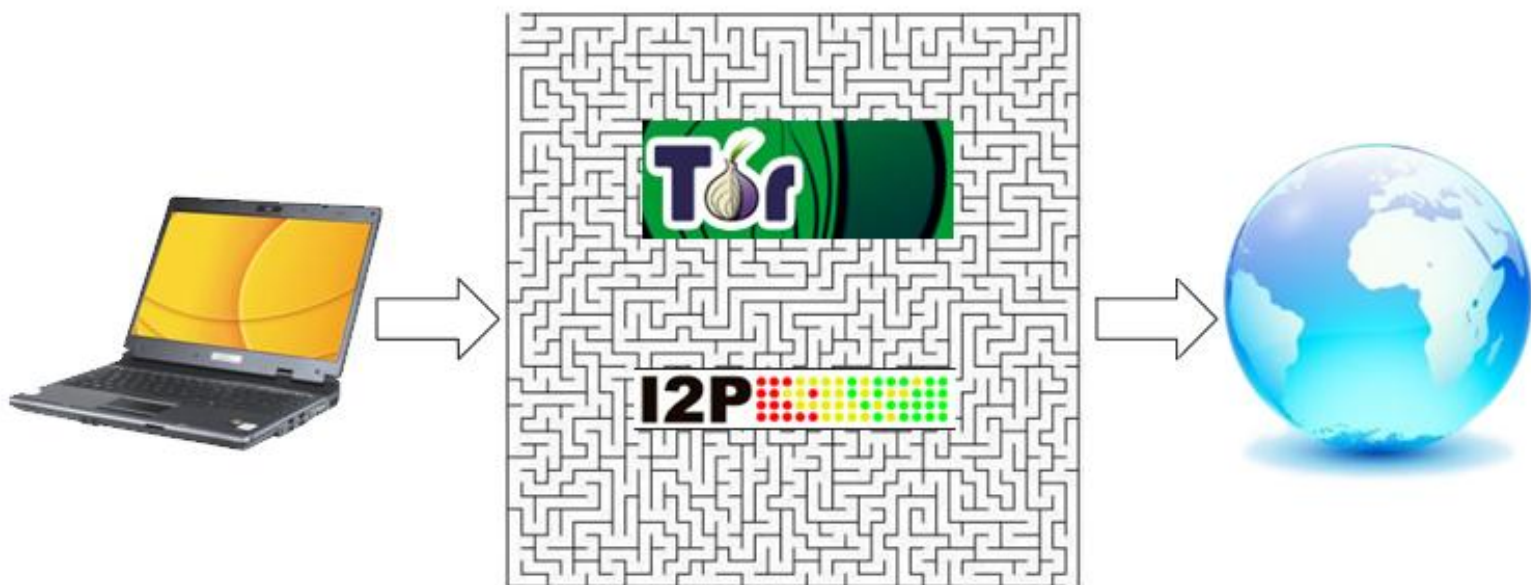


TUTORIEL D'INSTALLATION D'UNE SUITE DE LOGICIEL AIDANT A L'ANONYMAT SUR INTERNET



AVANT PROPOS

Le but de ce tutoriel est d'aider l'utilisateur à améliorer sensiblement son anonymat lors de son activité sur Internet, et ce par l'installation d'une suite de logiciels et la configuration des navigateurs Internet.

Cet anonymat a pour objectif le droit à la protection de sa vie privée, en ces temps de surveillance numérique accélérée...

En aucun cas il n'est question de promouvoir le partage, l'échange, la vente etc. de fichiers protégés par les droits d'auteur. L'utilisateur est entièrement responsable du bon usage de ce tutoriel et des logiciels/solutions/réseaux présentés.

Il est important de rappeler quelques points concernant l'anonymat sur Internet :

- **Celui-ci ne peut être garanti à 100%** par les créateurs de ces logiciels/réseaux ! Ces logiciels étant toujours en développement, ils aident fortement au renforcement de l'anonymat mais des failles peuvent toujours exister.
- **Vous êtes toujours responsable de votre activité sur Internet (navigation, partage de fichiers...) ! Vous devez être respectueux des chartes écrites par leur créateurs !**
- Il est important d'avoir un système d'exploitation sain et sécurisé :
 - Antivirus
 - Firewall
 - Navigateurs Internet sécurisés
 - Système d'exploitation **à jour !**
- Votre comportement sur Internet est la base de votre sécurité (vous êtes votre meilleur antivirus !) et votre anonymat ! Le téléchargement de fichiers sensibles/protégés est à vos risques et périls... Ne donnez pas d'adresses mails « officielles », utilisez des pseudos qui ne vous compromettent pas, ne dévoilez pas votre lieu de résidence ou autre information personnelle (IP, configuration matérielle/logicielle précise)

Il ne sert à rien d'utiliser des solutions d'anonymat si vous dévoilez des indices qui facilitent votre repérage sur le réseau !

Sommaire :

AVANT PROPOS.....	2
1. PRELIMINAIRES : SECURISER SON PC	4
1.1 ANTIVIRUS / ANTISPYWARES.....	4
1.2 FIREWALL.....	4
1.3 NAVIGATEUR INTERNET	4
1.4 MISES A JOUR DU SYSTEME D'EXPLOITATION	5
2. TELECHARGEMENT / INSTALLATION DES ELEMENTS NECESSAIRES	5
3. AVANT D'INSTALLER : PRESENTATION DES LOGICIELS D'ANONYMAT.....	6
3.1 I2P	6
3.2 TOR.....	6
4. INSTALLATION ET CONFIGURATION.....	8
4.1 I2P	8
4.1.1 ROUTEUR.....	8
4.1.2 CREATION DES PROFILS FIREFOX	8
4.1.3 CONFIGURER FIREFOX POUR I2P :.....	9
4.1.4 INSTALLER I2P.....	10
4.1.5 PRESENTATION - CONFIGURER I2P	11
4.1.6 TELECHARGER DES TORRENTS AVEC I2P (une des fonctions d'I2P).....	13
4.1.6.1 PRESENTATION D'I2PSNARK	14
4.1.6.2 TELECHARGER AVEC I2PSNARK.....	15
4.1.6.3 UPLOADER (PARTAGER) DES FICHIERS AVEC I2PSNARK	15
4.1.7 POUR FINIR.....	17
4.2 TOR.....	18
4.2.1 ROUTEUR.....	18
4.2.2 INSTALLATION/CONFIGURATION DU PACK VIDALIA.....	18
4.2.2.1 INSTALLER L'EXTENSION « TORBUTTON » SUR VOTRE FIREFOX « INTERNET ANONYME » ...	18
4.2.2.2 CONFIGUREZ PRIVOXY.....	18
4.2.2.3 CONFIGUREZ TOR POUR QUE PRIVOXY SE LANCE AU DEMARRAGE DE CELUI-CI.....	18
4.2.3 PARTICIPER AU RESEAU TOR EN PARTAGEANT VOTRE BANDE PASSANTE	20
4.2.4 UTILISATION DE TOR.....	22
4.2.5 POUR ALLER PLUS LOIN DANS L'ANONYMAT AVEC TOR.....	22

1. PRELIMINAIRES : SECURISER SON PC

1.1 ANTIVIRUS / ANTISPYWARES

Divers antivirus, plus ou moins performants sont à votre disposition, je ne les listerais pas tous, une recherche sur Internet vous donnera une liste non exhaustive de sites/forums qui les présentent et les testent.

Voici une liste d'antivirus gratuits suffisants pour votre surf quotidien...n'oubliez pas que le meilleur antivirus se situe derrière votre clavier ;-)

- Avira Antivir : <http://www.01net.com/telecharger/windows/Securite/antivirus-antitrojan/fiches/13198.html>
- Avast : <http://www.avast.com/fre/download-avast-home.html>
- AVG : <http://free.avg.com/>

Antispywares :

- Malwarebytes : <http://www.malwarebytes.org/mbam.php>

1.2 FIREWALL

De même que pour l'antivirus, l'utilisation d'un pare-feu (firewall) est plus que conseillée, ceci afin de réguler/surveiller le trafic entrant et sortant sur votre ordinateur, ainsi que surveiller les applications qui ont accès à Internet. Si vous êtes novices en sécurité et dans l'utilisation de tels logiciels, de nombreux tutoriels existent sur Internet et je vous invite à les consulter.

Vous pouvez utiliser au minimum le pare-feu inclus dans votre OS (dans XP et Vista, il se trouve dans le « panneau de configuration »), mais sachez que souvent ils ne régulent que le trafic entrant dans votre ordinateur.

Voici une petite liste de pare-feux gratuits :

- Outpost Firewall : <http://free.agnitum.com/>
- Comodo Firewall : <http://personalfirewall.comodo.com/>
- Jetico Firewall : <http://www.jetico.com/index.htm#/jpfirewall.htm>

1.3 NAVIGATEUR INTERNET

Sans publicité particulière, je vous déconseille l'utilisation d'Internet Explorer pour la mise en place d'un protocole d'anonymat sur votre ordinateur, celui-ci étant limité dans sa configuration et dans ses modules complémentaires possibles.

Afin de mettre en place notre suite logicielle, il vous faut installer le navigateur Mozilla Firefox (<http://www.mozilla-europe.org/fr/firefox/>)

1.4 MISES A JOUR DU SYSTEME D'EXPLOITATION

Je vous conseille très fortement de vérifier (via le panneau de configuration → mises à jour) que votre système d'exploitation soit correctement mis à jour afin d'éviter toute faille de sécurité.

2. TELECHARGEMENT / INSTALLATION DES ELEMENTS NECESSAIRES

Voici la liste des différents logiciels/modules complémentaires... qui seront nécessaires. Vous ne serez pas obligés de tous les installer, vous jugerez au fur et à mesure de ce tutoriel, en fonction de vos besoins.

Je vous conseille de créer un dossier, auquel vous donnerez le nom que vous voulez (par exemple « internet anonyme ») sur votre bureau, dans lequel vous pourrez télécharger tous ces éléments.

- Vérifiez que vous avez au minimum Java 1.5 sur votre machine (allez dans Démarrer→Exécuter et tapez `cmd`, ensuite tapez `java -version`) sinon, installez Sun Java : <http://java.com/fr/download/index.jsp>
- Installez l'add-on pour firefox « profile manager » disponible ici (Il faut vous inscrire, mais ce n'est pas long et ca ne coûte rien) : <https://addons.mozilla.org/fr/firefox/addon/9452>
- Téléchargez I2P (dernière version en date : 0.7.3): <http://www.i2p2.de/download.html>
- Téléchargez le pack Vidalia : <http://www.torproject.org/dist/vidalia-bundles/vidalia-bundle-0.2.0.34-0.1.10.exe>

3. AVANT D'INSTALLER : PRESENTATION DES LOGICIELS D'ANONYMAT

A partir d'ici, je vais vous guider dans l'installation des 2 principaux logiciels d'anonymat que sont I2P et TOR.

**/ ! \ Vous n'êtes pas obligés d'installer les 2 / ! **

En effet, il est important de comprendre le rôle de chacun de ces logiciels, dont voici une petite présentation (issue de Wikipédia, que je vous invite à consulter) :

3.1 I2P (<http://fr.wikipedia.org/wiki/I2P>)

*« **I2P (Invisible Internet Project)** est un réseau anonyme, offrant une simple couche logicielle que les applications peuvent employer pour envoyer de façon **anonyme et sécurisée** des messages entre elles. La communication est chiffrée d'extrémité à extrémité. Au total il y a quatre couches de chiffrement utilisées pour envoyer un message. L'anonymat est assuré par le concept de "Mixed Network" qui consiste à supprimer les connections directes entre les pairs qui souhaitent échanger de l'information. A la place le trafic passe par une série d'autre pairs de façon à ce qu'un observateur ne puisse déterminer qui est le destinataire ou le destinataire de l'information. Chaque pair peut, pour se défendre, dire que les données ne lui étaient pas destinées. »*

I2P est donc un « internet dans l'internet », offrant différents supports identiques à l'Internet « normal » :

- Sites spécifiques (« eepsite », domaine en .i2p, consultables uniquement avec I2P)
- Clients d'échanges de fichiers (**NON COPYRIGHTES !**) - Peer to Peer –
- Chat IRC anonyme
- Mails anonymes
- ...

3.2 TOR ([http://fr.wikipedia.org/wiki/Tor_\(r%C3%A9seau\)](http://fr.wikipedia.org/wiki/Tor_(r%C3%A9seau)))

*« **The Onion Router (Tor)** (littéralement : **le routage en oignon**) est un réseau mondial décentralisé de routeurs, organisés en couches, appelés nœuds de l'oignon, dont la tâche est de transmettre de manière anonyme des paquets TCP. C'est ainsi que tout échange Internet basé sur TCP peut être anonymisé en utilisant Tor. Tor est un logiciel libre distribué sous licence BSD révisée. »*

TOR est donc un logiciel de routage, apparenté à un « proxy », qui permet d'anonymiser le trafic internet en passant par plusieurs nœuds, rendant difficile l'identification de l'utilisateur

2 choix s'offrent donc à vous :

- Installer uniquement I2P, ce qui vous permettra d'être anonyme dans le réseau I2P (surfer sur les « eepsites », échange de fichier entre utilisateurs d'I2P, ...), mais de ne pas être anonyme sur le reste de l'internet (http/https)
- Installer I2P et TOR en parallèle, ce qui vous permettra d'utiliser I2P comme décrit ci-dessus, et TOR pour le reste de votre navigation internet. Vous bénéficierez donc d'un anonymat très renforcé pour vos activités sur internet.

Dans les deux cas, sachez que ce tutoriel vous permet de « créer » deux profils pour le navigateur internet Firefox, à savoir :

- Un profil « Internet anonyme », qui utilisera soit I2P seul, soit I2P & TOR
- Un profil « Internet normal », qui n'utilisera aucun des 2 logiciels, vous permettant de surfer normalement sans anonymat, et sans ralentissement (**en effet, il est important de savoir que l'utilisation de logiciels/réseaux d'anonymat se fait au détriment de la « bande passante », c'est-à-dire votre vitesse de navigation !**)

Vous aurez donc, pour résumer, 2 icônes Firefox sur votre bureau : une icône « Internet normal » (non anonyme), et une icône « internet anonyme », que vous pourrez utiliser en même temps.

4. INSTALLATION ET CONFIGURATION

4.1 I2P

4.1.1 ROUTEUR

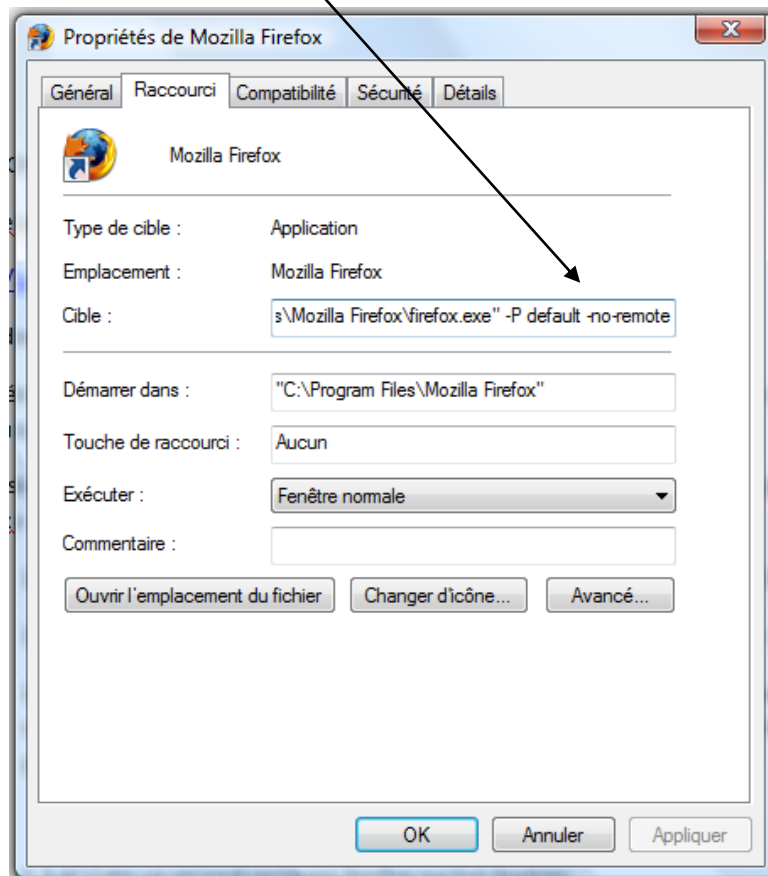
Préparez votre routeur NAT et/ou votre pare-feu, il faudra ouvrir les ports suivants :
Le port 123 en UDP, le port 8887 en UDP, le port 8887 en TCP

4.1.2 CREATION DES PROFILS FIREFOX

Configurez le module complémentaire « profile manager » (add-on) pour Firefox :
Ouvrez Firefox, et ouvrez Outils > PROFILE MANAGER AND SYNCHRONIZER

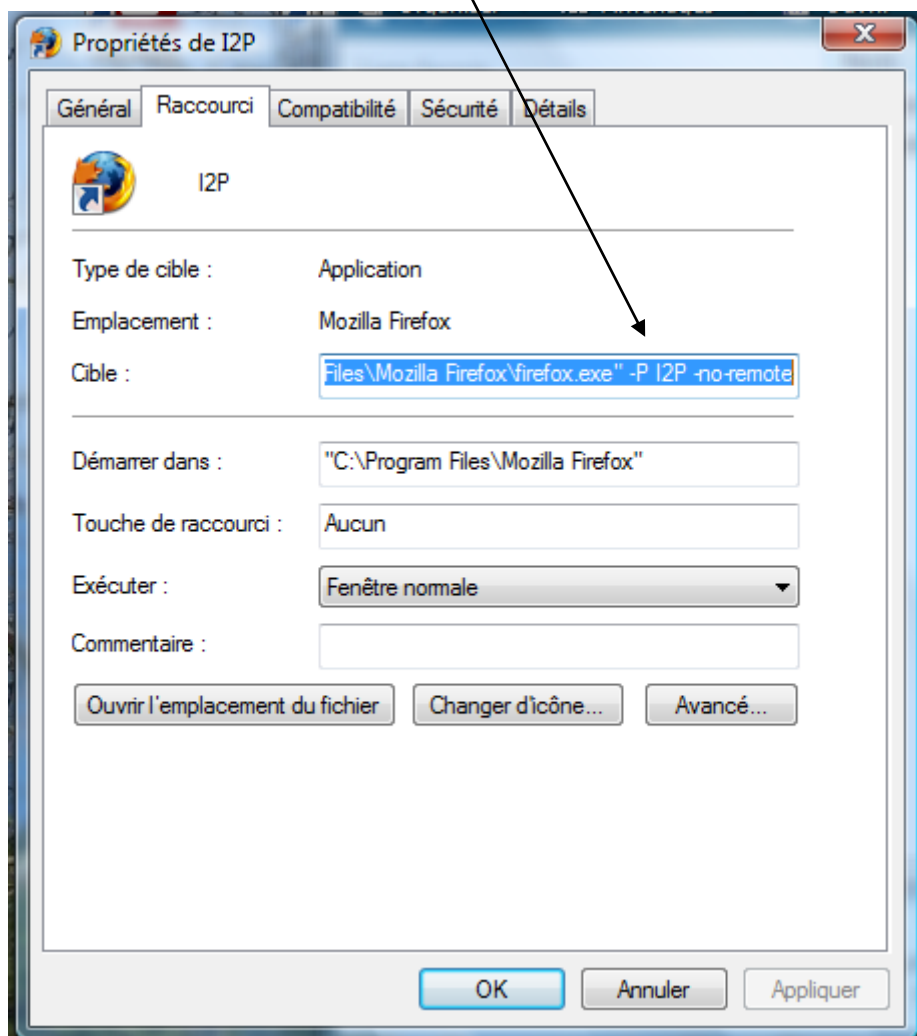
Créez un nouveau profil, par exemple « I2P » (n'effacez pas le profil « default » !). **Le but ici est de pouvoir avoir un Firefox configuré pour naviguer via I2P (et/ou TOR), et un autre configuré pour naviguer normalement, et de pouvoir utiliser les 2 en même temps.**

Dans les propriétés de votre raccourci Firefox sur votre bureau (celui que vous utiliserez pour naviguer normalement), rajoutez la commande « P », le nom du profil par défaut et la commande « -no-remote », ce qui devrait donner ça (il y a un espace entre le « et -P mais pas entre -no et -remote)



Renommez ensuite votre icône en « Internet Normal » (par exemple...)

Créez un second raccourci Firefox sur votre bureau, renommez le comme vous voulez (« Internet Anonyme » par exemple) et dans les propriétés de celui-ci (clic droit dessus), rajoutez la commande « P », le nom du profil I2P et la commande « -no-remote », ce qui devrait donner ça



Vous avez maintenant 2 sessions de Firefox, ce qui vous permettra de naviguer normalement (sans anonymat) sur une, et de naviguer/télécharger etc. via I2P (et/ou TOR) sur l'autre.

4.1.3 CONFIGURER FIREFOX POUR I2P :

Ouvrez Firefox «Internet Anonyme », et dans OUTILS > OPTIONS > AVANCE > RESEAU > PARAMETRES, choisissez « configuration manuelle du proxy », et rentrez les données suivantes :

Proxy http : 127.0.0.1 Port : 4444
Socks : V4

Allez aussi dans OUTILS > OPTIONS > GENERAL, et dans la « page d'accueil », rentrez ceci : <http://127.0.0.1:7657/index.jsp>

Votre Firefox « Internet Anonyme » est maintenant prêt à se connecter sur I2P

4.1.4 INSTALLER I2P

Allez dans votre dossier « internet anonyme » crée au début, et installez I2P (suivez les instructions).

Lancez I2P avec le raccourci « I2P (no window) » se trouvant sur votre bureau.

I2P va démarrer, cela prend un petit peu de temps... une fois lancé, il ouvrira sa console de routeur dans Firefox, mais cela risque de ne pas être dans le bon Firefox (« Internet anonyme ») mais dans celui avec le profil « default ». Quittez Firefox « Internet Normal », et démarrez celui « Internet Anonyme »...

Voilà, si tout va bien, vous êtes dans l'interface routeur d'I2P qui ressemble à ca :

I2P Router Console - home - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://localhost:7657/index.jsp
I2P Router Console I2PSnark forum.i2p Planet.i2p postman.i2p susimail v0.13 - Login
I2P Router Console - home I2PSnark - anonymous bittorrent

I2P [Susimail](#) | [SusiDNS](#) | [I2PSnark](#) | [My Eepsite](#)
[I2PTunnel](#) | [Tunnels](#) | [Profiles](#) | [NetDB](#) | [Logs](#) | [Jobs](#) | [Graphs](#) | [Stats](#)

[Configuration](#) [Help](#)

General
Ident: ([view](#))
Version: 0.7.1-0
Uptime: 4h
Now: 12:43:57 (-36s skew)
Reachability: [OK](#)

Peers
Active: 169/361
Fast: 9
High capacity: 19
Well integrated: 6
Known: 878

Bandwidth in/out
1s: 35,60/56,95KBps
5m: 50,64/80,46KBps
Total: 38,49/53,73KBps
Used: 565,33MB/789,71MB

Local destinations
* shared clients
[Details](#) [Config](#)
* I2PSnark
[Details](#) [Config](#)

Tunnels in/out
Exploratory: 2/2
Client: 6/5
Terminé

• 2009-03-29: **0.7.1 Released**

The 0.7.1 release optimizes I2P towards better performance and introduces new features.

Multiple bugs are fixed, replacements to the SimpleTimer class should waste less time on object locking. Some old components are dropped and several classes refactored to avoid repeating code.

Support for encrypted LeaseSets (for creation of links over I2P which an adversary cannot obstruct by attacking its gateways) becomes more complete. New tunnel types like IRC server tunnels and new options like delayed start and idling of tunnels also gain support, along with improved usability of the I2P Socks proxy mechanism.

Work continues on streamlining and expanding the Router Console, on the BOB protocol, on I2P ports for Debian and Slackware Linux, on the I2PSnark client, on TCP connection properties and multiple other fronts. Updating is highly recommended.

News last updated 4h ago

[Deutsch](#) | [English](#) | [Français](#) | [Nederlands](#) | [Svenska](#)

Si vous venez juste de lancer I2P, les chiffres sur la gauche à côté de Active devraient commencer à augmenter dans les prochaines minutes et vous verrez un "Shared client" en destination locale listés sur la gauche (si non, [voir plus bas](#)). Une fois qu'ils apparaissent, vous pouvez:

- **parcourir les "eepsites"** - sur I2P il y a des sites web anonymes hébergés - dites à votre navigateur d'utiliser le **HTTP proxy à l'adresse localhost port 4444**, ensuite vous pouvez naviguer sur les eepsites.
 - [inproxy.tino.i2p](#) et [perv.i2p](#): listent les eepsites actifs
 - [forum.i2p](#): une connexion sécurisée et anonyme vers [forum.i2p2.de](#)

4.1.5 PRESENTATION - CONFIGURER I2P



[Configuration](#) [Help](#)

General
Ident: [\(view\)](#)
Version: 0.7.1-0
Uptime: 4h
Now: 12:43:57 (-36s skew)
Reachability: [OK](#)

Peers
Active: 169/361
Fast: 9
High capacity: 19
Well integrated: 6
Known: 878

Bandwidth in/out
1s: 35,60/56,95KBps
5m: 50,64/80,46KBps
Total: 38,49/53,73KBps
Used: 565,33MB/789,71MB

Local destinations
 * shared clients
[Details](#) [Config](#)
 * I2PSnark

Voilà le bandeau d'info d'I2P, quelques informations importantes :

Reachability : I2P testes si vous avez des soucis de firewall ou de NAT, il doit être sur OK.

Peers : là, c'est important ! vous devez avoir des peers pour commencer votre activité sur I2P ! Il faut attendre un peu pour qu'I2P se connecte correctement aux nœuds du réseau... il atteint un nombre conséquent de peers en général au bout de 3 ou 4 min... ca dépend du nombre existant. N'hésitez pas à rafraichir de temps en temps pour voir le nombre de peers (touche F5)

Allez dans « configuration », et rentrez ces chiffres (vous pouvez les changer en fonction de votre connexion internet)

*Inbound rate : 700 KBps , maximum burst: 800 KBps
 Outbound rate: 90 KBps, maximum burst: 100 KBps
 Bandwith share percentage: up to 80%*

Puis sauvegardez en cliquant sur "save changes"

Allez ensuite dans « Configuration », puis « clients » :

- Vérifiez que « sambridge » et « bob » soient cochés en tant que « run at startup »
- Décochez « console browser », ce qui empêchera de démarrer Firefox quand vous lancerez I2P. I2P démarrera en tache de fond, et si vous voulez l'utiliser il n'y aura qu'à cliquer sur votre icône Firefox « Internet Anonyme », celui-ci démarrera alors sur la console d'I2P
- Cliquez sur « save client configuration »
- Redémarrez I2P (« shutdown »)

[Configuration](#) [Help](#)

General
Ident: [\(view\)](#)
Version: 0.7.3-0
Uptime: 2h
Now: 08:17:11 (-43s skew)
Reachability: [OK](#)

Peers
Active: 162/307
Fast: 9
High capacity: 23
Well integrated: 7
Known: 1017

Bandwidth in/out
1s: 14,06/41,52KBps
5m: 15,53/30,66KBps
Total: 9,86/25,17KBps
Used: 94,90MB/242,09MB

Local destinations

[Network](#) | [Service](#) | [Update](#) | [Tunnels](#) | [Clients](#) | [Peers](#) | [Keyring](#) | [Logging](#) | [Stats](#) | [Advanced](#)

Client Configuration

The Java clients listed below are started by the router and run in the same JVM.

Client	Run at Startup?	Start Now	Class and arguments
webConsole	<input checked="" type="checkbox"/>		net.i2p.router.web.RouterConsoleRunner 7657 1,127.0.0.1 ./webapps/
SAMBridge	<input checked="" type="checkbox"/>		net.i2p.sam.SAMBridge sam.keys 127.0.0.1 7656 i2cp.tcp.host=127.0.0.1 i2cp.tcp.port=7654
Tunnels	<input checked="" type="checkbox"/>		net.i2p.i2ptunnel.TunnelControllerGroup i2ptunnel.config
eepsite	<input checked="" type="checkbox"/>		org.mortbay.jetty.Server eepsite/jetty.xml
consoleBrowser	<input type="checkbox"/>	<input type="button" value="Start"/>	net.i2p.apps.systray.UrlLauncher http://127.0.0.1:7657/index.jsp
BOB	<input checked="" type="checkbox"/>		net.i2p.BOB.BOB null

Voilà, vous pouvez maintenant utiliser I2Pet ses fonctionnalités

Je vous conseille de garder l'interface routeur ouverte dans un onglet et de naviguer dans un autre onglet (ctrl+T).

La navigation est plus lente que la normale, c'est le prix de l'anonymat...

RAPPEL : l'efficacité de l'anonymat n'est maximale que lorsque vous utilisez I2P sur le réseau I2P, celui-ci étant, comme définit plus haut, un « internet dans l'internet ».

Je vous déconseille fortement de naviguer sur l'internet « normal » avec I2P, cela n'est pas son but premier... il en est de même pour l'échange de fichier (« peer to peer »), qui n'est anonyme qu'entre utilisateurs (voir chapitres suivants).

Si vous comptez naviguer sur les sites « normaux » anonymement, vous devrez installer une solution adaptée telle que TOR (voir chapitre suivant approprié) !

/!\ IMPORTANT /!

Lorsque vous voulez quitter I2P, utilisez bien le bouton « shutdown » dans le bandeau d'I2P, ne coupez pas tout à l'arrache en fermant les fenêtres, cela permet aux personnes qui bénéficient de votre bande passante (un des principes de fonctionnement d'I2P) de passer tranquillement sur d'autres bandes passantes partagées... le temps de « shutdown » est de 11 minutes afin de laisser le temps aux routeurs des autres utilisateurs de créer d'autres connections. Vous pouvez effectuer un « shutdown immediately », mais ne l'utilisez qu'en cas de nécessité, par respect pour les autres utilisateurs du réseau I2P S.V.P !

4.1.6 TELECHARGER DES TORRENTS AVEC I2P (une des fonctions d'I2P)

Je rappelle que vous êtes responsable du contenu des torrents que vous téléchargez ou mettez à disposition, ainsi que de l'utilisation que vous faites d'I2P !! I2P inclut un client qui permet l'échange de fichiers, mais je n'encourage en aucun cas le partage de fichiers copyrightés !!

Là c'est différent des torrents habituels, dans le sens que I2P (comme 99% des systèmes anonymes), ne supporte pas les torrents habituels, il faut que ceux-ci soient des torrents compatibles I2P (inutile donc d'utiliser des torrents qui proviendraient de Pirate Bay par exemple)

Vous pouvez trouver des torrents régulièrement mis à jours sur le eepsite (le nom des sites gérés par I2P) de Postman..., la majorité sont en anglais et en allemand, mais vous en avez quelques un en français... ca devrait s'agrandir dans les mois qui viennent ;-)

Pour télécharger, I2P utilise un client intégré, I2PSnark :

Dans votre page principale, vous pouvez le voir dans le menu du haut.



[I2PTunnel](#) | [Susimail](#) | [SusidNS](#) | [I2PSnark](#) | [My Eepsite](#)
[Tunnels](#) | [Profiles](#) | [NetDB](#) | [Logs](#) | [Jobs](#) | [Graphs](#) | [Stats](#)

[Configuration](#) [Help](#)
General

• 2009-03-29: **0.7.1 Released**

Personnellement, je l'ai mis en raccourci (« marque page ») dans ma barre personnelle de Firefox, et je l'ouvre dans un 2eme onglet (ctrl+t) afin d'avoir toujours un œil sur la console I2P.

4.1.6.1 PRESENTATION D'I2PSNARK

I2PSnark - anonymous bittorrent - Mozilla Firefox

http://localhost:7657/i2psnark/

I2PSnark Starting up torrent
Many I2P trackers require you to register new torrents
Torrent added:
Torrent created
Starting up torrent

Status (Show Peers)	Torrent	ETA	Downloaded	Uploaded	Down Rate	Up Rate	Stop All
OK (4/4 peers)		42h	431MB/1401MB	0B	7KBps	0Bps	Stop
OK (4/4 peers)		10h	291MB/700MB	49MB	11KBps	4642Bps	Stop
Seeding (6/6 peers)			701MB	141MB		3618Bps	Stop
Seeding (5/5 peers)			705MB	134MB		4881Bps	Stop
Seeding (4/4 peers)			701MB	107MB		7KBps	Stop
Seeding (0/0 peers)			792MB	0B		0Bps	Stop
Seeding (0/0 peers)			1038MB	0B		0Bps	Stop
Seeding (0/0 peers)			3872MB	0B		0Bps	Stop
Seeding (0/0 peers)			3300MB	0B		0Bps	Stop
Totals (9 torrents, 23 connected peers)			242MB	432MB	17KBps	20KBps	

Add Torrent:
From URL: Add torrent

Create Torrent:
Data to seed: I2psnark
Tracker: Select a tracker or http:// Create torrent

Configuration:
Data directory: I:\i2psnark (Edit i2psnark.config and restart to change)
Auto start: Total uploader limit: 30 peers
Up bandwidth limit: 50 KBps (Router Up BW / 2 recommended)
Use open trackers also: Announce URL: http://tracker.welterde.i2p/a

Mettez l'autostart, la limite d'upload à 50 et le nombre de peers à 30 max (vous pourrez changer ces données)

Par défaut, vos torrents (downloads et uploads) seront dans «c:/program files/I2P/I2Psnark », si vous voulez changer ca :

- Vous devez arrêter tous les téléchargements (mais j'imagine que vous n'en avez pas encore !), arrêter le routeur (dans la page principale, cliquez sur le bouton « shutdown » en haut à gauche... **c'est important** !! sinon vous coupez à l'arrache toutes les connections qui utilisent votre bande passante, ce n'est pas sympa pour les autres!!)
- dans c:/program files/I2P, éditez (avec notepad) le fichier i2psnark.config, et dans le fichier, à la ligne :
`i2psnark.dir=i2psnark`
Changez la valeur par le chemin que vous voulez ... par ex:
`i2psnark.dir=D:\i2psnark`
- Vous devrez redémarrer le routeur I2P et rouvrir votre Firefox « Internet Anonyme »

4.1.6.2 TELECHARGER AVEC I2PSNARK

En haut à gauche de l'interface I2PSnark, vous avez un lien « Postman »... c'est l'un des sites où vous pouvez trouver des torrents (idem, je l'ai mis en favori de barre personnelle, et je l'ouvre dans un nouvel onglet)... il y en a aussi sur <http://planet.i2p.to/> ... il y a d'autres sites, mais il faut chercher...

Sur l'épse de Postman, vous trouverez des torrents, cliquez sur leur nom et enregistrez le fichier torrent dans votre répertoire I2PSnark (voir plus haut).

Une fois ajouté, l'interface I2PSnark va intégrer le .torrent dans sa liste au bout de 3 minutes (un message en haut vous l'indique)

Une fois l'interface rafraîchie et le .torrent intégré, vous pouvez cliquer sur « start » situé à droite du fichier .torrent.

Et voilà... votre téléchargement commence.

Ce n'est pas hyper rapide, quoique ça dépend des peers et de la bande passante partagée. J'ai téléchargé un film (libre) à environ 70 ko/s, ce qui n'est pas si mal pour du p2p anonyme, et c'est le prix à payer pour cet anonymat...

4.1.6.3 UPLOADER (PARTAGER) DES FICHIERS AVEC I2PSNARK

Il faut créer un torrent, et l'intégrer (l'inscrire) dans un site (« tracker ») qui répertorie ces fichiers torrent (ex : Postman)

- Créer le torrent :

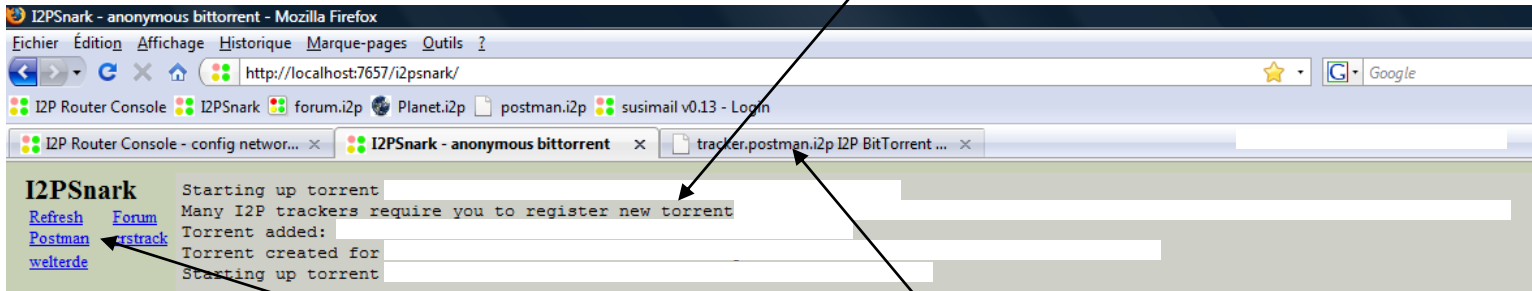
Dans votre interface I2PSnark, indiquez le fichier que vous voulez partager (ex : monfichierlibre.rar), après l'avoir mis dans votre dossier I2PSnark (voir plus haut)

The screenshot shows the I2PSnark web interface with three main sections:

- Add Torrent:** Includes a 'From URL' input field and an 'Add torrent' button. Below it, a note states: 'Alternately, you can copy .torrent files to I:\i2psnark. Removing that .torrent file will cause the torrent to stop.'
- Create Torrent:** Includes a 'Data to seed' input field (with an arrow pointing to it from the text above), a 'Tracker' dropdown menu (with an arrow pointing to it from the text below), and a 'Create torrent' button.
- Configuration:** Includes a 'Data directory' input field, an 'Auto start' checkbox, a 'Total uploader limit' of 30 peers, an 'Up bandwidth limit' of 50 KBps, and 'Use open trackers also' checked with an 'Announce URLs' field containing 'http://tracker.welterde.i2p/a'.

Sélectionnez le type de tracker (je vous conseille Postman, le plus utilisé)
Cliquez sur le bouton « Create Torrent »
Ça prend un peu de temps (1min ou 2) pour créer le torrent.

Une fois que c'est fait, en haut, vous verrez un message de ce type



Cela veut dire qu'il faut que vous enregistriez votre torrent sur un site qui les héberge.

C'est là où vous allez sur Postman (ouvert dans un nouvel onglet)

Il faut vous inscrire, cela ne prend pas longtemps et c'est gratuit...

Une fois inscrit sur Postman, allez dans « upload », rentrez tout ce qu'il y a à rentrer (n'oubliez pas le chemin du fichier .torrent !), un max d'infos c'est plus sympa... puis cliquez sur « Do It ! », voila, votre torrent est enregistré.

Dernier point, il faut démarrer votre upload... dans l'interface I2PSnark, cliquez sur « start all » à droite des torrents. Si vous devez arrêter les uploads, surtout cliquez bien sur « Stop All » et ensuite arrêtez correctement votre routeur I2P en cliquant sur « Shutdown » !, histoire que ceux qui téléchargent soient prévenus ;-)

4.1.7 POUR FINIR

Si vous ne voulez installer/utiliser qu'I2P, ce tutoriel s'arrête là. Les chapitres suivants sont consacrés à TOR, qui en addition avec I2P vous permettra de naviguer sur les sites « normaux » avec un anonymat renforcé.

Juste un petit mot pour vous inciter à **distribuer et faire la promotion d'I2P**... le réseau deviendra plus gros, la bibliothèque disponible s'agrandira aussi, et de même pour la bande passante d'où un meilleur taux de DL/UP...

N'hésitez pas à poser toute vos questions :

- sur le forum I2P, à la section « non english yadda yadda » :
<http://forum.i2p/index.php>
- sur ce nouveau forum francophone : <http://forum-fr.i2p.tin0.de/index.php>
- sur mon mail i2p :
ihavenoname@mail.i2p
ou bien
ihavenoname@i2pmail.org

BON SURF !!

4.2 TOR

4.2.1 ROUTEUR

Préparez votre routeur NAT et/ou firewall, il faudra ouvrir les ports suivants:
Le port 9001 en TCP et le port 9030 en TCP

4.2.2 INSTALLATION/CONFIGURATION DU PACK VIDALIA

Installez le pack téléchargé dans votre dossier « internet anonyme » en suivant les instructions (tout installer)

Cette partie est à suivre si vous voulez que les sites .i2p passent par I2P et que le reste (http et https) passe par TOR, ce qui permet une navigation générale quasi anonyme :

4.2.2.1 INSTALLER L'EXTENSION « TORBUTTON » SUR VOTRE FIREFOX « INTERNET ANONYME »

Disponible ici : <https://addons.mozilla.org/fr/firefox/addon/2275>

4.2.2.2 CONFIGUREZ PRIVOXY

allez dans « C:\Program Files\Vidalia Bundle\Privoxy », éditez le fichier « config.txt » et copiez/collez ces lignes tout au début du fichier :

```
#this directs ALL requests to the tor proxy
forward-socks4a / localhost:9050 .
#this forwards all requests to I2P domains to the local
I2P
#proxy without dns requests
forward .i2p localhost:4444
```

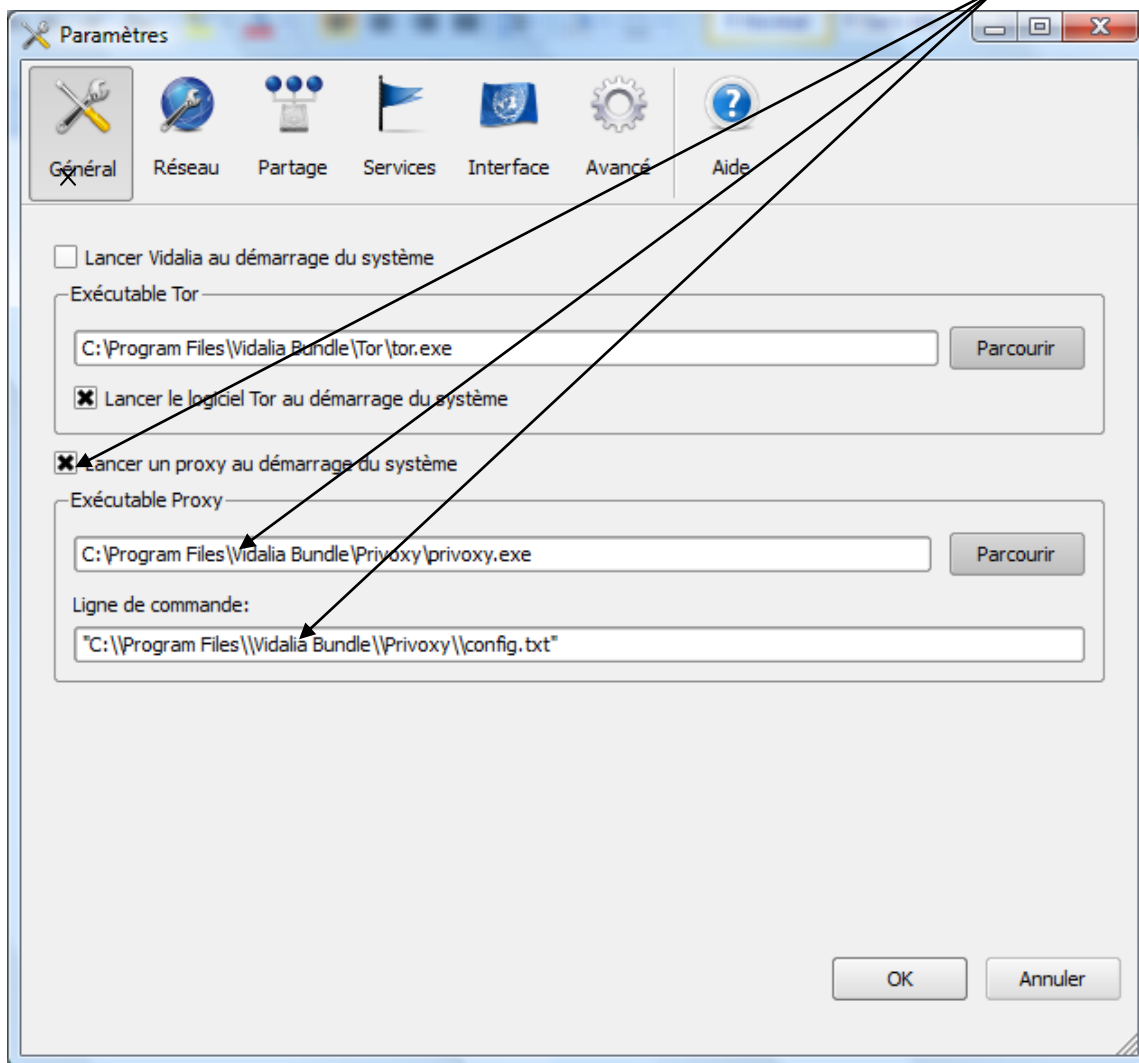
Sauvegardez le fichier et fermez-le.

4.2.2.3 CONFIGUREZ TOR POUR QUE PRIVOXY SE LANCE AUTOMATIQUEMENT AU DEMARRAGE DE CELUI-CI

Dans la barre des tâches, ouvrez Tor/Vidalia (icône en forme d'oignon)



Dans Tor/Vidalia, allez dans « paramètres », puis « général » et rentrez ces éléments :

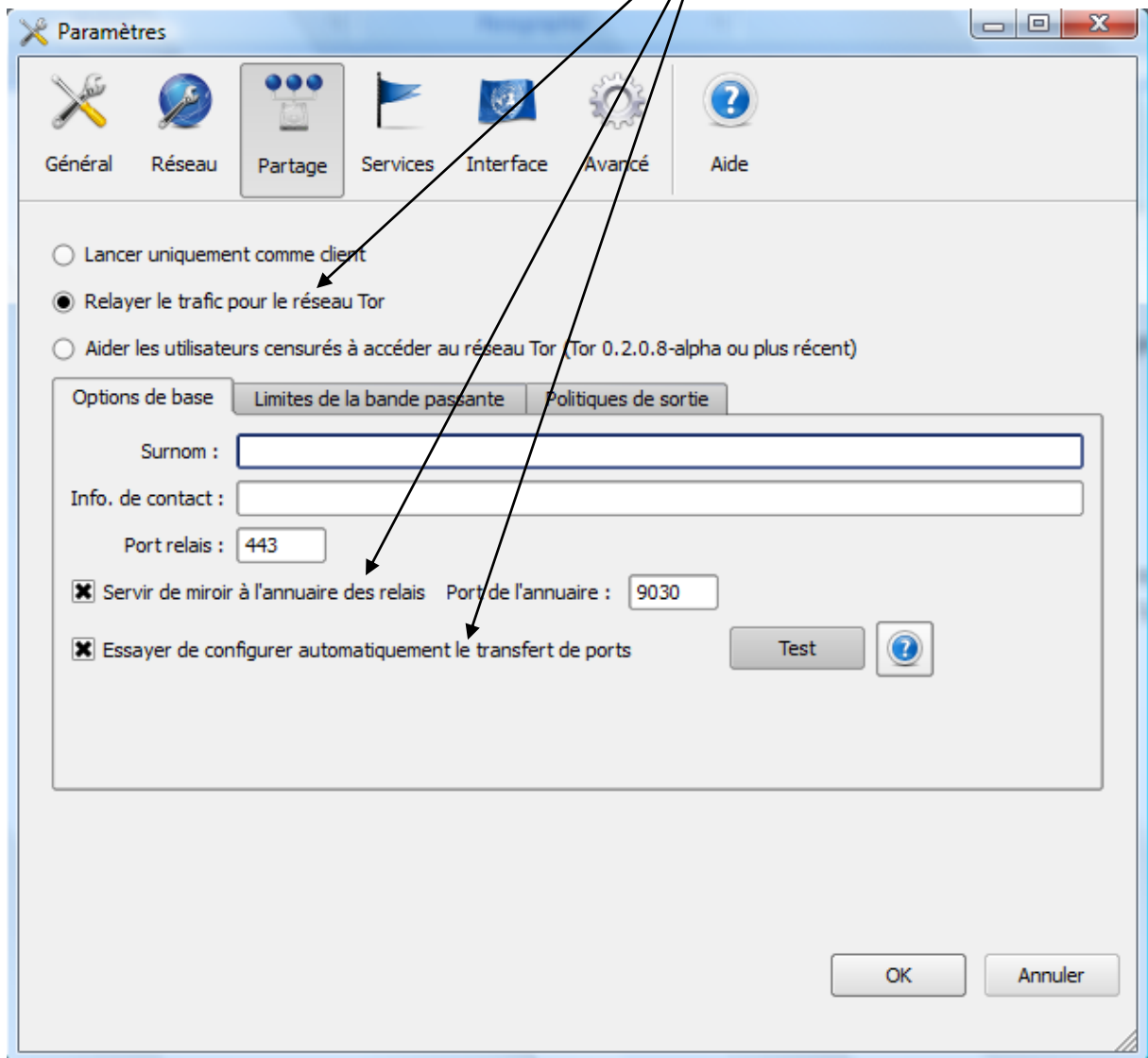


Si vous ne voulez pas que Vidalia se lance au démarrage de l'ordinateur, mais que lorsque vous lancez Vidalia, Privoxy et Tor se lancent, voici un petit truc :

- Dans « paramètres » → « Général » (voir ci-dessus), décochez « lancer Vidalia au démarrage du système », mais gardez coché « lancer le logiciel Tor au démarrage du système » et « Lancer un proxy au démarrage du système ».
- Puis allez dans votre menu « démarrer » → « exécuter » et tapez « msconfig » (sans les guillemets). Dans MSCONFIG, allez dans l'onglet « démarrage » et décochez « Vidalia », puis redémarrez le PC. Voilà, Vidalia ne démarrera pas à chaque boot du PC, mais lorsque vous le lancerez, Tor et Privoxy se lanceront en même temps.

4.2.3 PARTICIPER AU RESEAU TOR EN PARTAGEANT VOTRE BANDE PASSANTE

Allez dans « paramètres » → « partage » et rentrez ces paramètres :



Dans « limite de bande passante » choisissez ce qui vous convient.

Puis allez dans « politique de sortie » afin de choisir les sorties que vous autorisez sur votre relais. **Il est important de spécifier celles-ci, cela afin de vous protéger en cas d'utilisation de votre relais pour du P2P ou autre activité dont vous ne voudriez pas !**

Pour information, voici un extrait de la rubrique « aide » de TOR à propos des politiques de sortie :

« Les politiques de sortie vous permettent de spécifier les ressources Internet auxquelles les utilisateurs du réseau Tor peuvent accéder par le biais de votre relais. Par défaut, Tor utilise une liste de politiques de sortie qui empêche l'utilisation de certains services, notamment l'envoi de courriels (afin d'éviter les spams) et certains ports de partage de fichiers (afin de réduire l'usage abusif du réseau Tor).

Chaque case représente un type de ressources. Vous pouvez permettre ou refuser aux utilisateurs de Tor de passer par votre relais pour y accéder. Si vous décochez une case, les utilisateurs de Tor ne seront pas autorisés à accéder à la ressource correspondante à travers votre relais. Si la case *Autres services* est cochée, les utilisateurs de Tor pourront accéder aux services non couverts par les autres cases à cocher ou par la politique de sortie par défaut de Tor.

Pour information, le tableau suivant liste les numéros de ports des politiques de sortie. La colonne **Description** signale les ressources auxquelles les clients Tor pourront accéder à travers votre relais, si la case correspondante est cochée.

Case à cocher	Ports	Description
Sites web	80	Normal, navigation web non chiffrée
Sites web sécurisés (SSL)	443	Accès aux sites web sécurisés
Téléchargement des courriels (POP, IMAP)	110, 143, 993, 995	Téléchargement des courriels (ne permet pas d'en envoyer)
Messagerie instantanée (IM)	703, 1863, 5050, 5190, 5222, 5223, 8300, 8888	Applications de messageries instantanées telles que Jabber, MSN Messenger, AIM et ICQ
Chat (IRC)	6660-6669, 6697	Clients et serveurs IRC
Autres services	*	Toutes les autres applications non couvertes par les précédentes cases à cocher

Si vous ne voulez pas autoriser les utilisateurs de Tor à sortir du réseau par votre relais, vous pouvez décocher toutes les cases. Même dans ce cas, votre relais est utile pour le réseau Tor, car il permet encore aux utilisateurs de s'y connecter. Il permet également de relayer du trafic entre les autres relais Tor. »

4.2.4 UTILISATION DE TOR

Ouvrez Firefox « Internet Anonyme », et cliquez sur le texte ou l'icône en bas à droite « Tor inactif » (« torbutton »), il passez au statut « Tor actif », et vous voilà sur le réseau Tor !



Vous pouvez configurer (par un clic droit sur cet icône) Torbutton pour qu'il soit actif au démarrage de Firefox (je vous le conseille fortement)

**/\ \ IMPORTANT / **

Si vous voulez quitter Tor et que vous partagez de la bande passante, allez dans Firefox et cliquez sur le Tor-button pour qu'il indique « Tor inactif », et ensuite, ouvrez Vidalia et cliquez sur « arrêter Tor », il vous proposera de fermer « gracieusement » Tor, acceptez. De cette façon, les bénéficiaires qui passent par votre relai auront le temps de se rediriger.

4.2.5 POUR ALLER PLUS LOIN DANS L'ANONYMAT AVEC TOR

Comme je l'ai indiqué plus haut, de nombreux plugins tels que Flash, Java, JavaScript... récupèrent et envoient des informations vous concernant (adresse IP, historique de navigation...)

Si vous désirez optimiser au maximum votre anonymat (au détriment du confort visuel sur Internet), vous pouvez appliquer ces quelques recommandations :

- Contrôlez Java/JavaScript, en installant l'addon QuickJava, disponible ici : <https://addons.mozilla.org/en-US/firefox/addon/1237>
Il vous permettra d'activer/désactiver à la volée Java et JavaScript
- Désactivez Flash, en utilisant l'addon FlashBlock, disponible ici : <https://addons.mozilla.org/en-US/firefox/addon/433>
- Empêchez Firefox de dévoiler vos derniers sites visités :
 - Dans la barre d'adresse, rentrez :
About:config
 - Puis cherchez :
network.http.sendRefererHeader
 - Et changez la valeur par 0 (zéro)

D'autres techniques existent, n'hésitez pas à consulter les sites/forums qui discutent de ces applications.