Pour les handicappés de la technologie parmi nous, il existe également un tutoriel vidéo très simple et très bien fait, qui explique comment installer un VPN. Cela pèse 450 Mo et se trouve sur la quasi totalité des serveurs bittorrent.

[Philou sur TrackerNews - 2/01/2010]

Anti-Hadopi.VPN.Video.Tutorial.XP-Win7.FR-NzB.zip – http://isohunt.com/torrent_details/148969293/?tab=summary

LES SOLUTIONS POUR CONTRER HADOPI
Bonjour à tous et à toutes,
Énième rebondissement dans la saga tragicomique de la loi Hadopi.
Alors que les premiers courriels ne seraient envoyés qu'en Avril prochain (dans le meilleur des cas), voici quand même quelques points IMPORTANTS à savoir sur le sujet:
- « La mule » (Réseau ED2K) a été confirmée comme étant la cible prioritaire.
- HADOPI sera géré par une poignée d'employé(e)s uniquement.

- Il y a des techniques déjà en place, pour éviter de recevoir des « pourriels » en provenance d'HADOPI.
Maintenant, tous ceux et celles concernés, veuillez prendre une grande respiration et arrêtez de paniquer!
HADOPI ne pourra ABSOLUMENT rien contre ceux qui se protègeront… Si un jour HADOPI voit son ombre…
Malgré tout, voici tel que promis dans le billet précédent, comment vous protéger:

- ***1- Location d'une Seedbox HORS FRANCE.***
- ***2- Location d'un serveur VPN HORS FRANCE.***
- ***3- Utilisation d'accès réseau sans-fil (WIFI) non-protégé ou publique***

- ***4- Déménager HORS FRANCE.*** 😉

0- Location d'une Seedbox HORS FRANCE:

Une Seedbox est un serveur informatique privé qui est dédié au téléchargement et à l'émission de fichiers numériques.
La location d'une Seedbox est de plus en plus fréquente depuis déjà plusieurs mois. Non pas uniquement afin d'éviter que votre adresse IP personnelle circule sur les réseaux P2P, mais aussi et surtout, afin d'automatiser vos transferts afin de « seeder » et « leecher » via une large bande passante 24/24, 7/7, à longueur d'année.

Les Seedbox sont généralement utilisées par les « Uploaders », mais c'est accessible à tous.
Les coûts d'une Seedbox sont généralement de 25€/mois jusqu'à 100€+/mois. Plus votre Seedbox sera performante (Processeur, Mémoire, Bande passante, etc), plus le prix sera important.
L'avantage d'une Seedbox est que vos transferts sont effectués via l'adresse IP liée à votre Seedbox fournis par l'hébergeur. Vous pouvez donc récupérer tous vos fichiers via FTP, une fois que ceux-ci seront complétés et sans risque de voir votre adresse IP circuler.

Cette solution est efficace, mais elle requiert en général, de meilleures connaissances informatiques.
Certaines compagnies offrent par contre, des Seedbox « clé en main » faciles d'utilisation.
Avantages:
- Rapidité des transferts.
- Anonymat sur les réseaux P2P.
- Récupération facile et rapide.
Désavantages:
- Coûts parfois élevés.
- L'envoi de vos torrents (Upload) sur la Seedbox via FTP est généralement lente dû à la limitation des vitesses d'upload par les FAI.
- Connaissances en informatique de niveau intermédiaire à avancé, recommandées.
Quelques adresses de fournisseurs de Seedbox

gratuits:
- A venir…

Quelques adresses de fournisseurs de Seedbox payants:
- http://www.seedboxhosting.com
- http://www.dediSeedbox.com
- http://tor.imageshack.us/tor
- http://www.w00tsite.com
- http://www.leasetorrent.com
- http://www.seedboxworld.net/

2- Location d'un serveur VPN HORS France :
Un VPN (Réseau privé virtuel) repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données de passer d'une extrémité à l'autre du VPN tout en étant sécurisées par des algorithmes de cryptographie.
Autrement dit, lorsque vous vous connectez au serveur, votre identité se masque pour devenir celle du fournisseur du service VPN.
Vous assurez donc ainsi votre anonymat complet par l'utilisation d'une connexion sécurisée et encryptée entre vous et le serveur VPN.

La connexion s'effectue généralement via un client, tel que OpenVPN, mais certaines entreprises offrent la connexion directe sans utilisation de client additionnel.

Les coûts liés à la location vont de 5€/mois jusqu'à +/- 35€/mois. La différence vient du type de service désiré. Le type de connexion, le niveau d'encryption, le nombre de Pays désiré, sont tous des facteurs.
Il est fortement recommandé d'utiliser des serveurs qui sont le plus près physiquement de votre lieu de résidence. Le plus gros inconvénient demeurera toujours la chute des performances de votre connexion Internet une fois la connexion établie avec le serveur VPN.
Les gens avec peu d'aptitude informatique sauront

très bien s'en sortir avec la configuration très peu complexe de cette solution.

Le faible coût ainsi que le niveau de sécurité offert par ce type de protocole en font le choix #1 afin de naviguer de façon anonyme sur le net.

Avantages:

- Facilité d'utilisation même pour les débutants.
- Coût très faible.
- Excellent niveau d'anonymat.

Désavantages:

- Perte de vitesse de votre bande passante.
- Déconnexion du serveur possible. (Contournable avec ADSL Autoconnect pour les connexions directes pour Windows XP)

Quelques adresses de fournisseurs de VPN gratuits:

- http://www.itshidden.com
- http://www.peer2me.com
- http://s6n.org/arethusa/fr.html
- http://www.hotspotshield.com

Une fois installé sur ton ordinateur, une simple connexion à Peer2Me te permet de :

Explorer et télécharger les fichiers privés de tes amis en te connectant de chez toi et en privé à leurs ordinateurs et aux données qu'ils contiennent (films, photos, musique)	***Améliorer l'ensemble de tes logiciels Internet (MSN Messenger, Yahoo! Messenger, Skype, FTP...) : Plus grande rapidité de téléchargement et confidentialité stricte.***	***Accéder à distance à ton ordinateur depuis n'importe où (travail, cybercafé, hotspot Wi-Fi…) pour avoir toujours à ta disposition l'ensemble de tes dossiers informatiques.***
Démo / En savoir plus	***Démo / En savoir plus***	***Démo / En savoir plus***

100% GRATUIT, une simple inscription suffit !

Clique sur le bouton ci-dessous pour t'inscrire et télécharger dès maintenant le programme d'installation Peer2Me

Arethusa VPN

-

À propos

Arethusa VPN est un service qui rend votre connexion internet plus anonyme et sécurisée. Votre adresse IP réelle est cachée et votre FAI ne peut pas surveiller ou filtrer votre activité.

Cela fonctionne en établissant un tunnel crypté entre votre ordinateur et nos serveurs, en utilisant un VPN. Toute votre activité Internet semblera provenir de nos adresses IP, et non pas de votre IP réelle. Un service de VPN est utile pour les personnes utilisant des réseaux censurés, filtrés, ou surveillés, des points d'accès WiFi, pour les dissidents politiques.

Pour vérifier quelle est votre adresse IP actuelle, cliquez ici ou ici ou ici.

Nous ne stockons aucune donnée sur votre trafic réseau. Nous ne stockons jamais votre adresse IP réelle.

Caractéristiques

Offre Premium v2 :

Bande passante dédiée non limitée. Maximum 30 Mbps par utilisateur.

Adresse IP dynamique (NAT). 10 ports entrants ouverts (plus sur demande). Compatible avec toutes les applications, y compris le P2P et la VoIP, si configuré correctement.
Méthodes de connexion disponibles : PPTP, OpenVPN (TCP ou UDP).
Coût : 5 EUR par mois. Pas de frais de mise en service.

Offre Premium v1 : (serveurs pleins)

Bande passante partagée non limitée.
Adresse IP dédiée et fixe. Tous les ports sont ouverts. Compatible avec toutes les applications, y compris le P2P et la VoIP.
Méthodes de connexion disponibles : PPTP, OpenVPN (TCP ou UDP).
Coût : 5 EUR par mois. Pas de frais de mise en service.

Offre gratuite (Free) : (temporairement fermée)

Bande passante de faible qualité. 100 Mbps partagés entre tous les utilisateurs.
Adresse IP partagée (NAT). Tous les ports entrants sont fermés. Port 25 bloqué (pas de mail).
Méthode de connexion : OpenVPN (TCP) uniquement.
Gratuit. Aucun support fourni.

Avertissement :
Notre service cache votre adresse IP réelle et crypte votre connexion. Rien de plus, rien de moins.
Si votre ordinateur a des failles de sécurité, vous serez quand même hacké ou infecté par des virus. Si votre connexion Internet était filtrée ou derrière un pare-feu auparavant, votre ordinateur est désormais directement accessible depuis Internet.
Notre service ne vous empêchera pas non plus de dévoiler volontairement vos informations personnelles sur Internet.
Si vous utilisez Windows, vous devriez vraiment vérifier que vous avez un anti-virus installé et que votre pare-feu est activé sur votre connexion VPN.
Pour de meilleurs résultats, vous devriez utiliser le

*VPN sur un ordinateur équipé de Linux ou *BSD, sans aucun document personnel dessus.*
Assurez-vous de toujours installer toutes les mises à jour de sécurité de votre système d'exploitation.

Plusieurs méthodes de connexion sont disponibles pour l'offre premium. OpenVPN est meilleur, mais plus difficile à configurer sous Windows. N'utilisez jamais PPTP si vous pensez que quelqu'un espionne votre connexion.

	PPTP (GRE)	OpenVPN
Cryptage	Faible (MPPE 128 bits)	Fort (auth : RSA 2048 bits; données : AES 256 bits)
Compression	Non	Oui (LZO)
Nécessite l'installation d'un logiciel	Non	Oui
Fonctionne sur Windows/Linux/MacOS	Oui	Oui
Fonctionne sur une large gamme de périphériques	Oui	Non
Capacité à fonctionner derrière un firewall	Moyenne (utilise le port 1723 TCP + le protocole 47)	Excellente (utilise le port 443 UDP ou TCP)

Configuration

D'abord, connectez-vous à notre panneau de contrôle.
Si vous n'avez pas encore créé de tunnel, cliquez sur "Ajouter" pour en demander un.
Cherchez l'adresse du serveur, le nom d'utilisateur et le mot de passe pour le tunnel que vous voulez configurer.
Pour OpenVPN, vous devez aussi cliquer sur "CA" et "Config", et sauver ces deux fichiers sur votre ordinateur.

OpenVPN

Windows

- *Si vous n'avez pas OpenVPN 2.1, vous devez l'installer. Cliquez ici pour télécharger la dernière version puis lancez-le (vous devez être Administrateur). Cliquez "Next >", "I Agree", "Next >" (laissez toutes les cases cochées), "Install", "Next >", décochez "Show readme" puis "Finish".*
- *Ouvrez le dossier de configuration d'OpenVPN (Démarrer -> Programmes -> OpenVPN -> Shortcuts -> OpenVPN configuration file directory) et copiez les fichiers CA et Config dans ce dossier.*
- *Lancez OpenVPN GUI (en Administrateur) : Démarrer -> Programmes -> OpenVPN -> OpenVPN GUI.*
- *Localisez l'icône OpenVPN GUI dans le systray. Faites un clic droit sur l'icône et cliquez sur "Connect".*
- *Entrez le nom d'utilisateur et mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Ok".*
- *Cliquez ici si vous voulez enregistrer votre mot de passe et vous connecter automatiquement au démarrage de Windows.*

Linux (toute distro avec NetworkManager)

- *Installez le plugin OpenVPN pour NetworkManager. Pour Ubuntu / Debian: sudo aptitude install network-manager-openvpn . Vous pouvez avoir à relancer votre session pour que cela prenne effet.*
- *Cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", puis "Configurer le VPN...".*
- *Si vous avez un bouton "Importer", cliquez dessus et selectionnez le fichier Config ("arethusa.ovpn"). Votre connexion sera créée et préremplie avec toutes les données nécessaires sauf le nom d'utilisateur et le mot de passe.*
- *Cliquez sur "+ Ajouter".*
- *Selectionnez "OpenVPN" puis cliquez sur "Créer..." ou "-> Suivant".*

- *Entrez le nom que vous voulez dans "Nom de la connexion" (par exemple "Arethusa VPN").*
- *Entrez l'adresse du serveur (se trouve dans notre panneau de contrôle) dans "Passerelle".*
- *Selectionnez "Type d'authentication : Mot de passe". Entrez le nom d'utilisateur (se trouve dans notre panneau de contrôle).*
- *Cliquez sur le bouton à côté de "Certificat du CA" et sélectionnez le fichier CA.*
- *Cliquez sur "Avancé...". Entrez "Utiliser un port de passerelle personnalisé : 443". Cochez "Utiliser la compression de données LZO". Cochez "Utiliser une connexion TCP" si vous voulez vous connecter en TCP. Dans l'onglet "Sécurité" ou "Certificats", selectionnez "Chiffrement : AES-256-CBC". Cliquez sur "Valider".*
- *Cliquez sur "Appliquer" ou "-> Suivant".*
- *Pour lancer votre connexion VPN, cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", et sélectionnez la connexion que vous venez de créer.*
- *Entrez le mot de passe (trouvé dans notre panneau de contrôle) et cliquez sur "Ok".*

Mac OS X 10.4 et plus (avec Tunnelblick)

- *Téléchargez Tunnelblick et double-cliquez sur le fichier .dmg téléchargé. Sélectionnez Tunnelblick.app et déposez-le sur le dossier Applications.*
- *Ouvrez le dossier Applications et double-cliquez sur Tunnelblick.app. Autorisez l'application. Le nom d'utilisateur et le mot de passe de votre compte administrateur vous seront demandés.*
- *Tunnelblick vous demandera ensuite de placer votre fichier de configuration dans un certain dossier. Copiez les fichiers CA et Config (fournis par nous) dans ce dossier. Cliquez sur "Continue".*
- *Localisez l'icône Tunnelblick dans la barre des menus en haut de l'écran, habituellement entre l'horloge et l'icône Spotlight. Cliquez dessus, puis cliquez sur "Connect 'arethusa'".*

- *Entrez le nom d'utilisateur et mot de passe (trouvés dans notre panneau de contrôle).*

PPTP

Windows XP / 2003

- *Lancez l'"Assistant Nouvelle Connexion" : Démarrer -> Programmes -> Accessoires -> Communications -> Assistant Nouvelle Connexion.*
- *Cliquez sur "Suivant >".*
- *Sélectionnez "Connexion au réseau d'entreprise" et cliquez sur "Suivant >".*
- *Sélectionnez "Connexion réseau privé virtuel" et cliquez sur "Suivant >".*
- *Entrez le nom que vous voulez pour cette connexion, par exemple "Arethusa VPN" et cliquez sur "Suivant >".*
- *Il peut vous être demandé s'il est nécessaire d'établir une autre connexion au préalable. Si votre connexion internet figure dans la liste, sélectionnez-la, sinon choisissez de ne pas établir de connexion initiale. Cliquez sur "Suivant >".*
- *Entrez le nom d'hôte du serveur (se trouve dans notre panneau de contrôle sous "Adresse du serveur") et cliquez sur "Suivant >".*
- *Choisissez d'ajouter un raccourci si vous le souhaitez et cliquez sur "Terminer".*
- *Pour lancer votre connexion VPN, ouvrez "Connexions réseau" (Démarrer -> Programmes -> Accessoires -> Communications -> Connexions réseau) et cliquez sur la connexion tout juste créée pour le VPN.*
- *Entrez le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Se connecter".*

Windows Vista / 7

- *Ouvrez le "Panneau de configuration" (Démarrer -> Panneau de configuration), puis cliquez sur "Réseau et Internet".*

- *Cliquez sur "Centre Réseau et Partage", puis "Configurer une connexion ou un réseau".*
- *Sélectionnez "Connexion à votre espace de travail" et cliquez sur "Suivant".*
- *Sélectionnez "Utiliser ma connexion Internet (VPN)".*
- *Entrez l'adresse Internet du serveur (se trouve dans notre panneau de contrôle sous "Adresse du serveur"), entrez le nom que vous voulez dans "Nom de la destination" (par exemple "Arethusa VPN"), et cliquez sur "Suivant".*
- *Entrez le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Créer".*
- *Quand l'emplacement du réseau VPN vous est demandé, choisissez "Lieu public" pour une sécurité maximale.*

Mac OS X 10.4

- *Dans le Finder, cliquez sur "Aller".*
- *Ouvrez "Applications", puis "Connexion à Internet", puis "VPN".*
- *Sélectionnez "PPTP" comme type de connexion.*
- *Entrez l'adresse du serveur, le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle).*
- *Cliquez sur "Se connecter".*
- *Dans les "Options" de "Connexion à Internet", cochez "Envoyer tout le trafic sur la connexion VPN".*

Mac OS X 10.5

- *Ouvrez "Préférences Système" puis "Réseau".*
- *Cliquez sur "+".*
- *Dans la fenêtre popup, choisissez "VPN" pour Interface, et "PPTP" pour Type de VPN.*
- *Entrez le nom que vous voulez dans "Nom du service" (par exemple "Arethusa VPN"), et cliquez sur "Créer".*
- *Entrez l'adresse du serveur (se trouve dans notre panneau de contrôle), entrez le nom d'utilisateur*

dans "Nom du compte", et cliquez sur "Réglages d'authentification...".

- *Sélectionnez "Mot de passe :", entrez le mot de passe (se trouve dans notre panneau de contrôle) et cliquez sur "OK".*
- *Cliquez sur "Avancé...".*
- *Cochez "Envoyer tout le trafic sur la connexion VPN" et cliquez sur "OK".*
- *Cliquez sur "Appliquer".*
- *Cliquez sur "Se connecter".*

Linux (toute distro avec NetworkManager)

- *Installez le plugin PPTP pour NetworkManager. Pour Ubuntu / Debian: sudo aptitude install network-manager-pptp . Vous pouvez avoir à relancer votre session pour que cela prenne effet.*
- *Cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", puis "Configurer le VPN...".*
- *Cliquez sur "+ Ajouter".*
- *Sélectionnez "Protocole de tunnel Point-to-Point (PPTP)" ou "pppd tunnel (PPTP ...)" puis cliquez sur "Créer..." ou "-> Suivant".*
- *Entrez le nom que vous voulez dans "Nom de la connexion" (par exemple "Arethusa VPN").*
- *Sélectionnez "Type: Windows VPN (PPTP)" (si cette option existe).*
- *Entrez l'adresse du serveur (se trouve dans notre panneau de contrôle) dans "Passerelle", et le nom d'utilisateur (si cette option existe).*
- *S'il y a un bouton "Avancé...", cliquez dessus, cochez "Utiliser le chiffrement Point-to-Point (MPPE)" et cliquez sur "Valider".*
- *Cliquez sur "Appliquer" ou "-> Suivant".*
- *Pour lancer votre connexion VPN, cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", et sélectionnez la connexion que vous venez de créer.*
- *Entrez le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Ok".*

Divers

Serveur SMTP (premium uniquement): smtp.s6n.net

Serveur DNS (premium v1 uniquement): 94.23.190.1

Serveur DNS (premium v2 et serveur gratuit): 10.10.10.10

Conditions du service

- ***Pas d'activité illégale.***
- ***Pas de spam, flood, diffusion de virus, hacking, scan de réseau, harcèlement envers des personnes.***
- ***Pas d'activité qui amènerait une de nos adresses à être blacklistée, ou qui mettrait en danger la qualité du service pour les autres utilisateurs.***
- ***Le service doit être payé d'avance et renouvelé avant la date d'expiration.***
- ***Toute violation de ces conditions entraînera la fermeture immédiate de votre compte sans remboursement possible.***
- ***Vous êtes entièrement responsable de vos activités lorsque vous utilisez notre service.***
- ***Nous essayerons de fournir la meilleure qualité de service possible.***
- ***Nous ne révélerons aucun détail personnel à des tiers et nous n'essayerons pas d'identifier nos clients, sauf lorsque requis par la loi.***

Quelques adresses de fournisseurs de VPN payants:

- ***http://www.ipredator.se***
- ***http://www.strongvpn.com***
- ***http://www.perfect-privacy.com/french/index.html***
- ***http://www.yourprivatevpn.com/?q=fr***
- ***http://www.psilo.fr***
- ***http://www.hidemynet.com***
- ***http://www.mullvad.net/en***
- ***http://www.unblockvpn.com***
- ***http://www.vpnboy.com***
- ***http://www.torrentfreedom.com***

- http://www.acevpn.com
- http://www.ipodah.net
- http://www.vpngates.com
- http://www.linkideo.com
- http://www.flashvpn.com
- http://www.purevpn.com
- https://www.relakks.com
- https://www.ananoos.com
- https://www.connectionvpn.com/fr

silo : internet l'esprit libre !

Psilo est un nouveau service de VPN vous permettant de naviguer, blogger, participer à des forums, partager en toute confidentialité.

Toutes vos communications internet passent par votre connexion sécurisée Psilo. Grâce au réseau Psilo, vous remplacez votre adresse IP publique par une adresse anonyme !

Au travail, dans un cyber-café, à l'hôtel, ou tout simplement chez vous, vous n'êtes plus surveillé, et vous profitez pleinement d'internet en toute liberté !

- **Connexion cryptée (AES 256 bits)**
- **Tunnel OpenVPN compatible Windows/Linux/MacOS X**
- **Pour le web, les forums, le chat... et le P2P**
- **Connexions P2P optimales grâce à la redirection de ports**
- **Transférez jusqu'à 200 Go de données par mois !**
- **Aucun log, aucune surveillance par Psilo**

Seulement 4,50 € par mois !

Plus d'informations

Vous devrez lire et accepter la charte pour utiliser le service Psilo.

Psilo est encore expérimental. Nous sommes actuellement en phase de tests, mais les inscriptions sont suspendues. Merci de votre compréhension !

A bientôt sur Psilo.fr !

contact - blog - MAJ 19 janvier 2010

Bienvenue à YourPrivateVPN!

1. Naviguer anonyme	*6. Connexion chiffrée*
2. À grande vitesse	*7. Sécurité de hotspot*
3. Le trafic illimité	*8. Aucun logiciel additionnel exigé*
4. Connexion réseau 1GBit	*9. Surpasser les barrières du Web*
5. Appuis individuel	*10. Paiement sécurisé*

L'accès privé et sécurisé à Internet devient de plus en plus difficile. Êtes-vous inquiet que tout ce que vous dites et faites sur Internet soit observé et enregistré? YourPrivateVPN.com offre une solution d'intimité par l'accès à grande vitesse de VPN utilisant des serveurs situés dans les Pays Bas. Vous êtes complètement anonyme, votre trafic est entièrement chiffré, et vous êtes totalement protégé.

VPN – C'est quoi?

VPN (réseau privé virtuel) est un réseau privé d'Internet. Traditionnellement, les compagnies importantes l'emploient pour communiquer avec leurs employés partout dans le monde. De nos jours VPN peut servir à maintenir votre intimité en surfant Internet. Comparé au travail que peut faire un serveur proxy, tout le trafic est chiffré dans une connexion de VPN et votre adresse IP est cachée.

Pourquoi choisir YourPrivateVPN ?

1. L'intimité – notre premier but est d'assurer votre intimité et votre sécurité. Pour cette raison, nos serveurs sont configurés de manière à ce que votre vrai IP ne soit jamais stocké, si bien qu'on ne

trouve aucune trace de votre vrai IP sur nos serveurs. En outre, quand vous commandez votre accès anonyme, vous pouvez payer facilement avec PayPal ou Ukash. Ainsi nous ne recevons aucune information sur vos données de paiement. En effet, nous n'avons même pas besoin de votre nom ; votre adresse e-mail est suffisante.

2. La vitesse - nos serveurs aux Pays Bas et États Unies sont extrêmement vites - 1.000 mbps. Contrairement à d'autres fournisseurs de VPN ou à des serveurs proxy, où vous pourriez souffrir d'un ralentissement substantiel de la connexion, nous réservons la largeur de bande suffisante pour nos clients. Ainsi, si vous commandez par exemple un Gold Account avec 6000 Kbps, vous pouvez télécharger un film d'une durée de 90 minutes, en environ 20 minutes.

3. La sécurité - avec YourPrivateVPN, toutes vos données sont transférées sous la forme chiffrée. Pas même votre fournisseur des Services Internet peut voir ce que vous faites sur Internet. Vous pouvez surfer inaperçu, écrire des e-mails ou créer des blogs, mais aussi échanger des données ou des dossiers.

4. Non censuré - YourPrivateVPN vous permet de surmonter toutes les restrictions d'accès imposées par votre fournisseur Internet ou votre employeur. Ainsi vous pouvez visiter sans risques tous les sites Internet qui sont fermés au votre lieu de travail, ou que votre gouvernement ne veut pas que vous voyiez. Idem pour des services de VoIP comme Skype, MSN et ICQ. Ainsi vous pouvez également employer ces services sur votre smartphone ou iphone.

5. Volume illimité - YourPrivateVPN n'a pas de restrictions de volume, à la différence d'autres fournisseurs de VPN. Vous recevez le même service de qualité, si vous employez 100 MB ou 100GB de largeur de bande. Nous demandons seulement que vous ne maltraitiez pas notre service en employant d'énormes quantités de largeur de bande.

6. Localisation - nos serveurs sont stratégiquement situés aux Pays Bas et États Unies . Ils offrent la vitesse la plus élevée due à l'accès direct aux backbones des services européens et americaines. D'une part ils sont proches de beaucoup de pays qui ont un accès restreint à Internet - Moyen-Orient ou encore la Chine. Cela permet donc un accès rapide pour les utilisateurs de ces pays.

7. Croissance - en tant que jeune compagnie grandissante nous investissons constamment dans de nouvelles infrastructures de serveurs. En faisant partie de notre clientèle, vous profiterez de notre croissance, puisque vous pourrez utiliser tous les futurs serveurs utilisant le même compte.

Pour plus d'informations et pour s'enregistrer cliquez >> ici

Social Networks:

Encrypter votre Internet,

Vous avez trouvé Perfect Privacy. Nous encryptons votre connexion Internet et protégeons votre identité et votre confidentialité, à l'abri des regards indiscrets. Nous rendons votre connexion sécurisée, encryptée et anonyme, où que vous vous trouvez.

Enfin libre de faire ce que vous voulez,

Perfect Privacy, vous permet d'anonymiser et d'encrypter entièrement votre activité Internet. Que soyez en train de naviguer, éditer un blog, écrire des emails, conduire une activité commerciale, transférer de l'argent, télécharger de images, échanger des fichiers ou simplement chatter, vous êtes sécurisé et invisible en permanence pendant vos sessions en ligne.

Facile à utiliser,

Perfect Privacy vous fournit un client personnalisé exclusif et des logiciels pré-configurés qui réalisent tout le travail de connexion à votre place. Pas besoin d'être un expert en informatique pour retrouver la confidentialité de vos activités en ligne.

En de bonnes mains,

En vous fournissant un service personnalisé, nous garantissons que pendant que vous utilisez notre service, vous serez anonyme, protégé et sécurisé à tout moment. Nous ne voulons pas savoir qui vous êtes. Vous pouvez payer de façon anonyme. Nos serveurs anonymes encryptés sont répartis internationalement dans des juridictions sélectionnées pour permettre une confidentialité maximale de vos données. Le meilleur étant que vous avez accès en permanence, non seulement au serveur de votre choix, mais également à l'ensemble de notre parc de serveurs (en ce moment , , , , , , 2×, , , 5×, 2×, 8×, 4×, , , 2×, 3×, et) - non seulement à un service de cryptage et d'anonymisation mais à plusieurs (VPN, SSH2 tunnels, Squid Web proxy, SOCKS 5 proxy, etc.), selon vos choix et vos besoins du moment.

Confort d'utilisation,

Nous offrons de nombreuses méthodes de payement possibles, dont l'argent liquide, les cartes de crédit, PayPal, Liberty Reserve, PaySafeCard et WebMoney.

IL EST STRICTEMENT DÉFENDU D'UTILISER LE SERVICE « TOR » À D'AUTRES FINS QUE LA NAVIGATION ANONYME SUR LE WEB! TOR N'EST PAS UN SERVICE OFFERT POUR LE PARTAGE DE FICHIERS! MERCI DE NE PAS SATURER LES SERVEURS OFFERTS GRATUITEMENT PAR UNE POIGNÉE DE BIENFAITEURS, D'ENTREPRISES, D'UNIVERSITÉS ET D'ORGANISMES À BUT NON LUCRATIF, POUR LE BIEN DE CETTE COMMUNAUTÉ! CEUX QUI UTILISENT LE RÉSEAU TOR POUR TÉLÉCHARGER, HONTE À VOUS!

3- Utilisation des accès réseau sans-fil (WIFI) non-protégés ou publics :

La technologie WIFI est extrêmement populaire depuis quelques années. La possibilité de naviguer partout, grâce à l'utilisation de réseaux sans-fil est très agréable.

Il existe trois types de réseau sans-fil: L'offre payante, les « HotSpots » gratuits et les réseaux privés.
Le type d'accès réseau sans-fil qui vous intéressera ici est l'offre gratuite. Celle-ci est généralement offerte par des FAI, des entreprises privées (Ex. Restaurants) ou encore par des particuliers/entreprises possédants un réseau sans-fil non-sécurisé.
En aucun cas, nous ne vous encouragerons à utiliser une connexion Internet qui ne vous appartient pas!
4- Déménager HORS FRANCE.
Pour ceux qui recherchent l'aventure, le monde s'ouvre à vous! Profitez-en pour voir du pays. Pourvu que vous sortiez de la France, HADOPI ne pourra plus rien contre vous. 😉
Voilà!
Je vous recommande de masquer votre IP, si vous être résidant en France, dès que possible jusqu'à l'annonce de la mort d'HADOPI.
Vu l'ampleur des fonds publics, littéralement gaspillés, que nécessitera cette farce qu'est HADOPI, il ne fait aucun doute que sa mort viendra. Patience!
Bon partage!
PS: Pour plus d'informations sur la configuration d'une Seedbox, d'un serveur VPN ou autre… Sachez que chacun de ces fournisseurs, mentionnés ci-haut, offrent une section « FAQ » sur leur site respectif. Merci de faire votre part en consultant celles-ci au lieu de poser vos questions dans la section « commentaires »! Google demeurera toujours un bon ami si besoin est…

Mai s attention HADOPI est une grosse merde qui éclaboussera quelques français au début et de plus en plus aprèe …..bye philou

PROTEGEZ VOUS!!!!!

http://libertesinternets.wordpress.com

e PDG de Dailymotion est l'ancien directeur de campagne électorale de Sarkozy…. alors vous croyez quoi ? Qu'on allait vous laisser dire ce que vous voulez ? Bienvenue dans la réalité du Net où la liberté d'expression appartient à celui qui possède les tuyaux… comme dans la vraie vie d'ailleurs, où ne peuvent s'exprimer que ceux qui ont accès aux médias, qui possèdent une presse d'imprimerie ou un émetteur radio.
Il serait peut-être temps de penser à cette vieille idée : appropriation des moyens de production par le peuple. Parce que tant qu'on continuera à dépendre du bon vouloir des MM. Bouyges, Sarkozy, Google et Nasdaq pour notre communication, on sera toujours à la merci de leur censure et leur manipulation…

CENSURE CHEZ DAILYMOTION
[Blueman - 04/02/2010]
Depuis plus d'une semaine une trentaine de personnes ont vu leurs comptes supprimés définitivement, avec en totalité plus de 4000 vidéos, censurer sans vraiment une raison valable à part celui de rayer la libre expression et une véritable informations, ceci est un énorme danger pour notre liberté.. Cela nous concerne tous,
Voici des liens que vous pourrez consulter :
http://www.ubest1.com/index.php?option=com_seyret&Itemid=27&task=commentaire&nom_idaka=5056&anarana=video&ecrit=NiZuB_BlaBla&vi=NiZuB_BlaBla_1265203497_video.flv
http://www.blueman.name/Des_Videos_Remarquables.php?NumVideo=559

1. Pourquoi crypter vos e-mails?

1.1 Itinéraire d'un e-mail

Vos e-mails cheminent sur Internet par copies successives

Les e-mails se déplacent sur Internet par le biais de copies successives d'un serveur Internet (ordinateur du fournisseur d'accès à Internet (FAI)) à un autre serveur Internet.

Si vous habitez à Paris 6e et envoyez un e-mail à un correspondant qui habite à Paris 11e, voici les copies qui vont se créer :

Votre ordinateur (copie originale) -> un premier ordinateur chez votre fournisseur d'accès (copie 1) -> un second ordinateur chez votre fournisseur d'accès (copie 2) -> un premier ordinateur chez le fournisseur d'accès de votre destinataire (copie 3) -> un second ordinateur chez le fournisseur d'accès de votre destinataire (copie 4) -> l'ordinateur de votre ami (copie chez le destinataire).

Pour traverser trois arrondissements de Paris, ce e-mail a été inscrit au moins quatre fois sur quatre disques durs différents (quatre serveurs Internet chez les FAI) en autant de copies parfaites. Et derrière chacun de ces quatre disques durs, se cachent des entreprises commerciales, des informaticiens curieux, des administrations publiques diverses et variées...

Ces copies multiples de vos e-mails étaient jusqu'ici en théorie effacées au bout de quelques heures par chaque fournisseur d'accès. Cependant, de nouvelles législations européennes contre le "cyber" crime prévoient la conservation de ces copies pendant un an.

Un e-mail qui n'a pas été "crypté" (*) et est envoyé sur Internet est comme une carte postale sans enveloppe : les postiers, le facteur, la concierge, les voisins, peuvent lire la carte postale dans votre dos...

1.2 Confidentialités multiples, secret professionnel, vie privée et intimité

On ne saurait trop rappeler que l'utilisation de cryptographie sert non seulement à protéger voter confidentialité, mais aussi celle de vos correspondants.

1.2.1 Secrets non liés aux personnes : négociations, finances, justice

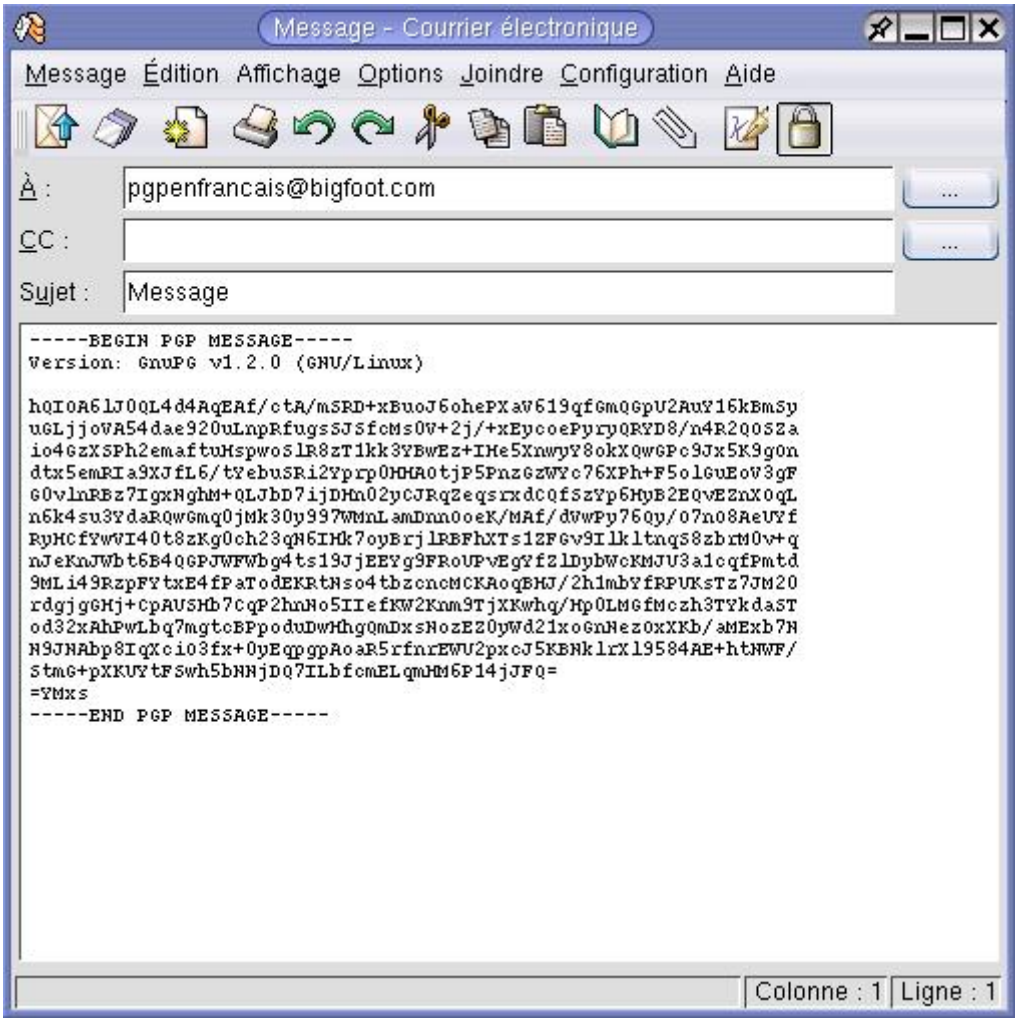
Journalistes, avocats, huissiers, médecins, cadres commerciaux... nombreux sont les professionnels qui, contractuellement, déontologiquement, ou légalement, sont tenus au secret professionnel. Ils sont aussi de plus en plus nombreux à utiliser l'internet de façon professionnelle. Ils sont donc dans l'obligation de crypter leurs e-mails afin de ne pas laisser se diffuser librement dans les labyrinthes d'Internet une proposition commerciale, un dossier judiciaire ou un dossier médical.

S'ils ne cryptent pas, ils ne prennent pas les précautions minimales pour préserver ce secret professionnel et s'exposent alors à des risques juridiques et financiers considérables.

1.2.2 Secrets liés aux personnes : vie privée, intimité, sentiments, famille

Vous ne cryptez pas car vous savez n'avoir "rien à cacher" ? Certes, mais cependant vous vous préoccupez de votre intimité, puisque lorsque vous êtes dans votre appartement, vous tirez les rideaux des fenêtres.

Vous n'aimeriez pas qu'un inconnu assis derrière les ordinateurs de votre fournisseur d'accès à Internet sourit en lisant à ses heures perdues les e-mails que vous échangez avec votre petit(e) ami(e). Si vous n'avez pas crypté vos e-mails, un inconnu a peut-être déjà lu ce que vous écriviez...



Message crypté au format OpenPGP

2. Principe de base : le cadenas, et la clé du cadenas

Tout le monde possède le cadenas, mais vous seul possédez la clé du cadenas.

On appelle ce système la cryptographie à clé publique. Le programme de cryptographie à clé publique le plus connu est PGP© (pour "Pretty Good Privacy", en anglais : "Assez Bonne Confidentialité").

Le format OpenPGP est le standard de cryptographie issu de PGP©. OpenPGP est un standard ouvert ("open"). Il est considéré par les cryptographes comme le plus sûr des procédés de cryptage pour e-mails.

OpenPGP est adopté par deux logiciels : GPG (gratuit) et PGP© (payant).
GPG et PGP© sont compatibles l'un avec l'autre.

OpenPGP fonctionne avec un cadenas (dite clé publique), et une clé (dite clé privée ou secrète) :
- votre cadenas est public
- la clé qui ouvre votre cadenas est secrète : vous êtes le seul à détenir cette clé.

2.1 Cryptage d'un message : on ferme le "cadenas" (clé PGP du destinataire)

Lorsque vous envoyez un message crypté, vous fermez le cadenas : vous cliquez sur l'icône OpenPGP du logiciel e-mail et le message va être automatiquement crypté avec le cadenas du destinataire (sa clé publique).

2.2 Déchiffrement du message : le destinataire ouvre le cadenas avec sa clé secrète (privée)

Le destinataire déchiffre automatiquement le message crypté car il possède la clé du cadenas (sa clé secrète).

3. Télécharger et installer OpenPGP

3.1 OpenPGP pour Windows

3.1.1 GPG : GNU Privacy Guard
WinPT-GPG

http://sourceforge.net/project/shownotes.php?release_id=135357 ***(WinPT + GPG)***

+ Accepte des plug-ins automatiques pour les e-mails
+ Compatible avec PGP 6, 7, 8
+ Gratuit pour tous, et librement adaptable/modifiable par les entreprises ou les particuliers (licence GNU GPL)

- Traduction française partielle
- Prise en main délicate

Installation de WinPT-GPG (Windows)

3.1.2 PGP© : Pretty Good Privacy

PGPfreeware 8.0
http://www.pgp.com/display.php?pageID=83

+ Convivial
+ Documentation fournie (en anglais)

- Aucun plug-in automatique pour les e-mails
- Payant pour les entreprises et les professions libérales
- N'existe qu'en anglais

3.2 OpenPGP pour MacOS X

3.2.1 MacGPG (Mac GNU Privacy Guard)

MacGPG
http://macgpg.sourceforge.net/fr/index.html (divers logiciels à installer)

+ Accepte des plug-ins automatiques pour les e-mails
+ Compatible avec PGP 6, 7, 8
+ Gratuit pour tous, et librement adaptable/modifiable par les entreprises et les particuliers (licence GNU GPL)

- Traduction française partielle
- Prise en main délicate

3.2.2 PGP© : Pretty Good Privacy

PGPfreeware 8.0
http://www.pgp.com/display.php?pageID=83

+ Convivial
+ Documentation fournie (en anglais)

- Aucun plug-in automatique pour les e-mails
- Payant pour les entreprises et les professions libérales
- N'existe qu'en anglais

3.3 OpenPGP pour Linux

GnuPG
(Préinstallé dans toutes les distributions Linux - commande gpg)

3.4 OpenPGP pour les autres systèmes (MacOS 8/9, Palm, WindowsCE)

PGP© 2.6, PGP© 6.5, etc.
Voir une liste sur le site OpenPGP en français
http://www.geocities.com/openpgp/intimite.htm#telechar

4. Mise en place des clés PGP

Avant d'utiliser OpenPGP, il est nécessaire de se créer sa propre paire de clés et de se procurer la clé publique de ses correspondants.

4.1 Générer votre paire de clés

Cette paire de clés sera unique normalement, et vous pouvez la conserver durant des années. Donc, entrainez-vous avant de diffuser la clé publique issue de cette paire de clés.

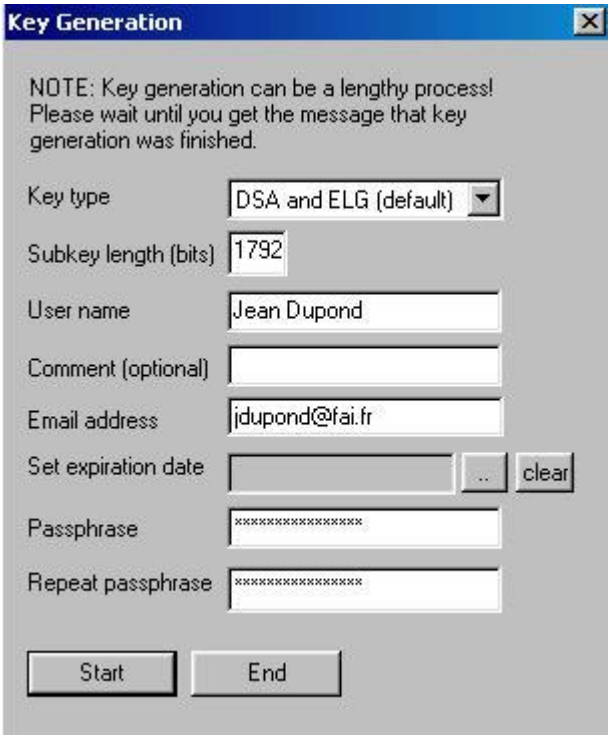
GPG ou PGP© vous proposent de générer votre paire de clés lors du premier lancement.

Cette paire de clés contient une clé publique + une clé privée :

PAIRE DE CLÉS OpenPGP :

une clé publique (le cadenas)
+
une clé privée (la clé ouvrant le cadenas)

Génération des clefs :



Génération de clef dans WinPT-GPG (Windows)

Génération de clef dans Enigmail-Mozilla (Windows, Linux)

Génération de clef dans Kgpg (KDE) (Linux)

4.2 Exporter votre clé publique et envoyer une copie de cette clé publique à vos correspondants

Cette clé publique est le "cadenas" qui permettra à vos correspondants de crypter les e-mails qu'ils vous envoient.

GPG ou PGP© permettent l'exportation de votre clé publique par leur fonction "export".

Ces correspondants doivent avoir une copie de votre clé publique PGP, qui ressemblera à ceci (en plus long) :

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (GNU/Linux)

mQGiBDm+dJYRBACyoHzCRdJXXXFai0bENERmPYFQwx9gOWm7kZRnD
27tzLjuQVWt
oFgooN/li04QIAn0o6fXolGIbPH//x4QstrZDVqxC8iEwEghHkjfJ
JM8GBECAAwF
Ajm+dL0FCQPCZwAACgkQvatgyKeVS0gbuwCePu5P6uEzIeOKtXGVO
oCZB1C8yPkA
oJFot6R8KbweB58KBR4fCihwKhKa
=fytL

-----END PGP PUBLIC KEY BLOCK-----

4.3 Importer la clé publique de ses correspondants pour la stocker dans votre "trousseau"

GPG ou PGP© permettent l'importation de la clé de vos correspondants dans votre trousseau de clés publiques par la fonction "import".

Ensuite, lorsque vous enverrez un e-mail à un de ces correspondants, le plug-in courrier se chargera de trouver le "cadenas" de ce correspondant (sa clé publique) dans votre trousseau de clés publiques PGP, puis il cryptera automatiquement le message avant envoi.

5. Utiliser OpenPGP

5.1 L'aspect technique : les plug-ins courrier

La façon la plus simple d'utiliser OpenPGP est d'installer un "plug-in" (une extension) : ce plug-in ajoute dans le logiciel e-mail une icone OpenPGP sur laquelle il suffira de cliquer pour crypter ou déchiffrer le message (ou signer et vérifier).

PGPfreeware 8.0 ne fournit pas de plug-ins courrier. Pour obtenir les plug-ins PGP© 8.0, il faut acquérir la version payante (voir http://www.pgpeurope.com). Les opérations de chiffrement peuvent cependant être réalisées dans PGPfreeware 8.0 par le presse-papiers

ou la barre d'outils flottante (voir la FAQ ci-dessous).

Pour GPG, il faut télécharger les plug-ins et les installer, suivant le logiciel de courrier utilisé :

Windows

Netscape 7 - Mozilla : Enigmail (libre)
http://enigmail.mozdev.org/

Outlook Express 5 / 6 : inclus dans WinPT 1.0 (libre)

Eudora 4 / 5 : EudoraGPG (libre)
http://www.adobner.de/eudoragpg/english/index.html

Outlook : G-Data (libre)
http://www.gdata.de/gpg/download.html

Pegasus Mail : QDGPG (libre)
http://community.wow.net/grt/qdgpg.html

The Bat! : Ritlabs (shareware)
http://www.ritlabs.com/the_bat/pgp.html

Becky! 2 : BkGnuPG (freeware)
http://hp.vector.co.jp/authors/VA023900/gpg-pin/index_en.html

Linux

KMail (KDE) : inclus dans KMail

Netscape 7 - Mozilla : Enigmail (libre)
http://enigmail.mozdev.org/

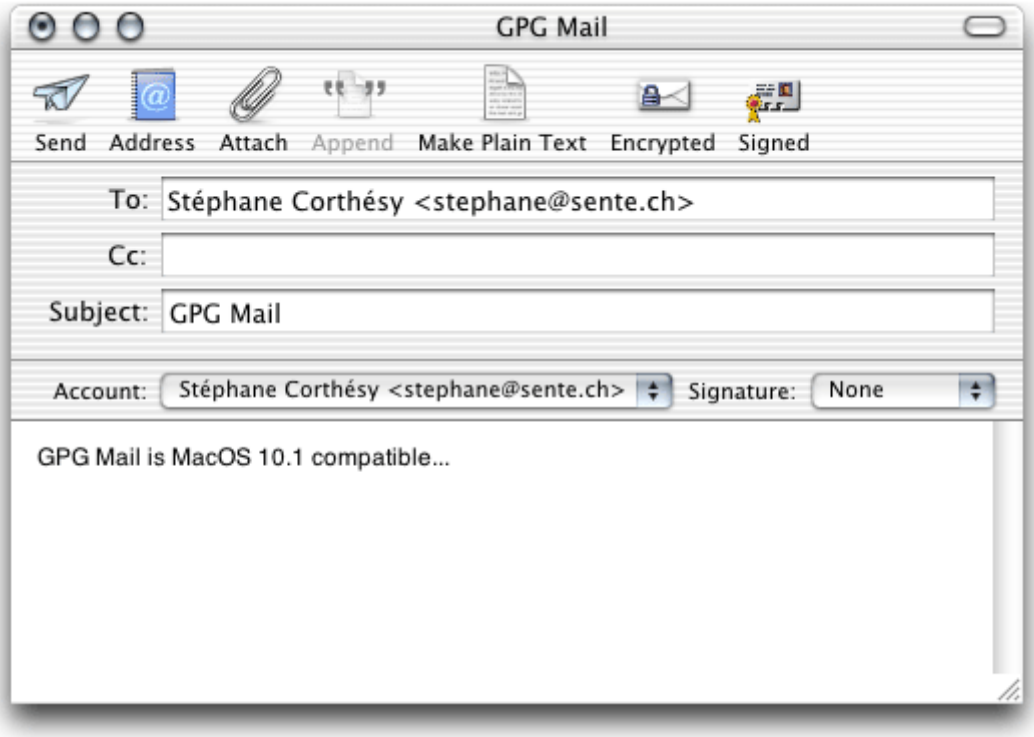
Evolution (Gnome) : inclus dans Evolution

MacOS X

Apple Mail : GPGMail for OSX (libre)
http://www.sente.ch/software/GPGMail/

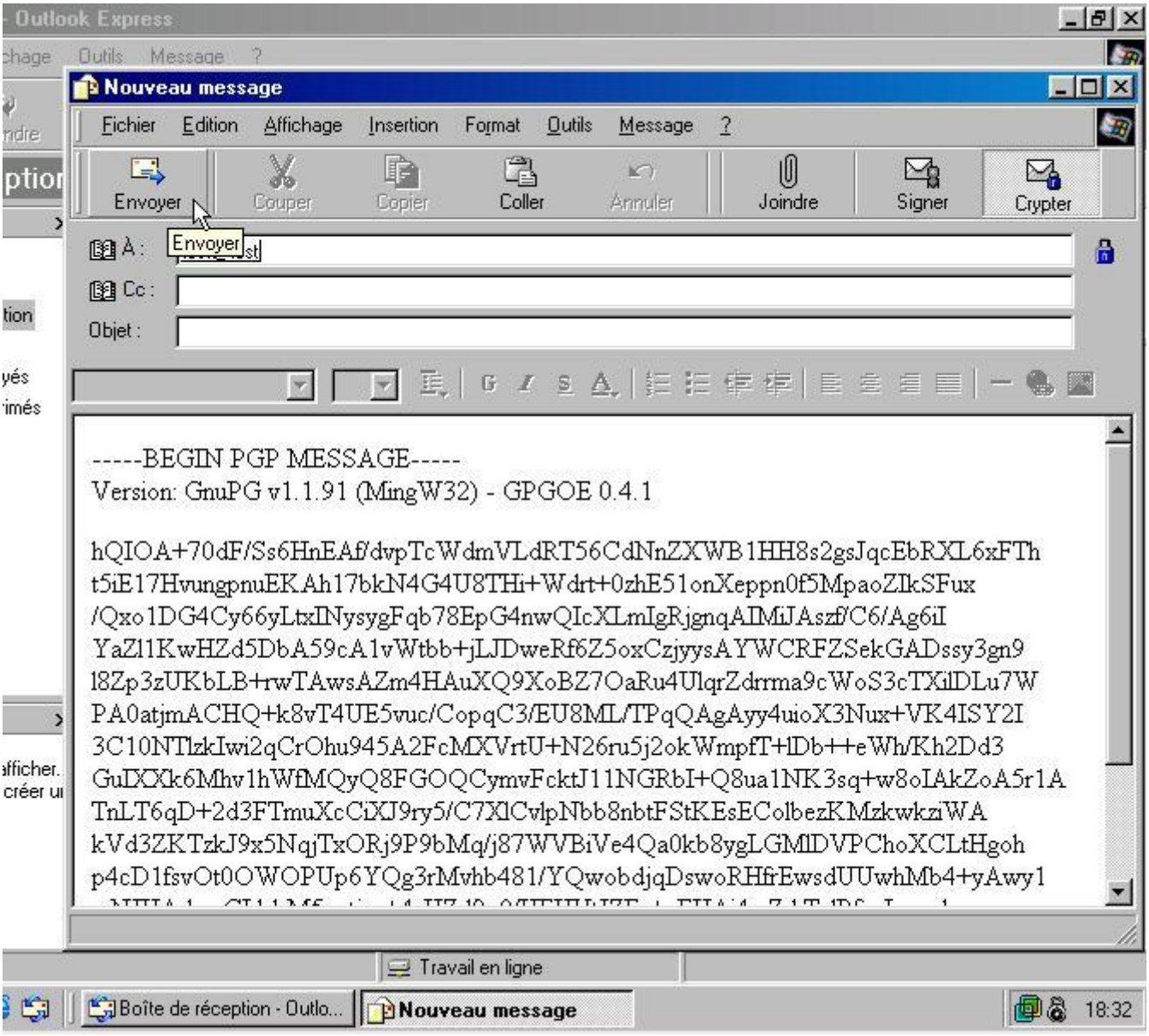
Eudora : Eudora-GPG (libre)
http://mywebpages.comcast.net/chang/EudoraGPG/

Entourage : EntourageGPG (libre)
http://entouragegpg.sourceforge.net/fr_readme.html



GPG et et le "plug-in" GPGMail pour Mail (MacOS X)

GPG et le "plug-in" Enigmail pour Netscape 7 / Mozilla



GPG et le "plug-in" GPGOE pour Outlook Express

5.2 L'aspect humain : décider vos correspondants à crypter

Voir la première partie : "Pourquoi crypter vos e-mails ?"

6. Documentations

Mode d'emploi de GPG Windows (Windows Privacy Tray) :
http://www.winpt.org/fr/faq.html

Mode d'emploi de GPG ligne de commande :
http://www.gnupg.org/gph/fr/manual.html

Mode d'emploi de MacGPG :
http://macgpg.sourceforge.net/fr/index.html#docs

PGP© 8.0 pour Windows XP :
www.pgpsupport.com

Page web de GPG :
www.gnupg.org

International PGP© Home page :
www.pgpi.org

OpenPGP en français :
www.openpgp.fr.st

7. Foire Aux Questions sur OpenPGP

7.1 Pourquoi la clé PGP générée est une "paire" de clés ?

La clé publique est le cadenas : elle sert à crypter
La clé privée est la clé du cadenas : elle sert à déchiffrer

Ce qui a été crypté avec la clé PGP (publique) de monsieur X, ne peut être déchiffré que par la clé privée de monsieur X, qui est seul à la détenir.

Quand vous envoyez un message PGP à quelqu'un, ce message est crypté avec sa clé publique (et il le déchiffrera avec sa clé privée).

7.2 Le cryptage est-il automatique ?

Oui, à trois conditions :
1) que le plug-in GPG/PGP© correspondant au logiciel e-mail utilisé (par exemple Outlook Express ou Netscape 7) ait été installé;
2) que le destinataire possède déjà une clé publique PGP et vous l'ai envoyé;
3) que vous cliquiez sur l'icone "cryptage OpenPGP" de votre logiciel e-mail avant l'envoi.

7.3 Ai-je besoin de choisir un mot de passe pour crypter en PGP ?

Non, le e-mail est crypté par le "cadenas" du destinataire (sa clé publique).

Contrairement aux logiciels de cryptage habituels, l'élément qui sert à crypter est différent de celui qui sert à déchiffrer : c'est comme un coffre-fort qui devrait être fermé avec une clé n° 1 et rouvert avec une clé n°2, chaque clé ne pouvant pas faire autre chose. Ici, la clé publique (ou "cadenas") sert à crypter et uniquement crypter.

7.4 Pourquoi OpenPGP me demande une "phrase de passe" ?

PGP demande au destinataire une "phrase de passe" pour utiliser la clé secrète de déchiffrement. Cette phrase de passe empêche quelqu'un qui touche à votre ordinateur de se servir à votre insu de votre clé privée.

C'est une double sécurité : même si quelqu'un réussissait à vous voler une copie de votre clé privée, il devrait encore entrer un code pour pouvoir s'en servir et déchiffrer les messages que vous

recevez ou signer un message à votre place.

7.5 Suis-je obligé de crypter tous mes e-mails ?

Dans l'idéal, oui. Sinon, cela met en évidence le caractère secret des rares e-mails cryptés, et surtout les noms de leur destinataire.

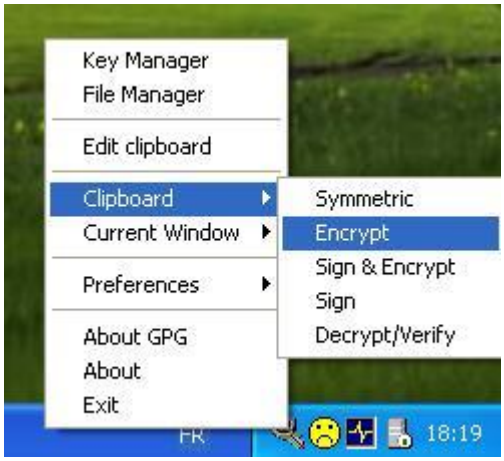
7.6 Si j'envoie un e-mail crypté à un destinataire qui n'utilise pas OpenPGP, que se passe-t-il ?

Ce cas de figure est théoriquement impossible : si le destinataire n'utilise pas OpenPGP, il n'a pas généré de paire de clés PGP, et n'a donc pas pu vous envoyer sa clé publique. OpenPGP crypte les e-mail à l'aide du "cadenas" du destinataire (sa clé publique PGP). Si OpenPGP ne trouve aucune clé publique correspondant au destinaire, il ne crypte pas.

7.7 Puis-je crypter un fichier sans l'envoyer ou avant de l'envoyer?

Oui, à l'aide de la fonction "Encrypt clipboard" (Crypter le presse-papiers) de GPG ou PGP©, qui cryptera la partie de texte mise en mémoire :

PGPfreeware 8.0 dans Windows 98



GPG dans Windows XP

La barre d'outils flottante de PGPfreeware 8.0

7.8 Puis-je crypter tout mon disque dur avec OpenPGP ?

En théorie, oui. Mais en pratique, OpenPGP est surtout un outil pour les e-mails, et il est mal adapté au cryptage de tout le disque.

L'outil PGPdisk est fourni dans la version payante de PGP©, mais il existe aussi sous Windows les logiciels gratuits E4M http://www.samsimpson.com/scramdisk.php#dloade (Windows XP), ou Scramdisk http://www.samsimpson.com/scramdisk.php#dload (Windows 95/98/Me), sous Linux le cryptage loopback du disque http://www.openpgp.fr.st/linux.htm, et sous MacOS X le cryptage d'images disques http://www.apple.com/fr/macosx/technologies/security.html.

(*) Les termes scientifiques corrects sont "chiffrement", "déchiffrement", "chiffrer", "déchiffrer". "Décrypter" possède un sens précis en cryptologie. Cryptage et crypter n'existent pas (même si les dictionnaires leur reconnaissent un certain statut).

Rédaction :
pplf (http://www.openpgp.fr.st)
et les membres de la FIL(http://www.vie-privee.org)

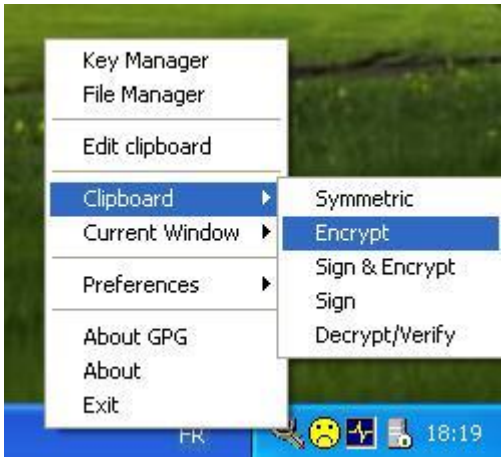
---

r>

7.7 Puis-je crypter un fichier sans l'envoyer ou avant de l'envoyer?

Oui, à l'aide de la fonction "Encrypt clipboard" (Crypter le presse-papiers) de GPG ou PGP©, qui cryptera la partie de texte mise en mémoire :

PGPfreeware 8.0 dans Windows 98



GPG dans Windows XP

La barre d'outils flottante de PGPfreeware 8.0

7.8 Puis-je crypter tout mon disque dur avec OpenPGP ?

En théorie, oui. Mais en pratique, OpenPGP est surtout un outil pour les e-mails, et il est mal adapté au cryptage de tout le disque.

L'outil PGPdisk est fourni dans la version payante de PGP©. Comme programmes gratuits, existent : sous Windows le logiciel Scramdisk http://www.samsimpson.com/scramdisk.php#dload (Windows 95/98/Me), sous Linux (Mandrake, SuSE, Knoppix) le cryptage loopback du disque http://openpgp.vie-privee.org/linux.html, et sous MacOSX 10.3 l'outil FileVault http://www.apple.com/fr/macosx/panther/file_vault.html.

8. Législation française

1. Principe : la réglementation des programmes informatiques de cryptographie

La France reste, pour des raisons assez incompréhensibles, la seule grande démocratie qui interdise aux citoyens de chiffrer en toute liberté leurs propres données privées ou leurs communications. Les multiples lois et décrets actuellement en vigueur (notamment les lois du 29 décembre 1990 et du 10 juillet 1991, et les décrets du 24 février 1998 et du 17 mars 1999) ainsi que la future "Loi pour la confiance dans l'économie numérique" (projet de loi en 2003) posent le principe de la liberté d'utilisation des outils de cryptographie, mais soumettent dans le même temps ces outils à des régimes complexes de déclaration ou d'autorisation.

2. En pratique : autorisation des outils OpenPGP en France

GPG : en 2002, la FSF-France ("Free Software Foundation"), une association liée au mouvement des logiciels libres Linux, a déposé un dossier de demande d'autorisation auprès de l'administration compétente (la DCSSI), pour le logiciel GnuPG (GPG). Cette demande a été acceptée, rapidement et dans des conditions très larges. GPG 1.x est donc librement utilisable dans toutes ses fonctions en France par tous, particuliers comme entreprises.

PGP© : en 2000, la société Network Associates France, propriétaire à l'époque de PGP©, avait obtenu une autorisation de la DCSSI (alors SCSSI) pour PGP version 6.0.2. Il est difficile de savoir si cette autorisation concernait, comme GPG, également les versions futures (par exemple PGP 8.0.3). Pour plus de détails sur PGP©, consulter la DCSSI (voir site web plus bas).

Liens :
Autorisation de GPG accordée à la FSF
Site de la DCSSI *(cache Google - site ssi.gouv.fr souvent injoignable)*
Textes de lois et décrets *(rechercher le terme "cryptologie")*
Projet de Loi pour la confiance dans l'économie numérique
Les législations du monde entier

(*) Les termes scientifiques corrects sont "chiffrement", "déchiffrement", "chiffrer", "déchiffrer". "Décrypter" possède un sens précis en cryptologie et signifie "casser" le code. Cryptage et crypter n'existent pas (même si les dictionnaires leur reconnaissent un certain statut).

Tor: l'anonymat en ligne

Résumé

Pourquoi Tor?

Qui utilise Tor?

Qu'est-ce que Tor?

Télécharger Tor

Donner pour soutenir Tor!

Aidez-nous à atteindre 5,000 noeuds en 2010 !

1755

Tor est un logiciel libre et un réseau ouvert qui aide à la défense contre une forme de surveillance de réseau qui menace les libertés individuelles et l'intimité, les activités commerciales et relationnelles, et la sécurité d'état connu sous le nom d'analyse de trafic.

Tor vous protège en faisant rebondir vos communications à l'intérieur d'un réseau distribué de relais maintenus par des volontaires partout dans le monde : il empêche qu'une tierce personne scrutant votre connexion internet connaisse les sites que vous avez visité, et empêche les sites que vous avez visité de connaître votre position géographique. Tor fonctionne avec beaucoup de nos applications existantes, comme les navigateurs web, les clients de messagerie instantanée, les connexions à distance et tout un nombre d'applications se basant sur le protocole TCP.

Des centaines de milliers de personnes à travers le monde utilisent Tor pour une grande variété de raisons : les journalistes et les blogueurs, les défenseurs des Droits de l'Homme, les agents d'application des lois, les soldats, les entreprises, les citoyens de gouvernement répressif, et de simples citoyens. Voyez Qui utilise Tor? sur cette page par quelques exemples typiques d'utilisateurs Tor. Consultez la vue d'ensemble pour une explication plus détaillée de ce que Tor fait, pourquoi cette diversité d'utilisateurs est importante.

Tor ne chiffre pas, comme par magie, toute votre activité internet. Vous devriez comprendre ce que Tor peut et ne peut pas faire pour vous.

La sécurité de Tor s'accroît autant que le nombre d'utilisateurs augmente et tant que le nombre de volontaires pour monter un relais croît. (Ce n'est pas aussi compliqué qu'on peut le croire, et cela peut étendre votre propre sécurité de manière significative.) Si vous ne souhaitez pas faire tourner un relais, nous avons besoin d' aide sur plusieurs points du projet, et nous avons besoin d'un financement pour continuer à rendre le réseau Tor plus rapide et plus facile à utiliser tout en maintenant une bonne sécurité.

Tor est une association américaine à but non lucratif (NDT : équivalent loi 1901 en France) dont la mission

est de prévenir l'analyse de votre trafic Internet.
Faites un don exonéré d'impôt.

Nouvelles

- *19 janvier 2010: version stable de Tor 0.2.1.22. Corrige un problème critique concernant les annuaires de passerelles. Cette mise à jour change également les clefs et les adresses de deux des sept annuaires d'autorités. Consultez l'annonce pour obtenir la liste complète des corrections.*
- *21 décembre 2009: version stable de Tor 0.2.1.21. Corrige les problèmes liés à OpenSSL et améliore la gestion des noeuds de sortie. Lisez l'annonce pour toute la listes des corrections.*
- *12 mars 2009 : Tor lance la campagne et le plan performance. Lisez la Publication de Presse pour plus d'information.*
- *19 décembre 2008 : Tor publie une feuille de route sur 3 ans. Lisez la Publication de presse pour plus d'information.*
- *Nous recherchons activement de nouveaux sponsors et de nouveaux fonds. Si votre organisation peut contribuer à rendre le réseau Tor plus utilisable et plus rapide, contactez nous. Les sponsors du projet Tor bénéficient d'une attention particulière, d'un meilleur support technique, de publicité (s'ils le souhaitent), et peuvent influer sur le cours des recherches et du développement. Merci de faire un don.*

Tor: Vue d'ensemble

Thèmes

Tor est un réseau de tunnels virtuels qui permet d'améliorer la protection de la vie privée et la sécurité sur Internet. Il offre également la possibilité aux développeurs de créer de nouveaux outils de communication respectueux de la vie privée. Tor fournit les bases grâce auxquelles de multiples applications vont permettre à des organisations et à des individus d'échanger des informations sur les réseaux publics sans compromettre leur intimité.

Des particuliers utilisent Tor pour empêcher les sites web de pister leurs connexions et celles de leurs familles, ou bien pour se connecter à des services de news, de messagerie instantanée ou autres lorsque ceux-ci sont bloqués par leurs fournisseurs d'accès. Les services cachés de Tor permettent de publier des sites web, ou de proposer d'autres services, uniquement accessibles via Tor, sans avoir à révéler l'emplacement géographique du site. Des particuliers utilisent aussi Tor dans le cadre de communications personnelles sensibles: forums de discussion pour victimes de viol ou d'agressions, services médicaux, etc.

Tor permet à des journalistes de communiquer de manière plus sécurisée avec des contacts ou des dissidents. Des organisations non gouvernementales (ONG) utilisent Tor pour permettre à leurs membres de se connecter à leur site web lorsqu'ils sont dans un pays étranger,sans dévoiler alentour pour qui ils travaillent.

Des groupes comme Indymedia recommandent à leurs membres l'usage de Tor pour protéger leur confidentialité et leur sécurité. Des groupes activistes comme l'Electronic Frontier Foundation (EFF) recommandent le recours à Tor qu'ils voient comme un moyen de préserver les libertés civiles sur Internet. Des entreprises utilisent Tor pour étudier leurs concurrents sans être surveillées et pour protéger leurs tractations des oreilles indiscrètes. Elles l'utilisent aussi pour remplacer les VPNs traditionnels, qui ne masquent ni la quantité des données échangées, ni la durée des connexions. Dans quelles entreprises les employés travaillent-t-ils tard ? Quelles sont les organisations dont les employés consultent des sites d'offre d'emploi ? Quels bureaux d'étude ont communiqué avec quels cabinets d'avocats d'affaire ?

Une des divisions de l'US Navy utilise Tor comme outil de renseignement dont le code est ouvert. Une de ses équipes s'est également servie de Tor récemment

lorsqu'elle était déployée au Moyen-Orient. La police utilise Tor pour visiter ou surveiller des sites web sans que les adresses IP gouvernementales n'apparaissent dans les logs des serveurs, ainsi que lors de certaines opérations, pour des raisons de sécurité.

La diversité des utilisateurs est en fait une composante importante de la sécurité de Tor. Vous êtes mêlés aux autres utilisateurs de Tor; plus la base d'utilisateurs est nombreuse et variée, meilleure est la protection de l'anonymat.

Pourquoi nous avons besoin de Tor

Tor protège de « l'analyse de trafic », une forme courante de surveillance sur Internet. L'analyse de trafic peut être utilisée pour découvrir qui parle à qui sur un réseau public. En connaissant la source et la destination de votre trafic Internet, on peut découvrir vos habitudes et vos centres d'intérêt. Cela peut avoir des conséquences financières si par exemple, un site de commerce en ligne ne propose pas les mêmes prix en fonction de votre pays ou institution d'origine. Il y a même des cas où votre emploi ou bien votre sécurité physique peuvent être compromis si vous dévoilez qui et où vous êtes. Si par exemple vous voyagez à l'étranger, et que vous vous connectez à l'ordinateur de votre employeur pour recevoir ou envoyer des emails, vous risquez de révéler votre pays d'origine et votre situation professionnelle à quiconque est en train d'observer le réseau, et ce même si la communication est chiffée.

Comment fonctionne l'analyse de trafic ? Les paquets de données Internet se composent de deux parties : une charge utile, et un en-tête utilisé pour le routage. La charge utile correspond aux données que l'on veut effectivement envoyer : un email, une page web, un fichier audio, etc. L'en-tête contient entre autres l'origine, la destination, la taille des données, des variables relatives aux durées de transmission, etc... Même si vous chiffrez vos données, les en-têtes restent visibles, et une analyse du trafic peut révéler beaucoup de choses sur ce que vous faites, et peut-être ce que vous dites.

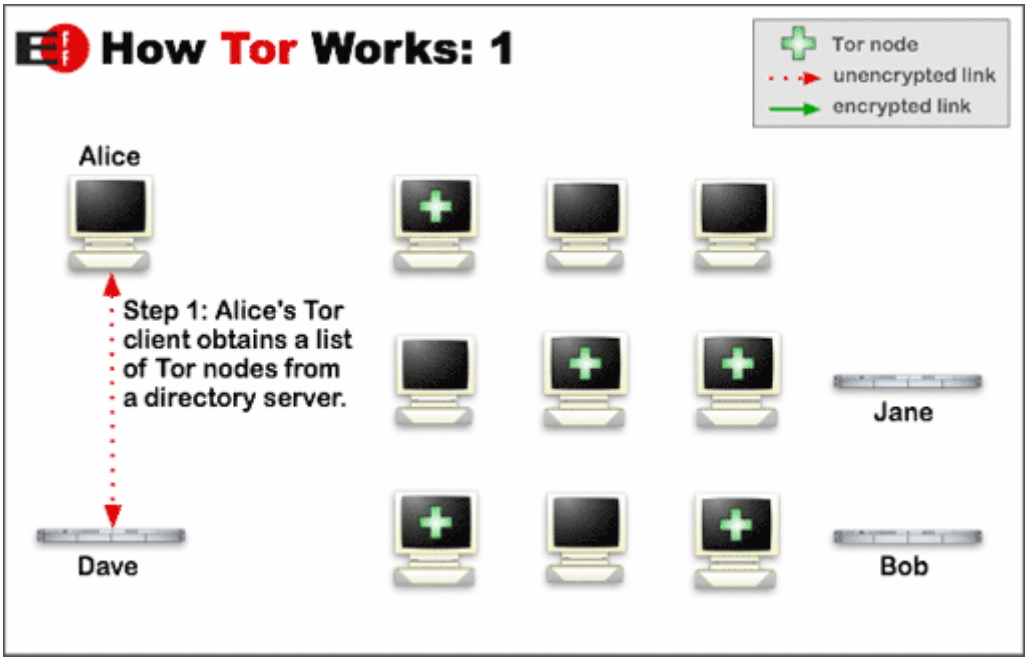
Un problème classique de protection de la vie privée est que les destinataires de vos communications peuvent savoir que vous en êtes l'auteur en regardant les en-têtes.

Les intermédiaires autorisés, comme les fournisseurs d'accès Internet, ainsi que parfois, des intermédiaires non autorisés, le peuvent également. Une forme d'analyse de trafic très simple consiste donc par exemple à capturer le trafic entre un expéditeur et un destinataire, et à regarder les en-têtes.

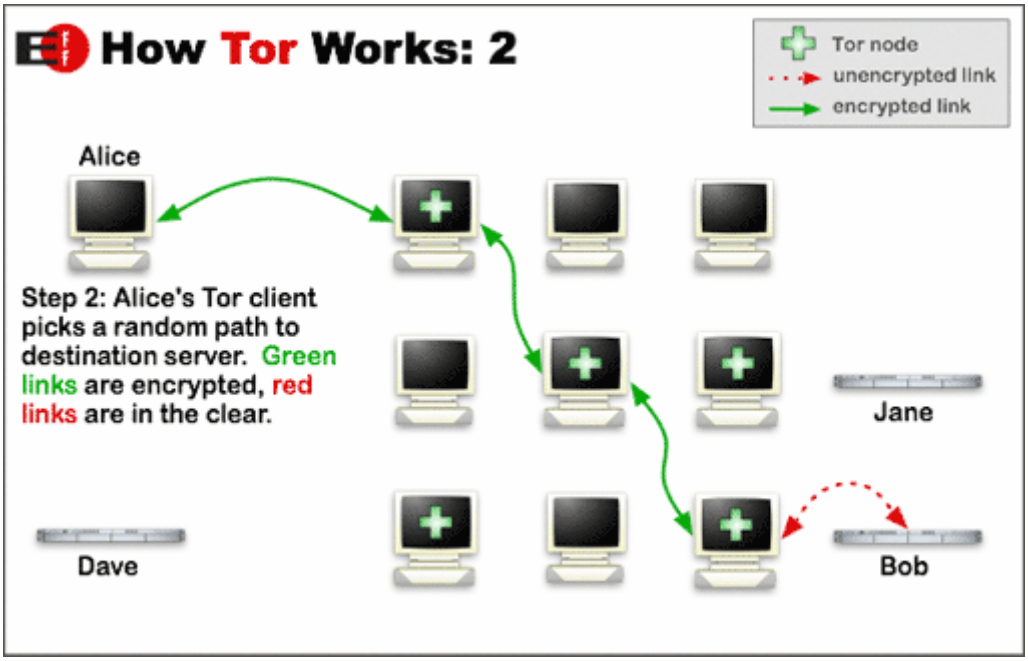
Mais il existe des formes d'analyse de trafic plus poussées. Certains attaquants épient plusieurs endroits de l'Internet, et se servent de techniques statistiques sophistiquées pour observer des motifs dans les communications. Le chiffrement ne dissimule que le contenu du trafic et pas les en-têtes. Il ne protège donc pas contre ces attaques.

La solution : une réseau anonyme décentralisé

Tor réduit les risques d'analyses de trafic simples ou sophistiquées, en répartissant vos transactions entre plusieurs endroits de l'Internet. On ne peut donc pas, en observant un seul point, vous associer à votre destinataire. C'est comme utiliser un chemin tortueux et difficile à suivre pour semer un poursuivant (tout en effaçant de temps en temps ses traces) . Au lieu d'emprunter un itinéraire direct entre la source et la destination, les paquets de données suivent une trajectoire aléatoire à travers plusieurs relais qui font disparaître vos traces. Personne ne peut donc déduire de l'observation d'un point unique, d'où viennent, ni où vont les données.

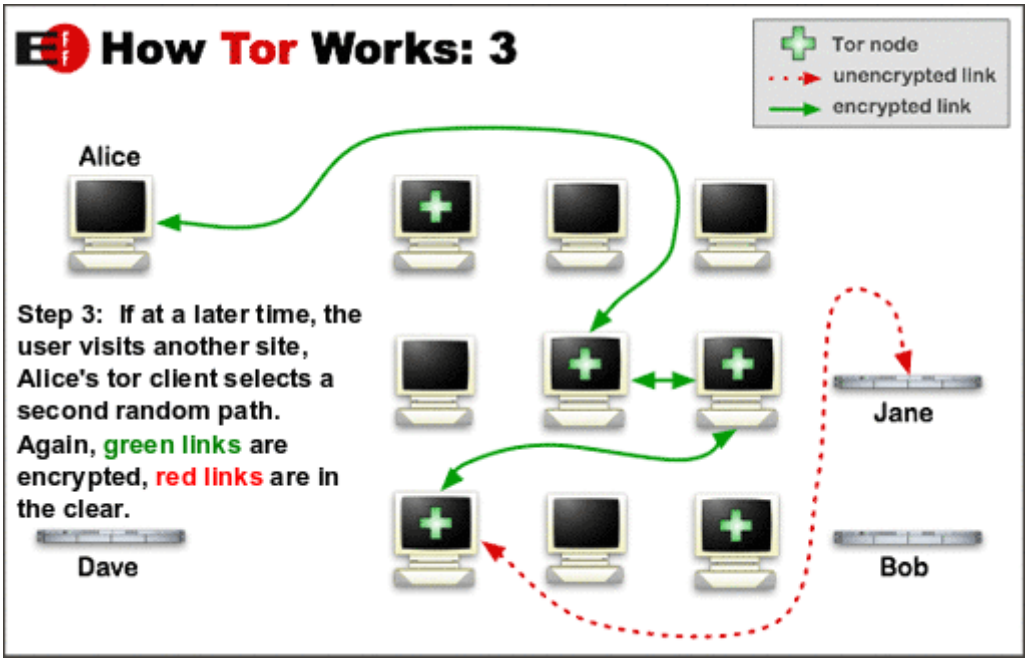


Pour définir un trajet privé à travers le réseau Tor, le logiciel de l'utilisateur détermine au fur et à mesure un circuit de connexions cryptées à travers les relais du réseau. Le circuit est construit étape par étape, et chaque relais le long du chemin ne connaît que celui qui lui a transmis les données, et celui auquel il va les retransmettre. Aucun relais ne connaît à lui tout seul le chemin complet pris par un paquet de données. Le client négocie indépendamment une paire de clé de chiffrement avec chaque serveur du circuit. Aucun d'eux ne peut donc intercepter la connexion au passage.



Une fois le circuit établi, différents types de données peuvent être échangées, et plusieurs sortes d'applications peuvent être utilisées via le réseau Tor. Vu que chaque serveur ne voit pas plus d'une étape dans le circuit, ni un éventuel intermédiaire, ni un noeud compromis ne peuvent analyser le trafic pour établir une relation entre la source et la destination d'une connexion.

Pour des raisons d'efficacité, le logiciel Tor utilise le même circuit pour des connexions qui ont lieu dans les mêmes dix minutes. Les requêtes ultérieures utiliseront un nouveau circuit, afin d'éviter que l'on puisse faire le lien entre vos actions précédentes, et les nouvelles.



Les services cachés

Les utilisateurs de Tor ont également la possibilité d'offrir des services, comme par exemple la publication d'un site web ou un serveur de messagerie instantanée, tout en masquant le lieu géographique de ce service. Les autres utilisateurs de Tor peuvent se connecter à ces services cachés en utilisant le système de « points de rendez-vous » de Tor. Ni le serveur, ni l'utilisateur ne peuvent alors découvrir avec qui ils communiquent. Ces services cachés permettent de mettre en place un site web sur lesquels des auteurs publieraient sans craindre la censure. Personne ne pourrait savoir qui a mis en place le site, et personne ne pourrait savoir qui a posté sur le site, pas même celui qui l'a mis en place. Plus d'information sur la configuration des services cachés et comment le protocole des services cachés fonctionne.

Rester anonyme

Tor ne résout pas tous les problèmes d'anonymat. Il ne s'occupe que du transport des données. Vous devez utiliser des programmes appropriés aux différents protocoles si vous voulez éviter que les sites que vous visitez puissent vous identifier. Vous pouvez par exemple utiliser un proxy web comme Privoxy, pour bloquer les cookies et les informations spécifiques à votre navigateur lorsque vous surfez.

Pour protéger votre anonymat, soyez malin. Ne rentrez pas votre nom ou d'autres informations personnelles dans les formulaires web. Soyez conscients que, comme tout réseau d'anonymat suffisamment rapide pour du surf sur le web, Tor ne protège pas contre certaines attaques temporelles : si votre attaquant peut observer à la fois le trafic sortant de votre poste, et le trafic arrivant à votre destination, il va pouvoir, grâce à des analyses statistiques, établir un lien entre les deux.

Le futur de Tor

Le paris de mettre en place un réseau d'anonymat utilisable aujourd'hui sur l'Internet n'est pas encore gagné. Nous voulons que le logiciel corresponde aux besoins des utilisateurs. Nous voulons aussi que le réseau reste fiable et puisse supporter le maximum d'usagers possible. Sécurité et facilité d'utilisation ne sont pas des notions antagonistes : plus Tor deviendra simple à utiliser, plus le nombre d'utilisateurs grandira, plus il sera difficile de pister une personne parmi toutes les connexions possibles, meilleure sera la sécurité pour tout le monde. Nous progressons, mais nous avons besoin de votre aide. Pourquoi ne pas mettre en place un relais, ou vous investir dans le développement.

Les tendances législatives et technologiques actuelles menacent de plus en plus notre anonymat, restreignant ainsi notre liberté d'expression et d'accès à l'information sur l'Internet. Cela fragilise également la sécurité nationale et les infrastructures critiques en rendant les communications entre les individus, les organisations, les sociétés, et les gouvernements, vulnérables à l'analyse de trafic. Chaque utilisateur et chaque relais introduit de la diversité, renforçant ainsi la possibilité offerte par Tor de nous laisser reprendre le contrôle de notre sécurité et de notre vie privée.

.
, il existe une solution : le réseau Freenet qui est un réseau totalement anonyme et crypté, idéal pour échapper à la censure. Voici l'article Wikipedia : http://fr.wikipedia.org/wiki/Freenet
J'ai eu l'occasion de le tester : ça marche bien quoique un peu lent et peu fourni. L'installation du logiciel d'accès ne pose pas de problème particulier : il suffit de bien lire la documentation et de bien suivre les indications à l'écran. Amitiés, Yann

Freenet

Un article de Wikipédia, l'encyclopédie libre.

Aller à : Navigation, rechercher

Freenet

Page d'accueil de FProxy (Freenet 0.7)

Développeur	Ian Clarke
Dernière version	0.7.5 (12 juin 2009) [+/−]
Environnement	indépendant
Type	Client P2P
Licence	GNU GPL
Site Web	freenetproject.org

modifier

Freenet est un réseau informatique anonyme et décentralisé construit sur l'Internet. Il vise à permettre une liberté d'expression et d'information totale fondée sur la sécurité de l'anonymat, et permet donc à chacun de lire comme de publier du contenu. Il offre la plupart des services actuels d'Internet (courriel, téléchargement, web, etc.)

Freenet a été créé suite à une inquiétude croissante à propos des libertés sur internet. Cette citation de Mike Godwin datant de 1996 résume cette inquiétude :

« Je suis tout le temps soucieux au sujet de mon enfant et d'Internet, bien qu'elle soit encore trop jeune pour se connecter. Voilà ce qui m'inquiète. Je redoute que dans 10 ou 15 ans elle vienne me voir et me demande : "Papa, où étais-tu quand ils ont supprimé la liberté de la presse sur Internet ?" » (I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say "Daddy, where were you when they took freedom of the press away from the Internet?")

Deux versions cohabitent actuellement : la 0.5 considérée comme « caduque » (car n'est plus développée) et la 0.7 qui est un réseau de type ami à ami.

Sommaire

[masquer]

Principe de fonctionnement [modifier]

Chaque ordinateur du réseau Freenet stocke une partie des informations disponibles sur le réseau ; les ordinateurs connectés à Freenet sont des nœuds du réseau. L'espace alloué par le nœud sert à stocker des fragments de données du réseau chiffrés localement, dont l'utilisateur ne connait pas le contenu. Pour récupérer une information, identifiée par une clé unique, l'ordinateur client demande à

d'autres ordinateurs du réseau la clé en question. Ceux-ci peuvent la renvoyer ou, s'ils ne l'ont pas dans leur cache, peuvent la demander à leur tour à d'autres nœuds, la limite de profondeur de la requête étant gérée par un maximum : le HTL, pour Hops To Live, littéralement sauts à vivre.

Ainsi, un ordinateur qui demande ou envoie un contenu ne se révèle pas, car il peut avoir initié l'envoi ou la demande d'envoi, ou l'avoir simplement relayée. De plus, il n'est pas possible de savoir à quoi correspond le trafic transitant par son nœud si l'on n'est pas déjà en possession du contenu.

Un ordinateur qui fait transiter une information peut en garder une copie dans son cache. Ainsi, les données les plus demandées sont présentes dans plus de nœuds et sont plus faciles à obtenir — on peut même parler de déplacement dynamique des données sur le réseau en fonction de la demande — tandis que les données rarement demandées sont peu à peu remplacées par d'autres et disparaissent du réseau après un délai indéterminé. L'ajout de données au réseau passe par leur inclusion au cache local, et par leur envoi vers d'autres machines pour forcer l'inclusion. Cette conception du stockage et du transfert de l'information garantit sa conservation en fonction de la demande, et permet à quiconque d'héberger tout contenu, sous réserve que celui-ci soit téléchargé de temps à autre. Il est également impossible de supprimer ou de censurer une information. Le réseau peut donc être utilisé pour diffuser des données illégales, ou plus ou moins douteuses.

La conception décentralisée du réseau interdit à quiconque — même à ses concepteurs — de stopper son fonctionnement.

Logiciels [modifier]

Les fondateurs et responsables du réseau Freenet sont également les auteurs du logiciel Fred (Freenet REference Daemon), qui est un logiciel libre programmé en Java permettant de communiquer selon le

protocole du réseau Freenet. Chaque ordinateur possédant un moyen de faire fonctionner Java peut le faire fonctionner et donc accéder à Freenet (Windows, Mac OS, Linux, Unix, etc.).

Après l'installation de Fred, l'utilisateur choisit de lui attribuer :

- Une certaine quantité de bande passante réseau (que Fred essaiera de ne pas dépasser)
- Une certaine quantité d'espace disque (de préférence, au moins quelques Giga-octets)

Fred n'étant qu'un démon, il est nécessaire d'utiliser un navigateur web pour s'y connecter (à l'adresse http://localhost:8888/). Fred est capable de générer l'interface de gestion du nœud, et intègre par ailleurs un système de signets. Mozilla Firefox ou d'autres navigateurs libres sont généralement recommandés du point de vue de la sécurité et de l'anonymat, bien que ce point soit parfois sujet à discussions.

Il existe également des outils utilisant le réseau Freenet :

- FIW (pour insérer et gérer des freesites, remplacé par JSite sous freenet 0.7)
- Frost (Groupes de discussion à la Usenet pour Freenet 0.5 et 0.7 (mais pas les deux à la fois), souffre beaucoup du spam et du flood)
- FMS (Remplacant de Frost, résistant au spam et basé sur une "toile de confiance", pour Freenet 0.7 uniquement)
- Fuqid (gère les insertions et les téléchargements à la chaîne de fichiers sur Freenet 0.5 et 0.7)
- Freemail (gère les courriers électroniques envoyés sur Freenet pour la 0.5, en cours de réécriture pour la 0.7)
- FMB (IRC moins performant que Frost, mais permet de jouer aux échecs en ligne, n'existe que sous freenet 0.5)
- Spider (robot d'indexation qui fait un annuaire des freesites présents sur Freenet)

- *pm4pigs (Un logiciel de messagerie plus simple que freemail)*
- *Thaw, qui effectue les mêmes tâches que FUQID, pour freenet 0.7*
- *FreeMule, Programme de partage de fichier indirectement au travers du reseau freenet. Existe pour freenet 0.5 et 0.7 en deux versions bien spécifiques.*

Freesites [modifier]

***Un Freesite est simplement un site web contenu dans Freenet.** Il est identifié par une clé (longue chaîne de caractères l'identifiant de façon unique) et un activelink (petite image permettant de savoir si le freesite est accessible).*

Sur Freenet 0.5 [modifier]

Il existe trois types de Freesites :

1. *One shot : comme son nom l'indique, ce type de site est publié une seule fois, il ne sera plus possible de le modifier par la suite ;*
2. *Edition : chaque édition contient des liens vers les versions suivantes. Les personnes naviguant sur une ancienne édition voient par les activelink qu'une nouvelle est disponible ;*
3. *DBR (Date Base Redirect) : la redirection vers le site s'effectue d'après la date courante. Il est utilisé pour les sites évoluant souvent.*

Le logiciel permettant d'insérer des Freesites est FIW.

Sur Freenet 0.7 [modifier]

1. *CHK (Content Hash Key) : clef pour l'insertion d'un fichier unique, sans mise à jour par la suite ;*
2. *SSK (SubSpace key) : pour l'insertion d'un freesite, sans mises à jour ultérieures mais possibilité de rajouter des fichiers dans le subspace ;*

3. USK : subspace avec redirection, possibilité de mettre à jour ;
0. KSK : clef directement compréhensible par un utilisateur, peu utilisée en pratique pour des fichiers car peu sécurisée.

Le logiciel permettant d'insérer des Freesites est jSite.

Voir aussi [modifier]

Liens connexes [modifier]

- Darknet

Outils utilisant le réseau Freenet [modifier]

- Frost
- FMS
- Fuqid
- Freemail
- FIW
- Freemule
- Thaw
- jSite
- Freekiwiki (permet de créer des wikis anonymes sur Freenet)

Autres réseaux anonymes [modifier]

- ANts P2P : échange de fichiers, anonymisation de serveur web HTTP, et Chat (non anonymisé).
- Entropy
- GNUnet : échange de fichiers anonyme multi fonctions (multiplateforme)
- I2P
- Mnet
- MUTE : échange de fichiers
- OFFSystem : système de partage de fichiers
- Omemo
- OneSwarm : Le protocole Bittorent modifié pour faire du p2p entre ami(e)s
- StealthNet (anciennement Rshare) : échange de fichiers

- *Tor : The Onion Router ; naviguer sur Internet de manière anonyme*
- *Fidonet : Réseau de communications par ligne téléphonique*

Liens externes [modifier]

- *(en) Site officiel de Freenet*
- *(en) Wiki officiel de Freenet*
- *(fr) Documentation sur Freenet en français*
- *(fr) Freenet : la face cachée de l'internet, 7 novembre 2005, Bruno Fay*

07 novembre 2005

Freenet : la face cachée de l'internet

Vous ne voulez pas laisser de traces sur le web, vous voulez vous sentir libre, découvrir un nouvel univers : Freenet est pour vous ! Un réseau parallèle à l'internet, totalement anonyme, crypté et clandestin, pour garantir la confidentialité des échanges.

L'exploration de Freenet ressemble aux premiers pas de l'homme sur la lune. C'est le même parfum de découverte, la même apréhension face à l'inconnu, l'impression de pénétrer dans une cité interdite. En haut de la page d'accueil, le dessin d'un petit lapin bleu. Comme Néo, il faut suivre le rongeur pour entrer dans la

matrice. Ici on avance à tatons, sans moteur de recherche. On découvre les pages comme on pousserait des portes au hasard dans un vieux château écossais. Les freesites sont généralement assez sobres et les photos sont rares pour ne pas occuper trop d'espace mémoire. Oubliez l'Adsl, les premières pages consultées peuvent mettre 30 mn avant de s'afficher. Avec le temps la vitesse s'améliore sensiblement… mais le lapin bleu n'ira jamais beaucoup plus vite qu'un bon vieux minitel. « Je ne pense pas que l'on puisse accélérer un jour la vitesse », explique un habitué qui traîne souvent ici sous le pseudo de FreenetFR, « car la lenteur est justement le seul moyen de garantir l'anonymat des gens.»

Ian Clarke, le génie écossais

En 1999, Ian Clarke n'a que 22 ans lorsqu'il invente le logiciel libre Freenet (à ne pas confondre avec la société Free et la Freebox), un réseau parallèle au web avec ses groupes de discussion, son propre système de mails et de téléchargement anonymes. L'étudiant surdoué de l'Université d'Edimbourg, en Ecosse, imagine le monde comme un gigantesque disque dur unique dont chacun détiendrait une parcelle. Contrairement au web, il n'y a pas de serveurs pour héberger les sites. Freenet est un réseau décentralisé où les informations sont cryptées, dupliquées, découpées et stockées par petits bouts directement sur les ordinateurs des utilisateurs sans

que personne ne sache qui héberge quoi. Quand on cherche un site, l'ordinateur récupère des morceaux de pages cryptés en fouillant dans le disque dur des ordinateurs qu'il connaît, qui interrogent à leur tour les autres ordinateurs qu'ils connaissent, etc. En bref, Freenet rend l'identification et la censure impossible, même pour ses concepteurs. « Ici on a le sentiment de pouvoir tout dire », résume Dieppe, fraîchement débarqué sur le réseau. Freenet garantit la liberté d'expression la plus totale, avec ses avantages mais aussi ses excès.

Cette liberté, regrette un freenaute américain en référence aux nombreux sites pédophiles qui gangrènent le réseau, doit s'accompagner d'une plus grande responsabilité que beaucoup de gens n'assument pas ». « Si vous refusez la liberté d'expression à ceux que vous méprisez, alors vous ne croyez pas en la liberté d'expression… mais c'est parfois une pilule dure à avaler, ajoute-t-il, même pour un libertaire comme moi ! » Il est en effet difficile de surfer sur Freenet sans tomber sur des sites aux titres comme ''Underage sex'', ''garçons nus'', ''confession d'un pédophile''… Peut-on pour autant parler de paradis des pédophiles ? Pour Marc Daniel, expert informatique auprès de la Cour d'appel de Paris, la réponse est négative : «la plupart des pédophiles ne sont pas des informaticiens, ils récupèrent le plus souvent les images sur les réseaux classiques de P2P et ils ne sont qu'une très faible minorité à savoir utiliser des outils comme Freenet.». Des propos rassurants pour les utilisateurs comme FreenetFR ou Wam qui en ont « assez d'entendre dire que c'est un repaire de pédophiles ». Alors, que trouve-t-on sur Freenet ?

Au nez et à la barbe de la police

Outre les freesites anarchistes ou paranos, l'anonymat attire la plupart des activités illégales imaginables : fabrication d'explosifs, prostitution, fabrication et trafic de drogues, terrorisme, hacking… On trouve aussi un rapport confidentiel réalisé en interne par Cap Gémini sur le filtrage des réseaux haut débit ou encore des snuffs réalisés par de vrais assassins ! Lors de l'entretien, Ian Clarke m'a même révélé que la secte de la scientologie utiliserait son réseau pour passer ses transactions financières secrètes. Une information invérifiable puisqu'il est techniquement impossible de connaître l'existence d'un site si son concepteur n'en communique pas la clé. Pour FreenetFR, fidèle parmi les fidèles, « quelqu'un qui a envie de faire un site vraiment illégal ne va pas le publier dans l'annuaire ni l'annoncer sur les groupes de discussion, il va

directement communiquer l'adresse de son site à la personne avec qui il souhaite discuter en toute confidentialité ».

Difficile d'imaginer que des terroristes se privent d'un tel outil pour communiquer entre eux, au nez et à la barbe des pandores du monde entier… Interrogés par mes soins, le ministère de l'Intérieur et la gendarmerie nationale choisissent d'ailleurs la

politique de l'autruche pour résumer leur désarroi face à Freenet : « trop confidentiel, on ne peut rien dire. » A moins, comme le suggère fourbement le freenaute Daneel, « qu'ils ne connaissent même pas notre existence et qu'ils ne veuillent pas passer pour des buses en disant des conneries ! ».

Sus à la censure !

La liberté de pouvoir tout dire, de pouvoir traiter les flics de buses et de pouvoir écrire « Sarko facho », c'est peut-être ça la vraie richesse du projet. Sur Frost, le forum crypté et anonyme de Freenet, les débats sont enflammés, libres et souvent de haute qualité. On s'interroge à haute voix sur les dérives sécuritaires et liberticides, on évoque sans tabou les bavures policières. Bastochard, qui se présente lui même comme un vieux praticien du P2P, trouve ici un air de liberté : «L'atmosphère législative et judiciaire devenant irrespirable, je cherchais depuis une paire d'année des systèmes plus discrets, plus sécurisés.» D'autres Freenautes comme Wam apprécient particulièrement le bon esprit de la communauté francophone : « ce sont des gens curieux, doués d'un bon esprit critique, et qui osent se défendre quand on les agresse.» Ceux qui utilisent le réseau pour télécharger des disques et des films sont finalement plutôt rares, lenteur oblige.

Les choses pourraient rapidement changer, la prochaine version de Freenet devrait être plus simple, plus rapide. Elle devrait surtout permettre de corriger une faille découverte par le régime chinois toujours en pointe en matière de censure. N'ayant aucun moyen d'identification et de contrôle sur le contenu, les maîtres de Pékin ont eu l'idée de brancher leurs propres ordinateurs sur Freenet pour bloquer à l'aveugle, en moins de 20 minutes, tous les échanges avec les autres ordinateurs connectés au réseau. Les Chinois sont malins mais peut-être pas autant que Ian Clarke qui promet de supprimer ce talon d'Achille. L'informaticien génial lance aujourd'hui un appel mondial pour un regroupement de développeurs afin de rendre Freenet à terme complètement invisible, même aux yeux des Chinois. Ce futur réseau a déjà un nom, il s'appellera Darknet, pour le pire comme pour le meilleur.

Bruno Fay

———-

Entretien avec Ian Clarke

"Si les gouvernements peuvent contrôler l'information délivrée aux électeurs, alors le processus démocratique est faussé"

Quelle était votre motivation première pour créer Freenet en 2000 ?
Il y avait deux motivations. D'abord, j'étais sensible au fait qu'il est extrêmement facile pour des gouvernements de contrôler les informations circulant sur internet. Cela me semblait contraire à

la liberté d'expression. Ensuite, Freenet représentait un challenge tecnologique intéressant. Je suis simplement motivé par ma foi en la démocratie. La démocratie s'appuie sur ses électeurs pour choisir en connaissance de cause ceux qui dirigeront le gouvernement. Mais si les gouvernements peuvent contrôler l'information délivrée aux électeurs, alors le processus démocratique est faussé.

Cinq ans après sa création, êtes-vous satisfait de Freenet ?
Freenet n'est pas aussi facile à utiliser que je l'espérais. Je crois que la principale raison est que Freenet est à la fois un projet de recherche et un projet de logiciel grand public. Le fait que Freenet soit utilisé pour la recherche rend son utilisation pour le grand public plus difficile. Notre intention est que la prochaine version de Freenet soit beaucoup plus facile à utiliser.

Quand on voit tous les Freesites pédophiles, n'avez-vous pas parfois le sentiment d'avoir créé une sorte de monstre qui vous aurait échappé ?

Je crois qu'il est inévitable que certaines personnes utilisent Freenet pour des choses que je trouve de mauvais goût, voire écoeurantes, mais c'est malheureusement toujours ainsi, quelle que soit la technologie utilisée. On ne peut pas condamner un intrument dans son ensemble juste à cause d'une petite minorité qui le détourne son utilisation première. Je crois que les effets positifs de Freenet sont de très loin supérieurs à ses effets négatifs.

Quels sont actuellement vos freesites préférés ?
En ce moment j'utilise rarement Freenet, je préfère me concentrer sur le développement de la prochaine version. La prochaine version de Freenet devrait constituer un progrès considérable. Nous allons passons du TCP à l'UDP et nous allons supprimer de nombreux problèmes qui ne servaient à rien.

Certains évoquent d'ailleurs une collaboration avec le réseau I2P ?
Nous pensons que le programme I2P est un grand logiciel de P2P, et nous sommes heureux de travailler avec eux quand besoin est. Mais il y a de grosses différences entre nos deux approches et je crois que chaque projet doit servir pour un usage bien précis.

Combien de personnes environ utilisent Freenet ?
C'est très difficile à dire, mais plus de 2 millions de personnes ont téléchargé notre logiciel depuis la création du projet.

Avez-vous rencontré des problèmes avec les autorités ?
Non, pas à ce que je sache.

Y a t-il vraiment beaucoup de sites qui ne pourraient pas exister sur internet ?
Il existe des Freesites chinois dont ont peut trouver la copie des adresses sur le site internet Freenet-China. A ma connaissance, les sites américains qui critiquent la guerre en Irak ne sont pas censurés, ils n'ont donc pas besoin de venir sur Freenet. Un exemple de ce que l'on peut trouver sur Freenet et que l'on ne trouverait pas ailleurs, ce sont les accords commerciaux secrets de l'église de scientologie. Quand le scandale sur le système de vote électronique Diebold a éclaté aux Etats-Unis, Freenet était également l'un des très rares endroits où l'on pouvait trouver des informations à ce sujet.

Propos recueillis par Bruno Fay

Description generale

Un article de Freenet Doc.

(Redirigé depuis Description générale)
Aller à : Navigation, Rechercher

> **Pour télécharger Freenet :**
> **http://freenetproject.org/download.html**

Sommaire

[masquer]

[modifier] D'où vient Freenet ?

Freenet est un projet logiciel créé en 1999 par Ian Clarke à l'Université d'Edimbourg.

La première publication du projet peut être consultée en ligne à l'adresse suivante : http://freenetproject.org/papers/ddisrs.pdf On y découvre un "système de stockage et de récupération d'information, distribué et décentralisé".

Depuis, le projet est devenu un logiciel libre et Ian a été rejoint par plusieurs développeurs, dont un - Matthew Toseland - travaillant à plein temps pour le projet et rémunéré grace aux dons.

[modifier] Quels sont ses objectifs ?

L'objectif premier de Freenet est de mettre à disposition de tous ceux qui le désirent un espace de totale liberté d'expression. Pour ce faire, il faut que tout le monde puisse s'exprimer sans craindre de

représailles, et donc, que tout le monde puisse être anonyme.

Mais cela ne suffit pas. Pour que tout le monde puisse s'exprimer, il faut combattre aussi toute forme de censure. On citera par exemple la Chine, qui met en place des moyens considérables pour filtrer les informations accessibles depuis internet pour ses habitants (souvent avec la complicité de grandes compagnies occidentales, comme Yahoo, Google, ...).

Il est aussi nécessaire que cet espace soit tout le temps accessible, et donc que personne ne puisse bloquer le fonctionnement du réseau.

Pour atteindre l'objectif principal de totale liberté d'expression, il faut donc atteindre trois autres objectifs secondaires, l'anonymat, la résistance à la censure, la résistance aux attaques. Les moyens pour atteindre ces objectifs sont différents, ils sont expliqués dans la Description technique.

[modifier] Comment ça fonctionne globalement ?

Freenet est un réseau à l'intérieur d'internet. On confond souvent le réseau web et le réseau internet. En fait, le web est aussi un réseau à l'intérieur d'internet. Internet, c'est l'ensemble des ordinateurs qui sont connectés via une connexion (adsl,cable,56k). Le web, c'est l'ensemble des serveurs web sur lesquels sont stockés les sites. Quand vous surfez sur le web, vous êtes simplement connectés à ces serveurs via internet. Votre navigateur web, qui est en fait le seul qui navigue sur internet, est un client.

C'est la même chose pour Freenet, sauf que le réseau ne fonctionne pas de la même façon. Pour faire une analogie avec le web, chaque utilisateur est en fait un serveur, et il stocke donc une partie du réseau sur son disque dur. Quand vous vous connectez sur Freenet, vous devenez donc en même temps client et serveur, mais pour vous, rien ne change vraiment. En effet, la partie serveur est gérée par un logiciel,

et c'est toujours votre navigateur qui joue le rôle de client. Cette structure particulière, bien utilisée, permet de devenir anonyme (si vous voulez savoir comment, jetez un oeil à la Description technique), et d'assurer la sécurité du réseau face à des attaques. En effet, sur le web, il suffit d'attaquer un serveur pour que le site associé ne soit plus accessible. Sur Freenet, comme les sites sont stockés sur plusieurs serveurs, et qu'on ne sait pas où ils sont stockés, il devient très compliqué de les rendre inaccessibles.

Freenet n'est donc rien de plus qu'un réseau à l'intérieur d'internet, tout comme le web mais aussi les réseaux ed2k (eMule), BitTorrent, etc. Seule la structure du réseau change, ainsi que ses objectifs. Qu'est-ce qui différencie donc Freenet des autres ?

Tout d'abord, Freenet n'est pas un réseau P2P. Contrairement à un réseau P2P, Freenet permet aussi de visualiser et d'insérer des sites dans le réseau. Contrairement au Web, Freenet est anonyme et résistant aux attaques.
Mais il n'y a pas que des avantages. Ainsi, Freenet est moins rapide que les réseaux P2P et que le web. Les sites ne sont pas non plus dynamiques.

Ainsi, il vous faudra choisir entre la vitesse et l'anonymat. Chaque réseau à des objectifs différents, choisissez celui qui vous convient le mieux (bien sûr, le web n'est ici cité qu'en exemple, vous n'aurez pas à choisir entre Freenet et le web).

[modifier] Que peut-on faire avec ?

Avec Freenet, vous pourrez, librement et en tout anonymat :

- *Surfer sur des freesites (l'équivalent des sites web) grâce à votre navigateur (voir Configurer Firefox pour Freenet),*
- *Insérer votre freesite sur le réseau (voir Insérer un Freesite),*

- *Discuter dans des forums de discussion semblables aux newsgroups,*
- *Echanger des fichiers.*

[modifier] Comment on s'y connecte ? Comment c'est organisé sur mon ordinateur ?

*Pour se connecter à FreeNet, vous devez installer sur une machine un nœud (on entend plus souvent le terme anglais node), qui va se charger de communiquer avec les autres nœuds du réseau, d'acheminer les données, de les transmettre, bref, de tout faire (pour savoir comment installer le nœud, rendez-vous ici). Une fois ce nœud installé, il faut que vous puissiez communiquer avec, que ce soit pour le configurer ou simplement pour naviguer sur FreeNet (puisque toutes les données passent d'abord par le nœud). Par défaut (donc ce sera surement votre cas), le nœud est installé sur la même machine, et est accessible par le port 8888. Concrètement, cela veut simplement dire que pour communiquer avec le noeud, vous avez juste à lancer votre navigateur préféré (Internet Explorer n'est *pas* recommandé), et à inscrire dans la barre d'adresse : http://localhost:8888/ Vous aurez alors accès à votre nœud, et vous pourrez par exemple le configurer. Le nœud utilise aussi un datastore, c'est à dire un dossier où il peut ranger toutes les clés dont il a besoin (pour reprendre le parallèle avec internet, c'est un peu comme la partie serveur des sites webs, où sont stockés les fichiers du site, sauf qu'ici vous ne savez pas ce que vous stockez). Enfin, vous l'aurez compris, il faut que votre noeud soit lancé pour que vous puissiez accéder à FreeNet. D'ailleurs, nous vous conseillons de le laisser allumé le plus longtemps que vous pouvez : cela améliorera votre intégration au réseau et donc vos performances, et même les performances du réseau (puisque les clés stockées chez vous seront accessibles plus de temps).*

[modifier] A quoi ça ressemble ?

Voici quelques captures de la page d'accueil de FreeNet. C'est ici que vous pourrez configurer votre

nœud, voir quelques informations dessus, lancer des plugins. Bref, c'est un peu l'incontournable.

Description technique

Un article de Freenet Doc.

Aller à : Navigation, Rechercher

Attention cet article est en cours de validation par l'équipe de documentation, par conséquent les informations que vous pouvez y trouver peuvent être erronées et/ou incomplètes (en savoir plus sur la validation des articles)

Sommaire

[masquer]

[modifier] Le stockage de l'information

Dans Freenet, tout est fichier : les pages et les images composant un Freesite, les messages que vous échangez dans les groupes de discussions, etc. Les fichiers sont découpés en morceaux de 32 Ko et identifiés par des clés. Quand un fichier fait plus de 32 Ko, sa clé pointe vers un fichier qui contient la liste des clés de chaque morceau qui le compose.

[modifier] Les clés

Il existe plusieurs types de clés. Chacune a son utilité :

[modifier] Les CHK

Content-Hash Key

Ces clés servent à désigner un fichier particulier contenu dans le réseau. Voici à quoi elles ressemblent :

CHK@SVbD9~HM5nzf3AX4yFCBc-A4dhNUF5DPJZLL5NX5Brs,bA7qLNJR7IXRKn6uS5PAySjIM6azPFvK~18kSi6bbNQ,AAEA--8

Elle se compose de 3 parties :

- SVbD9~HM5nzf3AX4yFCBc-A4dhNUF5DPJZLL5NX5Brs : le hash SHA256 du fichier, qui permet de l'identifier.

- ***bA7qLNJR7IXRKn6uS5PAySjIM6azPFvK~18kSi6bbNQ : la clé de déchiffrement.***
- ***AAEA--8 : méta-données contenant, entre autres, l'algorithme de chiffrement utilisé.***

[modifier] Les KSK

Keyword-Signed Keys

Elles ressemblent à cela :

KSK@monfichier.txt

Ces clés sont similaires aux clés CHK, mais leur nom est libre et donc spammable. Une KSK peut rediriger vers une CHK ou contenir directement le fichier. Elles sont peu utilisées.

[modifier] Les SSK

Signed-Subspace Key

Ces clés peuvent être vues comme des trousseaux de clés qu'il est possible de mettre à jour. Les Freesites reposent sur une clé SSK qui contient les clés CHK des fichiers composant le site.

Ces clés utilisent un chiffrement asymétrique. On a donc une clé privée (insert URI) qui permet d'insérer une nouvelle version de la clé dans Freenet et une clé publique (request URI) qui permet aux visiteurs de récupérer la clé.

Voici à quoi elles ressemblent :

SSK@GB3wuHmtxN2wLc7g4y1ZVydkK6sOT-DuOsUo-eHK35w,c63EzO7uBEN0piUbHPkMcJYW7i7cOvG42CM3YDduXDs,AQABAAE/testinserts-3/

Elle se compose de 5 parties :

- ***GB3wuHmtxN2wLc7g4y1ZVydkK6sOT-DuOsUo-eHK35w : le hash de la clé publique. C'est la seule partie qui est stockée par le nœud.***

- ***c63EzO7uBEN0piUbHPkMcJYW7i7cOvG42CM3YDduXDs : la clé de déchiffrement.***
- ***AQABAAE : méta-données contenant, entre autres, l'algorithme de chiffrement utilisé.***
- ***testinserts : le chemin choisi par le créateur du site.***
- ***3 : le numéro de version du site.***

[modifier] Les USK

Updateable Subspace Key

Il ne s'agit pas vraiment d'un type de clé mais plutôt d'une aide à l'utilisation des SSK. Prenons la clé SSK donnée ci-dessus et transformons-la en USK :

USK@GB3wuHmtxN2wLc7g4y1ZVydkK6sOT-DuOsUo-eHK35w,c63EzO7uBEN0piUbHPkMcJYW7i7cOvG42CM3YDduXDs,AQABAAE/testinserts/3/

Avec cette clé, votre nœud vous renverra la même chose qu'avec la SSK, mais si une nouvelle version a été insérée, c'est elle que vous recevrez, automatiquement.

Toutes les opérations de découpage, chiffrement, déchiffrement et vérification de signature sont gérées automatiquement par votre nœud Freenet. Il vous suffit de lui donner la clé et il se chargera de vous trouver le fichier ou le site.

[modifier] Le datastore

Chaque nœud met à disposition du réseau une partie de son disque dur, appelée datastore, afin de stocker des clés. Le datastore est découpé en deux parties de taille égale :

- ***Le cache : il stocke à peu près toutes les clés qu'il voit passer.***

- *Le store : il stocke les clés qui sont les plus proches de lui (le principe des positions est détaillé plus bas).*

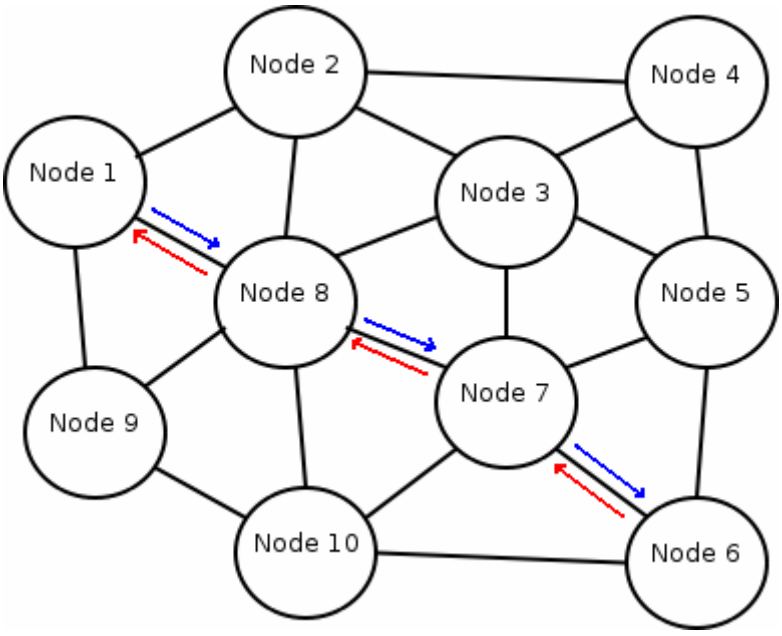
Quand le datastore est plein, il commence à supprimer les clés qui n'ont pas été accédées depuis longtemps.

[modifier] Fonctionnement du réseau

[modifier] Principe général

Chaque ordinateur faisant partie du réseau est appelé un "nœud" (ou "node" en anglais). Il partage une partie de son disque dur pour stocker les informations du réseau et il est connecté à un nombre limité d'autres nœuds. La théorie mathématique du "Small World" nous dit qu'il est possible de contacter n'importe quel nœud du réseau en passant par plusieurs nœuds intermédiaires. Bien évidemment, les communications entre les noeuds sont chiffrées.

Prenons un exemple :



Quand un nœud veut une information, il la demande à ses voisins immédiats. Si l'un d'eux a l'information, il la lui donne, sinon, il demande à ses propres voisins, etc. Dans l'exemple ci-dessus, si le nœud 1 veut une information détenue par le nœud 6 voici ce

qui va se passer (ce n'est qu'un exemple, le nombre de chemins possibles est infini) :

- *Chemin de la requête (en bleu) : 1 - 8 - 7 - 6*
- *Chemin de l'information (en rouge) : 6 - 7 - 8 - 1*

> *Chaque nœud dans la chaine sait seulement qui lui a demandé une information et à qui il l'a demandée lui même. Le nœud 8 sait seulement que 1 lui a demandé une information et qu'il l'a obtenue de 7. Il ne sait pas si 1 voulait cette info pour lui ou s'il ne faisait que relayer une demande d'un autre. Il ne sait pas si 7 avait l'info ou s'il l'a obtenue d'un autre.*

[modifier] Principe des positions

Les clés et les nœuds sont placés sur un cercle imaginaire qui va de 0 à 1. Cette position n'a rien à voir avec la position physique des ordinateurs :

- *La position des clés est déterminée en fonction de leur hash.*
- *La position des nœuds est déterminée aléatoirement au moment de leur création.*

Un algorithme de permutation de position (location swapping) permet aux nœuds d'échanger leurs positions pour se rapprocher de leurs peers. Les nœuds ont ainsi tendance à se rapprocher en fonction de leurs "affinités" pour un certain type de clés. Les nœuds consacrant la moitié de leur datastore aux clés dont ils sont "proches", cela aide considérablement la recherche d'informations : quand un nœud veut une clé, il va la demander à celui de ses peers qui est le plus proche de la position de la clé, et ainsi de suite.

[modifier] Les connexions

Tous les nœuds qui font tourner Freenet forment un seul réseau. Mais ils peuvent être connectés les uns aux autres de deux manières différentes. Chaque nœud peut utiliser les deux types de connexions simultanément, ou un seul selon les choix de son propriétaire.

[modifier] Connexions Darknet

C'est le mode de fonctionnement par défaut de Freenet, le plus sécurisé. Ces connexions sont faites entre des personnes qui se connaissent et se font confiance. Elles sont fixes et seul le propriétaire du nœud peut décider d'en ajouter ou d'en supprimer.

Un nœud qui n'a que des connexions Darknet est virtuellement indétectable puisqu'il n'acceptera aucune connexions venant de personnes qui ne sont pas ses amis. Une organisation ou un gouvernement qui voudrait localiser tous les nœuds Freenet ne pourrait pas le trouver.

Ces connexions répondent à la Théorie du Small-World qui est derrière le fonctionnement de Freenet. Elles aident considérablement le routage des informations au sein du réseau, à condition qu'elles soient vraiment faites entre des personnes qui se connaissent. Se connecter Darknet à une personne qu'on ne connait pas n'a aucun intérêt !

[modifier] Connexions Opennet

Ces connexions sont établies de façon automatique par les nœuds qui ont activé l'Opennet. Elles permettent aux gens qui ne connaissent personne dans le réseau (ou seulement 2-3 personnes) de s'y connecter quand-même.

Ce sont des connexions dynamiques qui évoluent dans le temps : votre noeud va automatiquement fermer les connexions les moins performantes pour en établir de nouvelles (20 au maximum).

Les noeuds qui utilisent l'Opennet bénéficient du même anonymat que les autres mais ils sont

détectables. Cela signifie qu'il est assez facile de savoir qu'ils font tourner Freenet, mais très difficile de savoir ce qu'ils font à l'intérieur du réseau.

[modifier] Mode mixte

Il est parfaitement possible (et raisonnable) d'utiliser les deux types de connexion en même temps.

Par exemple :

Une personne décide de se connecter à Freenet mais elle ne connait personne dans le réseau. Elle active donc l'Opennet et obtient automatiquement 20 connexions à des personnes qu'elle ne connait pas.

Elle explore le réseau et découvre que c'est le meilleur du monde. ;-) Elle en parle donc à son meilleur ami, qui installe Freenet à son tour. Cet ami active également l'Opennet et obtiens 20 connexions.

Les deux amis peuvent alors établir une connexions Darknet entre leurs deux nœuds. Ils auront donc chacun 1 connexion Darknet et 19 connexions Opennet. Au fil du temps, si d'autres personnes de leur connaissance découvrent Freenet, ils pourront se connecter en Darknet avec eux également.

Dès qu'une personne a une dizaine de connexions Darknet, elle peut se permettre de désactiver l'Opennet pour bénéficier d'un peu plus de sécurité...

[modifier] Comment Freenet atteint ses objectifs ?

[modifier] Anonymat

Le fonctionnement du réseau décrit plus haut fait qu'il est impossible de savoir qui demande une information et qui la met à disposition. Le plus gros des données chiffrées qui transitent par votre nœud ne vous appartiennent pas et sont à destination d'autres personnes.

Les données sont stockées en version chiffrées sur le disque dur. Or, la clé permettant de les déchiffrer se trouve dans le texte de la clé et non pas sur votre disque dur. On ne peut pas vous accuser de stocker une donnée interdite puisque vous ne pouvez pas savoir ce que contient votre datastore. Ce principe est appelé "Déni plausible".

[modifier] Résistance à la censure

Le seul moyen de censurer une information consisterait à éteindre tous les nœuds qui contiennent cette information.

Pour pouvoir faire ça, il faut commencer par trouver ces nœuds. La méthode pour le faire consisterait à faire une requête pour cette clé et à analyser soigneusement le trafic de tous les nœuds. Cela demanderait des moyens considérables : seuls des gouvernements ou de très puissantes organisations sont capables de faire cela.

Là où ça devient amusant, c'est qu'à chaque fois que vous demandez une information dans Freenet, un des nœuds sur le trajet peut décider d'en conserver une copie dans son cache. Le résultat, c'est que l'information que vous vouliez censurer se multiplie.

[modifier] Résistance aux attaques

[modifier] Harvesting

Comme il n'y a pas de serveurs centraux qu'on pourrait facilement éteindre, il faut s'attaquer à l'ensemble du réseau. Pour cela, il faut localiser la totalité des nœuds du réseau avant de pouvoir les bloquer. Ce genre d'attaque est également réservé aux gouvernements et aux organisations les plus puissantes. La technique consiste à faire tourner une version modifiée du nœud dont le but est de récupérer un maximum d'adresses IP. Tous les logiciels de peer2peer, cryptés ou non, sont vulnérables à cette attaque, puisque ce sont des Opennet.

La réponse du projet Freenet à cette attaque, c'est le Darknet : quand on ne peut pas savoir si une machine fait tourner Freenet ou non, il est difficile de justifier une perquisition ou la coupure de son accès internet...

[modifier] Location swapping

Une autre attaque consiste à s'en prendre à l'algorithme d'échange de positions. En se faisant passer pour une multitude de nœuds et en demandant à échanger sa place avec les nœuds d'une zone précise, on peut créer un "trou" et espérer faire disparaitre les clés de cette zone. Le réseau a subi cette attaque au début de l'année 2007 mais elle a échoué à cause du cache qui faisait que ces données étaient également stockées à d'autres endroits du réseau. Les performances ont baissé mais le réseau n'est pas tombé.

En réponse à cette attaque, un mécanisme a été mis en place : toutes les 2000 permutations, un nœud peut créer une nouvelle position aléatoire. Cela permet d'uniformiser la répartition des nœuds sur l'ensemble du cercle.

[modifier] Attaques légales

Ces menaces sont peu probables dans les démocraties occidentales mais le projet se doit de proposer des solutions aux personnes qui en ont le plus besoin : celles qui vivent dans des dictatures où l'information est strictement contrôlée.

Un gouvernement ou un FAI qui déciderait d'interdire purement et simplement Freenet aurait plusieurs armes à sa disposition :

- *Blocage de ports : chaque nœud utilise un numéro de port différent pour ses communications. Bloquer tous les ports reviendrait à bloquer tout accès à internet.*
- *Blocage de protocole : le traffic crypté d'un nœud Freenet ne contient aucune donnée*

reconnaissable. Il est impossible de le différencier de n'importe quelle autre communication cryptée. Une faille de Freenet 0.5 avait permis à la Chine de le bloquer de cette manière.

- *Interdiction du cryptage : le cryptage est utilisé partout dans le commerce en ligne. Aucun gouvernement ne voudrait faire ça.*
- *Pénaliser l'utilisation de Freenet : dans ce cas, seul le réseau Darknet pourra subsister. Le seul moyen de prouver que vous utilisez Freenet consistera à perquisitionner votre ordinateur. Et il faut un motif valable pour pouvoir le faire.*

De plus, le système a été conçu pour accepter des "Transport Plugins" qui permettront de camoufler le trafic de Freenet dans d'autres protocoles (images, streaming vidéo, webradios, etc.). Les possibilités sont illimitées. Ces mesures ne sont pas encore en place mais peuvent être déployées rapidement.

[modifier] Identification d'un utilisateur

Ces attaques ont besoin de beaucoup de requêtes pour pouvoir fonctionner. Elles peuvent porter sur :

- *Un grand fichier (splitfile). Pour info, récupérer un fichier de 4Go génère 270 000 requêtes !*
- *Une identité FMS (tous les messages sont insérés dans la même SSK).*

Ces attaques sont théoriquement impossibles contre un pur-darknet. Mais elles sont réalisables contre un nœud opennet, mixte ou faux-darknet (un nœud darknet qui se connecte à des gens qu'il ne connait pas vraiment).

Des solutions sont à l'étude pour compliquer la tâche de l'attaquant sur l'opennet.

[modifier] Attaque par corrélation

La technique consiste à analyser les requêtes d'un nœud auquel on est connecté directement pour essayer

de savoir si les requêtes viennent de lui ou s'il ne fait que transmettre celles d'un autre. Pour un fichier de 4Go, il faut 270 000 requêtes. Si une personne à qui on est connecté directement nous demande 13 500 morceaux (les nœuds ayant l'opennet ont 20 connexions), il y a de bonnes chances que la requête vienne de lui.

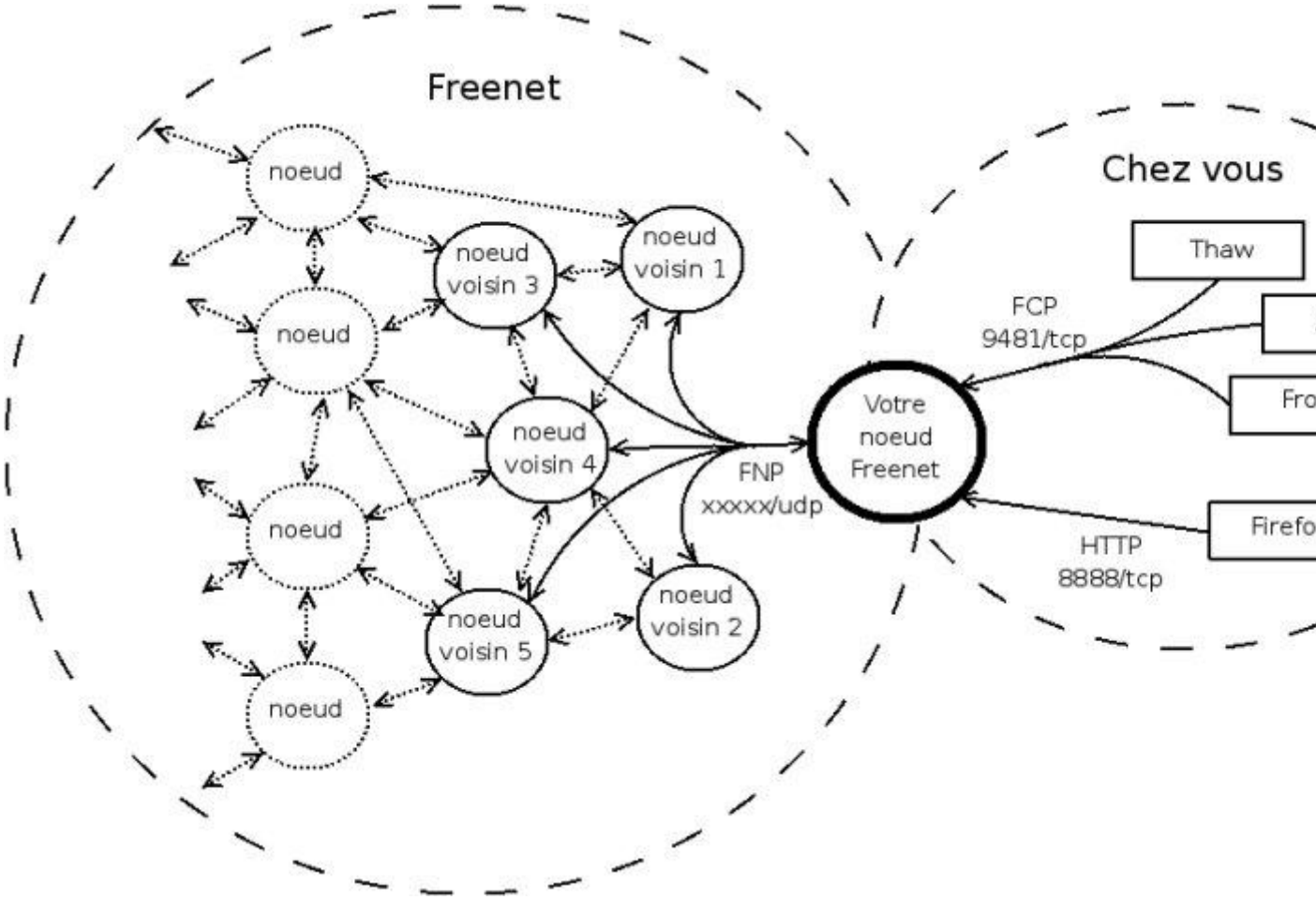
[modifier] Attaque adaptative

Cela consiste à se faire une idée grossière de l'origine d'une requête (une position approximative sur le cercle) et à s'en approcher petit à petit en établissant de nouvelles connexions. Si l'attaquant arrive à se connecter au nœud à l'origine de la requête, il peut lancer une attaque par corrélation comme indiqué plus haut.

[modifier] Autres attaques

Comme tous les autres logiciels réseau, Freenet peut contenir des failles qui ne sont pas encore découvertes. Le fait que ce soit un logiciel libre garantit simplement qu'elles seront corrigées rapidement une fois découvertes.

[modifier] Flux réseaux et ports utilisés



Note : Le port FNP est différent pour chaque noeud Freenet (choisi aléatoirement à l'installation) afin d'éviter qu'il soit possible de bloquer le réseau simplement en bloquant un port.

[modifier] Pour aller plus loin

Si vous voulez aller plus loin, lisez :

- ***Distributed routing in Small World Networks, une description du routage dans le Darknet, par Oskar Sandberg.***
- ***Searching in a Small World, la thèse de License d'Oskar Sandberg.***
- ***La vidéo de présentation de Freenet 0.7 faite par Ian Clarke et Oskar Sandberg au Chaos Computer Congress de Berlin, en Décembre 2005.***

Applications pratiques

Un article de Freenet Doc.

Aller à : Navigation, Rechercher

Cet article est actuellement en réaménagement. Les informations sont valides, mais la forme de l'article ne correspond pas aux critères de la documentation (en savoir plus sur la validation des articles)

La première chose que vous devez savoir c'est que Freenet est un réseau indépendant d'Internet. Si vous cherchez un moyen de surfer sur le web conventionnel de façon anonyme, c'est TOR que vous cherchez.

L'objectif final de Freenet est de permettre de faire toutes les choses que vous faites aujourd'hui sur internet (chat, streaming, etc...), de façon anonyme. Mais la route est longue jusqu'à la version 1.0 ! Cette page vous présente ce qu'il est possible de faire avec la version actuelle de Freenet : la 0.7.

Sommaire

[masquer]

[modifier] Consulter des sites FreeNet, Les Freesites

Ce sont des sites qui ressemblent aux sites Web mais qui ne sont accessibles qu'à l'intérieur de Freenet. Ils se composent de pages HTML et d'images mais ils sont statiques. Le Javascript ou le PHP sont

proscrits pour des raisons de sécurité (un auteur de site malicieux pourrait s'en servir pour compromettre votre anonymat). Quand un auteur veut modifier son Freesite, il doit insérer une nouvelle édition du site au complet.

Les Freesites sont référencés dans des index. Des sortes d'annuaires qui listent les Freesites existants, avec une courte description. Un outil de recherche par mots-clés (comme Google) est en cours de développement mais il n'est pas encore tout à fait au point.

On est donc encore loin du Web 2.0 mais cela suffit déjà largement pour mettre des informations à disposition ou faire un blog par exemple.

Des logiciels annexes (jSite, Echo, Thingamablog), livrés avec Freenet, vous permettent de créer votre propre Freesite et de l'insérer dans le réseau.

Il est possible de rechercher des Freesites sur le réseau à l'aide du plugin XMLLibrarian (il y a un champ de recherche sur la page d'accueil de FProxy ou bien il suffit de "visiter" le plugin).

[modifier] Discuter

Il existe des groupes de discussion à l'intérieur de Freenet. Si vous connaissez les newsgroups, vous ne serez pas dépaysé du tout. Il s'agit de messages textuels, sans mise en forme, groupés par conversations. Il existe des groupes pour différents sujets de conversation, dont plusieurs francophones.

L'accès à ces groupes se fait au moyen de logiciels spécifiques (Thaw, Frost, FMS), également livrés avec Freenet. Les temps de latence sont assez longs : il faut entre 10 minutes et une heure pour que tout le monde reçoive un nouveau message.

[modifier] Envoyer des emails

Freenet propose un service d'email crypté et sécurisé (Freemail). Freemail permet d'écrire, de façon

discrète, à d'autres utilisateurs de Freenet. Pour l'utiliser, vous devrez configurer votre client de messagerie habituel (Thunderbird, Outlook, etc...) pour qu'il utilise votre noeud Freenet comme serveur de messagerie.

[modifier] Echanger des fichiers

Freenet permet l'insertion et le téléchargement de fichiers à l'intérieur du réseau. Un logiciel spécifique (Thaw) permet de réaliser des indexes (listes de fichiers) et de consulter les indexes créés par d'autres utilisateurs.

Il existe quelques logiciels (Freemule, Frost) qui tentent de fournir une interface de recherche semblable à celle des logiciels de peer2peer comme eMule. Leurs défauts de conception, ajoutés à la lenteur intrinsèque de Freenet font qu'ils sont peu utilisés.

Rappelez-vous que Freenet a pour objectif principal la liberté d'expression. Il n'a jamais été conçu pour échanger de très gros fichiers rapidement. C'est possible, mais c'est lent.

[modifier] Bilan

FreeNet est donc assimilable à une version plus restreinte du web (moins rapide, moins dynamique et avec moins de contenu) mais beaucoup plus sûre pour l'utilisateur et l'auteur.

Les Freesites

Un article de Freenet Doc.

Aller à : Navigation, Rechercher
Sommaire

[masquer]

- 4 Insérer un Freesite

[modifier] Trouver un Freesite

- Trouver un Freesite avec les Index
- Trouver un Freesite avec le champ de recherche de FProxy
- Trouver un Freesite avec XMLLibrarian

[modifier] Consulter un Freesite

- Consulter un Freesite

[modifier] Créer un Freesite

- Avec Thingamablog
- Avec un éditeur html ou un IDE

[modifier] Insérer un Freesite

- Insérer un Freesite avec jSite

> Vous trouvez que la navigation sur les Freesites est lente ? Suivez le conseil de tonton batosai : Cliquez sur le lien "Activelink index" présent sur votre page d'accueil, et laissez charger. Allez faire un tour en forêt, allez dormir, revenez le lendemain. Avec les clés de tous les Freesites listés mises en cache dans votre noeud, vous découvrirez un monde nouveau ;)

Echange de fichiers

Un article de Freenet Doc.

Aller à : Navigation, Rechercher

Freenet est capable de stocker des fichiers et vous permet de les récupérer (ou d'en ajouter) en tout anonymat.

La récupération d'un fichier se nomme "Téléchargement", comme sur l'internet normal.

Par contre, pour mettre un fichier à disposition sur Freenet, le principe est différent et on utilise le terme "insérer". Cela consiste à donner le fichier à votre noeud qui se chargera de le découper en petits morceaux, de créer des blocs supplémentaires afin de pouvoir reconstituer le fichier s'il manquait des morceaux, et enfin, d'envoyer ces fragments aux autres noeuds du réseau. Ce processus est assez lent (environ 6Ko/s) mais sachez qu'une fois votre fichier inséré, il sera disponible même si votre noeud est éteint : il fera partie du réseau et tant que des gens le téléchargeront, rien ne pourra le faire disparaître.

Pour l'instant, seul Freemulet est capable de faire de l'insertion à la demande (signaler que vous partagez un fichier et ne l'insérer que si quelqu'un le demande). L'utilisation de Freemulet n'est pas recommandée car il utilise un format de fichier spécial qui fait que ses fichiers ne sont pas récupérables par les autres logiciels. Thaw devrait proposer l'insertion à la demande dans une prochaine version.

[modifier] Trouver un fichier

- ***Dans un Freesite***
- ***Demander sur Thaw/Frost***
- ***Avec Frost***
- ***Avec Freemule***
- ***Avec Thaw** (Thaw n'est plus maintenu et peut contenir des bugs)*

[modifier] Télécharger un fichier

- ***Télécharger avec Frost***
- ***Télécharger avec Freemule***
- ***Télécharger avec fProxy***
- ***Télécharger avec Thaw** (Thaw n'est plus maintenu et peut contenir des bugs)*

[modifier] Insérer un fichier

- *Insérer avec Frost*
- *Insérer avec Freemule*
- *Insérer avec fProxy*
- *Insérer avec Thaw (Thaw n'est plus maintenu et peut contenir des bugs)*

élécharger Freenet

Remarque importante pour les nouveaux utilisateurs

Afin d'obtenir les meilleures performances possibles, Freenet tourne en permanence. Cela ne devrait pas avoir d'incidence sur les performances de votre ordinateur, puisque cela nécéssite environ 200Mo de mémoire vive (RAM) et 10% de la puissance d'un processeur monocoeur, ainsi que quelques accès au disque. Nous vous recommandons fortement d'éteindre Freenet lorsque vous jouez à des jeux, etc... Sur Windows, vous pouvez couper Freenet via l'icone situé dans la zone de notification ; pour les autres systèmes, des liens sont fournis soit sur le bureau, soit dans le menu.

Normalement, Freenet devrait se connecter automatiquement et fonctionner tout seul, en se connectant de façon automatique aux autres nœuds (Inconnus). Cependant, si vous connaissez plusieurs personnes qui utilisent déjà Freenet, vous pouvez activer le mode "haute sécurité" et les ajouter en tant qu'amis ; Freenet ne se connectera alors qu'à eux, et le fait que vous utilisez Freenet sera quasiment indétectable. Vous pourrez bien sûr toujours accéder au reste du réseau via les amis des

amis etc... de vos amis. Néanmoins, les performances seront dégradées tant que vous n'ajouterez pas plus de 10 amis qui sont souvent en ligne en même temps que vous.

Instructions pour l'installation

Afficher les instructions pour : Windows,
Mac OSX,
Linux et autres Unix.

Windows

Téléchargez et éxécutez le programme d'installation (8MB)

Celui-ci installera automatiquement Freenet ainsi que les autres composants requis pour vous. Une fois l'installation achevée, votre navigateur internet s'ouvrira automatiquement et affichera l'interface utilisateur de Freenet.
Remarque : Freenet ne contient AUCUN logiciel espion ; c'est un Logiciel Libre ! Le code source est librement consultable en ligne.

Freenet fonctionne mieux avec Windows XP Professionel ou Vista. Quelques problèmes ont été rapportés avec le programme d'installation sur Windows 7, ils seront corrigés bientôt. Freenet ne s'exécutera pas sur les systèmes plus vieux que Windows 2000 Professionel (càd Windows 95/98/ME), et en aucun cas vous ne devriez utiliser un système d'exploitation dont le support a été arrêté.

Pares-feu et routeurs

Freenet devrait fonctionner normalement avec la majorité des routeurs, mais si vous rencontrez des problèmes et que vous avec un pare-feu ou un routeur, cliquez ici pour plus d'infos.

Bien, ça tourne, qu'est-ce que je fais ?

Quand le programme d'installation se ferme, il devrait ouvrir un navigateur internet affichant

l'assistant de configuration. Vous pouvez alors configurer les paramètres de base, et ensuite commencer à utiliser Freenet. Après cela, vous pourrez accéder à Freenet via le menu de la zone de notification (en bas à droite de l'écran), ou utiliser le raccourci "Browse Freenet" situé sur le bureau ou dans le menu démarrer. Si rien de tout cela ne fonctionne, ouvrez l'adresse http://127.0.0.1:8888/ dans votre navigateur.

Pour une meilleure sécurité, nous vous conseillons d'utiliser Freenet dans un navigateur différent de celui que vous utilisez habituellement, de préférence en mode de navigation privée.
Sur Windows, le menu de la zone de notification essaiera si possible d'ouvrir Google Chrome en mode incognito. Internet Explorer fonctionne mal avec Freenet, Firefox et Opera peuvent par contre être utilisés sans problème.

Si vous connaissez quelqu'un qui utilise Freenet, vous pouvez améliorer votre sécurité et aider à construire un réseau robuste en vous connectant à son nœud. Premièrement, ouvrez la page Ajouter un ami.
Vous et votre ami devez télécharger votre "référence". Envoyez alors le fichier à votre ami, et récupérez sa référence. Ajoutez sa référence en utilisant le formulaire en bas de la page "ajouter un ami". Votre ami doit procéder de la même façon avec votre référence.
Une fois que chacun a ajouté la référence de l'autre, le nœud de votre ami devrait être affiché sur la page de connexion aux amis, probablement en tant que "CONNECTÉ" ou "BUSY".
Vous pouvez donner un nom à votre nœud sur la page de configuration ; il sera ainsi plus facile de savoir à qui il appartient (seul vos amis pourront le voir).
N'ajoutez que des nœuds qui appartiennent à des personnes que vous connaissez vraiment (dans la vie réelle ou sur internet). Ajouter des inconnus fait chuter les performances et n'améliore pas votre sécuritéé (ils peuvent très bien être les méchants !).

Bien, je suis connecté, qu'est-ce que je fais ?

Freenet inclus des sites web anonymes ("freesites"), le partage de fichier, la recherche, et plus, mais vous pouvez utiliser des applications tierces (lien en anglais) pour discuter sur des forums, partager des fichiers, insérer votre freesite dans le réseau, etc...

Ça ne marche pas, alors ?

Si vous rencontrez des problèmes lors de l'installation ou de l'exécution de Freenet, merci de nous contacter (en anglais si vous pouvez, sinon en français, mais l'attente et la qualité des réponses ne seront peut-être pas les mêmes) sur la liste de support (inscription ici), ou de nous joindre sur IRC sur les canaux #freenet (anglophone) ou #freenet-fr (francophone) sur le serveur irc.freeode.net. (Essayez ici pour le canal anglophone, là pour le canal francophone).

Matériel requis

Un processeur tournant à 1GHz et 1Go de mémoire vive (RAM) devraient suffire. Freenet s'exécutera sur des systèmes moins performants, mais il utilisera au moins 128Mo de RAM, donc à moins que le système ne fasse rien d'autre, il fonctionnera mal si la quantité de RAM totale est de moins de 512Mo. En revanche, le processeur pose moins de problèmes, et certaines personnes ont fait tourner Freenet sur des Pentium 2, ou des ATOM cadencés à 400MHz ; néanmoins, les téléchargements et la navigation seront ralentis.

Freenet utilisera aussi une partie de votre disque pour y stocker des données. Vous pouvez configurer la taille utilisée, qui doit être supérieure à 100Mo. Nous recommandons d'allouer au moins 1Go.Freenet utilisera aussi de l'espace disque pour vos téléchargements.
L'empreinte mémoire de Freenet est d'approximativement 192Mo, plus 1Mo pour chaque 2Go

d'espace disque configuré (par défaut, Freenet utilisera donc environ 192Mo de mémoire vive).

Enfin, sur les systèmes Windows 64 bits, nous installons une machine virtuelle Java (JVM) 32 bits, à cause des limitations du Java Service Wrapper (lien anglais). Elle ne sera pas forcément mise à jour automatiquement, donc vous devrez peut-être la mettre à jour occasionnellement.

Mise à jour

Le nœud est maintenant fournit avec un mécanisme de mise-à-jour via le réseau Freenet : le nœud se tiendra automatiquement à jour à partir des autres nœuds Freenet, et cela fonctionnera même s'ils sont trop récents pour que nous nous connections à eux. C'est anonyme et sûr, et nous le recommandons aux utilisateurs. Néanmoins, si quelque chose ne fonctionne pas, vous pouvez toujours mettre à jour votre nœud depuis nos serveurs :

- *Les utilisateurs de Windows peuvent se mettre à jour vers la dernière version stable de Freenet depuis le menu de la zone de notification, ou en exécutant le fichier "update.cmd" (cliquez simplement dessus) du répertoire Freenet.*
- *Les utilisateurs de Mac et de Linux peuvent mettre à jour via le script update.sh du répertoire Freenet.*

Code source: Voir la page des développeurs pour obtenir un accès git, ou téléchargez la dernière archive stable ici.

rtagez, Discutez, Naviguez. Anonymement. Sur Freenet.

Freenet est un logiciel libre qui vous permet de partager des fichiers, de naviguer sur des freesites (sites web accessibles uniquement via Freenet) et d'en publier, ainsi que de discuter sur des forums, le tout anonymement, et sans crainte de censure. Freenet est décentralisé (il n'y a pas de serveur central) et donc moins vulnérable aux attaques ; s'il

est utilisé en mode "darknet", où vous vous connectez uniquement à vos amis, il est très difficile à détecter.
En savoir plus !

u'est-ce que Freenet ?

> *"I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?'"*
> *--Mike Godwin, Electronic Frontier Foundation*

Freenet est un logiciel libre qui vous permet de partager des fichiers, naviguer dans et publier des "freesites" (sites web accessibles uniquement à travers Freenet), discuter sur des forums, le tout de façon anonyme et sans craindre la censure. Freenet est décentralisé pour le rendre moins vulnérable aux attaques, et s'il est utilisé en mode "darknet", où les utilisateurs se connectent uniquement à leurs amis, il est très difficile à détecter.

Les communications des nœuds Freenet sont chiffrées et routées à travers d'autres nœuds de façon à rendre extrêmement difficile de déterminer qui demande l'information, son contenu, et qui la fournit.

Les utilisateurs contribuent au réseau en donnant de la bande passante et une partie de leur disque dur (appelée "datastore") pour y stocker des fichiers (ou des morceaux de fichiers) du réseau. Lorsque l'on demande un fichier disponible sur Freenet, on le reconstruit à partir des datastore des autres utilisateurs du réseau.
Les fichiers sont gardés ou détruits de façon automatique suivant qu'ils sont populaires ou non. Le moins populaire est détruit pour laisser la place aux nouveaux fichiers ou aux contenus plus populaires.
Les fichiers sont chiffrés, et les utilisateurs ne peuvent donc pas découvrir facilement quel est le

contenu de son datastore, et devrait ne pas pouvoir en être tenu responsable.
Les forums de discussion, les sites, et la fonction de recherche, sont tous construits à partir de ce datastore distribué.

Freenet a été téléchargé plus de 2 millions de fois depuis que le projet a débuté, et a été utilisé pour la diffusion partout dans le monde d'informations censurées, y compris dans les pays comme la Chine et le Moyen Orient. Les idées et concepts précurseurs de Freenet ont eu un impact significatif dans le milieu académique. Notre papier de 2000 intitutléé "Freenet: A Distributed Anonymous Information Storage and Retrieval System" (Freenet : un système de stockage et de récupération d'information anonyme et distribué) a été le papier de science informatique le plus cité de 2000 d'après Citeseer, et Freenet a aussi inspiré des papiers dans les mondes de la loi et de la philosophie.
Ian Clarke, le créateur de Freenet et le coordinateur du projet, a été sélectionné comme l'un des 100 plus grands innovateurs de 2003 par le magazine "MIT's Technology Review".

Le "darknet" est un développement récent, que peu d'autres réseaux possèdent : En se connectant uniquement aux personnes à qui ils font confiance, les utilisateurs peuvent grandement améliorer leur sécurité, et ils peuvent toujours se connecter au réseau principal à travers les amis des amis etc... de leurs amis. Ceci permet à certaines personnes d'utiliser Freenet dans des endroits où Freenet pourrait être illégal, rend Freenet très difficile à bloquer par les gouvernements, et ne se base pas sur le fait d'accéder au "monde libre" via un portail sécurisé.

projet Odebian

Anonymat et respect de la vie privée sur Internet

Présentation

En réaction aux lois qui visent à restreindre nos libertés de communication et notre droit au respect de la vie privée sur internet, la ligue Odebi lance le projet Odebian. L'objectif est de fournir un OS 'live' cumulant les avantages de debian (liberté, sécurité, fiabilité, communauté) et les valeurs défendues par la Ligue Odebi.

Il s'agit clairement une réponse Anti Loppsi. anonymat, cryptage, etc etc ... de plus étant un OS sur clé USB (ou live-cd) il ne devra laisser aucune trace sur le disque dur du pc que vous aurez utilisé, à chaque boot l'OS redeviendra 'vierge'.

Ce projet devra fournir un système accessible à tous nos concitoyens, madame michu compris. Le genre de truc à avoir dans sa poche afin de pouvoir utiliser de manière sécurisée n'importe quel pc, ou que l'on soit sur la planète. Ce qui impliquera de notre part un travail de tests et d'integration pour fournir un outils simple d'utilisation.

tout le monde est invité à participer à ce projet selon ses compétences. ne serait-ce que pour le tester, et tous les commentaires, réactions, critiques, coups de main seront les bienvenus.

] retour [

Restrictions

- ***Cet outil est encore en cours de preparation.***
- ***L'accès au réseau est vérouillé pour ne laisser sortir les communications que à travers Tor.***
- ***Seule la navigation internet est actuellement accessible.***
- ***Un serveur DHCP doit être disponible sur votre réseau (généralement dans votre box internet)***

] retour [

Licence

site en travaux ...

] retour [

Téléchargements

Images pour clé USB

- ***odebian-amd64-usb.img***
  - ***taille : 547 Mo***
  - ***date : 14/02/2010 - 19:33***
  - ***MD5 : 688b7b6671006cf8a35a3d72041b5da8 odebian-amd64-usb.img***
- ***odebian-i386-usb.img***
  - ***taille : 570 Mo***
  - ***date : 13/02/2010 - 09:49***
  - ***MD5 : 613d17c74a48fa5bc6736688eff54e4b odebian-i386-usb.img***

Images pour cd-rhum

- ***odebian-amd64-cd.iso***
  - ***taille : 536 Mo***
  - ***date : 14/02/2010 - 22:54***
  - ***MD5 : c96abe37f782a7e347419e1ecfee0d12 odebian-amd64-cd.iso***
- ***odebian-i386-cd.iso***
  - ***taille : 558 Mo***
  - ***date : 14/02/2010 - 21:06***
  - ***MD5 : 67a6f89bd424f7185305769d8bcbaf7a odebian-i386-cd.iso***

] retour [

Contact

En attendant mieux, vous pouvez nous contacter sur le site, le forum ou le salon jabber de la Ligue Odebi.

] retour [

Site et projet gérés par la Ligue Odebi

Pour la défense des droits fondamentaux dans la société de l'inform

De plus en plus d'outils pour filtrer son internet

Confidentielles il y a encore peu de temps, de plus en plus de solutions se développent pour offrir aux internautes un accès crypté pour contourner les lois Hadopi ou Loppsi.

Les Suédois de Pirate Bay ont récemment lancé leur propre VPN, iPredator (Sipa)

Depuis le vote de la loi Hadopi et avec l'arrivée de Loppsi, des internautes s'organisent pour sécuriser leur accès internet et le rendre le plus anonyme possible.
En ce sens, la Ligue Odebi propose gratuitement, depuis lundi 15 février, le système Odebian qui, avec une simple clé USB configurée, permet d'accéder à un internet anonyme, crypté et sécurisé.

Aurélien Boch, membre de l'équipe dirigeante de la Ligue, explique à Nouvelobs.com que l'objectif est de proposer "un système pour que les internautes restent anonymes, pour le respect de la vie privée". Une réponse à la Loppsi qui souhaite instaurer un filtrage critiqué des sites pédopornographiques.

"La connexion devient anonyme [mais] nettement ralentie"

Le représentant de la Ligue Odebi se défend d'un système fait pour télécharger illégalement sans risques. "Odebian n'est pas un outil de téléchargement, il ne s'inscrit pas dans cette démarche", lance-t-il. "Après, ce que font les gens avec leur ordinateur, cela ne nous regarde pas."
Et d'ajouter : "Ce système utilise un Tor, une technique lente et pas du tout adaptée au téléchargement". Pour les non-initiés, Aurélien Boch s'explique : "Avant d'accéder à un site, la connexion internet passe par différents serveurs avant d'arriver sur le site demandé", offrant ainsi un accès entièrement anonyme. Reste que "si la connexion devient anonyme, elle est nettement ralentie".
Des systèmes similaires sont déjà en place dans les pays où une importante censure s'opère sur Internet, en Iran, en Chine ou en Corée du Nord, par exemple.

Deux alternatives : VPN et proxys

Pour un internet "libre et sécurisé", d'autres techniques sont également à la disposition des internautes.
Avec les VPN (réseaux privés virtuels), les internautes peuvent accéder "en 5 clics, à une liaison sécurisée et cryptée via un serveur hébergé à l'étranger (bien souvent en Suède ou aux Pays-Bas)", note Aurélien Boch. Reste que ces VPN sont bien souvent payants, autour de 10 à 15 euros par mois.
Il y a également la technique des proxys. "Plus rapide que le Tor, la liaison passe par un serveur", détaille le représentant de la Ligue Odebi. Une

technique gratuite "très utilisée en Iran", mais "difficile à mettre en place" et qui n'est pas toujours bien compatible.
Si le gouvernement a déjà fait part de la possibilité de voir interdire les outils de contournement des filtrages, la Ligue Odebi juge cette possibilité invraisemblable. "Interdire des systèmes basés sur Linux, donc des logiciels open-source, serait un grand pas en arrière pour les libertés et les droits sur Internet".
Enfin, si toutes ces techniques restent pour l'instant réservées aux initiés, avec la loi Loppsi elles devraient "se développer auprès du grand public, en particulier le VPN", avance Aurélien Boch.
DEFICIT GREC

Pour les handicappés de la technologie parmi nous, il existe également un tutoriel vidéo très simple et très bien fait, qui explique comment installer un VPN. Cela pèse 450 Mo et se trouve sur la quasi totalité des serveurs bittorrent.

[Philou sur TrackerNews - 2/01/2010]

Anti-Hadopi.VPN.Video.Tutorial.XP-Win7.FR-NzB.zip - http://isohunt.com/torrent_details/148969293/?tab=summary

LES SOLUTIONS POUR CONTRER HADOPI
Bonjour à tous et à toutes,
Énième rebondissement dans la saga tragicomique de la loi Hadopi.
Alors que les premiers courriels ne seraient envoyés qu'en Avril prochain (dans le meilleur des cas), voici quand même quelques points IMPORTANTS à savoir sur le sujet:
- " La mule " (Réseau ED2K) a été confirmée comme étant la cible prioritaire.
- HADOPI sera géré par une poignée d'employé(e)s uniquement.

- Il y a des techniques déjà en place, pour éviter de recevoir des " pourriels " en provenance d'HADOPI.
Maintenant, tous ceux et celles concernés, veuillez prendre une grande respiration et arrêtez de paniquer!
HADOPI ne pourra ABSOLUMENT rien contre ceux qui se protègeront... Si un jour HADOPI voit son ombre...
Malgré tout, voici tel que promis dans le billet précédent, comment vous protéger:
**** 1- Location d'une Seedbox HORS FRANCE.***
**** 2- Location d'un serveur VPN HORS FRANCE.***
**** 3- Utilisation d'accès réseau sans-fil (WIFI) non-protégé ou publique***
**** 4- Déménager HORS FRANCE.***
1- Location d'une Seedbox HORS FRANCE:

Une Seedbox est un serveur informatique privé qui est dédié au téléchargement et à l'émission de fichiers numériques.
La location d'une Seedbox est de plus en plus fréquente depuis déjà plusieurs mois. Non pas uniquement afin d'éviter que votre adresse IP

personnelle circule sur les réseaux P2P, mais aussi et surtout, afin d'automatiser vos transferts afin de " seeder " et " leecher " via une large bande passante 24/24, 7/7, à longueur d'année.

Les Seedbox sont généralement utilisées par les " Uploaders ", mais c'est accessible à tous.
Les coûts d'une Seedbox sont généralement de 25€/mois jusqu'à 100€+/mois. Plus votre Seedbox sera performante (Processeur, Mémoire, Bande passante, etc), plus le prix sera important.
L'avantage d'une Seedbox est que vos transferts sont effectués via l'adresse IP liée à votre Seedbox fournis par l'hébergeur. Vous pouvez donc récupérer tous vos fichiers via FTP, une fois que ceux-ci seront complétés et sans risque de voir votre adresse IP circuler.

Cette solution est efficace, mais elle requiert en général, de meilleures connaissances informatiques. Certaines compagnies offrent par contre, des Seedbox " clé en main " faciles d'utilisation.
Avantages:
- Rapidité des transferts.
- Anonymat sur les réseaux P2P.
- Récupération facile et rapide.
Désavantages:
- Coûts parfois élevés.
- L'envoi de vos torrents (Upload) sur la Seedbox via FTP est généralement lente dû à la limitation des vitesses d'upload par les FAI.
- Connaissances en informatique de niveau intermédiaire à avancé, recommandées.
Quelques adresses de fournisseurs de Seedbox gratuits:
- A venir...

Quelques adresses de fournisseurs de Seedbox payants:
- http://www.seedboxhosting.com
- http://www.dediSeedbox.com
- http://tor.imageshack.us/tor
- http://www.w00tsite.com
- http://www.leasetorrent.com
- http://www.seedboxworld.net/

2- Location d'un serveur VPN HORS France :
Un VPN (Réseau privé virtuel) repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données de passer d'une extrémité à l'autre du VPN tout en étant sécurisées par des algorithmes de cryptographie.
Autrement dit, lorsque vous vous connectez au serveur, votre identité se masque pour devenir celle du fournisseur du service VPN.
Vous assurez donc ainsi votre anonymat complet par l'utilisation d'une connexion sécurisée et encryptée entre vous et le serveur VPN.

La connexion s'effectue généralement via un client, tel que OpenVPN, mais certaines entreprises offrent la connexion directe sans utilisation de client additionnel.

Les coûts liés à la location vont de 5€/mois jusqu'à +/- 35€/mois. La différence vient du type de service désiré. Le type de connexion, le niveau d'encryption, le nombre de Pays désiré, sont tous des facteurs.
Il est fortement recommandé d'utiliser des serveurs qui sont le plus près physiquement de votre lieu de résidence. Le plus gros inconvénient demeurera toujours la chute des performances de votre connexion Internet une fois la connexion établie avec le serveur VPN.
Les gens avec peu d'aptitude informatique sauront très bien s'en sortir avec la configuration très peu complexe de cette solution.

Le faible coût ainsi que le niveau de sécurité offert par ce type de protocole en font le choix #1 afin de naviguer de façon anonyme sur le net.
Avantages:
- Facilité d'utilisation même pour les débutants.
- Coût très faible.
- Excellent niveau d'anonymat.
Désavantages:
- Perte de vitesse de votre bande passante.
- Déconnexion du serveur possible. (Contournable avec ADSL Autoconnect pour les connexions directes pour Windows XP)
Quelques adresses de fournisseurs de VPN gratuits:
- http://www.itshidden.com
- http://www.peer2me.com
- http://s6n.org/arethusa/fr.html
- http://www.hotspotshield.com

ne fois installé sur ton ordinateur, une simple connexion à Peer2Me te permet de :

Explorer et télécharger les fichiers privés de tes amis
en te connectant de chez toi et en privé à leurs ordinateurs et aux données qu'ils contiennent (films, photos, musique)

Améliorer l'ensemble de tes logiciels Internet
(MSN Messenger, Yahoo! Messenger, Skype, FTP...) : Plus grande rapidité de téléchargement et confidentialité stricte.

Accéder à distance à ton ordinateur
depuis n'importe où (travail, cybercafé, hotspot Wi-Fi...) pour avoir toujours à ta disposition l'ensemble de tes dossiers informatiques.

Démo / En savoir plus
Démo / En savoir plus
Démo / En savoir plus

100% GRATUIT, une simple inscription suffit !

Clique sur le bouton ci-dessous pour t'inscrire et télécharger dès maintenant le programme d'installation Peer2Me

Arethusa VPN
*
À propos

Arethusa VPN est un service qui rend votre connexion internet plus anonyme et sécurisée. Votre adresse IP réelle est cachée et votre FAI ne peut pas surveiller ou filtrer votre activité.
Cela fonctionne en établissant un tunnel crypté entre votre ordinateur et nos serveurs, en utilisant un VPN. Toute votre activité Internet semblera provenir de nos adresses IP, et non pas de votre IP réelle.
Un service de VPN est utile pour les personnes utilisant des réseaux censurés, filtrés, ou surveillés, des points d'accès WiFi, pour les dissidents politiques.
Pour vérifier quelle est votre adresse IP actuelle, cliquez ici ou ici ou ici.
Nous ne stockons aucune donnée sur votre trafic réseau. Nous ne stockons jamais votre adresse IP réelle.
Caractéristiques
Offre Premium v2 :
Bande passante dédiée non limitée. Maximum 30 Mbps par utilisateur.
Adresse IP dynamique (NAT). 10 ports entrants ouverts (plus sur demande).
Compatible avec toutes les applications, y compris le P2P et la VoIP, si configuré correctement.
Méthodes de connexion disponibles : PPTP, OpenVPN (TCP ou UDP).
Coût : 5 EUR par mois. Pas de frais de mise en service.
Offre Premium v1 : (serveurs pleins)
Bande passante partagée non limitée.
Adresse IP dédiée et fixe. Tous les ports sont ouverts. Compatible avec toutes les applications, y compris le P2P et la VoIP.
Méthodes de connexion disponibles : PPTP, OpenVPN (TCP ou UDP).
Coût : 5 EUR par mois. Pas de frais de mise en service.
Offre gratuite (Free) : (temporairement fermée)
Bande passante de faible qualité. 100 Mbps partagés entre tous les utilisateurs.
Adresse IP partagée (NAT). Tous les ports entrants sont fermés. Port 25 bloqué (pas de mail).
Méthode de connexion : OpenVPN (TCP) uniquement.
Gratuit. Aucun support fourni.
Avertissement :
Notre service cache votre adresse IP réelle et crypte votre connexion. Rien de plus, rien de moins.
Si votre ordinateur a des failles de sécurité, vous serez quand même hacké ou infecté par des virus. Si votre connexion Internet était filtrée ou derrière un pare-feu auparavant, votre ordinateur est désormais directement accessible depuis Internet.
Notre service ne vous empêchera pas non plus de dévoiler volontairement vos informations personnelles sur Internet.
Si vous utilisez Windows, vous devriez vraiment vérifier que vous avez un anti-virus installé et que votre pare-feu est activé sur votre connexion VPN.
*Pour de meilleurs résultats, vous devriez utiliser le VPN sur un ordinateur équipé de Linux ou *BSD, sans aucun document personnel dessus.*
Assurez-vous de toujours installer toutes les mises à jour de sécurité de votre système d'exploitation.
Plusieurs méthodes de connexion sont disponibles pour l'offre premium.
OpenVPN est meilleur, mais plus difficile à configurer sous Windows.
N'utilisez jamais PPTP si vous pensez que quelqu'un espionne votre connexion.

PPTP (GRE)
OpenVPN
Cryptage
Faible (MPPE 128 bits)
Fort (auth : RSA 2048 bits; données : AES 256 bits)
Compression

Non
Oui (LZO)
Nécessite l'installation d'un logiciel
Non
Oui
Fonctionne sur Windows/Linux/MacOS
Oui
Oui
Fonctionne sur une large gamme de périphériques
Oui
Non
Capacité à fonctionner derrière un firewall
Moyenne (utilise le port 1723 TCP + le protocole 47)
Excellente (utilise le port 443 UDP ou TCP)
Configuration
D'abord, connectez-vous à notre panneau de contrôle. Si vous n'avez pas encore créé de tunnel, cliquez sur "Ajouter" pour en demander un.
Cherchez l'adresse du serveur, le nom d'utilisateur et le mot de passe pour le tunnel que vous voulez configurer.
Pour OpenVPN, vous devez aussi cliquer sur "CA" et "Config", et sauver ces deux fichiers sur votre ordinateur.
OpenVPN
Windows
** Si vous n'avez pas OpenVPN 2.1, vous devez l'installer. Cliquez ici pour télécharger la dernière version puis lancez-le (vous devez être Administrateur). Cliquez "Next >", "I Agree", "Next >" (laissez toutes les cases cochées), "Install", "Next >", décochez "Show readme" puis "Finish".*
** Ouvrez le dossier de configuration d'OpenVPN (Démarrer -> Programmes -> OpenVPN -> Shortcuts -> OpenVPN configuration file directory) et copiez les fichiers CA et Config dans ce dossier.*
** Lancez OpenVPN GUI (en Administrateur) : Démarrer -> Programmes -> OpenVPN -> OpenVPN GUI.*
** Localisez l'icône OpenVPN GUI dans le systray. Faites un clic droit sur l'icône et cliquez sur "Connect".*
** Entrez le nom d'utilisateur et mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Ok".*
** Cliquez ici si vous voulez enregistrer votre mot de passe et vous connecter automatiquement au démarrage de Windows.*
Linux (toute distro avec NetworkManager)
** Installez le plugin OpenVPN pour NetworkManager. Pour Ubuntu / Debian: sudo aptitude install network-manager-openvpn . Vous pouvez avoir à relancer votre session pour que cela prenne effet.*
** Cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", puis "Configurer le VPN...".*
** Si vous avez un bouton "Importer", cliquez dessus et selectionnez le fichier Config ("arethusa.ovpn"). Votre connexion sera créée et préremplie avec toutes les données nécessaires sauf le nom d'utilisateur et le mot de passe.*
** Cliquez sur "+ Ajouter".*
** Selectionnez "OpenVPN" puis cliquez sur "Créer..." ou "-> Suivant".*
** Entrez le nom que vous voulez dans "Nom de la connexion" (par exemple "Arethusa VPN").*
** Entrez l'adresse du serveur (se trouve dans notre panneau de contrôle) dans "Passerelle".*
** Selectionnez "Type d'authentication : Mot de passe". Entrez le nom d'utilisateur (se trouve dans notre panneau de contrôle).*
** Cliquez sur le bouton à côté de "Certificat du CA" et sélectionnez le fichier CA.*
** Cliquez sur "Avancé...". Entrez "Utiliser un port de passerelle personnalisé : 443". Cochez "Utiliser la compression de données LZO". Cochez "Utiliser une connexion TCP" si vous voulez vous connecter en TCP.*

Dans l'onglet "Sécurité" ou "Certificats", selectionnez "Chiffrement : AES-256-CBC". Cliquez sur "Valider".
** Cliquez sur "Appliquer" ou "-> Suivant".*
** Pour lancer votre connexion VPN, cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", et sélectionnez la connexion que vous venez de créer.*
** Entrez le mot de passe (trouvé dans notre panneau de contrôle) et cliquez sur "Ok".*
Mac OS X 10.4 et plus (avec Tunnelblick)
** Téléchargez Tunnelblick et double-cliquez sur le fichier .dmg téléchargé. Sélectionnez Tunnelblick.app et déposez-le sur le dossier Applications.*
** Ouvrez le dossier Applications et double-cliquez sur Tunnelblick.app. Autorisez l'application. Le nom d'utilisateur et le mot de passe de votre compte administrateur vous seront demandés.*
** Tunnelblick vous demandera ensuite de placer votre fichier de configuration dans un certain dossier. Copiez les fichiers CA et Config (fournis par nous) dans ce dossier. Cliquez sur "Continue".*
** Localisez l'icône Tunnelblick dans la barre des menus en haut de l'écran, habituellement entre l'horloge et l'icône Spotlight. Cliquez dessus, puis cliquez sur "Connect 'arethusa'".*
** Entrez le nom d'utilisateur et mot de passe (trouvés dans notre panneau de contrôle).*
PPTP
Windows XP / 2003
** Lancez l'"Assistant Nouvelle Connexion" : Démarrer -> Programmes -> Accessoires -> Communications -> Assistant Nouvelle Connexion.*
** Cliquez sur "Suivant >".*
** Sélectionnez "Connexion au réseau d'entreprise" et cliquez sur "Suivant >".*
** Sélectionnez "Connexion réseau privé virtuel" et cliquez sur "Suivant >".*
** Entrez le nom que vous voulez pour cette connexion, par exemple "Arethusa VPN" et cliquez sur "Suivant >".*
** Il peut vous être demandé s'il est nécessaire d'établir une autre connexion au préalable. Si votre connexion internet figure dans la liste, sélectionnez-la, sinon choisissez de ne pas établir de connexion initiale. Cliquez sur "Suivant >".*
** Entrez le nom d'hôte du serveur (se trouve dans notre panneau de contrôle sous "Adresse du serveur") et cliquez sur "Suivant >".*
** Choisissez d'ajouter un raccourci si vous le souhaitez et cliquez sur "Terminer".*
** Pour lancer votre connexion VPN, ouvrez "Connexions réseau" (Démarrer -> Programmes -> Accessoires -> Communications -> Connexions réseau) et cliquez sur la connexion tout juste créée pour le VPN.*
** Entrez le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Se connecter".*
Windows Vista / 7
** Ouvrez le "Panneau de configuration" (Démarrer -> Panneau de configuration), puis cliquez sur "Réseau et Internet".*
** Cliquez sur "Centre Réseau et Partage", puis "Configurer une connexion ou un réseau".*
** Sélectionnez "Connexion à votre espace de travail" et cliquez sur "Suivant".*
** Sélectionnez "Utiliser ma connexion Internet (VPN)".*
** Entrez l'adresse Internet du serveur (se trouve dans notre panneau de contrôle sous "Adresse du serveur"), entrez le nom que vous voulez dans "Nom de la destination" (par exemple "Arethusa VPN"), et cliquez sur "Suivant".*
** Entrez le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Créer".*
** Quand l'emplacement du réseau VPN vous est demandé, choisissez "Lieu public" pour une sécurité maximale.*

Mac OS X 10.4
** Dans le Finder, cliquez sur "Aller".*
** Ouvrez "Applications", puis "Connexion à Internet", puis "VPN".*
** Sélectionnez "PPTP" comme type de connexion.*
** Entrez l'adresse du serveur, le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle).*
** Cliquez sur "Se connecter".*
** Dans les "Options" de "Connexion à Internet", cochez "Envoyer tout le trafic sur la connexion VPN".*
Mac OS X 10.5
** Ouvrez "Préférences Système" puis "Réseau".*
** Cliquez sur "+".*
** Dans la fenêtre popup, choisissez "VPN" pour Interface, et "PPTP" pour Type de VPN.*
** Entrez le nom que vous voulez dans "Nom du service" (par exemple "Arethusa VPN"), et cliquez sur "Créer".*
** Entrez l'adresse du serveur (se trouve dans notre panneau de contrôle), entrez le nom d'utilisateur dans "Nom du compte", et cliquez sur "Réglages d'authentification...".*
** Sélectionnez "Mot de passe :", entrez le mot de passe (se trouve dans notre panneau de contrôle) et cliquez sur "OK".*
** Cliquez sur "Avancé...".*
** Cochez "Envoyer tout le trafic sur la connexion VPN" et cliquez sur "OK".*
** Cliquez sur "Appliquer".*
** Cliquez sur "Se connecter".*
Linux (toute distro avec NetworkManager)
** Installez le plugin PPTP pour NetworkManager. Pour Ubuntu / Debian: sudo aptitude install network-manager-pptp . Vous pouvez avoir à relancer votre session pour que cela prenne effet.*
** Cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", puis "Configurer le VPN...".*
** Cliquez sur "+ Ajouter".*
** Sélectionnez "Protocole de tunnel Point-to-Point (PPTP)" ou "pppd tunnel (PPTP ...)" puis cliquez sur "Créer..." ou "-> Suivant".*
** Entrez le nom que vous voulez dans "Nom de la connexion" (par exemple "Arethusa VPN").*
** Sélectionnez "Type: Windows VPN (PPTP)" (si cette option existe).*
** Entrez l'adresse du serveur (se trouve dans notre panneau de contrôle) dans "Passerelle", et le nom d'utilisateur (si cette option existe).*
** S'il y a un bouton "Avancé...", cliquez dessus, cochez "Utiliser le chiffrement Point-to-Point (MPPE)" et cliquez sur "Valider".*
** Cliquez sur "Appliquer" ou "-> Suivant".*
** Pour lancer votre connexion VPN, cliquez sur l'icône réseau dans le systray, puis "Connexions VPN", et sélectionnez la connexion que vous venez de créer.*
** Entrez le nom d'utilisateur et le mot de passe (trouvés dans notre panneau de contrôle) et cliquez sur "Ok".*
Divers
Serveur SMTP (premium uniquement): smtp.s6n.net
Serveur DNS (premium v1 uniquement): 94.23.190.1
Serveur DNS (premium v2 et serveur gratuit): 10.10.10.10
Conditions du service
** Pas d'activité illégale.*
** Pas de spam, flood, diffusion de virus, hacking, scan de réseau, harcèlement envers des personnes.*
** Pas d'activité qui amènerait une de nos adresses à être blacklistée, ou qui mettrait en danger la qualité du service pour les autres utilisateurs.*
** Le service doit être payé d'avance et renouvelé avant la date d'expiration.*
** Toute violation de ces conditions entraînera la fermeture immédiate de votre compte sans remboursement possible.*

** Vous êtes entièrement responsable de vos activités lorsque vous utilisez notre service.*
** Nous essayerons de fournir la meilleure qualité de service possible.*
** Nous ne révélerons aucun détail personnel à des tiers et nous n'essayerons pas d'identifier nos clients, sauf lorsque requis par la loi.*

Quelques adresses de fournisseurs de VPN payants:
- http://www.ipredator.se
- http://www.strongvpn.com
- http://www.perfect-privacy.com/french/index.html
- http://www.yourprivatevpn.com/?q=fr
- http://www.psilo.fr
- http://www.hidemynet.com
- http://www.mullvad.net/en
- http://www.unblockvpn.com
- http://www.vpnboy.com
- http://www.torrentfreedom.com
- http://www.acevpn.com
- http://www.ipodah.net
- http://www.vpngates.com
- http://www.linkideo.com
- http://www.flashvpn.com
- http://www.purevpn.com
- https://www.relakks.com
- https://www.ananoos.com
- https://www.connectionvpn.com/fr

silo : internet l'esprit libre !
Psilo est un nouveau service de VPN vous permettant de naviguer, blogger, participer à des forums, partager en toute confidentialité.
Toutes vos communications internet passent par votre connexion sécurisée Psilo. Grâce au réseau Psilo, vous remplacez votre adresse IP publique par une adresse anonyme !
Au travail, dans un cyber-café, à l'hôtel, ou tout simplement chez vous, vous n'êtes plus surveillé, et vous profitez pleinement d'internet en toute liberté !
** Connexion cryptée (AES 256 bits)*
** Tunnel OpenVPN compatible Windows/Linux/MacOS X*
** Pour le web, les forums, le chat... et le P2P*
** Connexions P2P optimales grâce à la redirection de ports*
** Transférez jusqu'à 200 Go de données par mois !*
** Aucun log, aucune surveillance par Psilo*
Seulement 4,50 € par mois !
Plus d'informations
Vous devrez lire et accepter la charte pour utiliser le service Psilo.
Psilo est encore expérimental. Nous sommes actuellement en phase de tests, mais les inscriptions sont suspendues. Merci de votre compréhension !
A bientôt sur Psilo.fr !
contact - blog - MAJ 19 janvier 2010

Bienvenue à YourPrivateVPN!
1. Naviguer anonyme
6. Connexion chiffrée
2. À grande vitesse
7. Sécurité de hotspot
3. Le trafic illimité

8. Aucun logiciel additionnel exigé
4. Connexion réseau 1GBit
9. Surpasser les barrières du Web
5. Appuis individuel
10. Paiement sécurisé
L'accès privé et sécurisé à Internet devient de plus en plus difficile. Êtes-vous inquiet que tout ce que vous dites et faites sur Internet soit observé et enregistré? YourPrivateVPN.com offre une solution d'intimité par l'accès à grande vitesse de VPN utilisant des serveurs situés dans les Pays Bas. Vous êtes complètement anonyme, votre trafic est entièrement chiffré, et vous êtes totalement protégé.

VPN - C'est quoi?
VPN (réseau privé virtuel) est un réseau privé d'Internet. Traditionnellement, les compagnies importantes l'emploient pour communiquer avec leurs employés partout dans le monde. De nos jours VPN peut servir à maintenir votre intimité en surfant Internet. Comparé au travail que peut faire un serveur proxy, tout le trafic est chiffré dans une connexion de VPN et votre adresse IP est cachée.

Pourquoi choisir YourPrivateVPN ?
1. L'intimité - notre premier but est d'assurer votre intimité et votre sécurité. Pour cette raison, nos serveurs sont configurés de manière à ce que votre vrai IP ne soit jamais stocké, si bien qu'on ne trouve aucune trace de votre vrai IP sur nos serveurs. En outre, quand vous commandez votre accès anonyme, vous pouvez payer facilement avec PayPal ou Ukash. Ainsi nous ne recevons aucune information sur vos données de paiement. En effet, nous n'avons même pas besoin de votre nom ; votre adresse e-mail est suffisante.

2. La vitesse - nos serveurs aux Pays Bas et États Unies sont extrêmement vites - 1.000 mbps. Contrairement à d'autres fournisseurs de VPN ou à des serveurs proxy, où vous pourriez souffrir d'un ralentissement substantiel de la connexion, nous réservons la largeur de bande suffisante pour nos clients. Ainsi, si vous commandez par exemple un Gold Account avec 6000 Kbps, vous pouvez télécharger un film d'une durée de 90 minutes, en environ 20 minutes.

3. La sécurité - avec YourPrivateVPN, toutes vos données sont transférées sous la forme chiffrée. Pas même votre fournisseur des Services Internet peut voir ce que vous faites sur Internet. Vous pouvez surfer inaperçu, écrire des e-mails ou créer des blogs, mais aussi échanger des données ou des dossiers.

4. Non censuré - YourPrivateVPN vous permet de surmonter toutes les restrictions d'accès imposées par votre fournisseur Internet ou votre employeur. Ainsi vous pouvez visiter sans risques tous les sites Internet qui sont fermés au votre lieu de travail, ou que votre gouvernement ne veut pas que vous voyiez. Idem pour des services de VoIP comme Skype, MSN et ICQ. Ainsi vous pouvez également employer ces services sur votre smartphone ou iphone.

5. Volume illimité - YourPrivateVPN n'a pas de restrictions de volume, à la différence d'autres fournisseurs de VPN. Vous recevez le même service de qualité, si vous employez 100 MB ou 100GB de largeur de bande. Nous demandons seulement que vous ne maltraitiez pas notre service en employant d'énormes quantités de largeur de bande.

6. Localisation - nos serveurs sont stratégiquement situés aux Pays Bas et États Unies . Ils offrent la vitesse la plus élevée due à l'accès direct aux backbones des services européens et americaines. D'une part ils sont

proches de beaucoup de pays qui ont un accès restreint à Internet - Moyen-Orient ou encore la Chine. Cela permet donc un accès rapide pour les utilisateurs de ces pays.

7. Croissance - en tant que jeune compagnie grandissante nous investissons constamment dans de nouvelles infrastructures de serveurs. En faisant partie de notre clientèle, vous profiterez de notre croissance, puisque vous pourrez utiliser tous les futurs serveurs utilisant le même compte.

Pour plus d'informations et pour s'enregistrer cliquez >> ici
Social Networks:

Encrypter votre Internet,
Vous avez trouvé Perfect Privacy. Nous encryptons votre connexion Internet et protégeons votre identité et votre confidentialité, à l'abri des regards indiscrets. Nous rendons votre connexion sécurisée, encryptée et anonyme, où que vous vous trouvez.

Enfin libre de faire ce que vous voulez,
Perfect Privacy, vous permet d'anonymiser et d'encrypter entièrement votre activité Internet. Que soyez en train de naviguer, éditer un blog, écrire des emails, conduire une activité commerciale, transférer de l'argent, télécharger de images, échanger des fichiers ou simplement chatter, vous êtes sécurisé et invisible en permanence pendant vos sessions en ligne.

Facile à utiliser,
Perfect Privacy vous fournit un client personnalisé exclusif et des logiciels pré-configurés qui réalisent tout le travail de connexion à votre place. Pas besoin d'être un expert en informatique pour retrouver la confidentialité de vos activités en ligne.

En de bonnes mains,
En vous fournissant un service personnalisé, nous garantissons que pendant que vous utilisez notre service, vous serez anonyme, protégé et sécurisé à tout moment. Nous ne voulons pas savoir qui vous êtes. Vous pouvez payer de façon anonyme. Nos serveurs anonymes encryptés sont répartis internationalement dans des juridictions sélectionnées pour permettre une confidentialité maximale de vos données. Le meilleur étant que vous avez accès en permanence, non seulement au serveur de votre choix, mais également à l'ensemble de notre parc de serveurs (en ce moment , , , , , , 2×, , , 5×, 2×, 8×, 4×, , , 2×, 3×, et) - non seulement à un service de cryptage et d'anonymisation mais à plusieurs (VPN, SSH2 tunnels, Squid Web proxy, SOCKS 5 proxy, etc.), selon vos choix et vos besoins du moment.

Confort d'utilisation,
Nous offrons de nombreuses méthodes de payement possibles, dont l'argent liquide, les cartes de crédit, PayPal, Liberty Reserve, PaySafeCard et WebMoney.

IL EST STRICTEMENT DÉFENDU D'UTILISER LE SERVICE " TOR " À D'AUTRES FINS QUE LA NAVIGATION ANONYME SUR LE WEB! TOR N'EST PAS UN SERVICE OFFERT POUR LE PARTAGE DE FICHIERS! MERCI DE NE PAS SATURER LES SERVEURS OFFERTS GRATUITEMENT PAR UNE POIGNÉE DE BIENFAITEURS, D'ENTREPRISES, D'UNIVERSITÉS ET D'ORGANISMES À BUT NON LUCRATIF, POUR LE BIEN DE CETTE COMMUNAUTÉ! CEUX QUI UTILISENT LE RÉSEAU TOR POUR TÉLÉCHARGER, HONTE À VOUS!

3- Utilisation des accès réseau sans-fil (WIFI) non-protégés ou publics : La technologie WIFI est extrêmement populaire depuis quelques années. La possibilité de naviguer partout, grâce à l'utilisation de réseaux sans-fil est très agréable.
Il existe trois types de réseau sans-fil: L'offre payante, les " HotSpots " gratuits et les réseaux privés.
Le type d'accès réseau sans-fil qui vous intéressera ici est l'offre gratuite. Celle-ci est généralement offerte par des FAI, des entreprises privées (Ex. Restaurants) ou encore par des particuliers/entreprises possédants un réseau sans-fil non-sécurisé.
En aucun cas, nous ne vous encouragerons à utiliser une connexion Internet qui ne vous appartient pas!
4- Déménager HORS FRANCE.
Pour ceux qui recherchent l'aventure, le monde s'ouvre à vous! Profitez-en pour voir du pays.
Pourvu que vous sortiez de la France, HADOPI ne pourra plus rien contre vous.
Voilà!
Je vous recommande de masquer votre IP, si vous être résidant en France, dès que possible jusqu'à l'annonce de la mort d'HADOPI.
Vu l'ampleur des fonds publics, littéralement gaspillés, que nécessitera cette farce qu'est HADOPI, il ne fait aucun doute que sa mort viendra. Patience!
Bon partage!
PS: Pour plus d'informations sur la configuration d'une Seedbox, d'un serveur VPN ou autre... Sachez que chacun de ces fournisseurs, mentionnés ci-haut, offrent une section " FAQ " sur leur site respectif. Merci de faire votre part en consultant celles-ci au lieu de poser vos questions dans la section " commentaires "! Google demeurera toujours un bon ami si besoin est...

Mai s attention HADOPI est une grosse merde qui éclaboussera quelques français au début et de plus en plus aprèe .....bye philou

PROTEGEZ VOUS!!!!!

http://libertesinternets.wordpress.com
e PDG de Dailymotion est l'ancien directeur de campagne électorale de Sarkozy.... alors vous croyez quoi ? Qu'on allait vous laisser dire ce que vous voulez ? Bienvenue dans la réalité du Net où la liberté d'expression appartient à celui qui possède les tuyaux... comme dans la vraie vie d'ailleurs, où ne peuvent s'exprimer que ceux qui ont accès aux médias, qui possèdent une presse d'imprimerie ou un émetteur radio.
Il serait peut-être temps de penser à cette vieille idée : appropriation des moyens de production par le peuple. Parce que tant qu'on continuera à dépendre du bon vouloir des MM. Bouyges, Sarkozy, Google et Nasdaq pour notre communication, on sera toujours à la merci de leur censure et leur manipulation...
CENSURE CHEZ DAILYMOTION
[Blueman - 04/02/2010]
Depuis plus d'une semaine une trentaine de personnes ont vu leurs comptes supprimés définitivement, avec en totalité plus de 4000 vidéos, censurer sans vraiment une raison valable à part celui de rayer la libre expression

et une véritable informations, ceci est un énorme danger pour notre liberté.. Cela nous concerne tous,
Voici des liens que vous pourrez consulter :
http://www.ubest1.com/index.php?option=com_seyret&Itemid=27&task=commentaire&nom_idaka=5056&anarana=video&ecrit=NiZuB_BlaBla&vi=NiZuB_BlaBla_1265203497_video.flv
http://www.blueman.name/Des_Videos_Remarquables.php?NumVideo=559