Contourner la Censure.net et préserver son anonymat

FLOSS MANUALS

Digital Freedom Coalition

FHIMT.COM

atln.info

fidh

Table des matières

Crédits et remerciements

Ce mini guide, l'eBook plus complet qui l'accompagne, et le site http://contournerlacensure.net ainsi que les opérations de promotion et de diffusion des connaissances contenus dans ces différents supports ont été rendus possibles par la collaboration des organisations et des individus suivants.

FLOSS Manuals est une collection de manuels sur les logiciels libres et open source ainsi que les outils utilisés pour les créer, et également sur la communauté utilisant ces outils. Cela comprend les auteurs, les correcteurs, les artistes, les développeurs de logiciels, les militants, et bien d'autres personnes encore

La Digital Freedom Coalition est une coalition d'associations, d'ONG, de média et de bloggeurs cherchant à partager leur expérience et leur savoir faire afin de faire avancer grâce au numérique la liberté d'expression et la démocratie.

Fhimt.com est un média social Tunisien créé au lendemain de la révolution, il cherche à expérimenter de nouvelle formes de journalisme de de traitement de l'information afin de les rendre accessibles au plus grand nombre et de participer à l'évangélisation des idéaux démocratiques dans la Tunisie de l'après Ben Ali.

L'Association Tunisienne des Libertés Numériques est une association citoyenne qui cherche a utiliser les nouvelles technologie pour assoir et imposer la démocratie en Tunisie à travers l'édition de média (dont Fhimt.com), de site et de service web ainsi que de manifestations et d'évènement culturels liés aux nouveaux média et au numérique en général.

Participation citoyenne

Nous tenons à remercier chaleureusement pour leur aide dans la traduction, l'adaptation et la mise à jour des informations contenues dans ce manuel Mathieui, Yohaz, Khannib, Shisoka et Skhaen ainsi que l'équipe du site Reflets.info pour les investigations complémentaires concernant certains logiciels de contournement de censure.

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 media 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 en 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 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 règlementées 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 l'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'accèsInternet (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 àInternet 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, 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.

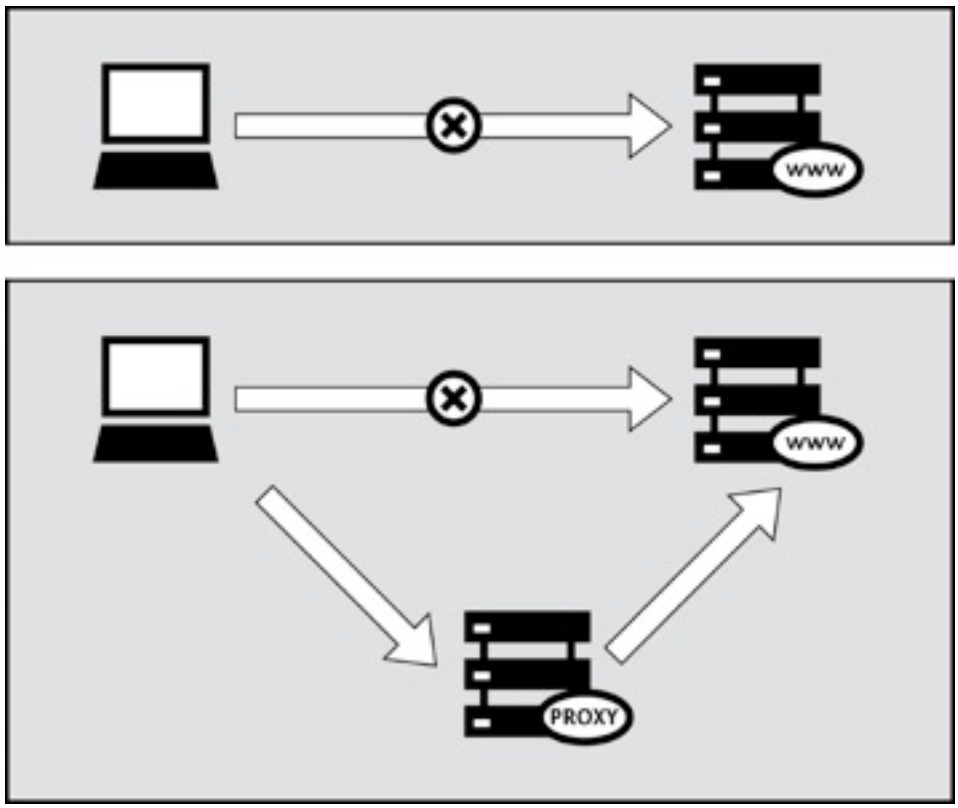
Quelles méthodes existent pour contourner le filtrage?

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 du manuel disponible sur http://contounerlacensure.net expliquent comment fonctionne Internet, décrivent différentes formes de la censure, et présentent des outils et techniques variés pour vous aider à contourner ces limites à la liberté d'expression. Le problème global de la vie privée et de la sécurité sur Internet y est étudié en commençant par traiter les bases, puis il s'intéresse à quelques sujets plus avancés et se termine par une brève section destinée aux webmasters et aux spécialistes qui souhaitent aider les autres à contourner la censure d'Internet.

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. La manuel complet disponible sur http://contournerlacensure.net 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 :

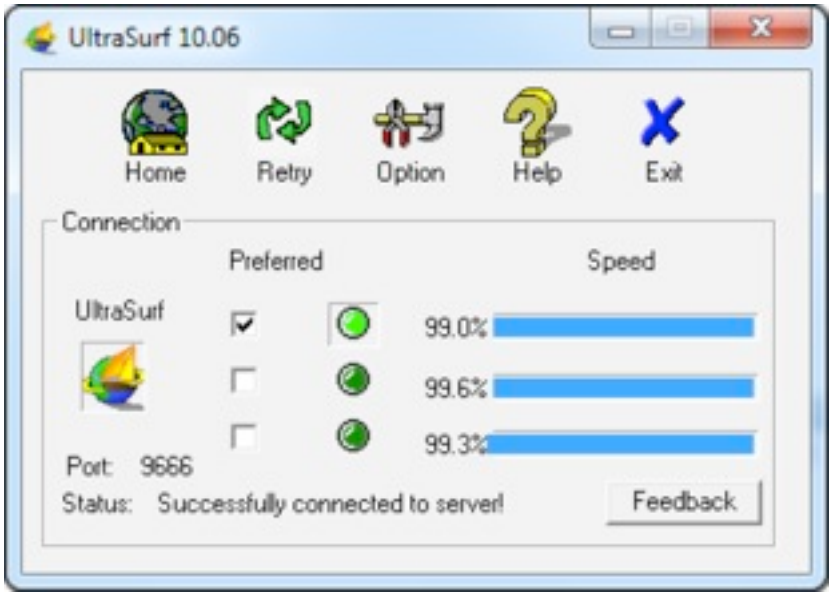
Appuyez sur Entrée ou cliquez sur GO et, si vous accédez au site demandé, cela fonctionne. Si le lien ci-dessus ne fonctionne pas, vous devrez trouver une autre méthode de contournement. Les chapitres sur les proxys Web et sur Psiphon disponible dans le manuel complet disponible sur http://contournerlacensure.net 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 le manuel disponible sur http://contounerlacensure.net, 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/ 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 avec 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, MacOS 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

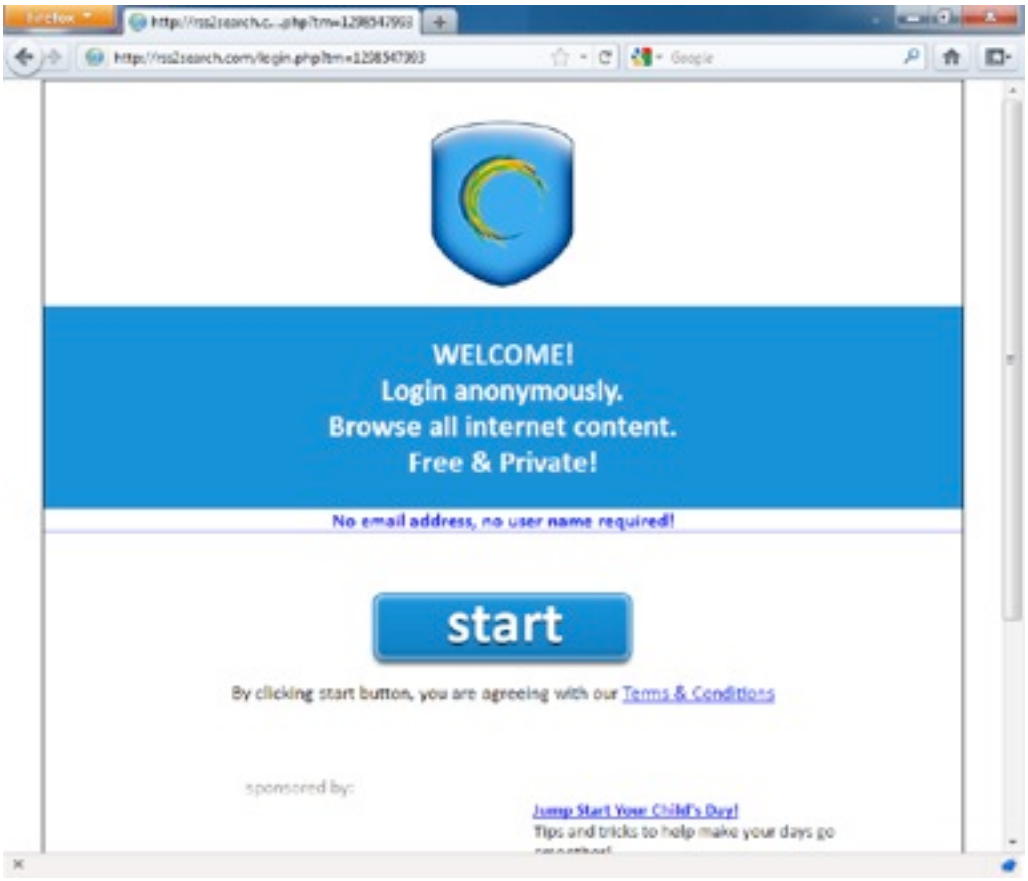
Si vous voulez accéder à des services Internet autres que le Web, comme les emails, via un client comme Outlook ou Thunderbird, une manière simple et sûre est d'utiliser un VPN (pour Virtual Private Network, soit Réseau privé virtuel). Un VPN va chiffrer dans un canal tout le trafic Internet entre vous 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 « HotspotShield 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 ».

Chiffrez votre navigation

Afin d'éviter de voir les informations que vous échangez ou que vous consultez lors de votre navigation, en particulier si vous utilisez un réseau sans fil et plus encore dans un lieu public, vous pouvez utiliser une extension au navigateur Firefox développée par l'Electronic Frontier Foundation appelé «https Everywhere». Disponible à https://www.eff.org/https-everywhere ce logiciel s'installe en un clic sur votre navigateur Firefox et permet d'accéder de façon chiffrée à une multitude de sites web tels que Google, Wordpress, Facebook et bien d'autre.

Retrouvez ce guide, le guide complet et exhaustif ainsi que les vidéos qui l'accompagne sur http://contournerlacensure.net