Tutoriel d'introduction à TOR.

v 1.0

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.

Ce tutoriel s'adresse aux utilisateurs de windows + firefox.

Site officiel de TOR :
http://www.torproject.org

We are Anonymous.
We are Legion.

Qu'est-ce que TOR ?

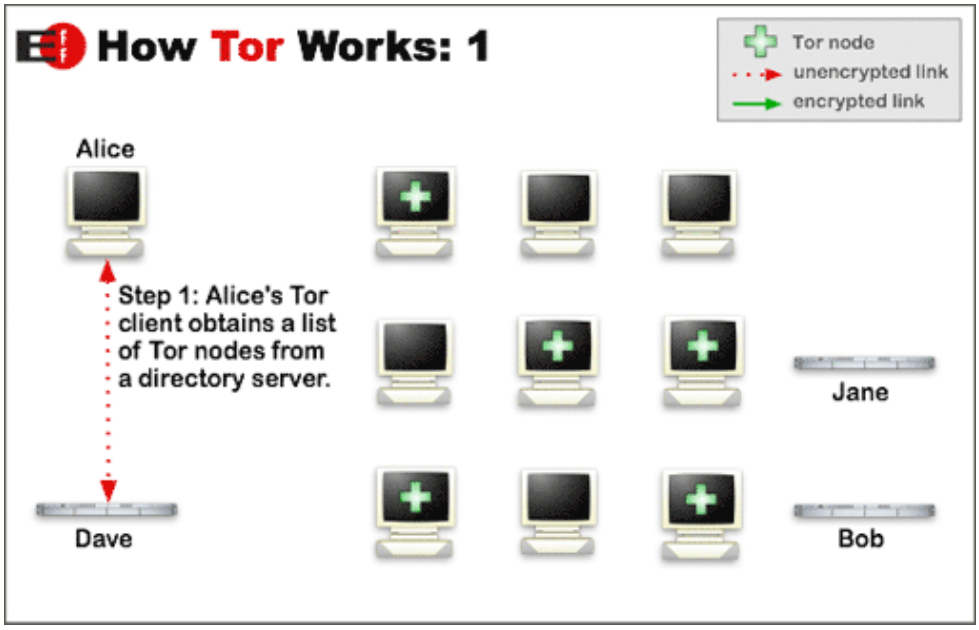
Tor est, à la fois, un logiciel libre et un réseau ouvert qui permet de se défendre contre une forme de surveillance de réseau qui menace les libertés individuelles et l'intimité, les activités commerciales, les mises en relations, ainsi que la sécurité de l'État. Cette surveillance est connue sous le 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 qui observe votre connexion internet puisse prendre connaissance des sites que vous avez visité. Il empêche également les sites que vous avez visités de connaître votre position géographique. Tor fonctionne avec beaucoup de vos applications existantes, comme les navigateurs web, les clients de messagerie instantanée, les connexions à distance et d'autres applications basées sur le protocole TCP.

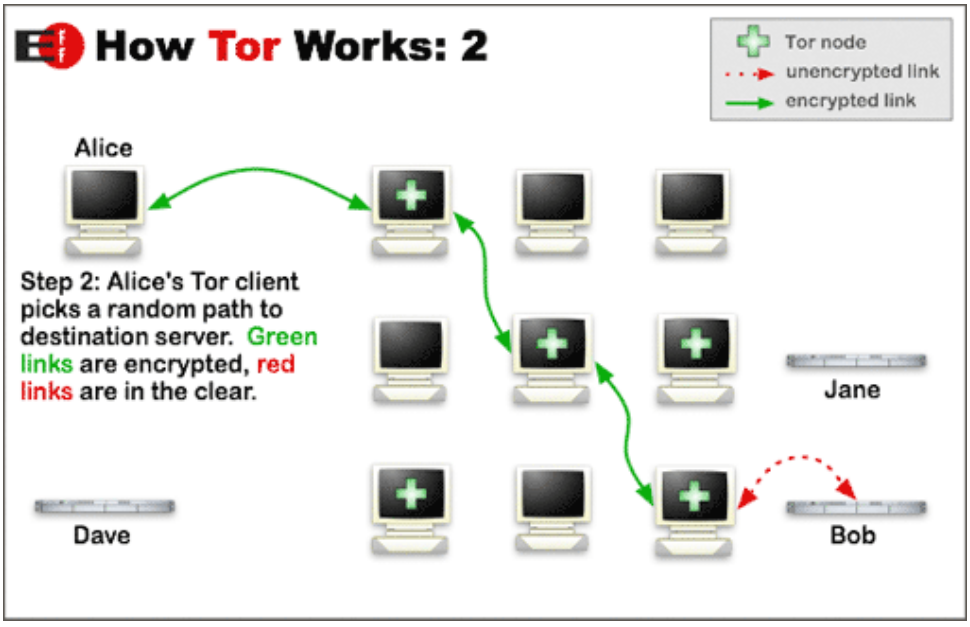
Des centaines de milliers de personnes à travers le monde utilisent Tor pour une multitude de raisons : les journalistes et les blogueurs, les défenseurs des Droits de l'Homme, les agents d'application des lois, les soldats, les entreprises, les citoyens de gouvernements répressifs, ou les simples citoyens. Consultez la page sur Qui utilise Tor? pour connaître quelques exemples typiques d'utilisateurs Tor. Consultez la vue d'ensemble pour une explication plus complète de ce que Tor fait et pourquoi la diversité des 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 avec le nombre d'utilisateurs et le nombre de volontaires pour faire tourner un relais (ce n'est pas aussi compliqué qu'on peut le croire, et cela peut améliorer votre propre sécurité de manière significative).

Principe de fonctionnement

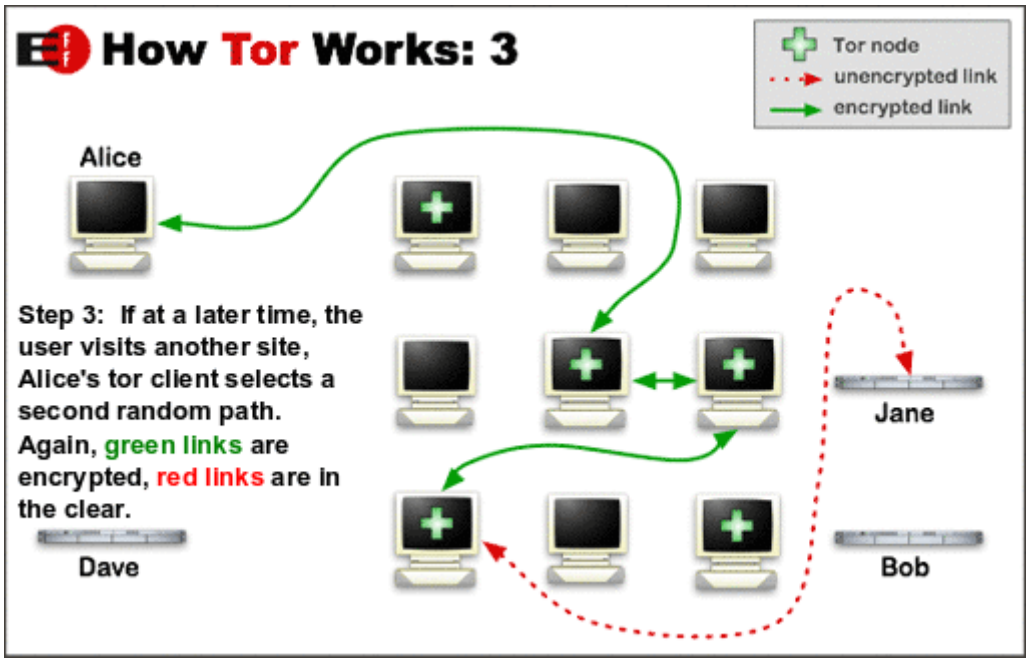
Alice, qui vient d'installer TOR sur son PC souhaite surfer anonymement. TOR consulte la liste des relais disponibles sur un des "relais/annuaire" disponibles (dans ce cas, le relais TOR installé sur le serveur **Dave**).



Une fois la liste des relais obtenues, lorsqu'**Alice** va vouloir surfer anonymement, TOR va définir un chemin aléatoire par lequel les données vont passer. Dans cet exemple, elle veut consulter anonymement un site internet qui se trouve sur un serveur qui s'appelle **Bob** (ce serveur ne fait pas partie du réseau TOR, et il héberge des sites internet de la manière la plus classique qui soit). Au lieu de consulter directement le serveur **Bob**, les relais TOR font transiter les informations d'un relais à l'autre. Les connexions sont toutes cryptées sauf celles entre le dernier relai et le serveur **Bob**.



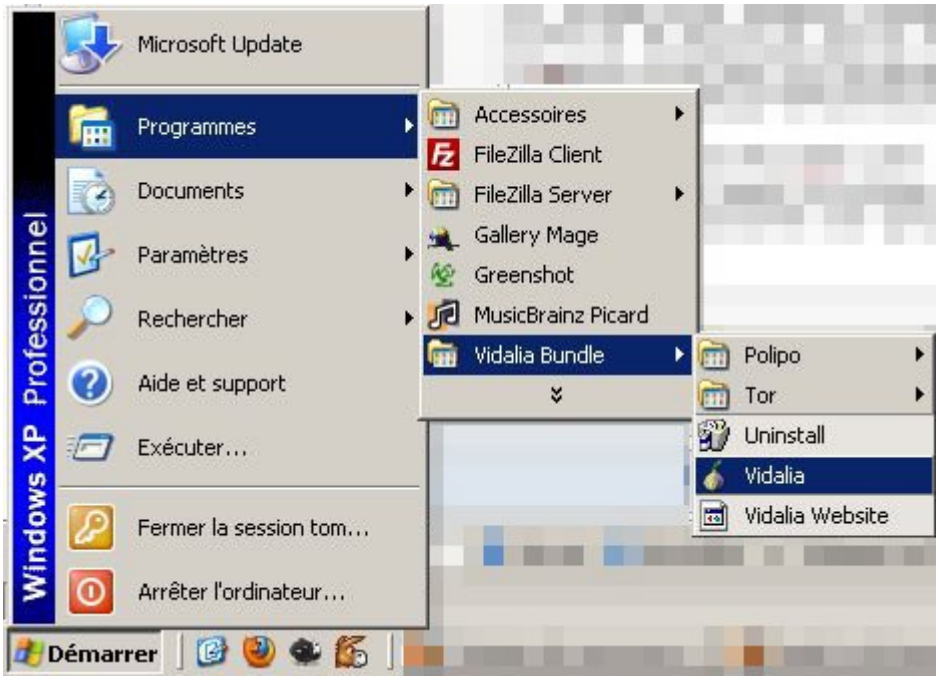
Si plus tard Alice souhaite consulter un autre site, le chemin par lequel vont transiter ses données aura été modifié afin de brouiller un peu plus les pistes :



Comment utiliser TOR ?

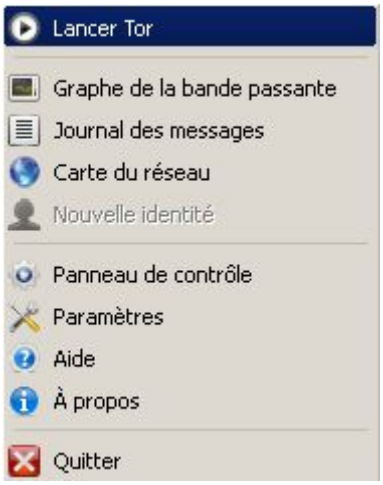
Téléchargez le pack d'installation pour windows et installez-le (laissez les options par défaut, contentez-vous de cliquer sur suivant/installer).

A la fin du setup, cochez la case pour lancer les composants installé et cliquez sur terminer. Si vous n'avez pas coché la case, vous devrez lancer manuellement Vidalia, l'interface graphique de TOR :



L'icône suivante doit maintenant se trouver en bas à droite de votre écran :

La croix rouge sur l'oignon signifie que Vidalia est lancé mais que TOR ne l'est pas.
Faites un clic droit sur l'icône puis cliquez sur *Lancer TOR* :



L'oignon va passer au jaune puis au vert une fois que TOR sera opérationnel :

Le fait que TOR fonctionne ne signifie pas que vous pouvez utiliser votre connexion de façon anonyme. Il faut encore configurer les logiciels que vous souhaitez utiliser anonymement afin qu'ils sachent qu'ils doivent utiliser TOR. Je vais vous expliquer comment faire avec firefox étant donné que la consultation de sites web est l'utilisation la plus courante mais gardez bien en tête que chaque logiciel qui utilise internet nécessite une reconfiguration pour utiliser TOR. Vous devrez indiquer à vos programmes de passer par un proxy (localhost:8118[1]) et un hôte SOCKS (localhost:9050[1]).
Mais avec firefox, vous allez voir que c'est bien plus convivial.
Le pack que vous avez installé au début de ce tutoriel, en plus d'avoir installé Vidalia et TOR a également installé un plugin pour firefox qui s'appelle *TOR Button*. Ce plugin vous évite d'avoir à configurer manuellement firefox pour qu'il utilise TOR. Il vous suffit maintenant d'un clic pour utiliser ou non TOR avec firefox.

Lancez firefox et vous verrez qu'en bas à droite de firefox, une case a fait son apparition :

Cette case vous permet non seulement de voir le statut actuel de TOR au sein de firefox mais aussi d'en changer l'état. Pour ce faire, il suffit de faire un clic gauche dans cette case et voilà le résultat :

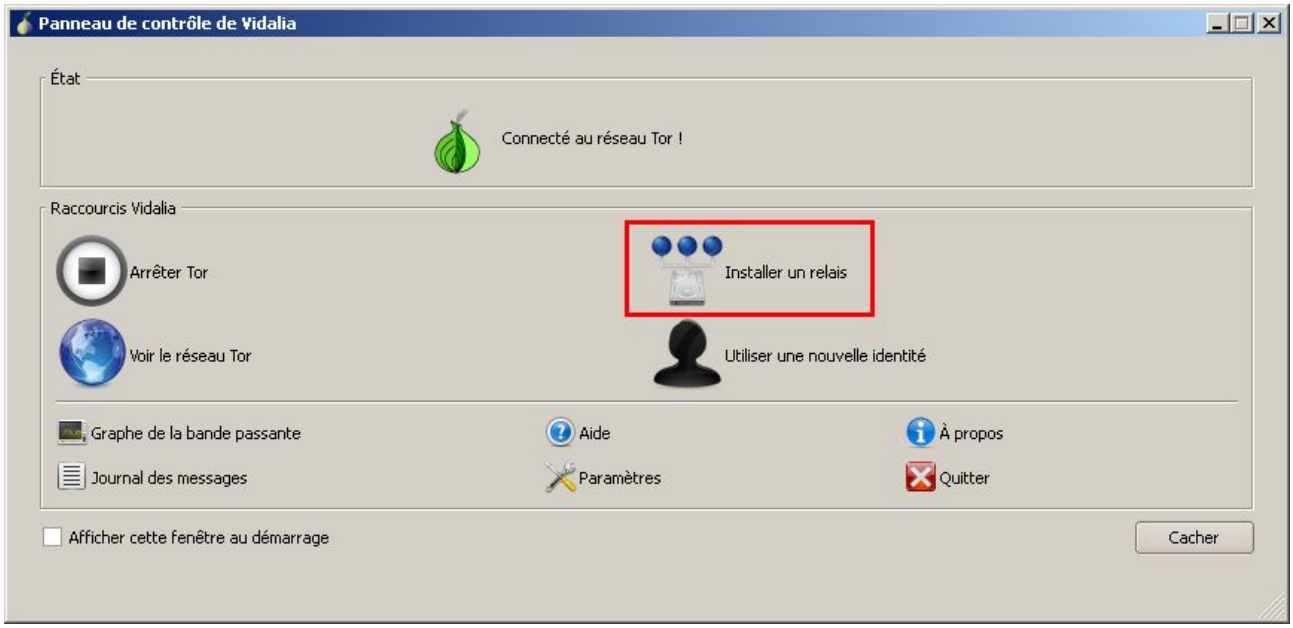
Pour vérifier que vous surfez en passant effectivement par le réseau TOR, une page de test a été mise à disposition par l'équipe de développement de TOR. Rendez-vous sur cette page et vous saurez immédiatement si vous utilisez le réseau TOR ou non :
https://check.torproject.org/

[1] : Ces valeurs de configuration seront valables si vous n'avez pas changé les ports dans la configuration de TOR.

Configuration d'un relais TOR (en seulement quelques clics) :

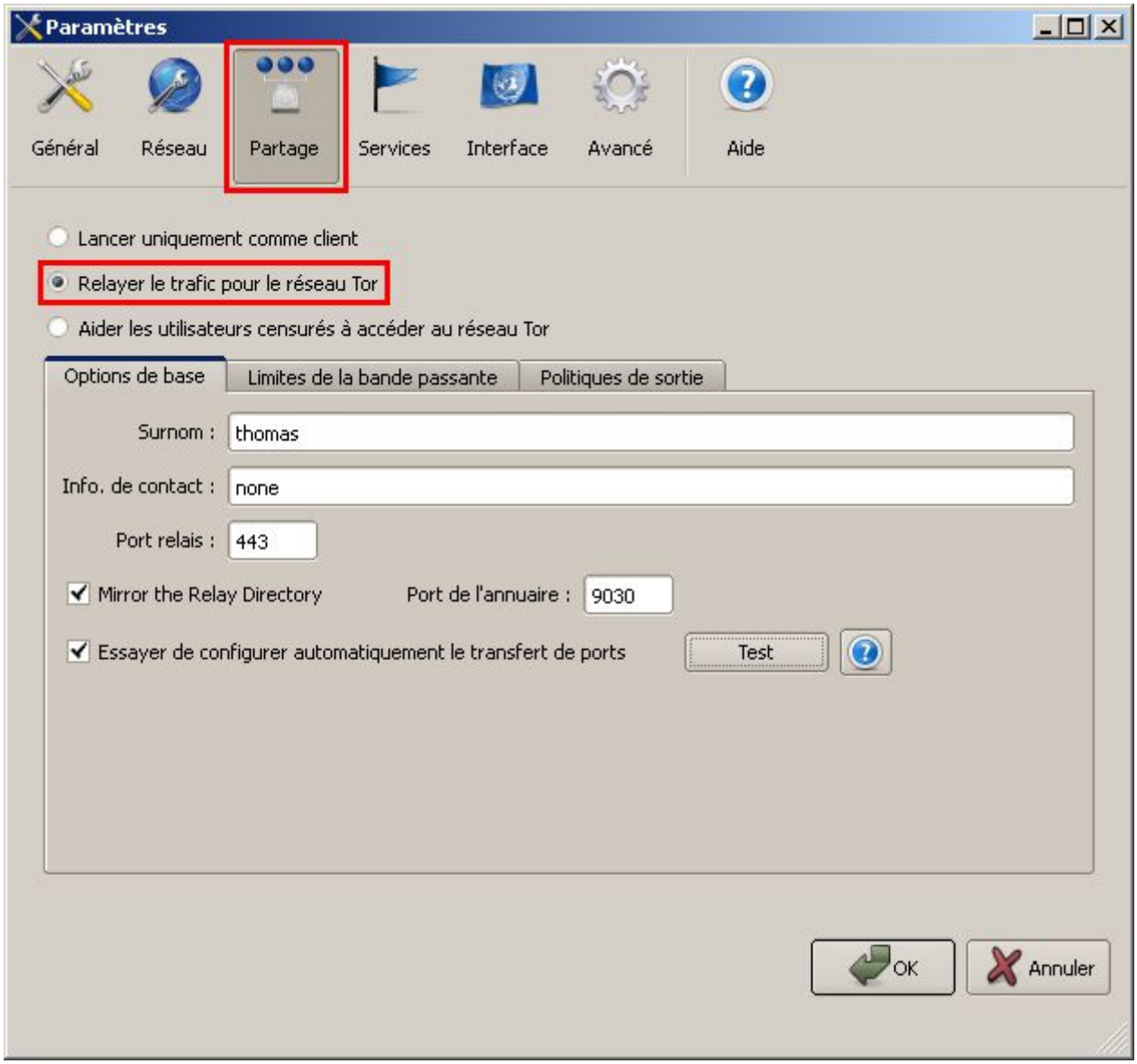
Installer un relais TOR sur votre ordinateur permet :
- d'augmenter votre sécurité (puisque votre ordinateur sert de relais, impossible de déterminer si la consultation du site X ou Y a été faite par vous ou bien par un autre utilisateur de TOR que vous avez relayé)
- d'améliorer la qualité du réseau TOR. Plus de relais, c'est plus de "chemins" disponibles sur le réseau donc plus de sécurité. Plus de relais, c'est aussi plus de bande passante donc un réseau qui est plus rapide et moins facilement saturé.

Pour mettre en place le relai, double cliquez sur l'oignon en bas à droite de votre écran. Cette fenêtre apparaît :



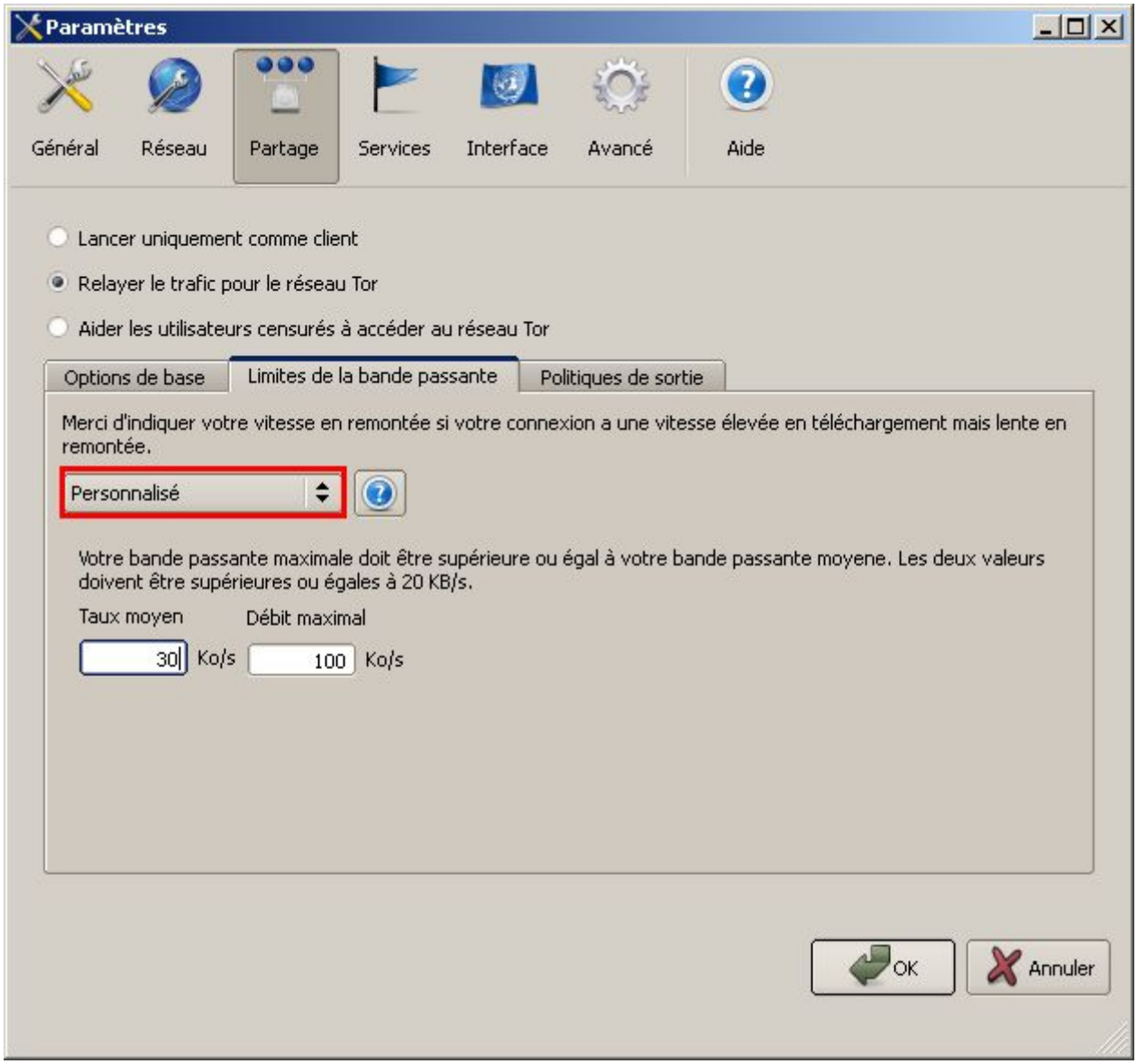
Cliquez sur *Installer un relais*.

La fenêtre suivante apparait :



Sélectionner l'option *Relayer le trafic pour le réseau TOR*.
Dans l'onglet *Options de base* :
- donnez le nom que vous voulez à votre serveur
- remplissez si vous le souhaitez *Info de contact* (une adresse mail pour que les admins du réseau TOR puissent vous contacter en cas de dysfonctionnement de votre relais)
- Cochez *Mirror the relay directory*

Dans l'onglet *Limite de la bande passante* :



- Sélectionnez *Personnalisé*
- Entrez les valeurs de votre choix (je vous fais un copier/coller de l'aide de TOR pour savoir à peu prêt quoi mettre comme valeur (il faut bien entendu que vous connaissiez le débit maximal de votre connexion pour faire ce réglage)).

> *Limites de la bande passante*
>
> *Un relais Tor peut consommer une grande quantité de bande passante. C'est la raison pour laquelle Tor vous permet de préciser le niveau de bande passante que vous souhaitez accorder au réseau Tor. Cela vous permet de faire fonctionner un relais Tor tout en conservant une connexion suffisante pour votre propre usage.*
>
> *Vous devez sélectionner dans la liste déroulante l'option qui correspond le mieux au débit de votre connexion. Si vous choisissez Personnalisé, vous pourrez paramétrer vous-mêmes les seuils.*

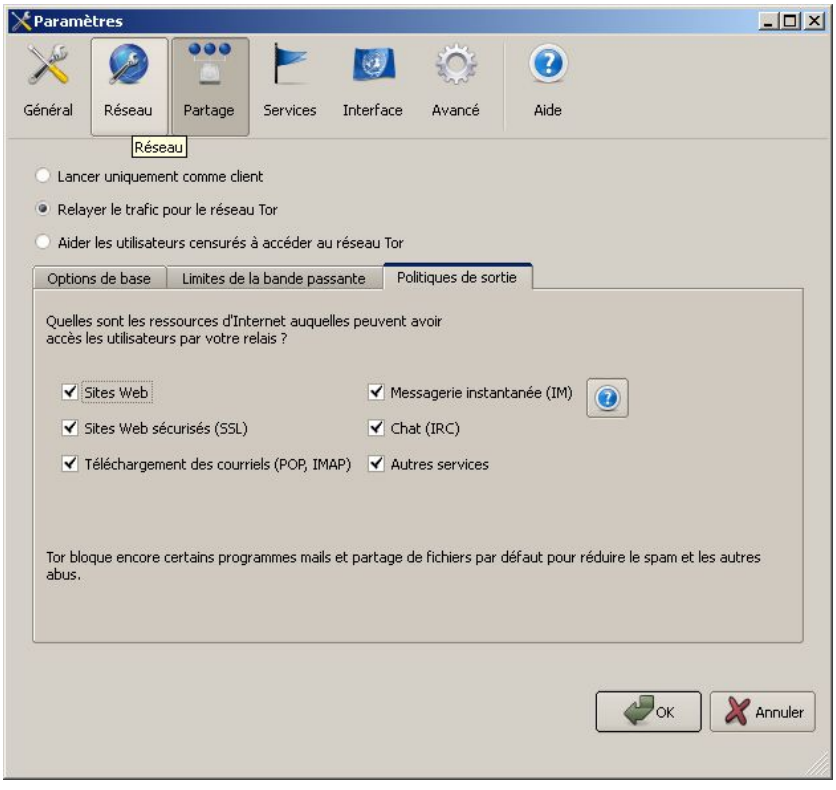
Limites personnalisées

Le débit maximal correspond au nombre d'octets utilisables pour répondre aux requêtes pendant les courtes périodes où le trafic est supérieur au débit moyen que vous avez spécifié, mais qui permet de respecter la moyenne sur une longue période. Un débit moyen bas et un débit maximal élevé améliorent le niveau de trafic à long terme en autorisant davantage de trafic lors des pics, tant que le débit moyen n'a pas été atteint. Si votre débit moyen est identique à votre débit maximal, alors Tor ne dépassera jamais ce débit. Le débit maximal doit toujours être supérieur ou égal au débit moyen.

Le débit moyen correspond à la bande passante moyenne maximale autorisée à long terme (en kilo-octets par seconde). Par exemple, vous pouvez choisir de contribuer au réseau Tor pour 2 méga-octets par seconde (2048 Kio/s) ou 50 kilo-octets par seconde (soit une connexion moyenne par cable). Tor a besoin au minimum de 20 kilo-octets par seconde pour faire fonctionner un relais.

Il est important de se rappeler que Tor mesure la bande passante en octets et non en bits. En outre, Tor comptabilise les octets entrants et non les octets sortants. De ce fait, si votre relais est également un miroir de l'annuaire des relais, vous enverrez davantage de données que vous n'en recevrez. Si vous constatez que cela constitue une contrainte trop forte pour votre bande passante, vous devrez penser à décocher la case Servir de miroir à l'annuaire des relais.

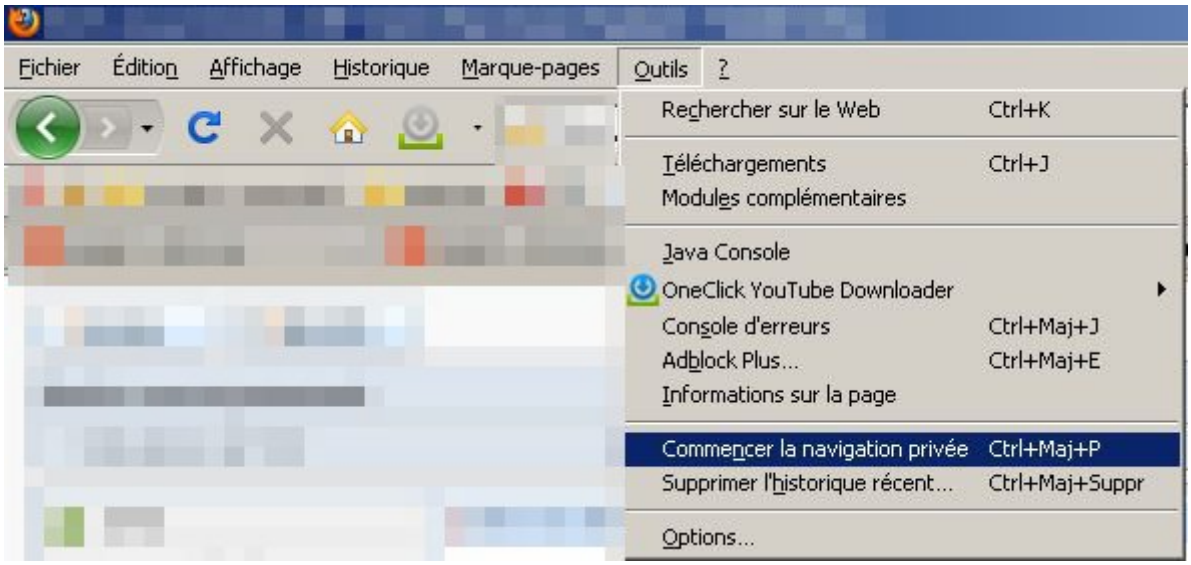
L'onglet *Politique de sortie* vous permet de choisir quel type de données votre relai TOR fera circuler. Si à vos yeux, certaines utilisations d'internet sont plus importantes que d'autres, ne cochez que les cases que vous souhaitez :



Maintenant que votre relai est configuré, il ne vous reste plus qu'à lui autoriser à communiquer avec le monde extérieur si jamais vous êtes derrière un routeur ou une machin-box. Si vous possédez un routeur, vous savez sans doute comment le configurer. Si vous possédez une machin-box, voilà une liste de tutoriels expliquant comment ouvrir des ports de communication pour chaque modèle de box.

Si vous voulez être sûr que votre relai TOR est bien opérationnel, vous pouvez consulter la liste des relais actifs en double-cliquant sur l'oignon en bas à droite de l'écran puis en cliquant sur V*oir le réseau*. Si vous avez choisi un nom de relais suffisamment original, vous devriez pouvoir le retrouver dans cette liste (il se peut que votre relais mette un peu de temps avant d'apparaitre dans la liste. Attendez 20 ou 30 minutes avant de chercher votre relai dans la liste).
Une autre façon de vérifier si votre relai est opérationnel est de retourner consulter la page https://check.torproject.org/ sans avoir activé TOR dans firefox. Si votre relai est opérationnel, le test sera toujours positif (puisque votre ordinateur fait maintenant partie du réseau TOR).

N'hésitez pas à utiliser la navigation privée de firefox si vous souhaitez ne pas trop laisser de traces sur votre ordinateur des sites que vous consultez :



Une fois ce mode activé, firefox n'enregistrera pas les URL des sites que vous visitez, les mots ou expressions que vous saisissez dans les formulaires ou les barres de recherches, les cookies des sites que vous visitez.