionner comme vous utilisez une application proxy publique, car beaucoup d'entre elles ne supportent pas les trafics HTTPS et FTP. Si, d'autre part, vos trafics HTTPS et/ou FTP sont bloqués, vous pouvez essayer de trouver une application proxy publique qui supporte ces trafics, et utiliser l'option « Utiliser ce serveur proxy pour tous les protocoles » dans Firefox.

Maintenant Firefox est configuré pour utiliser un proxy HTTP.

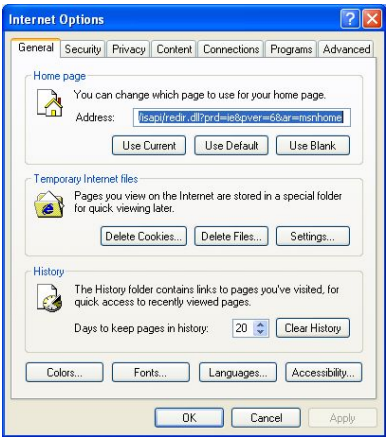
Microsoft Internet Explorer

Pour configurer Internet Explorer à utiliser un proxy http :

1. Sélectionnez « Outils > Options Internet » :

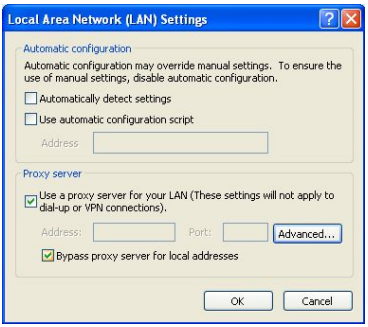


2. Internet Explorer affiche la fenêtre « Options Internet » ci-dessous :

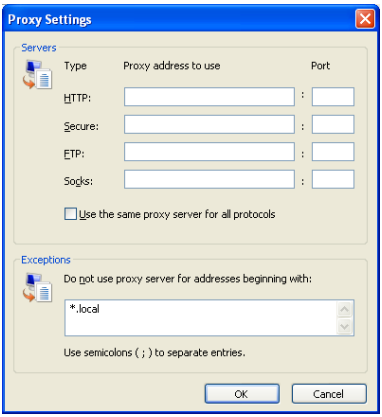


3. Cliquez sur l'onglet « Connexions ».

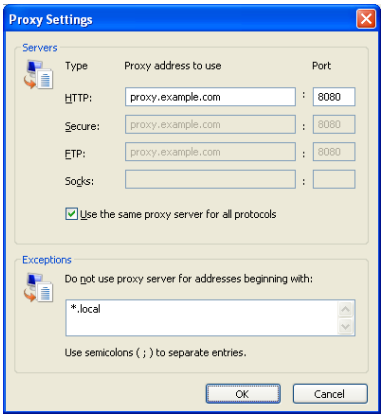
4. Cliquez sur « Préférences LAN ». La fenêtre Préférences LAN (réseau local) apparait :



5. Sélectionnez « Utiliser un serveur proxy pour mon réseau local » + IMAGE
6. Cliquez sur « Avancé ». La fenêtre de Préférences proxy apparait :



7. Saisissez l'adresse du proxy et son numéro de port dans la première ligne de champs.
8. Si vous cliquez sur « Utiliser ce serveur proxy pour tous les protocoles », Internet Explorer essaiera d'envoyer les trafics HTTPS (HTTP sécurisé) et FTP à travers ce proxy. Cela peut ne pas fonctionner comme vous utilisez une application proxy publique. Beaucoup d'entre elles ne supportent pas les trafics HTTPS et FTP. Si, d'autre part, vos trafics HTTPS et/ou FTP sont bloqués, vous pouvez essayer de trouver une application proxy publique qui supporte ces trafics, et utiliser l'option « Utiliser ce serveur proxy pour tous les protocoles » dans Internet Explorer.



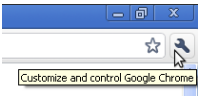
Maintenant, Internet Explorer est configuré pour utiliser un proxy HTTP.

Google Chrome

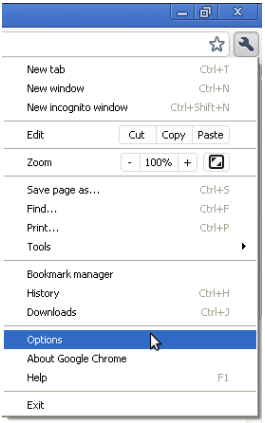
Google Chrome utilise la même connexion et les mêmes préférences proxy que le système d'exploitation Windows. Changer ces préférences affecte aussi Google Chrome aussi bien qu'Internet Explorer et d'autres programmes Windows. Si vous avez configuré votre proxy à travers Internet Explorer, vous n'avez pas besoin de suivre ces étapes pour configurer Chrome.

Suivez ces étapes pour configurer votre proxy http :

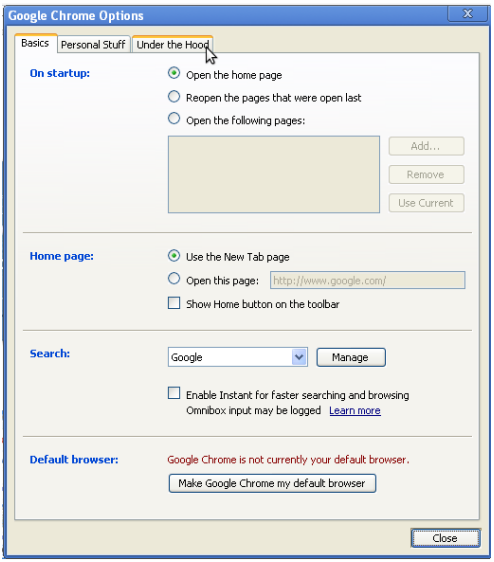
1. Cliquez sur le menu « Personnaliser et contrôler Google Chrome » à côté de la barre de saisie d'URL.



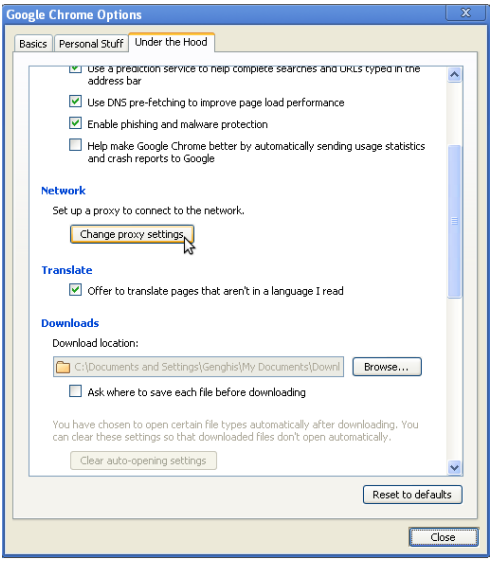
2. Cliquez sur « Options » :



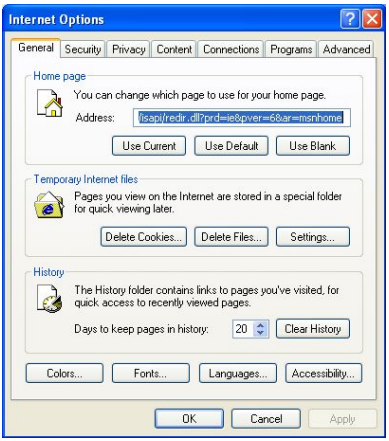
3. Dans la fenêtre d'options de Google Chrome, sélectionner l'onglet « A l'abri ».



4. Dans la section Réseau, cliquez sur le bouton « Changer les préférences de proxy » :



5. La fenêtre des Options va s'ouvrir. Suivez les étapes 2-8 de « Comment configurer un proxy HTTP sous Internet Explorer » (au dessus) pour finir de mettre en place votre proxy HTTP.



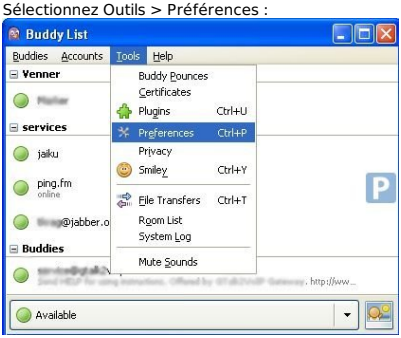
Chrome est maintenant configuré pour utiliser un proxy HTTP.

Client de messagerie instantanée Pidgin

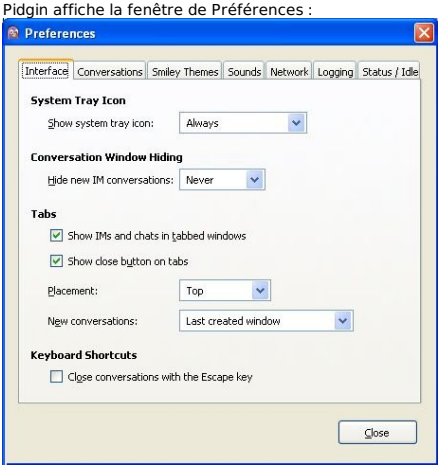
Certaines applications Internet autres que les navigateurs Internet peuvent aussi utiliser un proxy HTTP pour se connecter à Internet, et potentiellement contourner le blocage. Voici un exemple avec le client de messagerie instantanée Pidgin.

[Image : PidginConfigProxy1_1]

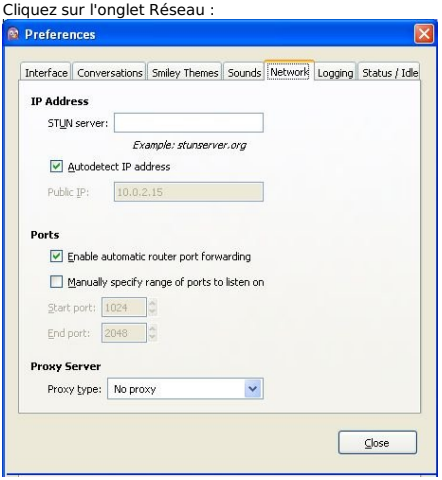
1. Sélectionnez Outils > Préférences :



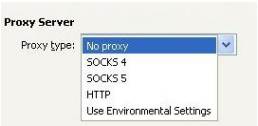
Pidgin affiche la fenêtre de Préférences :



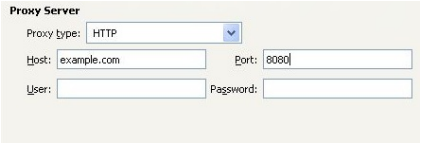
2. Cliquez sur l'onglet Réseau :



3. Comme type de proxy, sélectionnez HTTP, des champs additionnels apparaissent sous cette option.



4. Entrez l'adresse et le numéro de port de l'hôte de votre proxy HTTP.
5. Cliquez sur Fermer.



Pidgin est maintenant configuré pour utiliser un proxy HTTP.

Quand vous avez fini d'utiliser le proxy

Quand vous avez terminé d'utiliser un proxy, particulièrement sur un ordinateur partagé, restaurez les options que vous avez modifié à leurs précédentes valeurs. Autrement, ces applications continueront d'essayer d'utiliser le proxy. Cela peut devenir problématique si vous ne voulez pas que des personnes sachent que vous utilisez un proxy ou si vous étiez en train d'utiliser un proxy fourni par une application qui ne fonctionne pas tout le temps.

29. LA LIGNE DE COMMANDE

Avant de continuer votre lecture, il serait bon de savoir comment fonctionne la ligne de commande. Si vous n'êtes pas un familier, ce chapitre est destiné à vous aider à en assimiler les bases rapidement.

Bien des actions sur un ordinateur se produisent si rapidement que vous n'avez pas le temps d'y penser, mais chaque clic ou frappe au clavier est une commande à laquelle l'ordinateur réagit. Utiliser une ligne de commande revient au même, mais de façon plus consciente. Vous tapez une commande et pressez la touche « Entrée ». Par exemple :

date

Et l'ordinateur répond par : **Fri Feb 25 14:28:09 CET 2011**

Cette réponse est celle d'un ordinateur. Dans les chapitres suivants nous expliquerons comment demander la date dans un format plus complaisant. Nous expliquerons aussi en quoi utiliser cette commande dans des pays différents et dans plusieurs langues différentes change son résultat. L'idée à retenir ici est juste que vous avez interagi avec votre ordinateur.

LA LIGNE DE COMMANDE PEUT FAIRE BIEN MIEUX

La commande date, comme vue précédemment, faire piètre mesure par rapport au fait de regarder une horloge ou un calendrier. Le problème principal n'est pas l'aspect rebutant du résultat, mais l'impossibilité de faire quelque chose d'utile avec. Par exemple, si je regarde la date dans le but de l'insérer dans un document que je suis en train d'écrire, ou pour mettre à jour un évènement dans mon calendrier en ligne, je devrais tout d'abord la remettre en forme. Une ligne de commande peut faire bien mieux que cela.

Une fois que vous aurez appris les commandes basiques et quelques façon intéressantes de gagner du temps, vous trouverez dans ce livre plus d'informations pour envoyer la sortie d'une commande à une autre commande, automatiser certaines tâches, et sauvegarder des commandes pour une utilisation ultérieure.

QU'EST-CE QU'UNE LIGNE DE COMMANDE ?

Au début de ce chapitre nous utilisions le terme commande de manière très générale pour décrire une façon de dire que faire à votre ordinateur. Mais dans le contexte de ce livre, le terme commande a une signification particulière. C'est un fichier sur votre ordinateur et qui peut être exécuté, ou dans certain cas une action directement inclue dans votre ligne de commande. À l'exception des commandes inclues, l'ordinateur lance chacune des commandes en trouvant le fichier au nom correspondant et exécute ce fichier. Nous vous donnerons plus de détails à ce sujet en temps utile.

ENTRER UNE COMMANDE

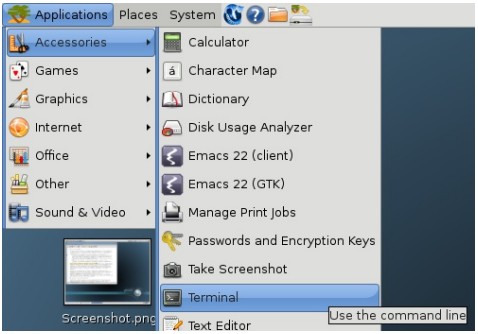
Pour pouvoir suivre ce livre, vous aurez besoin d'ouvrir un interpréteur de ligne de commande ou une interface de ligne de commande (appellée « shell » ou « terminal » sous GNU/Linux) sur votre ordinateur. Sur les anciens ordinateurs, la ligne de commande était présentée à l'utilisateur sitôt après s'est identifié. Aujourd'hui à peu près tout le monde, à part peut-être un administrateur système professionnel, attend de son système de lui proposer une interface graphique, même si l'interface en ligne de commande reste plus simple et plus rapide à utiliser dans un certain nombre de cas. Nous allons donc vous apprendre à vous servir d'un shell.

TROUVER UN TERMINAL

Vous pouvez obtenir une interface de terminal depuis votre bureau, mais il pourrait être plus simple de quitter le bureau et utiliser l'interface textuelle originelle. Utilisez la combinaison de touches <Ctrl + Alt + F1>. Vous allez obtenir un écran à peu près vide avec une invite de connexion. Entrez votre identifiant et votre mot de passe. Vous pouvez utiliser d'autres terminaux avec <Ctrl + Alt + F2> et ainsi de suite, lancer des sessions pour des utilisateurs différents (ou identiques) pour les tâches de votre choix. À n'importe quel moment, vous pouvez passer de l'un à l'autre en utilisant la combinaison de touches <Ctrl + Alt + F#> correspondante. L'une de ces combinaisons, probablement avec F7 ou F8, vous ramènera au bureau. Dans un terminal textuel, vous pouvez utiliser votre souris (si votre système possède gpm) pour sélectionner un mot, une ligne ou un bloc de lignes. Vous pourrez alors coller ce morceau de texte dans ce terminal, ou dans un autre terminal.

Les distributions GNU/Linux sont fournies avec différentes interfaces graphiques (GUI) offrant des esthétiques différentes et utilisant des manières différentes de nommer les composants. Celles tournant juste au-dessus du système d'exploitation se nomment « environnements de bureau ». GNOME, KDE et Xfce sont les plus utilisés. Presque tous les environnements de bureau fournissent un programme simulant une ligne de commande textuelle. Sur votre bureau, essayez de chercher dans les menus Applications un programme appelé « Terminal ». Souvent il se trouve dans le menu « Accessoires », ce qui n'est pas réellement approprié étant donné qu'une fois que vous aurez lu ce livre, vous allez probablement beaucoup vous servir du terminal dans votre utilisation quotidienne.

Sous GNOME sélectionnez « Applications > Accessoires > Terminal »



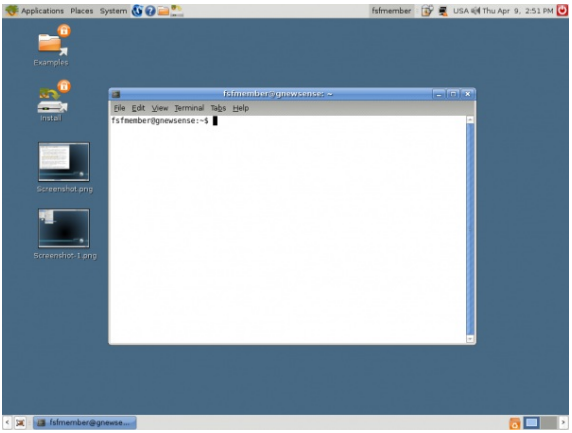
Sous KDE, sélectionnez « Menu K > Système > Terminal »

Sous Xfce, sélectionnez Menu « Xfce > Système > Terminal »

Quelque soit son emplacement, vous trouverez sans doute un terminal.

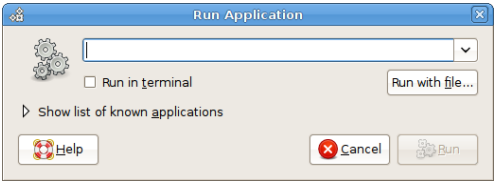
Quand vous lancez votre terminal, une fenêtre vide s'affiche. Vous êtes censé savoir quoi faire, nous allons vous montrez l'exemple.

L'illustration suivante montre la fenêtre de terminal ouverte dans l'environnement de bureau GNOME.



LANCER UNE COMMANDE INDIVIDUELLE

Bon nombre d'interfaces graphiques fournissent aussi une petite boite de dialogue dont le nom doit ressembler à « Lancer une commande ». Elle contient une petite zone de texte où vous pouvez taper une commande puis la valider en appuyant sur « Entrée ».



Pour lancer cette boite de dialogue, essayez la combinaison de touches <Alt + F2>, ou cherchez-la dans le menu des applications. Vous pouvez utiliser cette boite comme un raccourci pour lancer rapidement un programme dans un terminal installé sur votre ordinateur. Si vous travaillez sur un ordinateur dont vous n'êtes pas familier et que vous ne connaissez pas le nom du terminal par défaut, essayez d'y taper xterm pour lancer un terminal minimaliste (sans menus pour changer les couleurs ou la police d'écriture). Si vous avez désespérément besoin de ces fioritures :

- sous GNOME le terminal par défaut doit probablement être gnome-terminal
- sous KDE ce doit être konsole
- sous Xfce essayez terminal, ou la version spécifique à votre version de Xfce, par exemple xfce4-terminal sous Xfce4.

COMMENT NOUS VOYONS LES COMMANDES DE CE CHAPITRE

Il y aune convention commune dans les livres sur la ligne de commande. Lorsque vous démarrez un terminal, vous voyez un petit message indiquant que le terminal est prêt à accepter votre commande. Ce message est appelé « une invite », il peut être aussi simple que :**$**

Une fois que vous tapez votre commande et appuyez sur « retour » ou sur la touche « Entrée », le terminal affiche la sortie de la commande, s'il y a lieu, suivie par une autre, rapidement. Alors mon action antérieure serait montré dans le livre comme celle-ci :
$ **date**
Thu Mar 12 17:15:09 EDT 2009
$

Vous devez savoir comment interpréter des exemples.

Tout ce que vous tapez ici est la date. Ensuite, appuyez sur la touche « Retour ». Le mot date dans l'exemple est imprimé en caractères gras pour indiquer que c'est quelque chose que vous tapez. Le reste est sorti sur le terminal.

30. OPENVPN

OpenVPN est un logiciel VPN, Virtual Private Network, reconnu, gratuit, et open-source. Il fonctionne sur la plupart des versions de Windows (un support de Windows vista est attendu sous peu), Mac OS X et Linux. OpenVPN utilise SSL, ce qui veut dire qu'il utilise le même type de chiffrement que lorsqu'on visite des sites web où l'adresse commence par HTTPS.

INFORMATIONS GÉNÉRALES

Système d'exploitation supporté	
Langues	Anglais, Allemand, Italien, Français, et Espagnol
Site Web	https://openvpn.net/index.php/open-source.html
Support	Forum: https://forums.openvpn.net

OpenVPN n'est pas idéal pour une utilisation temporaire dans un cyber-café ou ailleurs sur des ordinateurs publics sur lesquels vous ne pouvez pas installer de logiciels.

Pour une présentation plus générale des VPN et des services qui fonctionnent directement, lisez le chapitre « Services VPN » de ce guide.

Dans un système OpenVPN, un ordinateur fait office de serveur qui ne subit pas la censure, et un ou plusieurs clients. Le serveur doit être configuré pour être accessible depuis Internet, non bloqué par un pare-feu, et avec une adresse IP publique (à certains endroits, la personne gérant le serveur peut avoir à le demander à leur fournisseur d'accès). Chaque client se connecte au serveur et crée un tunnel VPN à travers lequel le trafic du client passera.

Il y a des fournisseurs d'OpenVPN commerciaux, comme WiTopia http://witopia.net/personalmore.html auprès desquels vous pouvez acheter un accès à un serveur OpenVPN pour un prix d'environ 5-10 dollars US par mois. Ces fournisseurs vont également vous aider à installer et configurer OpenVPN sur votre ordinateur. Une liste des fournisseurs commerciaux est disponible à cette adresse : http://en.cship.org/wiki/VPN.

OpenVPN peut aussi être utilisé par un tiers de confiance, à un endroit non filtré, fournissant ainsi un serveur OpenVPN à un ou plusieurs clients et faisant transiter leur trafic vers son ordinateur avant de continuer vers Internet. Configurer ça correctement peut néanmoins se révéler compliqué.

ASTUCES POUR CONFIGURER OPENVPN

Pour configurer votre serveur et client, lisez la documentation fournie par OpenVPN sur http://openvpn.net/index.php/documentation/howto.html. Si vous voulez l'utiliser pour visiter des sites bloqués, les remarques suivantes sont importantes :

Client

GUI est une interface graphique disponible pour Windows. Elle devrait rendre le lancement et l'arrêt d'OpenVPN simple, et qui vous permet également de le configurer pour qu'il aille sur Internet en utilisant un proxy HTTP. Pour télécharger l'interface graphique, allez à cette adresse http://openvpn.se.

Pour configurer OpenVPN avec un serveur proxy sous Linux ou Mac OS X, lisez la section correspondante sur le site http://openvpn.net/index.php/documentation/howto.html#http.

Serveur

- Quand vous choisissez entre router et faire un pont, il n'y a pas d'avantage supplémentaire à gagner en configurant les ponts quand vos clients veulent juste l'utiliser pour contourner la censure d'Internet. Choisissez le routage.
- Accordez une attention spéciale à la section du guide qui explique comment s'assurer que tout le trafic du client est transmis à travers le serveur. Sans cette configuration le système ne vous aidera pas à visiter des pages bloquées http://openvpn.net/index.php/documentation/howto.html#redirect.
- Si le client est derrière un pare-feu très restrictif, et que le port d'openVPN par défaut est bloqué, il est possible de changer le port par contre OpenVPN. Une option est d'utiliser le port 443, qui est habituellement utilisé pour les sites sécurisés (HTTPS), et de régler le protocole par défaut à TCP au lieu d'UDP. Avec cette configuration, il est difficile pour les opérateurs de pare-feu de distinguer le trafic généré par OpenVPN et le trafic web sécurisé. Pour ça, en haut des fichiers de configuration du client et du serveur, remplacez « proto udp » par « proto tcp » et « port 1194 » par « port 443 ».

AVANTAGES ET RISQUES

Une fois installé et configuré correctement, OpenVPN peut fournir un moyen efficace pour contourner les filtres d'Internet. Comme tout le trafic est chiffré entre le client et le serveur, et peut passer à travers un seul port, il est très compliqué de le distinguer de n'importe quel trafic web sécurisé, comme des données allant à un site de boutique en ligne ou d'autres services chiffrés.

OpenVPN peut être utilisé pour tous les types de trafic internet, incluant le trafic web, l'e-mail, les messageries instantanées, et la VoIP.

OpenVPN fournit également un haut niveau de protection contre la surveillance, tant que vous faites confiance au détenteur du serveur et que vous avez suivi les instructions de la documentation sur la gestion des certificats et des clefs. Souvenez-vous que le trafic est seulement chiffré jusqu'au serveur OpenVPN, après lequel il passe en clair sur Internet.

Le point négatif principal d'OpenVPN est sa difficulté d'installation et de configuration. Il requiert également un accès à un serveur dans une région non censurée. OpenVPN n'assure également pas l'anonymat avec certitude.

31. TUNNELS SSH

Le SSH, le Secure Shell, est un protocole standard qui chiffre les communications entre votre ordinateur et un serveur. Ce chiffrement permet d'empêcher que ces communications soient inspectées ou modifiées par les opérateurs réseau. SSH est utilisé en général pour sécuriser un grand nombre de types de communications, la connexion à un serveur ou les transferts de fichiers (scp ou SFTP).

SSH est particulièrement pratique pour contourner la censure car il fournit des tunnels chiffrés et fonctionne comme un client proxy classique. Les censeurs peuvent ne pas avoir envie de bloquer SSH complètement car il a de nombreuses utilisations que le contournement de la censure. Il est, par exemple, utilisé par les administrateurs système pour administrer leur serveurs sur Internet.

Utiliser SSH nécessite un compte sur un serveur, généralement un serveur Unix ou Linux. Pour contourner la censure, ce serveur doit avoir un accès non restreint à Internet, et, si possible, être géré par un tiers de confiance. Certaines compagnies vendent également des comptes sur leurs serveurs, et beaucoup de formules d'hébergement web proposent un accès SSH. Une liste de comptes shells est disponible sur cette page : http://www.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers On y trouve des comptes shells pour environ 2-10 dollars US par mois.

Un client SSH appelé OpenSSH est déjà installé sur la plupart des ordinateurs Unix, Linux, et Mac OS comme un programme en ligne de commande appelé par « ssh » dans un terminal. Pour Windows, vous pouvez également obtenir une implémentation libre de SSH appelée PuTTY.

Toute version récente de SSH supporte la création d'un proxy SOCKS qui permet à un navigateur et un large panel de logiciels d'utiliser la connexion SSH pour communiquer avec un Internet non filtré. Dans cet exemple, nous allons décrire uniquement cet usage de SSH. Les étapes ci-dessous mettent en place un proxy SOCKS sur le port 1080 de votre ordinateur.

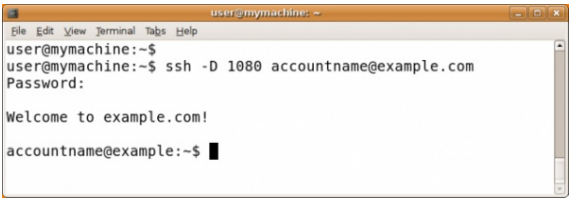
LIGNE DE COMMANDE POUR LINUX/UNIX ET MACOS (AVEC OPENSSH)

OpenSSH est disponible sur http://www.openssh.com mais est généralement préinstallé sur les ordinateurs Linux/Unix et MacOS.

La commande ssh que vous allez lancer contient un numéro de port local (typiquement, 1080), un nom de serveur, et un nom d'utilisateur. Elle ressemble à ça :

ssh -D numerodeportlocal nomdutilisateur@nomduserveur

Exemple :



On va vous demander votre mot de passe, puis vous serez connecté au serveur. En utilisant l'option -D, un proxy SOCKS local sera créé et existera tant que vous serez connecté. Important : vous devriez maintenant vérifier la clef de l'hôte et configurer vos applications, sinon vous n'utiliserez pas le tunnel que vous avez créé !

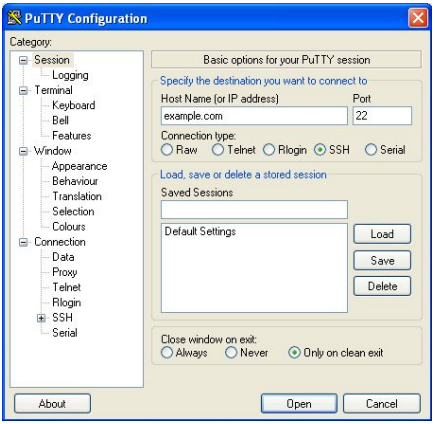
INTERFACE GRAPHIQUE SOUS WINDOWS

(AVEC PUTTY

PuTTY est disponible sur :
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

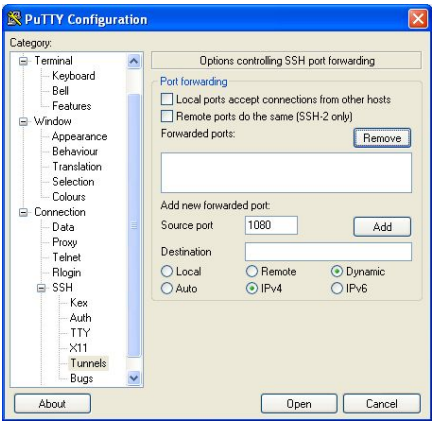
Vous pouvez sauvegarder le programme putty.exe sur votre disque dur pour une utilisation postérieure, ou le lancer directement depuis le site web, ce qui est souvent possible sur un ordinateur en accès libre, comme dans une bibliothèque ou un cybercafé.

Quand vous lancez PuTTY, un dialogue de configuration de la session apparaît. Commencez par entrer le nom de l'hôte (l'adresse) du serveur SSH auquel vous allez vous connecter (ici, example.com). Si vous connaissez uniquement l'adresse IP ou si un blocage DNS vous empêche d'utiliser le nom de l'hôte, vous pouvez utiliser l'adresse IP à la place. Si vous allez souvent utiliser cette configuration, vous pouvez créer un profil PuTTY qui sauvegardera ces options tout comme les options décrites ci-dessous afin qu'elles soient utilisées à chaque fois.



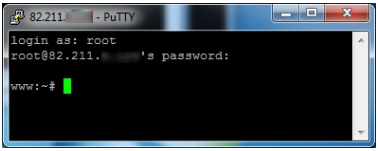
Dans la liste des catégories, choisissez « Connexion > SSH > Tunnels ».

Entrez 1080 comme port source, et cochez les cases Dynamique et IPv4.



Cliquez maintenant sur « Ajouter », puis sur « Ouvrir ». Une connexion s'établit avec le serveur, et une nouvelle fenêtre apparait, vous demandant votre nom d'utilisateur et mot de passe.

Entrez ces informations et vous serez connecté sur le serveur, et recevrez une ligne de commande. Le proxy SOCKS est alors établi. Important : vérifiez la clé de l'hôte et configurer vos applications, sinon vous n'utiliserez pas le tunnel que vous avez créé !



VÉRIFICATION DE LA CLÉ DE L'HÔTE

La première fois que vous vous connectez à un serveur, on devrait vous demander de confirmer l'empreinte de la clef pour ce serveur. L'empreinte de la clef est une longue séquence de lettres et de chiffres (de l'hexadécimal) comme 57:ff:c9:60:10:17:67:bc:5c:00:85:37:20:95:36:dd qui identifie de manière sécurisée un serveur particulier. La vérification de cette empreinte est une mesure de sécurité qui permet de confirmer que vous communiquez bien avec le serveur avec lequel vous penser communiquer, et que la connexion chiffrée ne peut pas être interceptée.

SSH ne fournit pas de moyen de vérifier ça de manière automatique. Pour obtenir les bénéfices de ce mécanisme de sécurité, vérifiez la valeur de l'empreinte de la clef avec l'administrateur du serveur que vous utilisez, ou demander à un tiers de confiance de tenter de se connecter au même serveur pour voir s'il obtient la même empreinte.

La vérification des empreintes de clés est importante car elle permet de s'assurer que SSH protège le secret de vos conversations contre l'observation, mais elle n'est pas nécessaire si vous voulez uniquement contourner la censure et n'êtes pas concerné par le fait que les opérateurs réseaux puissent voir le contenu de vos communications.

CONFIGURER LES APPLICATIONS POUR QU'ELLES UTILISENT LE PROXY

Le proxy créé dans les étapes ci-dessus devrait fonctionner jusqu'à ce que vous fermiez le logiciel SSH. Si la connexion avec le serveur est interrompue, vous devrez répéter ces étapes pour réactiver le proxy.

Une fois que le proxy fonctionne, vous devez configurer vos logiciels pour l'utiliser. En suivant les étapes ci-dessus, le proxy sera un proxy SOCKS situé sur localhost, port 1080 (aussi appelé 127.0.0.1, port 1080). Vous devriez vous assurer que vos applications sont configurées pour éviter les fuites DNS, ce qui rendrait SSH moins efficace pour protéger vos données et contourner la censure.

PLUS D'OPTIONS

Jusqu'ici, toutes ces commandes affichent une ligne de commande sur la machine distante depuis laquelle vous pouvez exécuter n'importe laquelle des commandes disponibles sur cette machine. Exécuter une seule commande sur la machine distante, puis retourner à la ligne de commande de votre machine locale est possible : Placez la commande à faire exécuter par la machine distante entre simple quotes.

$ ssh utilisateurdistant@autremachine.domaine.org 'mkdir /home/utilisateurdistant/newdir'

Parfois vous aurez besoin d'exécuter des commandes qui prennent du temps sur la machine distante, mais vous n'êtes pas sûr d'avoir assez de temps pendant votre session actuelle. Si vous fermez la connexion distante avant la fin de l'exécution d'une commande, cette dernière sera abandonnée. Pour éviter de perdre votre travail, lancez via ssh une session screen distante, puis détachez-la et reconnectez-la quand vous voudrez. Pour détacher une session screen, fermez simplement la connexion distante : une session screen détachée continuera à s'exécuter sur la machine distante.

SSH fournit beaucoup d'autres options. Vous pouvez également configurer votre système favori pour vous permettre de vous connecter ou lancer des commandes sans préciser de mot de passe à chaque fois. L'installation est compliquée mais vous pouvez gagner beaucoup de temps de frappe. Essayez de faire quelques recherches sur "ssh-keygen", "ssh-add", et "authorized_keys".

SCP : COPIE DE FICHIERS

Le protocole SSH va bien au-delà de la commande ssh basique. Une commande particulièrement pratique basée sur le protocole SSH est scp, la copie de fichier sécurisée (secure copy command). L'exemple suivant copie un fichier depuis le dossier courant de votre machine locale vers le dossier /home/me/stuff sur une machine distante.

$ scp myprog.py me@autremachine.domaine.org:/home/me/stuff

Soyez prévenus que cette commande écrasera tout fichier déjà présent avec le nom /home/me/stuff/myprog.py. (Ou bien vous aurez un message d'erreur s'il y a déjà un fichier de ce nom et que vous n'avez pas les droits pour l'écraser) Si /home/me est votre dossier personnel, le dossier cible peut être abrégé.

$ scp myprog.py me@autremachine.domaine.org:stuff

Vous pouvez aussi facilement copier dans l'autre direction : depuis la machine distante vers votre machine locale.

$ scp me@autremachine.domaine.org:docs/interview.txt yesterday-interview.txt

Le fichier sur la machine distante est interview.txt dans le sous-dossier docs de votre dossier personnel. Le fichier sera copié vers yesterday-interview.txt dans le dossier personnel de votre système local.

scp peut être utilisé pour copier un fichier d'une machine distante à une autre.

$ scp utilisateur1@hote1:file1 utilisateur2@hote2:otherdir

Pour copier récursivement tous les fichiers et sous-dossiers d'un dossier, utilisez l'option -r.

$ scp -r utilisateur1@hote1:file1 utilisateur2@hote2:otherdir

Lisez la page de manuel de scp pour plus d'options.

RSYNC : TRANSFERTS ET SAUVEGARDES EN MASSE AUTOMATISÉES

Rsync est une commande très pratique qui conserve un dossier distant synchronisé avec un dossier local. Elle est mentionnée ici car c'est une commande pratique pour faire du réseau, comme ssh, et parce que le protocole SSH est recommandé comme couche de transmission pour Rsync.

L'exemple ci-dessous est simple et pratique. Il copie les fichiers depuis votre dossier /home/myname/docs vers un dossier appelé backup/ dans votre dossier utilisateur sur le serveur quantum.example.edu. Rsync minimise les copies nécessaires à travers diverses vérifications compliquées.

$ rsync -e ssh -a /home/myname/docs
me@quantum.example.edu:backup/

L’option -e de ssh utilise le protocole SSH pour la transmission, comme ce qui est recommandé. L’option -a (pour « archive ») copie tout ce qui est dans le dossier spécifié. Si vous voulez supprimer les fichiers du système local pendant qu’ils sont copiés, ajoutez l’option --delete.

Se simplifier la vie quand on utilise SSH souvent

Si vous utilisez SSH pour vous connecter à beaucoup de serveurs différents, vous allez souvent faire des erreurs en tapant de travers des noms d’utilisateurs ou même des noms de domaines (imaginez-vous en train de retenir 20 combinaisons différentes utilisateur/domaine). Heureusement, SSH permet de gérer facilement les sessions dans un fichier de configuration.

Le fichier de configuration est caché dans votre dossier personnel sous le dossier .ssh (le chemin complet est quelque chose comme /home/jsmith/.ssh/config - si le fichier n’existe pas vous pouvez le créer). Utilisez votre éditeur préféré pour ouvrir ce fichier et préciser les serveurs comme ceci :

```
Host dev
HostName example.com
User fc
```

Vous pouvez configurer ainsi plusieurs serveurs dans votre fichier de configuration, et après l’avoir sauvegardé, vous connecter au serveur appelé « dev » via la commande suivante :

```
$ ssh dev
```

Souvenez-vous, plus vous utilisez ces commandes, plus vous gagnez du temps.

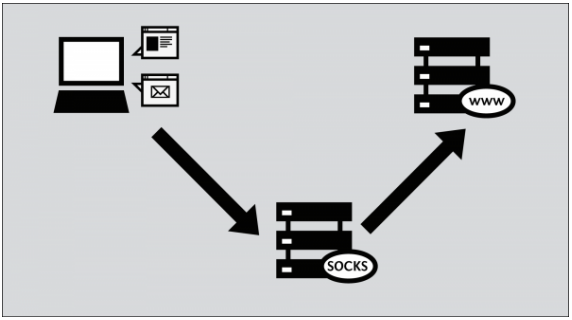
CommentContournerLaCensureSurInternet: ProxySocks

PROXY SOCKS

Derrière le terme SOCKS se cache un protocole internet qui correspond à un certain type de serveur Proxy. Par défaut les proxys SOCKS écoutent sur le port 1080. Ils peuvent aussi écouter sur d'autres ports. La principale différence entre un proxy HTTP et un proxy SOCKS est qu'un proxy SOCKS ne sert pas seulement à naviguer sur le Web mais aussi à utiliser d'autres applications comme les jeux vidéo, les logiciels de transferts de fichiers ou de messageries instantanée. Comme le VPN, ils utilisent un tunnel sécurisé.

Les principales versions de SOCKS sont 4, 4a et 5. La version 4 nécessite une adresse IP pour établir la connexion, ce qui veut dire que la résolution DNS doit être effectuée par le client. Ce prérequis ne permet pas de satisfaire la majorité des besoins de contournement de la censure. La version 4a utilise en général les noms d'hôtes. La version 5 introduit de nouvelles technologies comme l'authentification, le support des protocoles UDP et IPv6 mais utilise massivement les adresses IP ce qui en fait une solution imparfaite : Voir la section « fuites DNS » à la fin de ce chapitre.

Une grande variété de logiciels peut bénéficier des avantages des proxys SOCKS pour contourner les filtres ou toute autre restriction affectant les navigateurs comme un logiciel basé sur Internet, la messagerie et la messagerie instantanée.



Malgré l'existence de proxy SOCKS publics, un proxy SOCKS tourne en général localement sur la machine sous la forme d'un logiciel. Les tunnels SOCKS sont très flexibles, de nombreux logiciels utilisés pour contourner la censure créent un proxy localement, en utilisant le nom de machine « localhost » ou l'adresse IP locale lui étant associée : 127.0.0.1. Ce proxy local permet aux applications comme un navigateur Web de bénéficier des avantages d'un logiciel de contournement de la censure. Par exemple des outils comme Tor, Your-freedom et les tunnels SSH mis en place avec PuTTY utilisent ce principe.

Un T-Shirt pour les amateurs de proxy locaux (vous en voulez un ?)

Pour utiliser une application avec un proxy et contourner la censure, vous devez la paramétrer pour qu'elle utilise ce proxy pour communiquer avec les autres systèmes connectés à Internet.

Certaines applications ne supportent pas le fonctionnement au travers d'un proxy car leurs développeurs n'ont pas ajouté le support de communication via proxy. Beaucoup d'applications peuvent toutefois fonctionner avec un proxy SOCKS en utilisant le logiciel socksifier. Quelques logiciels fonctionnant avec socksifier :

- tsocks (http://tsocks.sourceforge.net)sur Unix/Linux
- WideCap (http://www.widecap.com) sur Windows
- ProxyCap (http://www.proxycap.com) sur Windows

CONFIGURER VOS APPLICATIONS

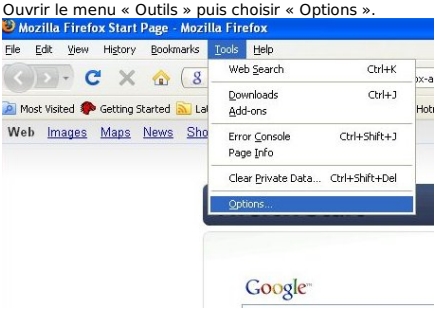
Configurer une application pour utiliser un proxy SOCKS ressemble beaucoup à la configurer pour l'utilisation d'un proxy HTTP. Les applications supportant les proxys SOCKS disposent d'un champ ou d'une fenêtre différente que celui réservé au proxy HTTP. Certaines applications vous demanderont de choisir la version du proxy SOCKS à utiliser : soit SOCKS 4 soit SOCKS 5. En général, SOCKS 5 est le meilleur choix. Certains proxys SOCKS ne fonctionnent cependant qu'avec SOCKS 4.

Certaines applications, comme Mozilla Firefox, autorisent l'utilisation du proxy HTTP et du proxy SOCKS en même temps. Dans ce cas, un navigateur réagissant normalement choisira le proxy HTTP en priorité et réservera le proxy SOCKS pour d'autres types de trafics comme le streaming vidéo.

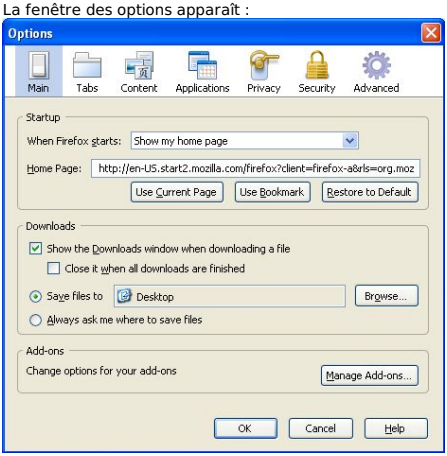
Mozilla Firefox

Configurer Mozilla Firefox pour utiliser un proxy SOCKS :

1. Ouvrir le menu « Outils » puis choisir « Options ».

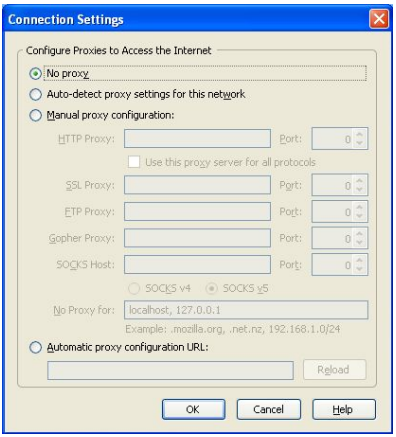


2. La fenêtre des options apparaît :



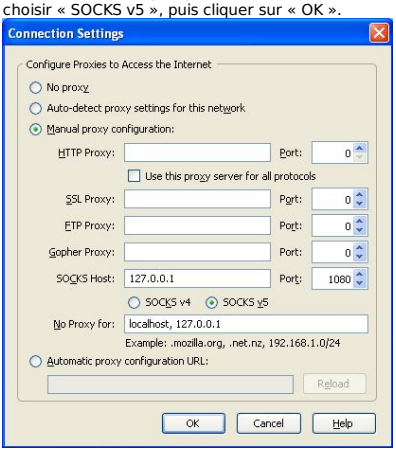
3. Dans la barre d'outils en haut de la fenêtre des options, choisir « Avancé ».

4. Cliquer sur l'onglet « Réseau ».
5. Cliquer sur le bouton « Paramètres ». La fenêtre de paramètres de connexion apparaît.



6. Sélectionner le radiobouton « Configuration manuelle du proxy ». Les champs en dessous de ce radiobouton doivent s'activer.

7. Entrez l'adresse du proxy SOCKS, entrer le numéro du port et choisir « SOCKS v5 », puis cliquer sur « OK ».



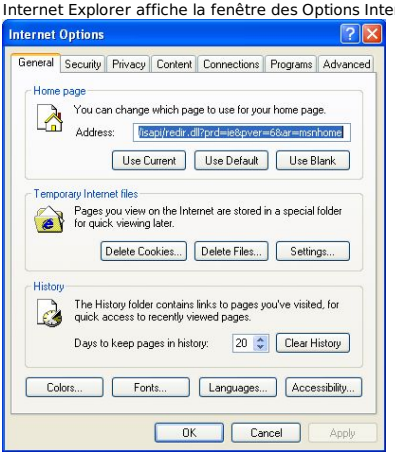
Maintenant, Firefox est configuré pour utiliser un proxy SOCKS.

Microsoft Internet Explorer

Configurer Internet Explorer pour utiliser un proxy SOCKS :

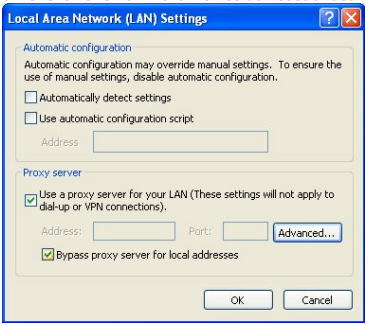
1. Ouvrir le menu « Outils » puis cliquer sur « Options Internet ».

2. Internet Explorer affiche la fenêtre des Options Internet.

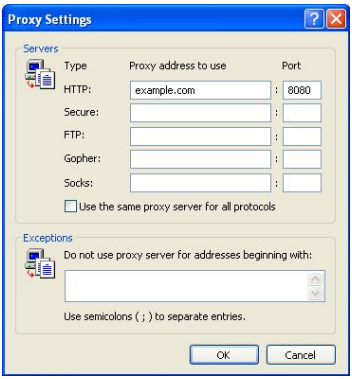


3. Cliquer sur l'onglet « Connexions ».

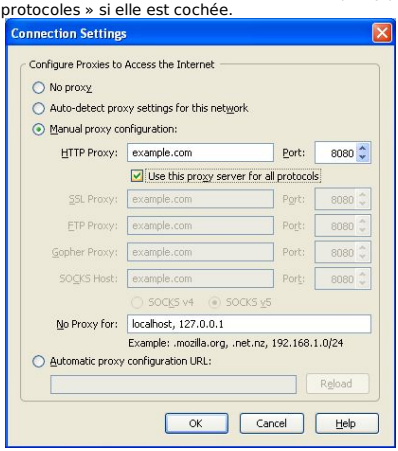
4. Cliquer sur le bouton « Paramètres réseau ». Internet Explorer affiche la fenêtre « Paramètres du réseau local ».



5. Cocher la case « Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliquent pas aux connexions d'accès à distance ou VPN) » et cliquer sur « Avancé ». Internet Explorer affiche la fenêtre des Paramètres du poxy.



6. Décocher la case « Utiliser le même serveur proxy pour tous les protocoles » si elle est cochée.



7. Dans la ligne « Socks », entrer l'adresse du proxy à utiliser le numéro de port à utiliser. Cliquer sur « OK ».

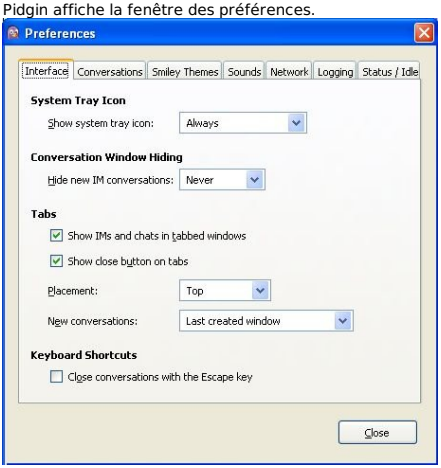
Maintenant, Internet Explorer est configuré pour utiliser un proxy SOCKS.

Configurer un proxy SOCKS pour d'autres applications

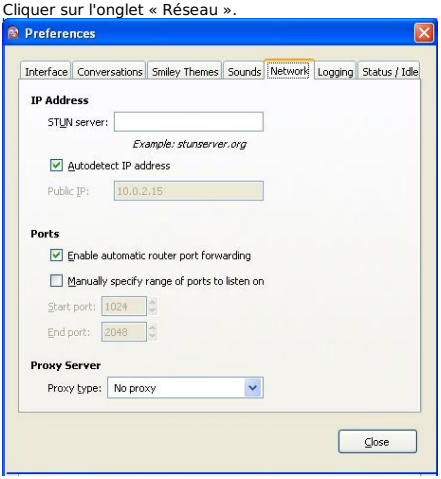
Beaucoup d'applications utilisant Internet peuvent utiliser un serveur Proxy pour accéder à Internet et, potentiellement, contourner son blocage. Voici un exemple avec le client de messagerie instantanée Pidgin. Cet exemple est typique mais les étapes pour configurer votre logiciel pour utiliser un proxy SOCKS peuvent différer.

1. Ouvrir le menu « Outils », puis cliquer sur « Préférences ».

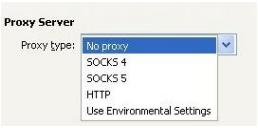
2. Pidgin affiche la fenêtre des préférences.



3. Cliquer sur l'onglet « Réseau ».



4. En type de Proxy, choisir l'option « SOCKS 5 ». Des champs supplémentaires apparaissent sous cette option.



5. Entrer l'adresse du serveur proxy SOCKS et le numéro de port de celui-ci.

6. Cliquer sur « Fermer ».

Pidgin est maintenant configuré pour utiliser un proxy SOCKS.

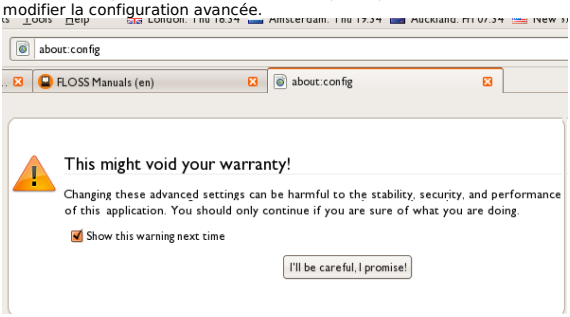
Quand vous avez fini d'utiliser le proxy

Quand vous avez fini d'utiliser le proxy, en particulier si vous utilisiez un ordinateur qui ne vous appartient pas, retourner dans les paramètres de votre logiciel et restaurez les valeurs qui étaient présentes avant votre passage. L'application pourrait continuer à utiliser le serveur proxy, ce qui pose problème si vous ne voulez pas que d'autres personnes sachent que vous avez utilisé un proxy ou si vous utilisiez un logiciel de contournement en local (ce qui empêcherait de faire fonctionner l'application si le logiciel de contournement n'est pas démarré).

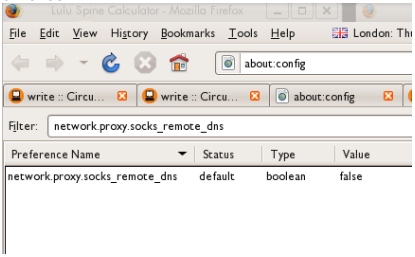
FUITES DNS

Certaines applications, supportant le fonctionnement avec un proxy SOCKS peuvent ne pas faire passer systématiquement toutes leurs communications par ce proxy. Par exemple, les requêtes DNS (Domain Name System) peuvent être effectuées sans passer par le proxy. Cela s’appelle une fuite DNS. Cette fuite peut représenter un problème pour la vie privée et peut vous laisser vulnérable à un blocage par DNS alors qu'un proxy est habituellement en mesure de contourner ce type de blocage. Ce genre de vulnérabilité par fuite DNS peut varier pour un logiciel selon les versions. Mozilla Firefox est, par défaut, vulnérable aux fuites DNS avec sa configuration par défaut. Pour éviter cela, il est possible de modifier la configuration de façon permanente pour éviter les fuites DNS:

1. Dans la barre d'adresse de Firefox, saisir `about:config` comme vous le faites habituellement pour saisir une URL. Vous devez voir un message d'avertissement vous indiquant que vous allez modifier la configuration avancée.



2. Si nécessaire, cliquer sur « je ferai attention, promis ! » pour confirmer que vous voulez changer les paramètres du navigateur. Le navigateur affiche une liste d'options de configuration.
3. Dans le champ « Filtre », entrez « network.proxy.socks_remote_dns ». Seule cette option est affichée.



4. Si ce paramètre est à la valeur *false*, effectuer un double clic sur le paramètre. La valeur doit passer à *true*. Firefox est maintenant configuré pour prévenir les fuites DNS. Une fois ce paramètre affiché avec une valeur à *true*, la configuration est automatiquement sauvegardée.

Il n'y a pas de documentation disponible pour prévenir des fuites DNS avec Microsoft Internet Explorer sans utiliser un programme tiers.

Au moment de la rédaction de ce guide, il n'y a aucune fuite DNS pour le logiciel Pidgin lorsqu'il est configuré pour utiliser un proxy SOCKS 5.

AIDER LES AUTRES

33. FAIRE DES RECHERCHES ET SE DOCUMENTER SUR LA CENSURE
34. CONTOURNER LES BLOCAGES DE PORTS
35. INSTALLER DES PROXYS WEB
36. METTRE EN PLACE UN RELAIS TOR
37. RISQUES LIÉS À L'HÉBERGEMENT D'UN PROXY
38. TRUCS ET ASTUCES POUR WEBMASTERS

33. FAIRE DES RECHERCHES ET SE DOCUMENTER SUR LA CENSURE

Dans beaucoup de pays, l'existence d'une censure d'Internet par le gouvernement n'est pas un secret. La portée de la censure et les méthodes utilisées ont été archivées, comme dans les livres « Access Denied : The Practice and Policy of Global Internet Filtering » http://opennet.net/accessdenied et « Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace » http://www.access-controlled.net. Des livres écrits par Ronald Delbert, John Palfrey, Rafal Rohozinski, et Jonathan Zittrain.

Quand un site populaire est largement bloqué, cela se sait publiquement dans le pays. Certains gouvernements, dont certains censeurs actifs, nient officiellement l'existence d'une censure et tentent de la déguiser en erreurs techniques. Si vous êtes victime de censure, vous pouvez aider les autres, dont les communautés académiques internationales qui étudient la censure, à la comprendre et à la connaître.

Bien sûr, vous devrez être prudent. Les gouvernements qui nient pratiquer la censure du réseau pourraient ne pas apprécier vos efforts pour la révéler.

RECHERCHER DES SOURCES D'INFORMATIONS SUR LA CENSURE

Certaines sources d'informations sur la censure ont été rendues publiques ces deux dernières années. Certaines sont gérées par les utilisateurs mais elles sont toutes contrôlées par des groupes de spécialistes. Elles sont constamment tenues à jour pour garder les listes de sites bloqués aussi exactes que possibles. En voici deux :

- https://www.herdict.org/
- https://www.alkasir.com/map

Sur un niveau géographique plus vaste, l'OpenNet Initiative et Reporters Sans Frontières (RSF) publient des documents sur l'état d'Internet dans chaque pays à partir de critères simples. Vous pouvez y accéder ici :

- Rapport de l'OpenNet Initiative: http://opennet.net/research
- Les ennemis d'Internet selon RSF : http://www.rsf.org/ennemis.html

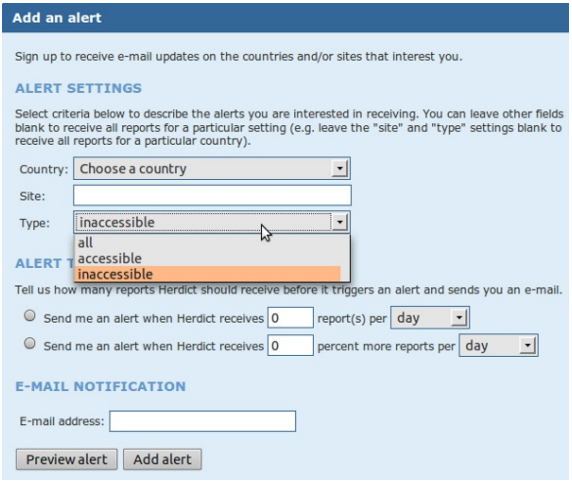
RAPPORTER UN SITE BLOQUÉ AVEC HERDICT

Herdict (https://www.herdict.org) est un site Web qui recense les sites inaccessibles. Il est géré par des chercheurs du Centre Berkman pour Internet et la Société de l'université de Harvard aux États-Unis qui étudient la manière dont Internet est censuré.

Les données de Herdict ne sont pas parfaites. Par exemple, nombre d'utilisateurs ne savent pas distinguer un site censuré d'un problème technique — voire s'ils se sont trompés dans l'adresse. Cependant, les informations sont toujours mises à jour partout dans le monde.

Ci-dessus, un aperçu du rapport sur Facebook

Vous pouvez aider les chercheurs en envoyant vos propres rapports à Herdict depuis leur site Web. C'est gratuit, facile à utiliser et vous n'avez pas besoin de vous inscrire. Vous pouvez aussi vous inscrire pour recevoir les mises à jour des informations sur le blocage d'un site Web.



Herdict propose aussi des extensions pour les navigateurs Mozilla Firefox et Internet Explorer afin de rendre le processus d'envoi d'un rapport plus simple.

RAPPORTER UN SITE BLOQUÉ AVEC ALKASIR

Alkasir est un outil de contournement de la censure avec un système incorporé permettant à ses utilisateurs de rapporter un site bloqué en cliquant sur « Rapporter des URL bloquées ». Alkasir maintient une liste efficace des sites bloqués dans chaque pays et teste automatiquement la disponibilité des URL soumises. En utilisant l'outil de rapport, vous pouvez facilement contribuer à l'étude.

Vous en saurez plus en lisant le chapitre « Utiliser Alkasir ».

PERMETTRE L'ACCÈS À DISTANCE À

D'AUTRES

Vous pouvez aussi aider à l'étude de la censure en donnant aux chercheurs un accès à distance à votre ordinateur afin qu'ils puissent s'en servir dans le but d'effectuer leurs propres tests. Vous ne devriez le faire que si vous faites confiance aux chercheurs en question pour l'utilisation de cet accès, puisqu'ils pourront avoir un accès complet à votre ordinateur et tout ce qu'ils feront semblera provenir de vous, aux yeux de votre FAI ou de votre gouvernement.

Concernant les systèmes d'exploitation basés sur GNU/Linux, un compte SSH est la meilleure option. Vous pouvez trouver de l'aide pour le mettre en place sur http://forum.ubuntu-fr.org et d'autres sites.

Concernant Windows, la fonctionnalité intégrée d'accès à distance au bureau. Vous trouverez les instructions sur http://www.howtogeek.com/howto/windows-vista/turn-on-remote-desktop-in-windows-vista. Vous devrez peut-être aussi configurer la redirection de port sur le modem-routeur dont vous vous servez pour accéder à Internet (voir http://portforward.com).

Une autre solution pour l'accès à distance est le logiciel gratuit TeamViewer (http://www.teamviewer.com) disponible pour les principaux systèmes d'exploitation.

COMPARER LES OBSERVATIONS

La technique de base pour récolter des informations sur la censure d'un réseau est d'essayer d'accéder à un grand nombre de ressources réseau — comme de longues listes d'URL — depuis plusieurs endroits sur Internet et comparer les résultats. Certains URL ont-elles put être chargée à tel endroit mais pas à tel autre ? Ces différences sont-elles occasionnelles ou permanentes ? Si vous possédez un outil de contournement fiable, comme le VPN, vous pouvez faire certains de ces tests par vous-même, en comparant l'aspect du réseau avec et sans contournement. Par exemple, aux États-Unis, cette méthode fut utilisée pour savoir comment les FAI coupaient les protocoles de partage P2P.

Ces comparaisons peuvent être faites de manière automatisée ou à la main.

PACKET SNIFFING

Si vous comprenez comment les protocoles sur Internet fonctionnent, un logiciel de « packet sniffing » comme Wireshark (http://www.wireshark.com) vous permettra de récupérer les paquets réellement échangés par votre ordinateur.

34. CONTOURNER LES BLOCAGES DE PORTS

Un pare-feu peut être utilisé pour bloquer toutes les communications dirigées vers un port particulier. Cela peut être utilisé pour tenter d'empêcher l'utilisation d'un protocole particulier ou d'un logiciel utilisant le réseau. Pour tenter de contourner ces restrictions, les FAI et les utilisateurs peuvent utiliser un port non standard pour accéder à ces services. Cela permet aux logiciels de contourner les blocages de ports les plus simples.

De nombreuses applications peuvent facilement être configurées pour utiliser des numéros de port non standard. Les adresses des sites Web ont une manière particulièrement efficace de faire ceci, directement dans l'URL. Par exemple, l'URL http://www.exemple.com:8000/foo/ demandera au navigateur de faire une requête HTTP vers exemple.com sur le port 8000, plutôt que sur le port 80 par défaut. Cela ne marchera que si le serveur web à www.exemple.com accepte les requêtes sur le port 8000.

TESTER LE BLOCAGE DE PORTS

Vous pouvez vérifier quels ports sont bloqués sur votre connexion en utilisant Telnet. Ouvrez simplement une ligne de commande, tapez « telnet login.icq.com 5555 » ou « telnet login.oscar.aol.com 5555 » et appuyez sur « Entrée ». Le numéro est le port que vous voulez tester. Si vous recevez des symboles étranges en retour, la connexion a réussie.

Si, à l'inverse, votre ordinateur rapporte que la connexion a échouée, a expiré, ou a été interrompue, déconnectée ou réinitialisée, le port est probablement bloqué. Gardez à l'esprit que certain ports peuvent être bloqués uniquement en conjonction avec certaines adresses IP.

35. INSTALLER DES PROXYS WEB

Si vous avez accès un serveur web dans un pays qui ne censure pas l'accès à internet, vous pouvez installer un proxy web.

C'est un petit logiciel écrit dans un langage de programmation tel que PHP, Perl, Python ou ASP.

Installer un programme de contournement pour le web demande une certaine expertise technique et quelques ressources (un hébergement web compatible et de la bande-passante).

Si vous voulez installer votre propre proxy web, vous aurez besoin d'un des outils suivants :

- Un espace de stockage web avec un support de PHP, ce qui peut être acheté pour quelques dollars US par an chez des hébergeurs comme http://www.dreamhost.com ou http://www.hostgator.com, ou fourni par votre école ou université.
- Un serveur virtuel (VPS) ou dédié, plus chers et plus compliqués à utiliser.
- Un PC connecté avec une adresse IP publique.

WEB PROXYS PUBLICS ET PRIVÉS

Des proxys web publics sont disponibles pour les gens qui ont la possibilité de les chercher, dans des moteurs de recherche comme Google, par exemple. Utilisateurs et entités qui implémentent le filtrage peuvent donc trouver très facilement ces proxys. Il y a des risques qu'ils soient donc sur liste noire.

L'emplacement des proxys web privé est connu uniquement des utilisateurs prévenus. Dans ce contexte, les proxy web privés sont donc plutôt prévus pour des utilisateurs qui ont besoin d'outils de contournement stables pour le trafic web, et qui ont des tiers de confiance dans des endroits non filtrés avec le niveau technique et la bande passante suffisante pour maintenir le proxy web.

FONCTIONNALITÉS DES PROXYS WEB

Les proxys web peuvent être installés avec des niveaux divers de personnalisations adaptés aux besoins de l'utilisateur final. Les personnalisations classiques contiennent notamment un changement du port sur lequel le serveur web écoute, et du chiffrement avec SSL, par exemple. Étant donné que certaines listes noires peuvent bloquer des mots clef associés à un logiciel de proxy populaire, changer des éléments comme l'adresse par défaut, le nom du script, ou des éléments de l'interface utilisateur réduit le risque d'une détection et d'un blocage automatique du proxy. Il est également possible de protéger l'utilisation du proxy web en activant le .htaccess avec un nom d'utilisateur et un mot de passe.

Quand vous utilisez SSL, il peut aussi être pratique de créer une page web inoffensive à la racine du site web et de cacher le proxy web avec un chemin et un nom de fichier aléatoires. Bien que les intermédiaires soient capables de déterminer sur quel serveur vous vous connectez, ils ne pourront pas savoir le chemin que vous utilisez, car cette partie est chiffrée. Par exemple, si un utilisateur se connecte à http://example.com/secretproxy/, un intermédiaire pourra savoir qu'il s'est connecté sur example.com mais ne pourra pas savoir que l'utilisateur a demandé le proxy web. Si le gestionnaire du proxy web met une page inoffensive sur example.com, le proxy web a moins de risques d'être découvert en surveillant le réseau. Vous pouvez trouver un certificat SSL valide qui sera accepté par tous les navigateurs populaires gratuitement sur https://www.startcom.org/.

Il y a plusieurs proxy web open source et gratuits disponibles sur Internet. Les différences principales entre eux sont les langages dans lesquels ils sont écrits, vu que tous les serveurs web ne supportent pas tous les langages de programmation. Autre grosse différence, la compatibilité avec des technologies comme AJAX (utilisé par Gmail et Facebook) ou le streaming (utilisé par youtube).

Les proxys web populaires sont notamment :

- CGIProxy (http://www.jmarshall.com/tools/cgiproxy), un script CGI écrit en Perl qui sert à la fois de proxy HTTP et FTP.
- Peacefire's Circumventor http://www.peacefire.org/circumventor/simple-circumventor-instructions.html), Un installateur automatisé qui rend l'installation de CGIProxy sur une machine Windows pour les utilisateurs non avancés plus simple.
- SabzProxy (http://sabzproxy.com), un proxy HTTP et FTP. Il est basé sur le code de PHProxy, écrit en PHP, avec des fonctionnalités supplémentaires, comme un encodage de l'adresse aléatoire, ce qui le rend plus difficile à bloquer.
- Glyphe proxy (http://www.glype.com), un autre proxy web gratuit, également écrit en PHP.
  Les sites de ces proxys web fournissent des instructions d'installation. En général, ça inclut le téléchargement du script, l'extraction sur le disque dur local, la mise en ligne du script via FTP ou SCP sur le serveur web, le réglage des permissions, et le test du script. L'exemple suivant est pour l'installation de SabzProxy. Les étapes sont les mêmes pour les autres proxys web.

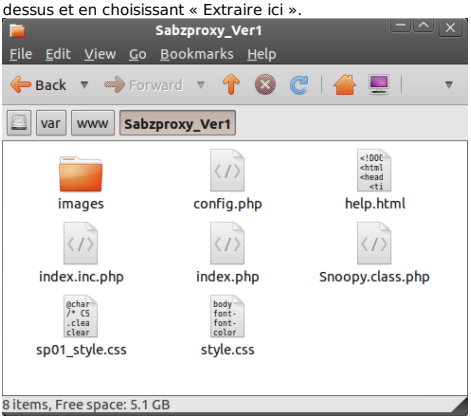
INSTALLER SABZPROXY

SabzProxy est disponible uniquement en Persan, mais l'interface graphique est simple et toujours facile à comprendre.

Ces instructions décrivent le cas le plus fréquent : utilisez FTP pour transférer SabzProxy sur un espace web qui supporte PHP. Pour cette technique, vous aurez besoin d'un client FTP comme FileZilla (http://filezilla-project.org).

Bien que cette méthode soit la plus courante, elle n'est pas utilisable à chaque fois. Quand vous configurez votre serveur depuis la ligne de commande, ce n'est pas possible, mais les étapes devraient être les mêmes.

1. La première étape est de télécharger l'archive de SabzProxy sur http://www.sabzproxy.com.
2. Ensuite, extrayez le contenu du fichier en faisant un clic droit dessus et en choisissant « Extraire ici ».

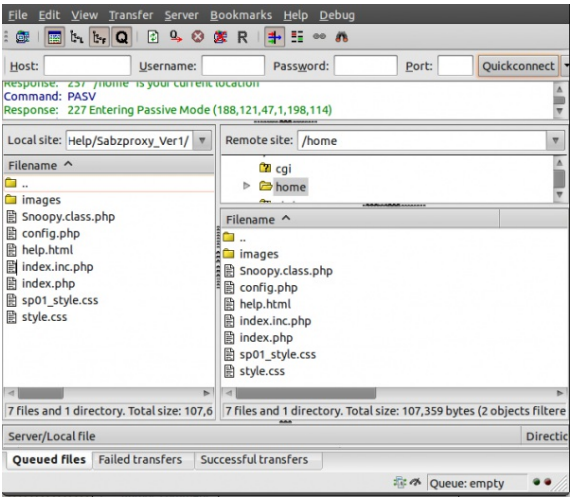


3. Ouvrez le fichier config.php avec un éditeur de texte basique (par exemple notepad sous windows, gedit ou nano sous linux, et texteditor pour Mac OS).
4. Éditez la ligne 8, celle qui commence par $config_key. Tapez une chaîne aléatoire entre "". Cette chaîne sera utilisée pour rendre l'encodage de l'adresse aléatoire, donc faites en sorte qu'elle soit aussi aléatoire que possible.

```php
<?php
    /**
     * Config Key ---------------------------------
     * Inja bayad yek kelid 5 ta 10 characteri vared konid
     */
    $config_key = "Type here a random string";

    /**
     * Bookmarks ----------------------------------
     * Linkdoonie shoma
     * Mitavanid be har tedad link ezafe konid. kafi ast ke az yek
     * va on ra edit konid.
     */
    $linkbox = array(
        ,"/http://www.balatarin.com" <= "بالاترین"//  );
```

5. Vous pouvez aussi configurer quelques options, comme le texte d'accueil et les liens.
6. Ouvrez Filezilla, entrez le serveur (hôte), nom d'utilisateur et mot de passe de votre espace de stockage web et cliquez sur connexion (ou quelque chose du genre si vous utilisez un autre client FTP).
7. La partie de gauche de la fenêtre du client FTP représente l'ordinateur local, donc vous pouvez trouver les fichiers de SabzProxy que vous vendez d'éditer.



8. Glissez-déposez les fichiers du côté gauche de la fenêtre vers le côté droit, qui représente le serveur FTP distant (votre espace web).
9. Vous pouvez maintenant accéder à SabzProxy en naviguant sur le domaine de votre service web et le dossier dans lequel vous avez installé SabzProxy. (Dans cet exemple, http://kahkeshan-e-sabz.info/home.)

Si ça ne fonctionne pas, votre compte ne supporte peut-être pas PHP, ou le support de PHP n'est pas activé, ou il peut demander des étapes supplémentaires. Référez-vous à la documentation de votre compte, ou le logiciel que votre serveur web utiliser. Vous pouvez également chercher un forum de support dédié ou demandez à l'administrateur de votre serveur web pour une aide supplémentaire.

36. METTRE EN PLACE UN RELAIS TOR

Si vous habitez dans une région où il n'y a que peu ou pas de censure, vous pouvez avoir envie de mettre en place un relai Tor, ou une passerelle Tor pour aider ses autres usagers à accéder à un internet non-censuré.

Le réseau Tor s'appuie sur des volontaires qui offrent de la bande passante. Plus il y a de gens qui mettent en place des relais, plus le réseau sera rapide et sûr. Pour aider les gens qui utilisent Tor à contourner la censure d'internet, mettez en place un relais passerelle plutôt qu'un relai ordinaire.

Les relais passerelles (ou passerelles pour faire court) sont des relais Tor non listés dans le répertoire Tor principal (et public). Même si un ISP (FAI) filtre les connections de tous les relais Tor connus, il ne sera probablement pas capable de bloquer toutes les passerelles.

LES RISQUES LIÉS À L'HÉBERGEMENT D'UN NOEUD TOR (RELAIS TOR)

Un nœud Tor est une sorte de proxy public, et en faire fonctionner un peut présenter les mêmes risques généraux que faire fonctionner un proxy, décrits dans le chapitre *Les risques liés à l'hébergement d'un proxy* de ce guide. Cependant, un nœud Tor est typiquement mis en place de l'une des deux manières suivantes : en tant que nœud sortant ou en tant que nœud intermédiaire (parfois appelé nœud non-sortant). Un nœud intermédiaire transmet exclusivement du trafic crypté aux autres nœuds Tor, et ne permet pas à des utilisateurs anonymes de communiquer directement avec des sites situés en dehors du réseau Tor. La mise en place de l'un ou l'autre de ces types de nœuds est utile à l'ensemble du réseau Tor. Mettre en place un nœud sortant est particulièrement utile puisqu'ils sont comparativement plus rares. Mettre en place un nœud intermédiaire est comparativement moins risqué, puisqu'il est moins susceptible d'attirer le genre de plaintes auxquelles s'expose un proxy public, dans la mesure où l'adresse IP d'un nœud intermédiaire n'apparaitra jamais dans les journaux de connexion.

Une passerelle n'est pas un nœud sortant, il est peu probable que vous soyez l'objet de plaintes concernant l'utilisation d'un bridge par d'autres.

Même s'il n'est pas susceptible d'attirer des plaintes spécifiques, la mise en place d'un nœud intermédiaire ou d'une passerelle peut entraîner l'intervention de votre fournisseur d'accès pour différentes raisons : Il peut désapprouver le réseau Tor, interdire à ses abonnés l'exécution de toute forme de service disponible publiquement, etc. Vous pouvez trouver d'avantage de « bonnes pratiques » sur les manières de sécuriser la mise en place d'un nœud sortant Tor sur : https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment.

INSTALLER UN RELAIS OU UNE PASSERELLE, CE DONT J'AI BESOIN

Il y a peu de prérequis pour faire tourner un relais Tor :

- Votre connexion doit avoir une bande passante d'au moins 20 KO/seconde dans les deux sens et la connexion doit pouvoir être utilisée en permanence quand votre ordinateur est allumé.
- Vous avez besoin d'une connexion avec une adresse IP publique et routable.
- Si votre ordinateur est derrière un NAT et que vous n'avez pas accès à son adresse IP publique (ou externe), vous devrez configurer la redirection de port sur votre routeur. Vous pouvez le faire via la gestion d'UPnP automatique de Tor, ou manuellement, en suivant les instructions dans le manuel de votre routeur ou sur portforward.com http://portforward.com/english/applications.

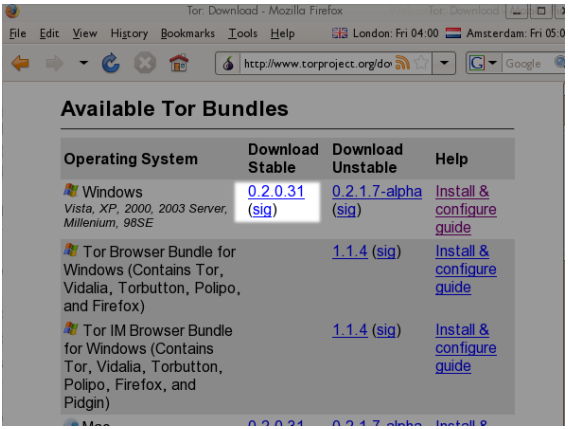
Ce dont vous n'avez pas besoin :

- Votre ordinateur n'a pas à être toujours allumé et en ligne, Tor détectera automatiquement quand il l'est et quand il ne l'est pas.
- Vous n'avez pas à avoir une adresse IP fixe.

TÉLÉCHARGER TOR

Pour télécharger Tor, allez sur le site https://www.torproject.org/ et cliquez sur « Télécharger » dans le menu de navigation.

Sur la page des paquets Tor disponibles, sélectionnez la version stable qui correspond à votre système d'exploitation.



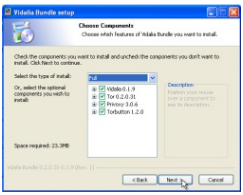
INSTALLER TOR SUR GNU/LINUX

Trouvez des instructions détaillées sur comment installer un relais Tor ou une passerelle sur https://www.torproject.org/docs/tor-doc-relay.html.en.

INSTALLER TOR SUR MICROSOFT WINDOWS

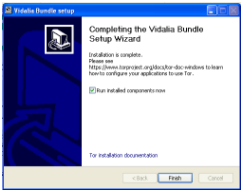
Lancez l'installateur et cliquez sur « suivant » quand on vous le demande.

Si vous utilisez Firefox, installez tous les composants proposés dans le dialogue ci-dessous :



Si vous n'avez pas Firefox, décochez Torbutton (on vous proposera d'installer Firefox et Torbutton plus tard).

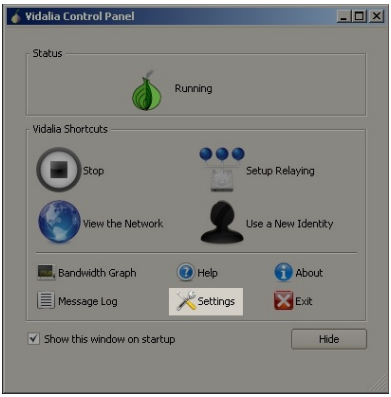
Une fois l'installation terminée, lancez Tor en cliquant sur « Terminer » en sélectionnant la case « Lancer les composants installés maintenant, » comme affiché dans le dialogue ci-dessous :



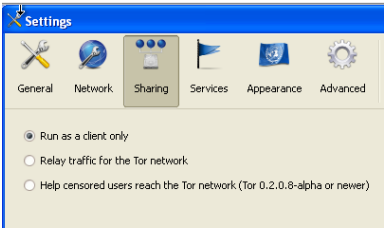
CONFIGURER TOR POUR ÊTRE UNE PASSERELLE

Pour activer la passerelle :

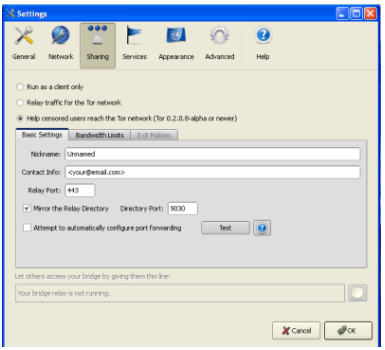
1. Ouvrez le panneau de contrôle Vidalia.
2. Dans le panneau de contrôle, cliquez sur « Paramètres ».



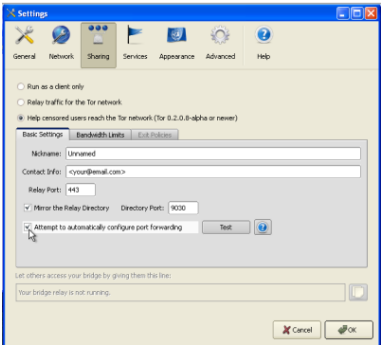
3. Dans la fenêtre des paramètres, cliquez sur « Partager ».



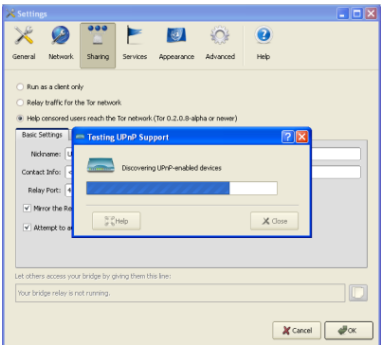
4. Pour activer la passerelle, cliquez sur « Aider des utilisateurs filtrés à rejoindre le réseau Tor ».



5. Si vous utilisez une IP NATée sur un réseau local, vous devez créer une règle de redirection de port dans votre routeur. Vous pouvez demander à Tor d'essayer de configurer la redirection de port pour vous en cliquant sur « Essayer de configurer automatiquement la redirection de port ».



6. Cliquez sur « Tester » pour voir si Tor a réussi à paramétrer la redirection sur le routeur.

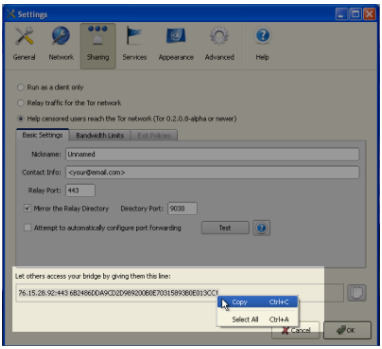


Si Tor n'a pas pu configurer la redirection de port, rendez-vous sur la FAQ pour voir la réponse à ce sujet : https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorFAQ#ServerForFirewalledClients

Félicitations ! Si tout s'est bien passé, votre passerelle fonctionne. Les informations seront ajoutées à l'index des passerelles et seront disponible pour ceux qui le demanderont.

PARTAGER VOTRE PASSERELLE AVEC DES AMIS

Si vous avez créé votre passerelle spécifiquement pour aider un ami à accéder au réseau Tor, vous pouvez copier les informations en bas de la fenêtre des paramètres et le lui envoyer :


Settings
General
Network
Sharing
Services
Appearance
Advanced
Help
Run as a client only
Relay traffic for the Tor network
Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)
Basic Settings
Bandwidth Limits
Exit Policies
Nickname:
Unnamed
Contact Info:
<your@email.com>
Relay Port:
443
Mirror the Relay Directory
Directory Port:
9030
Attempt to automatically configure port forwarding
Test
Let others access your bridge by giving them this line:
Copy
Ctrl+C
Select All
Ctrl+A
Cancel
OK

37. RISQUES LIÉS À L'HÉBERGEMENT D'UN PROXY

Quand vous faites fonctionner un proxy Web ou applicatif sur votre ordinateur pour aider les autres, les requêtes et les connexions transmises à travers votre proxy sembleront provenir de votre ordinateur. Le comportement de votre ordinateur dépend d'autres utilisateurs. Aussi, leurs activités pourraient vous être attribuées, comme si vous les aviez effectuées vous-même. Si quelqu'un utilise votre proxy pour envoyer ou recevoir du contenu interdit, vous pourriez recevoir des réclamations qui vous considèrent comme responsable et vous demandent d'arrêter ces activités. Dans certains cas, les activités en question pourraient engager des poursuites légales, ou une surveillance accrue des institutions chargées de faire respecter la loi dans votre pays ou un autre.

Dans certains pays, des hébergeurs de proxys ont reçus des accusations légales et, dans certains cas, les autorités ont même saisi les ordinateurs sur lesquels fonctionnaient les proxys. Cela peut arriver pour plusieurs raisons :

- quelqu'un peut penser à tort que l'hébergeur du proxy a commis lui-même les infractions.
- quelqu'un peut penser que l'hébergeur a la responsabilité légale d'arrêter certaines utilisations, même si elles sont faites par d'autres personnes.
- quelqu'un peut vouloir chercher des indices sur votre ordinateur pour identifier la personne à l'origine de ces activités.
  Si vous pensez que l'installation d'un proxy près de chez vous est risquées, il peut être plus sûr de l'installer sur un ordinateur dédié dans un datacenter. Ainsi, il n'attirera pas l'attention sur votre connexion personnelle.

Les lois varient selon les pays sur la manière et l'étendue dont la responsabilité des administrateurs de proxys est protégée. Pour connaître votre situation, consultez un avocat ou un expert légal qualifié dans votre juridiction.

LES RISQUES DE FAIRE FONCTIONNER UN PROXY PUBLIC

Les FAI peuvent se plaindre de votre proxy, en particulier s'ils reçoivent des réclamations concernant son utilisation abusive. Certains FAI peuvent considérer que l'utilisation d'un proxy va à l'encontre de leurs conditions d'utilisation, ou simplement qu'ils n'autorisent les utilisateurs à faire fonctionner des proxys publics. Ce genre de FAI pourra vous déconnecter ou vous menacer de déconnexion dans le futur.

Un proxy public peut être utilisé par beaucoup de gens à travers le monde et peut utiliser d'importantes quantités de bande passante et de trafic. Aussi, si votre FAI exerce un surcoût tarifaire, vous devriez prendre des précautions pour éviter de recevoir une grosse facture à la fin du mois.

LES RISQUES DE FAIRE FONCTIONNER UN PROXY PRIVÉ

Bien que demeurent certains risques lors du maintien lucratif d'un proxy destiné à un groupe restreint, la mise en place de proxys privés est bien moins risquée que celle de proxys publics.

Si un utilisateur de votre proxy privé est détecté et surveillé, la personne qui effectue la surveillance peut se rendre compte, ou deviner, qu'il y a une relation entre vous et l'utilisateur et que vous essayez d'aider cette personne à contourner le filtrage.

Même si votre FAI risque bien plus de s'opposer à l'utilisation d'un proxy public qu'à celle d'un proxy privé, certains FAI ont des politiques anti-proxys qui s'opposent au fonctionnement d'un proxy même privé sur leur réseau.

LES LOIS DE CONSERVATION DES DONNÉES POURRAIENT CONTRÔLER L'UTILISATION DU PROXY

Dans certains pays, les lois de conservation des données ou du même genre faites pour restreindre l'anonymat peuvent être invoquées afin de réguler les services de proxy. Pour plus d'informations sur la conservation des données, rendez-vous sur ce site https://secure.wikimedia.org/wikipedia/fr/wiki/Conservation_des_données.

38. TRUCS ET ASTUCES POUR WEBMASTERS

Faire fonctionner un site Internet, exposé à un public varié ou non, n'est pas toujours facile. Il est important de penser à votre sécurité personnelle ainsi qu'à celle des visiteurs. Souvent, les webmasters sont surpris quand leurs sites sont inopinément bloqués dans un certain pays. Si un grand nombre de visiteurs sont dans l'incapacité d'y accéder, l'opérateur de celui-ci peut aussi faire face à des problèmes économiques. Perdre le contenu ou le serveur de votre site, ou avoir à en installer un autre peut aussi être dérangeant et frustrant.

Ce chapitre tente de dresser une liste de bonnes pratiques et de conseils à avoir en tête lors de la mise en place de votre site Web.

PROTÉGER VOTRE SITE WEB

- Toujours **planifier des sauvegardes automatiques** (fichiers et bases de données) au moins sur une autre machine physique. Soyez sûr de la démarche pour les restaurer.
- **Surveillez votre trafic** pour apprendre depuis quel pays viennent vos visiteurs. Vous pouvez utiliser des bases de données de géolocalisation pour deviner depuis quel pays vient une adresse IP. Si vous remarquez une chute importante de trafic depuis un certain pays, votre site web a peut-être été bloqué dans celui-ci. Vous pouvez partager votre observation sur une base de données regroupant les sites Web bloqués comme Herdict (https://www.herdict.org/web).
- **Sécurisez votre site Web**, surtout si vous utilisez un CMS (Content Management System). Il faut toujours installer les dernières mises à jour stables pour corriger les failles de sécurité.
- **Sécurisez le logiciel de votre serveur Web** en le paramétrant pour un haut niveau de sécurité (vous pouvez trouver une quantité importante de ressources sur Internet pour sécuriser des serveurs Web tournant sous Linux).
- Enregistrez (ou transférez) votre nom de domaine vers un **autre fournisseur de nom de domaines** qui n'est pas votre aussi hébergeur Web. Dans le cas d'une attaque à l'encontre de votre fournisseur d'hébergement Web, vous pourrez facilement faire pointer votre nom de domaine vers un autre hébergeur Web.
- Vous pouvez aussi créer un **serveur miroir** tournant en mode standby vers lequel vous pouvez basculer très facilement. Apprenez à basculer facilement vos entrées DNS vers le site miroir.
- Il peut être intéressant d'**héberger votre site Web dans un pays étranger**, où le contenu sera moins soumis à la controverse et sera explicitement protégé légalement. Ce choix peut induire un petit délai supplémentaire lors de l'affichage des pages, en général quelques millisecondes, pour vos visiteurs mais vous évitera beaucoup de soucis si vous résidez dans un pays où le contenu de votre site Web est considéré comme litigieux.
- **Testez et optimisez** votre site Web avec les principaux outils de contournement que vos visiteurs utilisent en général. Vérifier et corriger la moindre page ou fonctionnalité cassée. Idéalement, rendez votre site utilisable par vos utilisateurs sans utiliser JavaScript ou un plugin puisque ceux-ci peuvent être bloqués si vos utilisateurs utilisent des serveurs proxy.
- **Evitez de transférer vos fichiers par FTP**. Le protocole FTP envoie les mots de passe en clair (c'est à dire non chiffrés) sur Internet, exposant vos informations de connexion une interception sur le réseau. Utilisez plutôt des protocoles comme SFTP (File Transfer Protocol over SSH), SCP ou du WebDAV sécurisé (sur HTTPS).
- **Utilisez des ports d'écoute différents** pour accéder à vos interfaces d'administration. Les hackers utilisent, en général, des scans automatiques de ports sur une plage de ports standards pour détecter des vulnérabilités. Vous devriez utiliser des valeurs de ports non-standard (comme pour SSH) pour minimiser les risques d'attaque.
- **Pour protéger votre serveur contre les attaques par force brute**, installez des outils comme DenyHosts http://denyhosts.sourceforge.net. Celui-ci permet de le protéger en utilisant des listes noires contenant les adresses IP ayant effectué trop de tentatives de connexions infructueuses.

PROTÉGEZ-VOUS

Vous trouverez ci-dessous des astuces pour vous protéger personnellement, si l'anonymat en tant que webmaster est important pour vous.

- Utilisez une adresse électronique anonyme qui n'est jamais utilisée en association avec votre identité réelle.
- Si vous avez acheté un nom de domaine, vous pouvez saisir de fausses informations dans la base de données publique **WHOIS** en utilisant un service souvent appelé « WHOIS proxy », « WHOIS protect » ou « domain privacy »
- Utilisez un service come TOR pour rester anonyme quand vous mettez à jour votre site Web.

PROTÉGEZ VOS VISITEURS

Outre la protection de votre site Web et de votre personne, il est aussi important de protéger vos visiteurs contre une potentielle détection d'une tierce partie, surtout s'ils soumettent du contenu sur votre site Web.

- **Mettez en place le protocole HTTPS** pour que vos utilisateurs puissent accéder à votre site au moyen d'une connexion chiffrée, ce qui rendra difficile de regarder automatiquement quel contenu est transféré et pour protéger les identités des différents utilisateurs (y compris la vôtre). Assurez-vous que la configuration de votre site Web utilise bien HTTPS chiffrer l'ensemble des échanges et suivez les autres bonnes pratiques de configuration d'HTTPS. Vous pouvez trouver des informations à propos de son bon déploiement sur https://www.eff.org/pages/how-deploy-https-correctly. Vous pouvez, aussi, utiliser des tests automatiques sur https://www.ssllabs.com/ pour contrôler beaucoup de paramètres techniques.
- **Minimisez la quantité d'information conservée** dans vos fichiers journaux. Evitez de conserver des adresses IP ou toute autre information personnelle concernant vos visiteurs plus longtemps que nécessaire.
- **Chiffrez les données critiques des utilisateurs** que vous conservez, comme les mots de passe, en utilisant, par exemple des salted hashes.
- Les services extérieurs comme **Google Analytic**s ou tout autre contenu tiers comme les services publicitaires sont difficiles à contrôler. Evitez-les.
- Créez une version **épurée et sécurisée** de votre site Web, sans Flash ou code JavaScript embarqué, respectueux de TOR et des connexions bas débit.

EDUQUEZ VOS VISITEURS

- **Apprenez à vos utilisateurs** comment utiliser des outils de contournement et comment améliorer leur sécurité sur Internet.
- **Créez des checklists**, accessibles à vos utilisateurs, concernant la sécurité, pour qu'ils puissent être sûrs de ne pas être surveillés ou attaqués.

PARTAGEZ LES OUTILS DE CONTOURNEMENT AVEC VOS UTILISATEURS

- **Hébergez des serveurs proxy Web**, comme SabzProxy ou Glype Proxy. Donnez-en l'accès à vos visiteurs, par email ou au moyen des réseaux sociaux.
- **Envoyez des invitations psiphon** si vous avez un compte sur un nœud privé.
- **Installez d'autres types de proxy Web et d'applications** si vous disposez d'un serveur dédié et partagez-les.
- **Postez une référence à ce guide** ou tout autre outil de contournement pertinent sur votre site Web.

MULTIPLIEZ LES CANAUX DE DISTRIBUTION

Les webmasters peuvent et devraient utiliser différentes action pour répandre leurs contenus le plus possible pour éviter qu'ils ne soient rendus indisponibles ou bloqués.

- **Mettez en place une liste de diffusion** et envoyez régulièrement par email des informations concernant les nouveaux contenus créés. Vous pourrez toujours échanger avec des utilisateurs même si votre site Web n'est plus du tout accessible.
- **Mettez en place un flux RSS** et vérifiez qu'il contienne les articles en entiers et pas seulement des résumés de ceux-ci. Ainsi, votre contenu peut être interprété très facilement par des sites Web tiers ou par des applications comme Google Reader, qui permet de lire votre contenu même depuis un endroit où il est habituellement bloqué. Partagez vos contenus sur des réseaux sociaux populaires comme Facebook ou Twitter, qui seront difficilement bloqués.
- **Diffusez vos contenus le plus possible**. Rendez votre contenu téléchargeable. Wikipedia, par exemple distribue gratuitement les exports du contenu de ses bases de données qui peuvent être facilement utilisés pour créer un site miroir, avec le même contenu dans un lieu différent.
- Pensez à **diffuser vos contenus sous une licence libre** (comme GPL ou Creative Commons) qui permettent à tout le monde de les réutiliser et de créer des miroirs.
- Enregistrez en miroir vos fichiers sur des **services de partage de fichiers gratuits** comme RapidShare.com ou MegaUpload.com et grâce à des logiciels de partage **peer to peer** comme Bittorrent.
- Configurez votre serveur Web autorisé l'accès à votre contenu des ports **différents des ports** standards (80 pour HTTP et 443 pour HTTPS).
- **Donnez accès à une API** (Application Programming Interface) qui permette aux autres utilisateurs d'accéder à votre contenu depuis des applications tierces comme Twitter ou Wikipedia qui le permettent.

RÉDUISEZ LES TEMPS DE CHARGEMENT DE VOS PAGES

Réduire le temps de chargement de vos pages Web ne va pas seulement vous faire économiser de la bande passante et de l'argent mais aussi aider vos visiteurs des pays en voie de développement à accéder plus facilement à l'information que vous mettez à disposition. Une liste de bonnes pratiques pour accélérer votre site Web est disponible à cette adresse http://developer.yahoo.com/performance/rules.html et https://code.google.com/speed/page-speed/.

- **Choisissez un style minimaliste**. Conservez le minimum d'images et utilisez CSS pour gérer le style et la mise en page de votre site Web. Une bonne introduction à CSS est disponible sur http://www.w3schools.com/css/css_intro.asp.
- **Optimisez vos images**. Utilisez des logiciels comme OptiPNG (http://optipng.sourceforge.net/) pour créer des images plus rapides à charger en les optimisant pour une utilisation Web. Ne réduisez jamais vos images grâce à HTML, sauf si vous en avez besoin (par exemple, si vous avez besoin d'une image de 60x60, réduisez là directement, plutôt que d'utiliser HTML).
- **Réduisez au maximum l'utilisation de Java, JavaScript, Flash** et de tout autre contenu exécuté sur l'ordinateur client. Souvenez-vous que certains cybercafés désactivent ce type de contenus pour des raisons de sécurité. Assurez-vous que l'information que vous souhaitez mettre à disposition est affichée en utilisant du HTML pur uniquement.
- **Utilisez des fichiers séparés pour vos styles CSS et vos scripts JavaScript**. Si vous utilisez un même style CSS ou un même code JavaScript sur plusieurs pages de votre site Web, transférez ce style ou ce code dans des fichiers séparés de celui de la page. Appelez ces fichiers dans l'entête du fichier HTML de chaque page en ayant besoin. Cette technique permet au navigateur internet de votre visiteur de mettre ces fichier en cache ce qui évite de recharger cette portion de code à chaque changement de page sur votre site Web.
- **Minimisez votre code** : Supprimez tous les retours à la ligne et tous les espaces inutiles. Certains outils le faisant de façon automatique sont disponibles sur http://javascriptcompressor.com.
- **Réduisez au minimum le nombre de requête serveur**. Si vous avez un site Web dynamique mais que le contenu n'évolue pas souvent, vous pouvez installer des extensions pour mettre en place un cache coté serveur. Celles-ci fourniront une version statique de vos contenus ce qui réduira drastiquement le nombre de requêtes sur votre base de données.

ANNEXES

39. GLOSSAIRE

Une bonne partie de ce contenu est fondée sur :
http://en.cship.org/wiki/Special:Allpages

ADDRESSE IP (INTERNET PROTOCOL)

Une adresse IP est un numéro d'identification d'un ordinateur particulier sur Internet. Dans la précédente version 4 du Protocole Internet, une adresse IP comportait à quatre octets (32 bits), souvent représentée par quatre nombres entiers dans l'intervalle 0-255 séparés par des points, tels que 74.54.30.85. Dans l'IPv6 (version 6 du Protocole Internet), qui remplace petit à petit son prédécesseur sur le Net, une adresse IP est quatre fois plus longue, et comporte 16 octets (128 bits). On peut l'écrire sous forme hexadécimale : 8 groupes de 4 chiffres séparés par le signe deux points, comme par exemple : 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

ADDRESSE IP PUBLIQUEMENT ROUTABLE

Les adresses IP publiquement routables (parfois appelé adresses IP publiques) sont celles accessibles sur Internet sur le mode habituel, à travers une chaîne de routeurs. Certaines adresses IP sont privées, comme le bloc 192.168.xx, et beaucoup ne sont pas attribuées.

AGGREGATEUR

Un agrégateur est un service qui rassemble des informations syndiquées à partir d'un ou de plusieurs sites et les rend consultables sur une adresse différente. Autres appellations : agrégateur RSS, agrégateur de flux, lecteur de flux ou lecteur d'actualités. (A ne pas confondre avec le lecteur d'actualités d'Usenet).

ANALYSE DE MENACES

Une analyse de la menace de sécurité est à proprement parler une étude détaillée et formelle de tous les moyens connus pour attenter à la sécurité des serveurs ou des protocoles, ou bien des procédés les utilisant à des fins précises, comme le contournement. Les menaces peuvent être d'ordre technique, par exemple le « code-breaking » (décryptage de code) ou l'exploitation de bugs logiciels, ou bien d'ordre social, comme le vol de mots de passe ou le soudoiement d'une personne possédant des connaissances spécialisées. Peu de sociétés ou de particuliers possèdent les connaissances et les compétences nécessaires pour effectuer une analyse complète des menaces possibles, mais toutes les personnes concernées par le contournement se doivent de procéder à une évaluation de ces questions.

ANALYSE DU TRAFIC

L'analyse du trafic est l'analyse statistique des communications cryptées. Dans certains cas, l'analyse du trafic peut révéler des informations sur les personnes qui communiquent et sur les informations communiquées.

ANONYMAT

(A ne pas confondre avec vie privée, pseudonyme, sécurité ou confidentialité)

L'anonymat sur Internet est la capacité à utiliser des services sans laisser d'indices sur son identité. Le niveau de protection dépend des techniques d'anonymat utilisées et de l'importance de la surveillance. Parmi les techniques les plus efficaces pour protéger l'anonymat figure la création d'une chaîne de communication à l'aide d'un processus aléatoire pour sélectionner certains liens, dans laquelle chaque lien n'a accès qu'à des informations partielles sur le processus. Le premier connaît l'adresse IP de l'utilisateur mais pas le contenu, la destination ou l'objet de la communication, du fait que le contenu du message et les informations de destination sont cryptées. Le dernier connaît l'identité du site contacté, mais non l'origine de la session. Une ou plusieurs étapes intermédiaires évitent que le premier et le dernier lien ne partagent leur connaissance partielle pour connecter l'utilisateur et le site cible.

ASP (APPLICATION SERVICE PROVIDER)

L'ASP est une organisation qui propose des services logiciels sur Internet, permettant une mise à jour du logiciel et sa gestion centralisée.

ATTAQUE PAR FORCE BRUTE

Une attaque par force brute consiste à essayer tous les codes, combinaisons ou mots de passe possibles jusqu'à trouver le bon. C'est une des méthodes de piratage les plus banales.

BACKBONE (COLONNE VERTEBRALE)

Une colonne vertébrale est l'un des liens de communication à large bande qui relie entre eux des réseaux dans différents pays et des organisations à travers le monde pour constituer l'Internet.

BADWARE

Voir Malware.

BANDE PASSANTE

La bande passante d'une connexion est le taux de transfert de données maximal sur cette connexion, limitée par sa capacité et par celle des ordinateurs aux deux bouts de la connexion.

BARRE BLEUE

La barre d'adresse URL bleue (appelée Barre bleue dans le jargon de Psiphon) est le formulaire placé en haut de la fenêtre du navigateur du nœud Psiphon qui vous donne accès au site bloqué en y saisissant l'URL du site.

Voir aussi Nœud Psiphon.

BASH (BOURNE-AGAIN SHELL)

Le bash shell est une interface de ligne de commande pour les systèmes d'exploitation Linux/Unix, fondée sur le Bourne shell.

BITTORRENT

BitTorrent est un protocole de partage de fichiers peer-to-peer inventé par Bram Cohen en 2001. Il permet à des particuliers de distribuer de gros fichiers à moindre frais et de manière efficace, comme des images de CD, des vidéos ou des fichiers de musique.

BLOQUER

Bloquer consiste à empêcher l'accès à une ressource Internet, en faisant appel à diverses méthodes.

CACHE

Un cache est une partie d'un système de traitement d'informations utilisé pour stocker des données récemment ou fréquemment utilisées pour en accélérer l'accès répété. Un cache Web renferme les copies des fichiers de pages Web.

CADRE

Un cadre est une partie d'une page Web dotée de sa propre URL. Par exemple, les cadres sont souvent utilisés pour placer un menu statique à côté d'une fenêtre de texte défilant.

CENSURER

Censurer consiste à empêcher la publication ou la récupération d'informations, ou prendre des mesures, juridiques ou autres, contre des éditeurs et des lecteurs.

CGI (COMMONGATEWAY INTERFACE)

CGI est une norme commune utilisée pour permettre aux programmes sur un serveur Web de s'exécuter en tant qu'applications Web. De nombreux proxys sur el Web utilisent CGI et sont donc appelés également « proxys CGI ». (Une application proxy CGI très connue et écrite par James Marshall en utilisant le langage de programmation Perl s'appelle CGIProxy).

CHAT

Le chat, également appelé messagerie instantanée, est une méthode de communication entre deux ou plusieurs personnes, dans laquelle chaque ligne saisie par un participant à une session est transmise à tous les autres. Il existe de nombreux protocoles de chat, notamment ceux créés par des sociétés spécifiques (AOL, Yahoo !, Microsoft, Google, etc.), et des protocoles définis publiquement. Certains logiciels de chat client n'utilisent qu'un de ces protocoles et d'autres utilisent toute une gamme de protocoles populaires.

COMMONGATEWAY INTERFACE

Voir CGI.

CONFIDENTIALITE DE LA VIE PRIVEE

La protection de la vie privée signifie empêcher la divulgation de renseignements personnels sans la permission de la personne concernée. Dans le cadre du contournement, cela signifie empêcher les observateurs de découvrir qu'une personne a demandé ou reçu des informations qui ont été bloquées ou qui sont illégales dans le pays où cette personne se trouve à ce moment-là.

CONTOURNEMENT

Le contournement est la publication ou l'accès à du contenu malgré les tentatives de censure.

COOKIE

Un cookie est une chaîne de texte envoyée par un serveur Web au navigateur de l'utilisateur pour la stocker sur l'ordinateur de l'utilisateur, contenant les informations nécessaires pour maintenir la continuité de la session sur plusieurs pages Web, ou à travers plusieurs sessions. Certains sites Web ne peuvent être utilisés si l'on refuse un cookie et son stockage. Certaines personnes considèrent ceci comme une intrusion dans la vie privée ou un risque pour leur sécurité.

CRYPTAGE (CHIFFREMENT)

Le cryptage est toute méthode servant à recoder et brouiller des données ou les transformer mathématiquement pour les rendre illisibles à un tiers qui ne connaît pas la clé secrète servant à les déchiffrer. Il est possible de crypter des donner sur son disque dur local à l'aide d'un logiciel comme TrueCrypt (http://www.truecrypt.org) ou de crypter du trafic Internet avec SSL ou SSH.

Voir aussi décryptage.

DARPA (DEFENSE ADVANCED PROJECTSRESEARCH AGENCY)

La DARPA est le successeur de l'ARPA, qui a financé l'Internet et son prédécesseur,

DECRYPTAGE

Le décryptage est la récupération d'un texte brut ou d'autres messages à l'aide d'une clé.

Voir aussi le cryptage.

DNS (FUITE DE)

Une fuite de DNS se produit quand un ordinateur configuré pour utiliser un proxy pour sa connexion Internet effectue des requêtes DNS sans utiliser le proxy, et dévoile ainsi les tentatives de l'utilisateur pour se connecter à des sites bloqués. Certains navigateurs Web ont des options de configuration, ce qui leur permet d'utiliser obligatoirement le proxy.

DNS (SYSTEME DE NOMS DE DOMAINE)

Le Système de noms de domaines (DNS) convertit les noms de domaines, composés de combinaisons de lettres faciles à mémoriser, en adresses IP, qui sont des chaînes de numéros difficiles à mémoriser. Chaque ordinateur connecté à l'Internet possède une adresse unique (assez semblable à un indicatif régional + numéro de téléphone).

DOMAINE

Un domaine peut être de premier niveau (DPN) ou de second niveau sur Internet.

Voir aussi Domaine de premier niveau, Domaine national de premier niveau et domaine de second niveau.

DOMAINE NATIONAL DE PREMIER NIVEAU (CCTLD)

Chaque pays possède un code pays à deux lettres, et un DPN (domaine de premier niveau) basé sur lui, par exemple .ca pour le Canada ; ce domaine est appelé domaine national de premier niveau. Chaque ccTLD est lié à un serveur DNS qui consigne tous les domaines de second niveau inscrits dans le DPN. Les serveurs racines de l'Internet sont dirigés vers tous les DPN, et mettent en cache les informations fréquemment utilisées dans les domaines de niveau inférieur.

DOMAINE DE PREMIER NIVEAU (TLD)

Dans les noms sur Internet, le TLD ou domaine de premier niveau est le dernier composant du nom de domaine. Il ya plusieurs TLD génériques, notamment .com, .org, .edu, .net, .gov, .mil, .int, et un code pays à deux lettres (ccTLD) pour chaque pays figurant dans le système, comme .ca pour le Canada. L'Union européenne a également un code à deux lettres .eu.

ECOUTE ILLICITE

L'écoute illicite est le fait d'écouter du trafic vocal ou de lire ou de filtrer du trafic de données sur une ligne téléphonique ou une connexion de données numériques, généralement pour détecter ou empêcher des activités illégales ou indésirables ou bien contrôler ou surveiller les propos tenus.

EMAIL

Email, abréviation de "electronic mail" (courrier électronique, abréviation : "courriel") est une méthode pour envoyer et recevoir des messages sur Internet. Il est possible d'utiliser un service de messagerie Web ou d'envoyer des emails à l'aide du protocole SMTP et d'en recevoir à l'aide du protocole POP3 en passant par un client de messagerie comme Outlook Express ou Thunderbird. Il est relativement rare qu'un gouvernement bloque des emails, mais la surveillance des emails est courante. Si l'email n'est pas crypté, il peut facilement être lu par un opérateur de réseau ou un gouvernement.

ENREGISTREUR D'ECRAN

Un enregistreur d'écran est un logiciel capable d'enregistrer tout ce que l'ordinateur affiche à l'écran. La principale fonction d'un enregistreur d'écran est de capturer l'écran et de l'enregistrer sous forme de fichiers, pour le visionner à n'importe quel moment par la suite. Les enregistreurs d'écran peuvent être utilisés comme un puissant outil de contrôle. Il est important de savoir à tout moment si un enregistreur d'écran fonctionne sur l'ordinateur que vous utilisez.

EXPRESSION REGULIERE

Une expression régulière (également appelé regexp ou RE) est un motif de texte qui spécifie un ensemble de chaînes de texte dans la mise en œuvre d'une expression régulière particulière tels que l'utilitaire GREP sous Unix. Une chaîne de texte « correspond » à une expression régulière si la chaîne est conforme au motif, tels que défini par la syntaxe des expressions régulières. Dans chaque syntaxe RE, certains caractères ont une signification particulière, pour permettre à un motif de correspondre à plusieurs autres chaînes. Par exemple, l'expression régulière lo+se correspond à lose, loose, et looose.

FAI (FOURNISSEUR D'ACCES INTERNET)

Un FAI (fournisseur d'accès Internet) est une société ou un organisme qui fournit l'accès à l'Internet à ses clients.

FICHIER JOURNAL

Un fichier journal est un fichier qui enregistre une séquence de messages à partir d'un processus logiciel, qui peut être une application ou un composant du système d'exploitation. Par exemple, les serveurs Web ou les proxys peuvent conserver les fichiers journaux contenant des enregistrements au sujet des adresses IP qui ont utilisé ces services, du moment où elles les ont utilisés et quelles pages ont été consultées.

FILTRE A FAIBLE BANDE PASSANTE

Un filtre à faible bande passante est un service Web qui supprime ou alors compresse des éléments extérieurs comme la publicité et les images d'une page Web, pour accélérer le téléchargement de cette page.

FILTRE DE MOTS CLES

Un filtre de mots clés scanne tout le trafic Internet passant par un serveur pour bloquer des termes ou des mots interdits.

FILTRER

Filtrer consiste à chercher de diverses manières des modèles de données spécifiques pour bloquer ou autoriser des communications.

FIREFOX

Firefox est le navigateur Web libre et open source le plus populaire, développé par la Fondation Mozilla.

FORUM

Sur un site Web, un forum est un lieu de discussion où les utilisateurs peuvent envoyer des messages et des commentaires sur des messages déjà publiés. Il se distingue des listes de diffusion ou des groupes de discussion Usenet par la persistance de pages contenant les fils de messages. Les newsgroups et les archives de la liste de diffusion, par contre, affichent en général un message par page, avec des pages de navigation sur lesquelles ne figurent que les en-têtes des messages du fil.

FTP (FILE TRANSFERPROTOCOL)

Le protocole FTP est utilisé pour les transferts de fichiers. Beaucoup d'utilisateurs sen servent essentiellement pour des téléchargements ; il peut s'utiliser également pour télécharger des pages Web et des scripts sur certains serveurs Web. Il utilise normalement les ports 20 et 21, qui sont parfois bloqués. Certains serveurs FTP utilisent un port peu fréquent qui peut échapper au blocage basé sur le port.

FileZilla est un client FTP libre et open source populaire pour Windows et Mac OS. Il existe également aussi des clients FTP sur le Web utilisables avec un navigateur Web normal comme Firefox.

HOMME DU MILIEU

Un intermédiaire[1] ou « homme du milieu » est une personne ou un ordinateur qui capture le trafic passant dans un canal de communication, en particulier pour modifier ou bloquer sélectivement du contenu de manière à compromettre la sécurité cryptographique. Généralement, l'attaque d'un homme du milieu implique l'usurpation de l'identité d'un site Web, d'un service, ou d'une personne pour enregistrer ou modifier les communications. Les gouvernements peuvent effectuer des attaques de man-in-the-middle au niveau des passerelles pays, là où tout le trafic entrant ou sortant de ce pays doit passer.

HTTP (HYPERTEXT TRANSFER PROTOCOL)

HTTP est le protocole fondamental du World Wide Web (la Toile mondiale) ; il donne les moyens de demander et offrir des pages Web, de faire des requêtes et de créer les réponses à ces requêtes, et d'accéder à un large éventail de services

HTTPS (HTTP SECURISE)

Le HTTP sécurisé est un protocole de communication sécurisé utilisant des messages HTTP cryptés.

Les messages entre le client et le serveur sont cryptés dans les deux sens, grâce à des clés générées lors d'une demande de connexion et qui sont échangées en toute sécurité. Les adresses IP de source et de destination se trouvent dans les en-têtes de chaque paquet ; ainsi, le HTTPS ne peut pas dissimuler l'existence de la communication mais seulement le contenu des données transmises et reçues.

IANA (INTERNET ASSIGNED NUMBERS AUTHORITY)

L'IANA est l'organisme responsable de la partie technique de la gestion de l'infrastructure de l'Internet, notamment l'attribution des blocs d'adresses IP pour les domaines de haut niveau et l'enregistrement des domaines pour les ccTLD et les TLD génériques, la gestion des serveurs de noms racines sur Internet, ainsi que d'autres taches.

ICANN(INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS)

L'ICANN est une société créée par le département américain du Commerce pour gérer les niveaux les plus élevés d'Internet. Son travail technique est effectué par l'IANA.

INTERFACE DE LIGNE DE COMMANDE

Méthode de contrôle d'exécution de logiciels utilisant les commandes saisies sur un clavier, telle que la ligne de commande de Shell Unix ou Windows.

INTERMEDIAIRE

Voir homme du milieu.

INTERNET

L'Internet est un réseau de réseaux interconnectés utilisant le protocole TCP / IP et d'autres protocoles de communication.

IRC (INTERNET RELAY CHAT[2])

L'IRC est un protocole Internet datant d'il y a plus de 20 ans, utilisé pour les conversations texte en temps réel (chat ou messagerie instantanée). Il existe plusieurs réseaux IRC - les plus larges ont plus de 50 000 utilisateurs.

JAVASCRIPT

Javascript est un langage de script couramment utilisé dans les pages Web pour fournir des fonctions interactives.

LATENCE

La latence est une mesure du délai qui se produit dans le système, ici un réseau d'ordinateurs. Elle est mesurée par le temps écoulé entre le début d'une transmission de paquets et le début de la réception des paquets, entre l'extrémité d'un réseau (par ex. vous) et l'autre extrémité (par ex. le serveur Web). Une méthode très efficace de filtrage Web est de maintenir une latence très élevée, ce qui rend très difficile le recours à de nombreux outils de contournement.

LISTE BLANCHE

Une liste blanche est une liste de sites spécialement autorisés pour une forme particulière de communication. Le filtrage du trafic peut s'effectuer soit par une liste blanche (tout est bloqué sauf les sites sur la liste), une liste noire (tout est permis sauf les sites figurant sur la liste), une combinaison des deux, ou par d'autres politiques fondées sur des règles et des conditions spécifiques.

LISTE NOIRE

Une liste noire est une liste de personnes ou de choses interdites. Dans la censure sur Internet, des listes de sites Web interdits peuvent être utilisées comme listes noires ; l'outil de censure peut donner accès à tous les sites excepté ceux figurant sur sa liste noire. Une alternative est la liste blanche, ou liste de choses permises. Un système de liste blanche bloque l'accès à tous les sites excepté ceux énumérés dans la liste blanche. C'est une démarche moins courante en matière de censure sur Internet. Il est possible d'associer les deux démarches, en utilisant la technique de combinaison de chaînes ou d'autres techniques conditionnelles sur les URL qui ne correspondent à aucune de ces listes.

MALWARE (LOGICIELS MALVEILLANTS)

Malware est un terme générique pour les logiciels malveillants, notamment les virus, qui peuvent être installés ou exécutés à votre insu. Les malwares peuvent prendre le contrôle de votre ordinateur pour envoyer des spams par exemple. (Les malwares sont parfois appelé badwares)

MARQUE-PAGE

Un marque-page est un espace dans le logiciel contenant une référence à une ressource externe. Dans un navigateur, le marque-page est une référence à une page Web – en choisissant le marque-page, on peut rapidement charger le site Web sans avoir besoin de saisir son URL complète.

MESSAGERIE INSTANTANEE (IM)

La messagerie instantanée se présente sous deux formes : soit certaines formes de chat propriétaires utilisant des protocoles propriétaires soit le chat en général. Parmi les clients de messagerie instantanée les plus communs figurent MSN Messenger, ICQ, AIM ou Yahoo! Messenger.

MOTEUR DE PROPAGATION DE FICHIERS

Un moteur de propagation de fichiers est un site Web qu'une personne qui veut éditer peut utiliser pour contourner la censure. L'utilisateur n'a qu'à télécharger une fois un fichier à publier et le moteur de propagation de fichiers l'ajoute à un ensemble de services d'hébergement mutualisé (tels Rapidshare ou Megaupload).

NETWORK ADDRESS TRANSLATION (NAT)

Le NAT ou traduction d'adresses réseau est une fonction routeur destinée à dissimuler un espace d'adresses par remappage. Tout le trafic sortant du routeur utilise alors l'adresse IP du routeur qui sait comment acheminer le trafic entrant vers le demandeur. Le NAT est souvent mis en œuvre par les pare-feu. Du fait que les connexions entrantes sont normalement interdites par le NAT, il est difficile d'offrir un service au grand public, tel qu'un site Web ou un proxy public. Sur un réseau où le NAT est utilisé, proposer ce service nécessite un certain type de configuration du pare-feu ou méthode de traversée du NAT.

NOEUD

Un nœud est un dispositif actif sur un réseau. Un routeur est un exemple de nœud. Dans les réseaux Psiphon et Tor, un serveur est appelé nœud.

NOEUD DE NON-SORTIE

Voir aussi nœud intermédiaire.

NOEUD DE SORTIE

Un nœud de sortie est un nœud Tor qui transmet des données à l'extérieur du réseau Tor. Voir aussi nœud intermédiaire.

NOEUD INTERMEDIAIRE

Un nœud intermédiaire est un nœud Tor qui n'est pas un nœud de sortie. Exécuter un nœud intermédiaire peut s'avérer plus sûr que d'exécuter un nœud de sortie : en effet, un nœud intermédiaire ne s'affichera pas dans les fichiers journaux de tierces parties. (Un nœud intermédiaire est parfois appelé nœud de non-sortie.)

NOEUD OUVERT

Un nœud ouvert est un nœud propre à Psiphon qui peut être utilisé sans ouvrir une session. Il charge automatiquement une page d'accueil particulière, et se présente dans une langue particulière, mais peut ensuite être utilisé pour naviguer ailleurs.

Voir aussi nœud Psiphon.

NOEUD PRIVE

Un nœud privé est un nœud Psiphon qui demande pour fonctionner que l'utilisateur s'authentifie, autrement dit il faut s'inscrire avant de pouvoir l'utiliser. Une fois inscrit, on peut envoyer des invitations à ses amis et parents pour qu'ils utilisent ce nœud particulier.

Voir aussi nœud Psiphon.

NOEUD PSIPHON

Un nœud Psiphon est un proxy Web sécurisé conçu pour échapper à la censure sur Internet. Il est développé par la société Psiphon Inc. Les nœuds Psiphon peuvent être ouverts ou privés.

OBSCURCISSEMENT

L'obscurcissement consiste à obscurcir du texte au moyen de techniques de transformation faciles à comprendre et facilement inversables qui résisteront aux inspections superficielles, mais pas à la cryptanalyse, ou à apporter des modifications mineures dans des chaînes de texte pour éviter les associations[3] simples. Les proxys Web utilisent souvent l'obscurcissement pour dissimuler certains noms et adresses aux filtres de texte simple qui pourraient se laisser leurrer par l'obscurcissement. Un autre exemple : tout nom de domaine peut éventuellement contenir un point final, comme dans "somewhere.com.", mais certains filtres ne rechercheraient que "somewhere.com" (sans point final).

OPERATEUR DE RESEAU

Un opérateur de réseau est une personne ou un organisme qui dirige ou contrôle un réseau, ce qui lui permet de surveiller, bloquer ou modifier les communications passant par ce réseau.

OUTIL DE CENSURE

L'outil de censure est un logiciel utilisé pour filtrer ou bloquer l'accès à l'Internet. Ce terme est la plupart du temps utilisé en référence au logiciel de filtrage ou de blocage de l'Internet installé sur la machine client (le PC utilisé pour accéder à l'Internet). La plupart des outils de censure client est utilisée à des fins de contrôle parental.

Quelquefois, le terme outil de censure réfère également au logiciel utilisé aux mêmes fins et installé sur un serveur réseau ou un routeur.

PAQUET

Un paquet est une structure de données définie par un protocole de communication pour contenir des informations spécifiques sous des formes spécifiques, ainsi que des données arbitraires destinées à être communiquées d'un point à un autre. Les messages sont segmentés en paquets pour être envoyés, et ils sont réassemblés à l'autre bout du lien.

PARTAGE DE FICHIERS

Le partage de fichiers fait référence à tout système informatique où plusieurs personnes peuvent utiliser les mêmes informations, mais fait souvent référence au fait de mettre gratuitement à la disposition d'autrui de la musique, des films ou d'autres contenus sur Internet.

PASSERELLE

Une passerelle est un nœud connectant deux réseaux sur Internet. A titre d'exemple, une passerelle nationale qui exige que tout le trafic entrant ou sortant passe par elle.

PEER-TO-PEER

Un réseau peer-to-peer (ou P2P) est un réseau informatique entre paires égales. Contrairement aux réseaux client-serveur il n'y a pas de serveur central, le trafic est donc uniquement distribué parmi les clients. Cette technologie s'applique surtout à des programmes de

partage de fichiers

comme

BitTorrent,

eMule et Gnutella. Mais on peut également classer dans les systèmes peer-to-peer l'ancienne technologie d'

Usenet

ainsi que le programme de

VoIP

Skype.

Voir aussi Partage de fichiers.

PHP

PHP est un langage de script conçu pour créer des sites Web dynamiques et des applications Web. Il est installé sur un serveur Web. Par exemple, PHProxy, proxy Web populaire, utilise cette technologie.

PLAINTEXT

Plaintext est du texte non chiffré, ou un texte décrypté.

Voir aussi cryptage, SSL, SSH.

PONT

Voir pont Tor.

PONT TOR

Un pont est un nœud Tor intermédiaire qui ne figure pas dans le grand annuaire public Tor, et qui peut donc s'avérer utile dans les pays où les relais publics sont bloqués. Contrairement aux cas des nœuds de sortie, les adresses IP des nœuds ponts n'apparaissent jamais dans les fichiers journaux des serveurs et ne passent jamais par les nœuds de contrôle d'une façon qui pourrait être associée à une action de contournement.

POP3

Post Office Protocol version 3 est utilisé pour recevoir du courrier à partir d'un serveur, par défaut sur le port 110 avec un programme d'email comme Outlook Express ou Thunderbird.

PORT

Un port matériel sur un ordinateur est un connecteur physique avec un but précis, utilisant un protocole hardware particulier. Exemples : un port pour moniteur VGA ou un connecteur USB.

Les ports logiciels connectent également des ordinateurs et d'autres périphériques sur des réseaux utilisant différents protocoles, mais ils n'existent dans le logiciel que sous forme de numéros.

Les ports

sont en quelque sorte des portes numérotées donnant sur différentes pièces, chacune d'elles étant dédiée à un service spécial sur un serveur ou un PC. On les identifie par leur numéro qui va de 0 à 65535.

POT DE MIEL (PIEGE)

Un pot de miel est un site qui donne l'apparence d'offrir un service afin d'inciter des utilisateurs potentiels à s'en servir et de capter des informations sur eux ou leurs activités.

PROTOCOLE

C'est la définition formelle d'une méthode de communication, et la forme de données à transmettre pour la réaliser. C'est aussi le but de cette méthode. Par exemple, le protocole Internet (IP) utilisé pour transmettre des paquets de données sur l'Internet, ou le protocole de transfert hypertexte (HTTP) pour les interactions sur le World Wide Web.

PROXY WEB

Un proxy Web est un script qui s'exécute sur un serveur Web agissant comme un proxy/passerelle. Les utilisateurs peuvent accéder à un tel proxy Web avec leur navigateur habituel (par exemple Firefox) en entrant une URL dans le formulaire figurant sur ce site Web. Puis, le programme de proxy Web installé sur le serveur reçoit ce contenu Web qui s'affiche devant l'utilisateur. De cette façon, le FAI ne voit qu'une connexion au serveur à l'aide d'un proxy Web puisqu'il n'y a pas de connexion directe.

REEXPEDITEUR[4]

Un réexpéditeur anonyme est un service qui permet aux utilisateurs d'envoyer des emails de façon anonyme. Le réexpéditeur reçoit des messages par

email

et les transfère à leur destinataire après la suppression des informations qui permettraient d'identifier l'expéditeur d'origine. Certains établissements offrent également une adresse de retour anonyme qui peut être utilisée pour répondre à l'expéditeur d'origine sans divulguer son identité. Parmi les services Réexpéditeur les plus

connus figurent Cypherpunk, Mixmaster et Nym.

REEXPEDITEUR ANONYME

Un réexpéditeur anonyme est un service qui accepte les messages email contenant des instructions pour la transmission, et les envoie sans révéler leurs sources. Du fait que le réexpéditeur a accès à l'adresse de l'utilisateur, au contenu du message, et à la destination du message, les réexpéditeurs doivent être utilisés dans le cadre d'une chaîne de *multiples* réexpéditeurs*, afin* qu'aucun parmi eux ne connaisse l'ensemble de ces informations.

ROUTEUR

Un routeur est un ordinateur qui détermine l'itinéraire pour la transmission des paquets. Il utilise les informations relatives à l'adresse indiquées dans l'en-tête du paquet et les informations mises en cache sur le serveur pour faire correspondre les numéros des adresses avec les connexions hardware.

RSS (REAL SIMPLE SYNDICATION)

Le RSS est une méthode et un protocole pour permettre aux internautes de s'abonner au contenu d'une page Web, et de recevoir les mises à jour dès leur publication.

SAUT

Un saut est un maillon d'une chaîne de transferts de paquets d'un ordinateur à un autre, ou de n'importe quel ordinateur en chemin. Le nombre de sauts entre les ordinateurs peut fournir une mesure approximative du décalage (latence) dans les communications entre eux. Chaque saut individuel est également une entité qui a la capacité d'intercepter, bloquer ou altérer les communications.

SCHEMA

Sur le Web, un schéma est un mapping partant du nom jusqu'au protocole. Ainsi le schéma HTTP mappe les URL commençant par HTTP: jusqu'au protocole de transfert hypertexte. Le protocole détermine l'interprétation du reste de l'URL, de sorte que http://www.example.com/dir/content.html identifie un site Web et un fichier particulier dans un répertoire particulier, et mailto: user@somewhere.com est l'adresse email d'une personne ou d'un groupe particulier dans un domaine particulier.

SCRIPT

Un script est un programme généralement écrit dans un langage interprété et non compilé comme Javascript, Java ou dans un langage interpréteur de commandes comme bash. Beaucoup de pages Web contiennent des scripts pour gérer l'interaction de l'utilisateur avec la page Web, pour éviter que le serveur n'envoie une nouvelle page pour chaque changement.

SCRIPT INTEGRE

Un script intégré est un morceau de code logiciel.

SHELL

Un

shell

Unix est une interface de ligne de commande classique pour les systèmes d'exploitation Unix/Linux. Les shells les plus communs sont sh et

bash.

SERVEUR DNS

Un serveur DNS, ou serveur de nom, est un serveur qui fournit la fonction look-up du Système d'attribution des noms de domaine. Il le fait soit en accédant à un enregistrement existant de l'adresse IP d'un domaine spécifique mis en cache, ou en envoyant une demande de renseignements à un autre serveur DNS.

SERVEUR DE NOM RACINE

Un serveur de nom racine ou serveur racine est l'une des treize grappes de serveurs gérées par l'IANA pour diriger le trafic vers l'ensemble des

TLD

, et se trouve au cœur [5] du système DNS.

SERVEUR PROXY

Un serveur proxy est un serveur, un système informatique ou un programme d'application qui agit comme une passerelle entre un client et un serveur Web. Un client se connecte au serveur proxy pour demander une page Web à partir d'un autre serveur. Ensuite, le serveur proxy accède à la ressource en se connectant au serveur spécifié, et renvoie les informations vers le site demandeur. Les serveurs proxy peuvent servir à des fins diverses, notamment pour restreindre l'accès Web ou aider les utilisateurs à contourner des obstacles.

SMARTPHONE

Un smartphone est un téléphone mobile qui propose des fonctionnalités informatique et une connectivité plus avancées que celles d'un « feature telephone » actuel, par exemple l'accès Web, la capacité à faire fonctionner des systèmes d'exploitation élaborés et à exécuter des applications intégrées.

SOCKS

Un proxy

SOCKS

est un type spécial de serveur proxy. Dans le modèle ISO/OSI, il opère entre la couche d'application et la couche de transport. Le port standard pour les proxys Socks est le 1080, mais ils peuvent aussi fonctionner sur des ports différents. De nombreux programmes prennent en charge une connexion via un proxy SOCKS. Si vous ne pouvez pas installer un client SOCKS comme FreeCap, ProxyCap ou SocksCap qui peuvent contraindre les programmes à s'exécuter via le proxy Socks en utilisant la redirection de port dynamique. Il est également possible d'utiliser des outils

SSH

comme OpenSSH en tant que serveur proxy SOCKS.

SOUS-DOMAINE

Un sous-domaine fait partie d'un domaine plus grand. Si par exemple, « wikipedia.org » est le domaine correspondant à Wikipedia, « en.wikipedia.org » est le sous-domaine correspondant à la version anglaise de Wikipedia.

SPAM

Les spams sont des messages qui submergent un canal de communication utilisé par des personnes, tout particulièrement de la publicité envoyée à un grand nombre de particuliers ou de groupes de discussion. La plupart des spams font de la publicité pour des produits ou des services illégaux d'une manière ou une autre, comportant quasiment toujours un élément d'escroquerie. Le filtrage du contenu des emails pour bloquer le spam, avec la permission du destinataire, est presque universellement approuvé.

SSH (SECURE SHELL)

SSH (ou Secure Shell) est un protocole réseau qui permet la communication cryptée entre ordinateurs. Il a été inventé pour succéder au protocole non crypté de Telnet et est également utilisé pour accéder à un shell sur un serveur distant.

Le port standard SSH est le 22. Il peut être utilisé pour contourner la censure sur Internet avec une redirection des ports ou bien pour créer un tunnel pour d'autres programmes comme VNC.

SSL (SECURE SOCKETS LAYER)

Le SSL (ou Secure Sockets Layer) est l'une des normes cryptographiques utilisées pour effectuer des transactions Internet sécurisées. Elle a servi de base à la création de la norme connexe TLS (Transport Layer Security). Il vous est facile de voir si vous utilisez SSL/TLS en regardant l'URL dans votre navigateur (Firefox ou Internet Explorer) : si elle commence par https au lieu de http, votre connexion est alors cryptée.

STEGANOGRAPHIE

Stéganographie, du grec « écrit caché», se réfère à diverses méthodes utilisées pour envoyer des messages cachés, où non seulement le contenu du message est caché, mais le caractère secret lui-même de l'envoi est également dissimulé. Cela se fait généralement en dissimulant quelque chose à l'intérieur d'autre chose, comme une image ou un texte au thème innocent ou totalement sans rapport. Au contraire de la cryptographie, où il est clair qu'un message secret est transmis, dans la stéganographie, l'attention n'est pas attirée par le fait que quelqu'un tente de dissimuler ou de chiffrer un message.

SURVEILLER

Surveiller consiste à vérifier un flux de données de façon continue pour trouver des activités indésirables.

TCP/IP(TRANSMISSION CONTROL PROTOCOL OVER INTERNET PROTOCOL)

Les TCP et IP sont les protocoles de base d'Internet ; ils traitent la transmission de paquets et le routage. Peu d'autres protocoles sont utilisés à ce niveau de la structure d'Internet ; on peut citer l'UDP.

TEXTE BRUT

Le texte brut est un texte non formaté constitué d'une séquence de codes de caractères, comme dans le texte brut d'ASCII ou le texte brut d'Unicode.

TLS (TRANSPORT LAYER SECURITY)

TLS (

Transport Layer Security)

est une norme de cryptographie basée sur SSL, utilisée pour effectuer des transactions en ligne sécurisées.

TUNNEL

Un tunnel est un itinéraire différent pour passer d'un ordinateur à un autre ; il comprend généralement un protocole qui spécifie le cryptage des messages.

TUNNEL DNS

Un tunnel DNS est un moyen de créer un tunnel pour y faire passer quasiment tout vers des serveurs de noms DNS.
Du fait que vous « trompez » du système DNS de façon non intentionnelle, il permet uniquement une très lente connexion d'environ 3 kb/s ce qui est encore inférieur à la vitesse d'un modem analogique. Cela ne suffit pas pour utiliser YouTube ou partager des fichiers, mais devrait être suffisant pour des messageries instantanées comme ICQ ou MSN Messenger, ainsi que pour des emails au format texte simple.

Sur la connexion pour laquelle vous souhaitez utiliser un tunnel DNS, il suffit que le port 53 soit ouvert ; il fonctionne donc même avec de nombreux fournisseurs d'accès WiFi commerciaux sans devoir payer.

Le problème principal est qu'il n'est pas possible d'utiliser des serveurs DNS publics modifiés. Vous devez créer votre propre serveur DNS. Il vous faut un serveur avec une connexion Internet permanente sous Linux. Vous pouvez y installer le logiciel gratuit OzymanDNS en l'associant à SSH et un proxy comme Squid et utiliser le tunnel. Pour de plus amples informations, consultez http://www.dnstunnel.de/.

UDP (PROTOCOLE DE DATAGRAMME UTILISATEUR)

L'UDP est un autre protocole utilisé avec l'IP. La plupart des services Internet sont accessibles en utilisant un des deux protocoles, TCP ou UDP, mais il y en certains sont préétablis pour n'utiliser qu'une seule de ces alternatives. L'UDP est particulièrement utile pour les applications multimédia en temps réel comme les appels téléphoniques par Internet (VoIP).

URL (UNIFORM RESOURCE LOCATOR)

L'URL (Uniform Resource Locator) est l'adresse d'un site Web. Par exemple, l'URL de la section actualités mondiales du NY Times est http://www.nytimes.com/pages/world/index.html. Beaucoup de systèmes de censure peuvent bloquer une URL unique. Parfois, un moyen facile de contourner ce blocage est de cacher l'URL. A titre d'exemple, il est possible d'ajouter un point après le nom du site, ainsi l'URL http://en.cship.org/wiki/URL devient http://en.cship.org./wiki/URL. Si vous êtes chanceux, avec cette petite astuce vous pourrez avoir accès à des sites Web bloqués.

USENET

Usenet est un système de forum de discussion datant de plus de 20 ans accessible via le protocole NNTP. Les messages ne sont pas stockés sur un serveur, mais sur de nombreux serveurs qui distribuent leur contenu de manière ininterrompue. Pour cette raison, il est impossible de censurer Usenet dans son ensemble ; mais *l'accès* à Usenet peut être bloqué, ce qui arrive souvent ; et n'importe quel serveur particulier est susceptible de n'exécuter qu'un sous-ensemble des groupes de discussion Usenet localement acceptés. En faisant une recherche sur Google, on peut y trouver archivé tout l'historique des messages Usenet.

VOIP (VOICE OVERINTERNET PROTOCOL)

Le terme VoIP (en français Voix sur IP) recouvre plusieurs protocoles de communication vocale bidirectionnelle en temps réel sur l'Internet, ce qui est généralement beaucoup moins coûteux que de faire des appels sur les réseaux des compagnies de téléphone. Il n'est pas soumis aux types d'écoute pratiqués sur les réseaux téléphoniques, mais peut être contrôlé à l'aide de la technologie numérique. De nombreuses entreprises produisent des logiciels et du matériel d'espionnage pour les appels VoIP ; les technologies VoIP cryptées n'ont commencé à apparaître que récemment.

VPN (RESEAU PRIVE VIRTUEL)

Un VPN

(réseau privé virtuel)

est un réseau de communication privé utilisé par de nombreuses sociétés et organisations pour communiquer en toute sécurité sur un réseau public. Il est généralement crypté sur Internet ; ainsi, personne, sauf les utilisateurs aux deux extrémités de la communication peuvent regarder le trafic de données. Il existe diverses normes, comme IPSec, SSL, TLS ou PPTP. L'utilisation d'un fournisseur de VPN est une méthode très rapide, sûre et pratique pour contourner la censure sur Internet avec peu de risques mais généralement payante.

WEBMAIL

Le Webmail est un service d'email via un site Web. Ce service envoie et reçoit des messages pour les utilisateurs sur le mode habituel, mais fournit une interface Web pour la lecture et la gestion des messages, comme alternative à un client de messagerie tel qu'Outlook Express ou Thunderbird installé sur l'ordinateur de l'utilisateur. https://mail.google.com/ est un exemple de service Webmail populaire et gratuit.

WHOIS

WHOIS (traduction : qui est ?) est la fonction Internet bien nommée qui permet de rechercher dans des bases de données WHOIS distantes des informations sur des noms de domaines. Grâce à une simple recherche sur WHOIS, on peut découvrir quand et par qui un nom de domaine a été enregistré, les coordonnées correspondantes, etc.

Une recherche sur WHOIS peut également révéler le nom ou le réseau mappé à une adresse IP numérique.

WORLDWIDE WEB(WWW)

Le World Wide Web est le réseau de liens hypertexte des domaines et des contenus de page accessible par le protocole de transfert hypertexte et ses nombreuses extensions. Le World Wide Web est la partie la plus célèbre d'Internet.

[1] I also found the term in French : "intercepteur".
[2] En français : Discussion relayée par Internet.
[3] Please check ("simples matches").
[4] Please note: the title is "Remailer" and in the text, it says "anonymous remailer".
[5] Did not quite understand here « as the core of the DNS system".

40. DIX CARACTÉRISTIQUES

Par Roger Dingledine, chef de projet du Projet Tor

L'augmentation du nombre de pays qui répriment l'utilisation de l'Internet entraîne le développement de logiciels anti-censure, leur permettant d'accéder à des sites Web bloqués. De nombreux types de logiciels, qu'on appelle généralement outils de contournement, ont été créés en réponse à la menace qui pèse sur la liberté sur Internet. Ces outils fournissent différentes options et niveaux de sécurité, et il est important que les utilisateurs en comprennent les avantages et les inconvénients.

Cet article expose dix caractéristiques qui sont à prendre en compte pour évaluer un outil de contournement. Le but n'est pas de recommander un outil en particulier, mais d'indiquer quel type d'outil est utile selon la situation. J'ai choisi l'ordre des caractéristiques en me basant sur la facilité de présentation. Il ne faudra pas en conclure que la première est la plus importante.

Un logiciel de contournement sur Internet comprend deux éléments : un élément relais et un élément découverte.L'élément relais est ce qui établit une connexion vers un serveur ou proxy, effectue le chiffrement et envoie le trafic dans les deux sens. L'élément découverte est l'étape qui précède, le processus pour trouver une ou deux adresses accessibles.

Certains outils ne possèdent qu'un élément relais. Par exemple, si vous utilisez un proxy ouvert, son processus d'utilisation est simple : vous configurez votre navigateur Web ou une autre application pour qu'ils utilisent le proxy. Le plus difficile pour les utilisateurs d'un proxy ouvert est d'arriver à en trouver un qui soit fiable et rapide. Par ailleurs, certains outils possèdent des éléments de relais bien plus élaborés, constitués de proxys multiples, de couches de chiffrement multiples, etc.

Il faut au préalable que je dise tout de même que je suis l'inventeur et développeur d'un outil, Tor, utilisé aussi bien pour la confidentialité de la vie privée que le contournement de la censure. Si ma préférence pour des outils plus sûrs comme Tor transparaît ici et se fonde sur les caractéristiques que j'ai relevées (autrement dit, je soulève des questions qui me permettent de souligner les points forts de Tor et auxquelles d'autres développeurs d'outils n'accordent pas d'importance), j'ai également essayé d'inclure des caractéristiques considérées comme importantes par d'autres développeurs.

1. Utilisé par un ensemble varié d'utilisateurs

L'une des questions élémentaires que vous pouvez vous poser quand vous examinez un outil de contournement est : « Qui d'autre l'utilise ? ». Si l'éventail d'utilisateurs est large, cela signifie que si quelqu'un découvre que vous utilisez ce logiciel, ils ne peuvent en déduire la raison pour laquelle vous l'utilisez. Un outil qui préserve la confidentialité de la vie privée comme Tor est utilisé par des types d'utilisateurs très variés à travers le monde (cela peut aller de simples particuliers et défenseurs des droits de l'homme à des sociétés, des organes chargés de l'application de la loi et des militaires ; donc le fait que vous ayez Tor ne donne pas beaucoup d'autres indications sur votre identité et sur les sites Web que vous visiteriez. Par ailleurs, imaginez un groupe de blogueurs iraniens utilisant un outil de contournement conçu spécialement pour eux. Si quelqu'un découvre que l'un d'eux l'utilise, ce ne sera pas compliqué pour cette personne d'en deviner la raison.

Au-delà des caractéristiques techniques qui rendent un outil donné utile à quelques personnes dans un pays ou à beaucoup de gens à travers le monde, le marketing joue un grand rôle, dans lequel les utilisateurs interviennent. Beaucoup d'outils se font connaître par le bouche à oreille et ainsi, si les quelques premiers utilisateurs se trouvent au Vietnam et qu'ils le trouvent utile, les utilisateurs qui suivront seront en général plutôt des Vietnamiens aussi. Si un outil est traduit dans certaines langues et pas dans d'autres, ce facteur peut aussi influer sur le type d'utilisateur qu'il attirera ou pas.

2. Fonctionne dans votre pays

La question suivante à examiner est de savoir si l'opérateur de l'outil limite artificiellement la liste des pays où il peut être utilisé. Durant plusieurs années, la société commerciale Anonymizer.com offrait ses services gratuitement aux Iraniens. Ainsi, les connexions venant des serveurs d'Anonymizer étaient soit des clients payants (essentiellement aux Etats-Unis) ou des Iraniens qui tentaient de contourner les filtres de leur pays.

Citons quelques exemples plus récents :

Your-Freedom restreint l'utilisation gratuite à quelques pays comme la Birmanie, alors que parfois, des systèmes comme Freegate et UltraSurf bloquent carrément les connexions venant de tout pays en dehors des quelques-uns qu'ils ont choisi de desservir (Chine et, dans le cas d'Ultrasurf récemment, l'Iran). D'un côté, cette stratégie se comprend car cela limite les coûts en termes de bande passante. Mais d'un autre côté, si vous vivez en Arabie saoudite et que vous avez besoin d'un outil de contournement, certains outils par ailleurs utiles ne vous conviendront pas comme option.

3. S'accompagne d'un réseau durable et bénéficie d'une stratégie de développement de logiciels

Si vous comptez investir du temps pour comprendre comment utiliser un outil donné, vous devez vous assurer que celui-ci existera pendant un certain temps. Il existe plusieurs manières pour différents outils de perdurer sur le long terme. Les trois principales sont l'utilisation de bénévoles, la réalisation de bénéfices et l'obtention de financements par des sponsors.

Des réseaux comme Tor font appel à des bénévoles pour fournir des relais qui constituent le réseau.

Des milliers de gens dans le monde possèdent des ordinateurs et de bonnes connexions de réseau et désirent contribuer à l'avènement d'un monde meilleur. En les réunissant en un seul grand réseau, Tor s'assure l'indépendance de ce réseau par rapport à l'organisation qui réalise le logiciel ; de cette manière, le réseau poursuivra son œuvre même si le Projet Tor en tant qu'entité cesse d'exister. Psiphon adopte la seconde démarche : faire payer le service. Leur raisonnement est que s'ils réussissent à créer une entreprise rentable, celle-ci sera en mesure de financer le réseau de manière permanente. La troisième démarche consiste à compter sur des sponsors pour payer les coûts de bande passante. Le projet Java Anon Proxy ou « JAP Project » s'est appuyé sur des subventions gouvernementales pour financer sa bande passante ; maintenant que la subvention est épuisée, ils étudient une approche fondée sur le profit. Ultrareach et Freegate font appel au système de sponsorat avec une certaine efficacité, mais sont constamment en quête de nouveaux sponsors pour maintenir leur réseau.

Après la question sur la survie à long terme du réseau, la question suivante concerne la viabilité du logiciel lui-même. Ces mêmes trois approches sont valables ici également, mais les exemples sont différents. Le réseau de Tor fonctionne grâce à des bénévoles, mais Tor compte sur des sponsors (gouvernements et ONG) pour financer de nouvelles fonctionnalités et la maintenance logicielle. Ultrareach et Freegate, par contre, se trouvent dans une position plus viable en matière de mises à jour de logiciels : ils disposent d'une équipe composée de personnes à travers le monde, essentiellement des bénévoles, qui se consacrent à veiller à ce que les outils aient toujours une longueur d'avance par rapport aux censeurs.

Chacune des trois approches peut fonctionner, mais comprendre la démarche utilisée par un outil peut aider à anticiper sur les problèmes qu'il peut rencontrer dans l'avenir.

4. Une conception ouverte

La première étape vers la transparence et la réutilisation du logiciel et de la conception de l'outil est de distribuer le logiciel (pas simplement le logiciel client, mais aussi le logiciel serveur) sous licence en code source libre. Ce type de licence signifie que vous pouvez examiner le logiciel pour voir comment il fonctionne effectivement, et vous avez le droit de modifier le programme. Même si tous les utilisateurs ne tirent pas parti des avantages de cette opportunité (beaucoup de gens veulent simplement utiliser l'outil tel quel), le fait de proposer cette option augmente la probabilité que l'outil demeure sûr et utile. Sinon, il ne vous reste plus qu'à espérer qu'un petit nombre de développeurs aient pensé à tous les problèmes possibles et les aient tous réglés.

Avoir une licence en code source libre ne suffit pas. Les outils de contournement fiables doivent fournir une documentation claire et complète pour d'autres experts en sécurité, pas seulement sur la manière dont ils sont conçus mais aussi sur les fonctionnalités et buts recherchés par ses développeurs. L'ont-ils conçu pour protéger la vie privée ? Quelle sorte de cyber-attaquant et contre lesquels ? Comment utilise-t-il le chiffrement ? L'ont-ils conçu pour résister aux attaques des censeurs ? A quelles attaques pensent-ils résister et pourquoi leur outil résistera-t-il à ces attaques ? Si l'on ne voit pas le code source et qu'on ne sait pas à quoi les développeurs le destinent, il est plus difficile de décider si l'outil renferme des problèmes de sécurité, ou d'évaluer s'il atteindra ses objectifs.

Dans le domaine de la cryptographie, le principe de Kerckhoffs explique que l'on doit concevoir son système de manière à ce que le volume de ce que l'on veut garder secret soit aussi petit et bien compris que possible. C'est pourquoi les algorithmes de cryptographie ont des clés (la partie secrète) et le reste peut être expliqué publiquement à tout le monde. Historiquement, toute conception cryptographique contenant beaucoup d'éléments secrets s'est avérée moins sûr que le pensaient ses concepteurs. De même, dans le cas de conceptions secrètes pour des outils de contournement, les seuls groupes qui examinent l'outil sont les développeurs qui l'ont créé et ses cyber-attaquants ; les autres développeurs et utilisateurs qui pourraient contribuer à le perfectionner et le rendre plus viable n'ont pas leur mot à dire.

Les idées issues d'un projet pourraient être réutilisées au-delà de la durée de vie de ce projet. Un trop grand nombre d'outils de contournement sont le résultat d'une conception dont le secret reste gardé, dans l'espoir que les censeurs de gouvernements aient plus de mal à comprendre comment le système fonctionne, mais ceci a pour résultat que peu de projets peuvent tirer les enseignements d'autres projets et que le domaine du développement du contournement dans son ensemble évolue trop lentement.

5. Possède une architecture décentralisée

Une autre caractéristique à rechercher dans un outil de contournement est de savoir si son réseau est centralisé ou décentralisé. Un outil centralisé fait passer toutes les requêtes de ses utilisateurs par un ou quelques serveurs contrôlés par l'opérateur de l'outil. Une conception décentralisée comme celle de Tor ou JAP envoie le trafic à travers des emplacementsdifférentsmultiples, de sorte qu'il n'y a pas une seule localisation ou entité qui puisse observer à quels sites Web chaque utilisateur a accès.

Une autre manière de regarder cette division est basée sur la centralisation ou la décentralisation de la confiance. Si vous devez placer toute votre confiance dans une seule entité, tout ce que vous pouvez espérer alors est que figure un « Enoncé de confidentialité » pour protéger la vie privée, autrement dit, qu'ils possèdent toutes vos données et qu'ils promettent de ne pas les regarder, les perdre ou les vendre. L'autre option est ce que le Commissaire à l'information et à la protection de la vie privée de l'Ontario appelle « protection de la vie privée intégrée dans la conception », autrement dit que la conception du système elle-même est telle que la confidentialité de la vie privée des utilisateurs est garantie. Le caractère ouvert de la conception permet à tout le monde d'évaluer le degré de confidentialité de la vie privée offert.

Cette préoccupation n'est pas simplement théorique. Au début de l'année 2009, Hal Roberts, du Berkman Center, est tombé sur un article d'une rubrique FAQ relatif à un outil de contournement qui proposait de vendre les journaux de clics de ses utilisateurs. Plus tard, j'ai parlé avec un fournisseur différent d'outils de contournement qui m'a expliqué qu'ils disposaient de tous les journaux de chaque requête faite par le biais de leur système « parce qu'on ne sait jamais quand on pourrait en avoir besoin ».

Je n'ai pas donné les noms des outils ici parce que la question n'est pas que le fait que certains fournisseurs d'outils ont peut-être partagé les données d'utilisateurs ; la question est que tout outil reposant sur un modèle de confiance est susceptible de partager des données d'utilisateurs, et ses utilisateurs n'ont aucun moyen de s'en rendre compte si cela se produit. Pis encore, même si le fournisseur d'outil est de bonne foi, le fait que toutes les données passent par un seul lieu constitue une cible attirante pour d'autres cyber-attaquants qui viendront espionner.

Nombre de ces outils considèrent le contournement et la confidentialité de la vie privée de l'utilisateur comme des objectifs totalement distincts. Cette séparation n'est pas forcément mauvaise, tant que vous savez à quoi vous vous engagez ; par exemple, beaucoup de personnes vivant dans des pays qui pratiquent la censure nous disent que la simple lecture d'un site d'informations n'entraîne pas l'emprisonnement. Mais, comme nous nous en sommes rendu compte ces dernières années, dans de nombreux contextes, les grandes bases de données contenant des informations personnelles ont trop souvent tendance à être rendues publiques.

6. Vous protège des sites Web également

La confidentialité de la vie privée n'est pas seulement liée à la question de savoir si l'opérateur de l'outil peut consigner vos requêtes. Elle dépend aussi de la capacité des sites Web que vous visitez à vous reconnaître ou vous suivre. Souvenez-vous du cas de Yahoo qui avait communiqué des informations au sujet d'un des utilisateurs chinois de son service de courrier électronique ? Et si un agrégateur de blogs veut savoir qui publie des billets sur un blog, ou qui a ajouté le dernier commentaire, quels autres sites Web un blogueur particulier lit ? L'utilisation d'un outil plus sûr pour accéder à un site web signifie que ce site Web n'en aura pas autant à communiquer.

Certains outils de contournement sont plus sûrs que d'autres. A un extrême se trouvent les proxys ouverts. Ils transmettent souvent l'adresse du client avec la requête de recherche Web de ce dernier ; il est ainsi facile pour le site Web de savoir exactement d'où provient la requête. A l'autre extrême se trouvent les outils comme Tor qui comprennent des extensions client du navigateur permettant de dissimuler la version de votre navigateur, votre choix de langue, la taille de la fenêtre du navigateur, le fuseau horaire, etc. ; d'isoler les cookies, l'historique et le cache ; et d'empêcher des plugins comme Flash de divulguer des informations à votre sujet.

Ce degré de protection au niveau de l'application a cependant un prix : certains sites Web ne fonctionnent pas correctement. Comme de plus en plus de sites Web adoptent la dernière mode qu'est le « web 2.0 », ils ont besoin d'avoir des fonctionnalités de plus en plus invasives en matière de comportement du navigateur. La meilleure réponse est de désactiver les comportements dangereux, mais si quelqu'un en Turquie essaie d'accéder à YouTube et que Tor désactive son plugin Flash pour préserver sa sécurité, sa vidéo ne marchera pas.

Aucun outil n'a jusque-là n'a trouvé de solution à ces avantages et inconvénients. Le logiciel Psiphon évalue manuellement chaque site Web et programme son proxy central pour réécrire chaque page. Il effectue généralement cette réécriture no pour des raisons de confidentialité de la vie privée mais pour s'assurer que tous les liens sur la page ramènent vers leur service proxy, mais le résultat est que s'il n'a pas encore vérifié manuellement votre site de destination, cela ne marchera pas dans votre cas. Par exemple, il semble avoir toujours du mal à suivre le rythme des changements fréquents de la page d'accueil de Facebook. Actuellement, Tor désactive du contenu qui est probablement sûr en pratique, parce que nous n'avons pas mis au point une bonne interface pour laisser l'utilisateur décider en toute connaissance de cause. Cependant, d'autres outils laissent simplement passer tout contenu actif, signifiant par-là que démasquer leurs utilisateurs est un aspect négligeable.

7. Ne promet pas de crypter comme par magie tout l'Internet

Je dois ici faire une distinction entre chiffrement et confidentialité de la vie privée. La plupart des outils de contournement (tous à l'exception des outils vraiment simples comme les proxys ouverts) cryptent le trafic entre l'utilisateur et le fournisseur de contournement. Ce chiffrement leur est indispensable pour éviter le filtrage des mots clés par des censeurs comme le pare-feu mis en place par la Chine. Mais aucun des outils ne peut crypter le trafic entre le fournisseur et les sites Web de destination si un de ces sites n'accepte pas le chiffrement ; le trafic ne peut en aucun cas se retrouver crypté par un coup de baguette magique.

La solution idéale serait que chacun utilise le protocole https (connu également sous le nom de SSL) pour accéder à des sites Web, et que tous les sites Web acceptent les connexions en https. S'il est utilisé correctement, le protocole https offre un chiffrement entre votre navigateur et le site Web. Avec ce chiffrement « de bout en bout », personne sur le réseau (que ce soit votre FAI, les fournisseurs de backbones Internet à haut débit ou votre fournisseur de contournement) ne peut écouter le contenu de vos communications. Mais pour de multiples et diverses raisons, le chiffrement demeure omniprésent. Si site Web n'accepte pas le chiffrement, le mieux est de 1) ne pas envoyer d'informations sensibles ou permettant de vous identifier, comme indiquer le vrai nom dans le billet publié sur un blog ou un mot de passe que vous ne voulez pas divulguer à autrui, puis 2) utiliser un outil de contournement qui ne possède pas de goulots d'étranglement au plan de la confiance permettant à autrui d'établir un lien entre vous et vos destinations, malgré les précautions prises dans l'étape 1.

Malheureusement, les choses se gâtent quand vous ne pouvez pas vous empêcher d'envoyer des informations sensibles. Certaines personnes ont exprimé leur inquiétude à l'égard du concept réseau fonctionnant avec des bénévoles créé par Tor ; leur raisonnement est qu'au moins, avec les conceptions centralisées, on sait qui contrôle l'infrastructure. Mais en pratique, il est difficile pour des inconnus de lire votre trafic dans un sens ou dans l'autre. L'alternative se situe entre des inconnus bénévoles qui ignorent votre identité (autrement dit, ils ne peuvent vous cibler) ou des inconnus dévoués qui ont la possibilité de voir tout le profil de votre trafic (et de faire le lien entre vous et lui). Tous ceux qui promettent « 100 % de sécurité » cherchent à vendre leur produit.

8. Fournit une bonne qualité de latence et de débit

La caractéristique que vous rechercherez ensuite dans un outil de contournement sera probablement la rapidité. Certains outils ont tendance à être systématiquement rapides, d'autres systématiquement lents et certains ont des performances extrêmement imprévisibles. La rapidité dépend de nombreux facteurs, notamment du nombre d'utilisateurs que possède le système, de ce que ces utilisateurs font, de la capacité disponible et de la répartition de la charge dans le réseau.

Les modèles de confiance centralisés présentent deux avantages ici. D'abord, ils peuvent voir tous leurs utilisateurs et ce que ces derniers font ; ils sont donc bien placés pour les répartir uniformément et décourager les comportements qui posent des problèmes au système. Ensuite, ils ont les moyens de payer pour avoir plus de capacité, et plus ils payent, plus l'outil est rapide. Par contre, les modèles de confiance distribuée ont plus de difficulté à suivre leurs utilisateurs, et s'ils s'appuient sur des bénévoles pour fournir cette capacité, avoir plus de bénévoles est un processus plus complexe que de simplement acheter de la bande passante.

Le revers de la médaille en matière de performance est la flexibilité. De nombreux systèmes procurent une vitesse satisfaisante en limitant ce que les utilisateurs peuvent faire. Alors que Psiphon vous empêche d'accéder à des sites qu'il n'a pas vérifiés manuellement, Ultrareach et Freegate exercent une réelle censure et de manière active sur le choix de sites Web de destination auxquels vous pouvez accéder, et ils peuvent ainsi limiter les coûts liés à la bande passante. Tor, par contre, vous permet d'accéder à n'importe quel protocole et n'importe quelle destination ; par exemple, vous pouvez aussi l'utiliser pour de la messagerie instantanée ; mais l'inconvénient est que le réseau est souvent surchargé par les utilisateurs qui effectuent des transferts de gros fichiers.

9. Facilite l'acquisition du logiciel et des mises à jour

Quand un outil de contournement commence à être bien connu, son site Web ne tarde pas à être bloqué. S'il est impossible d'obtenir une copie de l'outil lui-même, qui se soucie de sa qualité ? La meilleure réponse à cela de ne pas avoir besoin d'un logiciel client spécialisé. Psiphon, par exemple, s'appuie sur un navigateur Web normal ; ainsi, si les censeurs bloquent son site Web, cela n'a aucune importance. Une autre méthode consiste à se servir d'un petit programme comme Ultrareach ou Freegate qui vous permet d'envoyer des mails à vos amis. La troisième option est le Pack de navigation Tor : il est proposé avec tous les logiciels dont vous avez besoin préconfigurés ; mais du fait qu'il comprend des programmes lourds tels Firefox, il est difficile à faire circuler sur Internet. Dans ce cas, la distribution se fait plutôt via les réseaux sociaux et par clé USB, ou en utilisant notre répondeur automatique de courrier électronique qui vous permet de télécharger Tor via Gmail.

Il vous faut ensuite étudier les avantages et inconvénients propres à chaque démarche. D'abord, quels systèmes d'exploitation sont-ils acceptés ? Là aussi, Psiphon est bien placé parce qu'il ne demande pas de logiciel client supplémentaire. Ultrareach et Freegate sont si spécialisés qu'ils ne fonctionnent qu'avec Windows, tandis que Tor et les logiciels qui l'accompagnent peuvent fonctionner pratiquement avec tous les systèmes d'exploitation. Ensuite, prenez en compte que le logiciel client peut automatiquement gérer une défaillance d'un proxy à un autre, et que vous n'avez pas besoin de saisir manuellement une nouvelle adresse si votre adresse du moment disparaît ou est bloquée.

Enfin, l'outil a-t-il de l'expérience pour réagir face à un blocage ? Par exemple, Ultrasurf et Freegate ont l'habitude de procéder à de rapides mises à jour quand la version en cours de leur outil cesse de fonctionner. Ils possèdent une grande expérience de ce jeu particulier du chat et de la souris ; on peut donc raisonnablement en déduire qu'ils sont prêts pour le prochain round. Dans le même ordre d'idée, Tor s'est préparé à un éventuel blocage en simplifiant ses communications en réseau pour qu'elles apparaissent plus comme une navigation sur Internet cryptée, et en intégrant des « relais-ponts » non publiés qui sont plus difficiles à trouver et à bloquer pour un cyber-attaquant que les relais publics de Tor. Tor s'efforce de séparer les mises à jour des logiciels de celles de l'adresse du proxy. Si le relais-pont que vous utilisez se bloque, vous pouvez conserver le même logiciel et simplement le configurer pour utiliser une nouvelle adresse de pont. Notre système de ponts a été mis à l'épreuve en Chine en septembre 2009, et des milliers d'utilisateurs sont passés sans difficulté des relais publics aux ponts.

10. Ne se présente pas en tant qu'outil de contournement

De nombreux outils de contournement font l'objet d'une forte médiatisation lors de leur lancement. Les médias aiment beaucoup cette démarche, et cela donne des articles à la une avec comme titre « Des hackers américains déclarent la guerre à la Chine ! » Mais même si cette attention portée sur eux contribue à leur attirer un soutien (bénévoles, profit, sponsors), la publicité attire également l'attention des censeurs.

Les censeurs bloquent généralement deux catégories d'outils : 1) ceux qui fonctionnent vraiment bien, c'est-à-dire qui ont des centaines de milliers d'utilisateurs, et 2) ceux qui font beaucoup de bruit. Bien souvent, la censure n'a pas tant comme but de bloquer tous les contenus sensibles que de créer une atmosphère de répression pour amener les gens à s'autocensurer. Des articles dans la presse menacent l'apparence de contrôle par les censeurs, et ceux-ci sont bien obligés de réagir.

La leçon à en tirer est que nous contrôlons le rythme de la course aux armements. Contrairement à la logique, même si un outil a plusieurs utilisateurs, tant que personne n'en parle beaucoup, il aura tendance à ne pas être bloqué. Mais si personne n'en parle, comment les utilisateurs en connaitront-ils l'existence. Une solution à ce paradoxe est de faire passer l'information de bouche à oreille et via les réseaux sociaux plutôt que par les médias plus classiques. Une autre démarche est de positionner l'outil dans un contexte différent ; par exemple, nous présentons Tor avant tout comme un outil conçu pour la protection de la vie privée et des libertés civiles plutôt que comme outil de contournement. Hélas, cet exercice d'équilibre est difficile à poursuivre face à une popularité grandissante.

Conclusion

Cet article explique quelques-uns des aspects que vous devez examiner quand vous évaluez les points forts et les points faibles des outils de contournement. J'ai délibérément évité de présenter un tableau des différents outils et de leur attribuer une note dans chaque catégorie. Quelqu'un le fera sûrement un jour et additionnera le nombre de cases cochées pour chaque outil, mais la question ici n'est pas de trouver le « meilleur » outil. Un éventail varié d'outils de contournement largement utilisé accroît la solidité de tous les outils, du fait que les censeurs doivent s'attaquer à toutes les stratégies à la fois.

Pour conclure, nous devons garder à l'esprit que la technologie ne résoudra pas tout le problème. Après tout, les pare-feu ont beaucoup de succès auprès du public dans ces pays. Tant que de nombreuses personnes dans les pays subissant la censure disent : « Je suis content, mon gouvernement protège ma sécurité sur Internet », les enjeux sociaux sont au moins aussi importants. Mais en même temps, il y a des gens dans tous ces pays qui désirent avoir des informations et les propager en ligne, et c'est pourquoi une solution technique efficace demeure une pièce essentielle du puzzle.

Roger Dingledine est chef de projet dans le cadre du Projet Tor, initiative américaine à but non lucratif qui mène une activité de recherche et développement en matière d'anonymat pour le compte d'organisations aussi diverses que l'US Navy, l'Electronic Frontier Foundation et la Voix de l'Amérique. En plus de toutes les casquettes qu'il porte pour Tor, Roger organise des congrès scientifiques sur l'anonymat, est intervenant dans une grande variété de conférences sectorielles[1] et conférences de hackers[2]. Il dirige également des stages sur le thème de l'anonymat pour les services répressifs étrangers et nationaux.

 Rédigé à l'origine pour le magazine *Index on Censorship* de mars 2010, puis adapté pour le « China Rights Forum » de juillet 2010 (traduction chinoise) [3]. Dernière mise à jour, le 25 mai 2010.

41. ALLER PLUS LOIN

Le contournement de la censure sur Internet est un sujet vaste. Des dizaines d'outils et de services sont disponibles. Il y a de nombreux aspects à considérer si vous souhaitez cacher le fait que vous contournez la censure, devenir anonyme sur Internet ou aider d'autres personnes à échapper à la censure. Voici quelques ressources conseillées (certaines peuvent être censurées ou inaccessibles à certains endroits).

MANUELS ET GUIDES

Contourner la censure d'Internet

- Reporters Sans Frontières : *Manuel des Bloggeurs et Cyberdissidents,* http://www.rsf.org/article.php3?id_article=26187
- Wiki sur la censure d'Internet (anglais) : http://en.cship.org/wiki/

Conseils de sécurité informatique pour les activistes

- NGO-in-a-Box, une collection d'applicatifs libres et portables (anglais) : https://security.ngoinabox.org
- Sécurité numérique et vie privée pour les défenseurs des droits de l'Homme (anglais) : https://www.frontlinedefenders.org/esecman
- Surveillance Self-Defense Internationale : https://www.eff.org/wp/surveillance-self-defense-international

Études sur la censure de l'Internet

- Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), ISBN 0-262-54196-3 http://www.opennet.net/accessdenied/
- Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), ISBN 0-262-51435-4 http://www.access-controlled.net
- Hal Roberts, Ethan Zuckerman, Jillian York, Rob Faris, John Palfrey, *2010 Circumvention Tool Usage Report* (Berkman Center for Internet & Society) http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage
- Plus de ressources sur la censure : http://bailiwick.lib.uiowa.edu/journalism/mediaLaw/cyber_censors.html

ORGANISATIONS TRAVAILLANT À DOCUMENTER, COMBATTRE OU CONTOURNER LES RESTRICTIONS SUR INTERNET

- Citizen Lab (http://www.citizenlab.org)
- Comité de protection des blogueurs (http://www.committeetoprotectbloggers.org)
- Comité de protection des Journalistes (https://www.cpj.org)
- Centre Berkman pour Internet et la société (http://cyber.law.harvard.edu)
- Fondation frontière électronique (https://www.eff.org)
- FrontLine (https://www.frontlinedefenders.org)
- Consortium sur la liberté d'Internet (http://www.internetfreedom.org)
- The Herdict (https://www.herdict.org/web)
- OpenNet Initiative (http://opennet.net)
- Peacefire (http://www.peacefire.org)
- Reporters Sans Frontières (http://www.rsf.org)
- Sesawe (https://sesawe.net)
- Tactical Tech Collective (https://www.tacticaltech.org)

PROXIES OUVERTS POUR LE WEB OU LES

APPLICATIONS

- Liste de centaines de proxys ouverts sur : http://www.proxy.org
- Peacefire, une mailing list qui répertorie et transmet la liste des nouveaux proxys mis à jour : http://www.peacefire.org/circumventor/,
- Application proxies:
  - http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists/
  - http://www.publicproxyservers.com

SOLUTIONS DE CONTOURNEMENT ET FOURNISSEURS DE SERVICES

- Access Flickr!: https://addons.mozilla.org/en-US/firefox/addon/4286
- Alkasir: https://www.alkasir.com/
- CECID: http://cecid.labyrinthdata.net.au/
- Circumventor CGIProxy: http://peacefire.org/circumventor/
- Codeen: http://codeen.cs.princeton.edu/
- Coral: http://www.coralcdn.org/
- CProxy: http://www.cproxy.com/
- Dynaweb FreeGate: http://www.dit-inc.us/freegate
- FirePhoenix: http://firephoenix.edoors.com/
- FoxyProxy: http://foxyproxy.mozdev.org/
- Glype: http://www.glype.com/
- GPass: http://gpass1.com/gpass/
- GProxy: http://gpass1.com/gproxy.php
- Gtunnel: http://gardennetworks.org/products
- Guardster: http://www.guardster.com/
- Hamachi LogMeIn: https://secure.logmein.com/products/hamachi/vpn.asp
- hopster: http://www.hopster.com/
- HotSpotVPN: http://hotspotvpn.com/
- HTTPS Everywhere: https://www.eff.org/https-everywhere
- httpTunnel: http://www.http-tunnel.com/
- JAP / JonDo: http://www.jondos.de/en
- Megaproxy: http://www.megaproxy.com/
- OpenVPN: http://www.openvpn.net/
- PHProxy: http://sourceforge.net/projects/poxy/
- Picidae: http://www.picidae.net/
- Proxify: http://proxify.com/
- psiphon: http://www.psiphon.ca/
- PublicVPN: http://www.publicvpn.com/
- SabzProxy: http://www.sabzproxy.com/
- Simurgh: https://simurghesabz.net/
- SmartHide: http://www.smarthide.com/
- Tor: https://www.torproject.org/
- TrafficCompressor: http://www.tcompressor.ru/
- UltraReach UltraSurf: http://www.ultrareach.com/
- Your-Freedom: http://www.your-freedom.net/

Une liste de fournisseurs de VPN à but commerciaux

- http://en.cship.org/wiki/VPN

Logiciels de Socksification (pour permettre à un logiciel non conçu pour fonctionner à travers un proxy d'utiliser un proxy SOCKS)

- tsocks: http://tsocks.sourceforge.net/
- WideCap: http://www.widecap.com/
- ProxyCap: http://www.proxycap.com/
- FreeCap: http://www.freecap.ru/eng/
- Proxifier: http://www.proxifier.com/
- SocksCap: http://soft.softoogle.com/ap/sockscap-download-5157.shtml

42. LICENCE

AUTEURS

Tous les chapitres © contributeurs, sauf indication contraire ci-dessous.

INTRODUCTION

Modifications
gravy - A Ravi Oli 2011
Mokurai - Edward Mokurai Cherlin 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
poser - Poser 2011
lalala - laleh 2011

À propos de ce guide

Modifications
Zorrino - Zorrino Hermanos 2011
booki - adam or aco 2011

Démarrage rapide

Modifications booki - adam or aco 2011
erinn - Erinn Clark 2011
puffin - Karen Reilly 2011
freerk - Freerk Ohling 2011
Zorrino - Zorrino Hermanos 2011
helen - helen varley jamieson 2011
poser - Poser 2011
schoen - Seth Schoen 2011

Comment fonctionne Internet

Modifications booki - adam or aco 2011
gravy - A Ravi Oli 2011
lalala - laleh 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

Internet et la censure

Modifications gravy - A Ravi Oli 2011
booki - adam or aco 2011
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

Contournement et sécurité

Modifications gravy - A Ravi Oli 2011
booki - adam or aco 2011
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011

Introduction

Modifications
booki - adam or aco 2010

À propos de ce manuel

Modifications
booki - adam or aco 2010

Techniques simples

Modifications
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
poser - Poser 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

Soyez creatif

Modifications
freerk - Freerk Ohling 2011
DavidElwell - David Elwell 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

Les proxys Web

Modifications
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
lalala - laleh 2011
poser - Poser 2011
booki - adam or aco 2011

Qu'est ce que le contournement ?

Modifications
booki - adam or aco 2010

Psiphon

Modifications
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
helen - helen varley jamieson 2011
poser - Poser 2011
booki - adam or aco 2011

Suis-je censuré ?

Modifications
booki - adam or aco 2010

Détection et anonymat

Modifications
booki - adam or aco 2010

Sabzproxy

Modifications
booki - adam or aco 2011

rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

Comment fonctionne Internet ?

Modifications
booki - adam or aco 2010

Introduction à Firefox

Modifications
SamTennyson - Samuel L. Tennyson 2011
booki - adam or aco 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
schoen - Seth Schoen 2011

Qui contrôle Internet ?

Modifications
booki - adam or aco 2010

Techniques de filtrage

Modifications
booki - adam or aco 2010

AdBlock Plus et NoScript

Modifications
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
scherezade - Genghis Kahn 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

HTTPS Everywhere

Modifications
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011

Techniques simples

Modifications
booki - adam or aco 2010

Configurer un proxy et FoxyProxy

Modifications
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

Utiliser un proxy Web

Modifications
gravy - A Ravi Oli 2011
freerk - Freerk Ohling 2011
erinn - Erinn Clark 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
poser - Poser 2011

Utiliser PHProxy

Modifications

Utiliser Psiphon

Modifications

Freegate

Modifications
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

Simurgh

Modifications
booki - adam or aco 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
freerk - Freerk Ohling 2011

Utiliser Psiphon2

Modifications

UltraSurf

Utiliser un nœud Psiphon2 public
Modifications

Les risques

Modifications

Services de VPN

Modifications
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
booki - adam or aco 2011

VPN sur Ubuntu

Modifications
SamTennyson - Samuel L. Tennyson 2011
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
freerk - Freerk Ohling 2011

Hotspot

Modifications
booki - adam or aco 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

Contextes avancés

Modifications

Les proxys HTTP

Modifications

Alkasir

Modifications
booki - adam or aco 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011

helen - helen varley jamieson 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

Tor : le routage en ognon

Modifications
freerk - Freerk Ohling 2011
erinn - Erinn Clark 2011
puffin - Karen Reilly 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
helen - helen varley jamieson 2011
lalala - laleh 2011

Installer Switch Proxy

Modifications

Utiliser Switch Proxy

Modifications

Jondo

Modifications
SamTennyson - Samuel L. Tennyson 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

Your-Freedom

Modifications
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

Tor : le routage en ognon

Modifications

Utiliser le navigateur Tor incorporé

Modifications

Domaines et DNS

Modifications
gravy - A Ravi Oli 2011
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

Utiliser la messagerie instantanée Tor incorporée

Modifications
SahalAnsari - Sahal Ansari 2010

Les proxys HTTP

Modifications
booki - adam or aco 2011
lalala - laleh 2011
scherezade - Genghis Kahn 2011
helen - helen varley jamieson 2011

Utiliser Tor avec des passerelles

Modifications

La ligne de commande

Modifications
booki - adam or aco 2011
helen - helen varley jamieson 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

Utiliser Jondo

Modifications

OpenVPN

Modifications Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

Les tunnels SSH

Modifications
freerk - Freerk Ohling 2011
booki - adam or aco 2011

Qu'est-ce que le VPN

Modifications

OpenVPN

Modifications

Les proxys SOCKS

Modifications
Zorrino - Zorrino Hermanos 2011
freerk - Freerk Ohling 2011
lalala - laleh 2011
booki - adam or aco 2011

Les tunnels SSH

Modifications

Les proxys SOCKS

Modifications

S'informer et se documenter sur la censure

Modifications
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
booki - adam or aco 2011

Passer outre le blocage de port

Modifications
booki - adam or aco 2011
schoen - Seth Schoen 2011
freerk - Freerk Ohling 2011

Installer un proxy Web

Modifications

Installer un proxy Web

Modifications
freerk - Freerk Ohling 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

Installer PHProxy

Modifications

Mettre en place un relai Tor

Modifications
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
booki - adam or aco 2011

Installer Psiphon

Modifications

Les risques d'héberger un proxy

Modifications
freerk - Freerk Ohling 2011
schoen - Seth Schoen 2011

---

trucs et astuces pour les webmaster

Modifications
freerk - Freerk Ohling 2011
helen - helen varley jamieson 2011
rastapopoulos - Roberto Rastapopoulos 2011
scherezade - Genghis Kahn 2011
booki - adam or aco 2011
Zorrino - Zorrino Hermanos 2011
schoen - Seth Schoen 2011

Mettre en place un relais Tor

Modifications

Les risques d'héberger un proxy

Modifications

Glossaire

Modifications
freerk - Freerk Ohling 2011
puffin - Karen Reilly 2011
rastapopoulos - Roberto Rastapopoulos 2011
helen - helen varley jamieson 2011
Mokurai - Edward Mokurai Cherlin 2011

---

10 choses

Modifications
Zorrino - Zorrino Hermanos 2011
booki - adam or aco 2011
puffin - Karen Reilly 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

Ressources supplémentaires

Modifications
booki - adam or aco 2011
rastapopoulos - Roberto Rastapopoulos 2011
schoen - Seth Schoen 2011
helen - helen varley jamieson 2011

Crédits

Modifications
booki - adam or aco 2011
The below is information for pre-2011 content

CREDITS

Modifications

Les informations ci-dessous concerne le contenu 2011

AUTEURS

À propos de ce guide

© Adam Hyde 2008
Modifications
Austin Martin 2009
Edward Cherlin 2008
Janet Swisher 2008
Tom Boyle 2008
Zorrino Zorrinno 2009

Contexte avancé
© Steven Murdoch And Ross Anderson 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Détection et anonymat
© Seth Schoen 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Risques
© Nart Villeneuve 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Austin Martin 2009

Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Proxys SOCKS
© Seth Schoen 2008
Modifications
Adam Hyde 2008
Freerk Ohling 2008, 2009

Tom Boyle 2008

Utiliser Switch Proxy
© Adam Hyde 2008, 2009

Modifications
Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

Crédits
© Adam Hyde 2006, 2007, 2008
Modifications
Edward Cherlin 2008

Technique de filtrages
© Edward Cherlin 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009

Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Ressources supplémentaires
© Adam Hyde 2008
Modifications
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008, 2009

Glossaire
© Freerk Ohling 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Suis-je censuré ?
© Adam Hyde 2008
Modifications
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

Comment Internet fonctionne ?
© Frontline Defenders 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Installer un proxy Web
© Nart Villeneuve 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

---

installer PHP proxy
© Freerk Ohling 2008
Modifications
Adam Hyde 2008
Alice Miller 2008

Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Installer Psiphon
© Freek Ohling 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009

Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Installer Switch Proxy
© Adam Hyde 2008
Modifications
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

Introduction
© Alice Miller 2006, 2008
Modifications
Adam Hyde 2008, 2009

Ariel Viera 2009

Austin Martin 2009

Edward Cherlin 2008
Janet Swisher 2008
Seth Schoen 2008
Tom Boyle 2008

Les risques d'héberger un proxy
© Seth Schoen 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Tom Boyle 2008

Les tunnels SSH
© Seth Schoen 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Freerk Ohling 2008, 2009

Sam Tennyson 2008
TWikiGuest 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Mettre en place un relais Tor
© Zorrino Zorrinno 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Techniques simples
© Ronald Deibert 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009

Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Tor: le routage en oignon
© Zorrino Zorrinno 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Ben Weissmann 2009

Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Utiliser Tor avec des passerelles
© Zorrino Zorrinno 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009

Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Utiliser Jondo
© Freerk Ohling 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

OpenVPN
© Tomas Krag 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008

Utiliser PHProxy
© Freerk Ohling 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

Utiliser Psiphon
© Freerk Ohling 2008
Modifications
Adam Hyde 2008

Alice Miller 2008
Austin Martin 2009

Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

Utiliser Psiphon2
© Freerk Ohling 2009

Modifications
Adam Hyde 2010

Austin Martin 2009

Zorrino Zorrinno 2009

Utiliser un nœud Psiphon2 public
© Freerk Ohling 2010

Modifications
Roberto Rastapopoulos 2010

Zorrino Zorrinno 2010

Utiliser le navigateur Tor incorporé
© Zorrino Zorrinno 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

Utiliser la messagerie instantanée Tor incorporée
© Zorrino Zorrinno 2008
Modifications
Adam Hyde 2008, 2009

Alice Miller 2008
Freerk Ohling 2008
Sahal Ansari 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

Les proxys HTTP
© Adam Hyde 2008
Modifications
Alice Miller 2008
Freerk Ohling 2008, 2009

Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

Utiliser un proxy Web
© Nart Villeneuve 2008
Modifications
Adam Hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008
Zorrino Zorrinno 2008