"Changer" son adresse IP

- Helpdesk - Tutoriels, astuces -

Date de mise en ligne : dimanche 25 décembre 2011

Description :

Il peut arriver, pour diverses raisons, qu'on veuille modifier son adresse IP, par exemple pour contourner des limitations d'usage, un bannissement sur un forum, par sécurité, etc.. Voici quelques façons de le mettre en oeuvre.

Inside Electronic Pipo

Prenons un exemple type : tranquillement installé, vous regardez un film sur Mégavideo, un grand site de streaming. Au bout d'une heure, vous êtes vraiment dedans, ça vous plait, il y a du suspense, de l'action, que sais-je... puis vient le drame : vous avez dépassé la limite quotidienne de 72 minutes.

Le phénomène est bien connu, et bien triste. Pour plein d'autres raisons, il peut vous arriver de vouloir changer votre adresse IP. Comment faire ?

Notons en préambule que cet article n'est pas une incitation à toute activité illégale ou frauduleuse : par exemple, contourner la limitation de Mégaupload ou un bannissement sur un forum concerne uniquement les rapports entre vous et ces sites Web, votre acceptation de leurs conditions d'utilisation, et votre éthique.

IP statique ou dynamique ?

Si vous souhaitez changer d'IP, vérifiez d'abord son type : statique ou dynamique ? Cela dépend de votre abonnement Internet. Une vérification simple et efficace consiste à vérifier votre adresse IP, à débrancher-rebrancher le routeur, et à voir si l'IP a changé.

Si l'IP a changé, votre IP et dynamique et vous avez déjà réussi à faire ce que ce tuto tente d'expliquer... Sinon, votre IP est statique et il faudra être un peu plus malin.

Je ne connais pas tous les fournisseurs, mais je sais qu'un abonnement Free (Freebox) et Numéricable vous fourniront une IP statique ; un abonnement Orange (Livebox) vous fournira une IP dynamique.

Utiliser un Proxy

La solution de base à tous vos soucis et à tous les kévins en manque de pseudo-piratage internet, c'est le proxy. Cela consiste à ce qu'il y ait un intermédiaire entre vous et le site que vous souhaitez visiter : ce dernier peut uniquement connaître l'adresse IP de l'intermédiaire et non votre IP réelle. Ainsi vous faites croire au site que vous avez une IP qui n'est en réalité pas la vôtre.

Il existe diverses façons d'utiliser un proxy. La plus simple reste sans doute le plug-in Firefox "FoxyProxy". Celui-ci automatise le système : il vous suffit de saisir l'adresse d'un proxy ; FoxyProxy se charge du reste.

Si vous êtes sur Chrome, vous pouvez utiliser un plug-in similaire : Proxy Switchy.

Si vous êtes sur Safari, c'est un peu plus compliqué. Je ne connais pas la configuration sur Windows, mais ça se passe dans vos préférences réseau. Sur Mac, allez dans les Préférences de Safari, puis "Avancé", puis "Proxys : Modifier les réglages". En général, vous aurez uniquement besoin d'un proxy HTTP et/ou HTTPS. Saisissez les informations nécessaires : IP du Proxy et port (8080). Confirmez puis cliquez sur "Appliquer". Vérifiez ensuite que vous êtes bien anonyme.

Si vous êtes sur Opera, vous pouvez configurer le proxy directement sur le navigateur, dans Préférences > Avancé > Réseau > Serveurs Proxy...

Pour d'autres navigateurs, c'est globalement la même chose et vous ne devriez pas avoir trop de problèmes.

Attention : un proxy n'est pas un garant d'anonymat. Il vous permet simplement d'avoir un intermédiaire fiable qui évite qu'un site connaisse votre adresse IP.
Ne pensez pas qu'un proxy permet de faire ce que vous voulez : si vous commettez une action illégale, par exemple le piratage d'un mot de passe, et qu'une plainte est déposée, les autorités peuvent simplement recueillir vos informations auprès du proxy que vous utilisez.
Ne pensez pas non plus qu'un proxy est un garant de sécurité. Il est en effet assez facile pour quiconque avec un minimum de compétences informatiques de vous "tracer", c'est-à-dire de remonter le fil de vos connexions pour identifier votre adresse IP. La méfiance est surtout de mise dans des environnements à risque que vous méconnaissez, par exemple sur des serveurs IRC.

Quel proxy utiliser ?

De très nombreux proxys publics et fiables sont disponibles. Vous pouvez les trouver sur de nombreux sites de référencement, dont voici un bon exemple.. Les proxys dits "transparents" sont inutiles car ils ne masquent pas efficacement votre adresse IP. Les proxys de type "Elite/Anonymous" sont plus efficaces.

Si le premier proxy ne fonctionne pas, essayez-en d'autres. En général, au bout de quelques tentatives, ça fonctionne assez bien. Votre connexion sera cependant naturellement ralentie.

Utiliser des sites spécialisés

Ces sites sont, disons, "la base" : vous les avez peut-être déjà utilisés au CDI de votre ancien collège ou lycée, pour visiter des sites bloqués par les filtres du réseau. Voici un exemple typique : Anonymouse.

Il vous suffit de rentrer l'adresse pour que le site vous serve de relaie et se connecte au site que vous souhaitez visiter.

Cette solution est très peu recommandable, pour trois raisons principales :

- Les proxys sont en général "transparents"

- Ils sont connus de nombreux sites et filtres
- Ils bloquent des scripts ou empêchent certains logiciels de fonctionner efficacement (Flash, Shockwave, etc.)

Un logiciel spécialisé : TOR

Si vous rencontrez des problèmes dans la configuration de votre proxy ou que vous ne trouvez pas de proxy efficace, ou que vous souhaitez un bon anonymat, vous pouvez utiliser TOR. En gros, TOR consiste en un réseau dense de différents serveurs : votre ordinateur s'y connecte en chaîne, mais chaque intermédiaire ne connaît les informations de connexions que de l'intermédiaire précédent et de la destination suivante ; par ailleurs, chaque chemin de connexion est encrypté. Pour plus d'information, consultez cette page.

La façon la plus facile d'utiliser TOR est d'utiliser son navigateur dédié : Il vous suffit de télécharger le client TOR Browser, de l'installer, puis de lancer le navigateur pour jouir d'un anonymat de bonne qualité. C'est certain : votre adresse IP sera bien planquée.

Attention : encore une fois, TOR n'est pas un garant d'anonymat et de sécurité complets. De nombreux utilisateurs compétents dénoncent de nombreuses failles dans le fonctionnement de TOR qui peuvent par exemple permettre à des crackers d'utiliser le réseau à leur profit. Par ailleurs, l'IP n'est pas le seul moyen d'obtenir des informations : votre navigateur, notamment, laisse également de nombreuses traces.

Toutes ces solutions ne fonctionnent pas pour certains logiciels, pour lesquels il est difficile voire impossible de configurer un proxy efficacement. C'est notamment le cas de Java.