Publié sur ***COAGUL*** (https://coagul.org/drupal)

Installer une passerelle Tor sur son serveur

dim, 08/06/2014 - 13:19 — Dlareg

Serveurs [1] | Débian [2] | Tor [3]

Tor, The Onion Router, est un réseau informatique superposé mondial et décentralisé. Il est composé de routeurs organisés en couches, appelés nœuds, qui transmettent de manière anonyme des flux TCP. Le réseau Tor peut ainsi rendre anonymes tous les échanges internet basés sur le protocole de communication TCP.

Lorsqu'un utilisateur envoie des données, elles passent par plusieurs relais (des « nœuds »), trois au minimum. Chaque relai chiffre les données avant de les transmettre à un autre relai qui les chiffre et ainsi de suite. Ainsi « le chemin des données est indéchiffrable ». L'adresse IP de l'expéditeur est intraçable.

« Tor fait comme quelqu'un qui marche dans la neige et efface ses traces de pas derrière lui », citation de Bikepunk.

Tor permet donc de contourner la censure sur Internet et l'absence de surveillance fait que des dérives sont possibles, mais comme avec n'importe quel outil.

Il est a noter que 60 % des financements proviennent du gouvernement américain pour le soutien à la liberté d'expression et à la recherche scientifique.

Si vous habitez dans une région où il n'y a que peu ou pas de censure, vous pouvez avoir envie de mettre en place un relai Tor pour aider ses autres usagers à accéder à un internet non-censuré.

Comme toutes les solutions de chiffrage, le principal défaut du réseau Tor est sa lenteur. Vous pouvez contribuer à y remédier en créant un serveur, sachant que plus il y aura de serveurs Tor, plus le réseau sera rapide.

Join the Tor challenge, Run a Tor relay today est un défi organisé par l'Electronic Frontier Foundation :

https://www.eff.org/torchallenge [4]

Rejoingnez le défi, mettez en place un relai aujourd'hui.

Pré-requis

Vous pouvez mettre en place Tor sur n'importe quel ordinateur mais idéalement il vaut mieux fournir un service en continu et donc l'installer sur un ordinateur qui sert déjà des services. Vous pouvez mettre en place un serveur auto-hébergé rien que pour mettre en place un relai Tor mais l'idée est plutôt de mettre à disposition un serveur déjà en production que l'on peut occuper en partie pour offrir une partie de votre bande passante.

Dans le présent article l'installation de Tor se fait sur une distribution Debian, si vous devez installer depuis les sources du projet pour votre distribution, veuillez impérativement vérifier la somme de l'archive.

Le relai peut être un nœud sortant ou un nœud de transfert. L'adresse IP du nœud sortant sera celle divulguée en lieu et place de celui qui navigue vers un contenu y compris si celui-ci est potentiellement illégal, mais présente l'avantage de masquer votre propre navigation. Dans le cas d'un nœud de transfert, le service relaie uniquement les requêtes. Cet article vous propose la configuration rapide d'un nœud de transfert. Celui-ci utilise moins de bande passante, il est donc approprié pour une connexion internet grand public ; la configuration est simple.

Il vous faudra également avoir configuré votre serveur pour qu'il mette à jour l'heure en NTP pour qu'il soit toujours à l'heure.

Installation

```
# apt-get install tor
```

À la fin de l'installation le service est lancé mais n'est pas configuré.

```
# service tor status
tor is running.
#
```

Configuration

Configuration de Tor

Il faut éditer le fichier de configuration, décommenter et modifier certaines lignes :

```
# vim /etc/tor/torrc
```

```
# port du socket
SocksPort 9050
# Avoir des logs de notification
Log notice file /var/log/tor/notices.log
# répertoire des données
DataDirectory /var/lib/tor
# le port utilisé depuis l'extérieur par le service Tor, c'est celui qu'il faudra ouvrir dans votre pare-feu et sur votre boîtier internet (Box du FAI).
ORPort 9001
# adresse du nœud Tor
Address <adresse IP publique ou nom DNS de votre machine>
# le nickname est plus simple qu'avec la clé pour les utilisateurs qui veulent se référer à votre nœud.
Nickname <un nom de relai>
# bande passante alloué, le stric minimum étant 20 KB
RelayBandwidthRate 20 KB # Throttle traffic to 100KB/s (800Kbps)
# indique une limite haute, en cas de gros trafic sur le serveur, qui permet d'apporter un peu de "punch" en cas de besoin, visiblement le double soit 40 KB
RelayBandwidthBurst 40 KB # But allow bursts up to 200KB/s (1600Kbps)
# Pour être contacté en cas de mauvaise configuration de votre nœud, la clé GPG permet de recevoir des messages chiffrés
ContactInfo 0xCléGPG pseudo adresse@mail.org
# ou si vous n'avez pas de clé GPG
ContactInfo pseudo adresse@mail.org
# le nœud est non sortant
ExitPolicy reject *:* # no exits allowed
# Un pont est un relais non répertorié qui permet aux gens de se rendre à des relais normaux, faire de votre machine un nœud entrant
BridgeRelay 1
```

Créer une clé GPG si besoin

```
$ gpg --gen-key
```

Réponse aux questions posées :

- clé RSA
- 4096 bits
- durée
- pseudo
- adresse mail

- pas de commentaire
- taper une VRAI passphrase

Envoyer la clé sur un serveur de clé, ce qui permet à ceux qui veulent chiffrer un message à votre intention de le faire

```
$ gpg --send-keys XXXXXXXX
```

Réaliser un certificat de révocation qu'il faudra mettre à l'abri

```
$ gpg --gen-revoke XXXXXXXX > revoke.txt
```

Configuration de votre boîtier FAI

Ouvrir le port 9001 et le rediriger vers la machine hébergeant Tor

Redémarrer le service Tor

```
# service tor restart
```

Si le fichier de configuration n'est pas bon, le service renvoit une notice.

Pour vérifier que tout va bien il faut regarder les journaux du serveur hébergeant le service Tor :

```
# tail -f /var/log/tor/notices.log
```

Le message suivant doit apparaître :

```
[notice] Now checking whether ORPort adresseIP:9001 is reachable... (this may take up to 20
minutes -- look for log messages indicating success)
```

Plus tard apparaît le message suivant, tout est en ordre :

```
[notice] Self-testing indicates your ORPort is reachable from the outside. Excellent.
Publishing server descriptor.
```

La clé de votre nœud

La clé de votre nœud se trouve dans le fichier /var/lib/tor/fingerprint :

```
# cat /var/lib/tor/fingerprint
```

Liens

Le réseau Tor sur Wikipédia :

https://fr.wikipedia.org/wiki/Tor_%28r%C3%A9seau%29 [5]

Tor : un internet parallèle incontrôlable financé par le gouvernement américain :

http://www.toulouseinfos.fr/index.php/actualites/societe/8127-tor-un-internet-parallele-incontrolable-finance-par-le-gouvernement-americain.html [6]

Comment contourner la censure sur Internet ? Livre numérique réalisé et publié sur Floss Manuals :

http://fr.flossmanuals.net/comment-contourner-la-censure-sur-internet/ [7]

D'autres informations intéressantes pour aller plus loin dans la configuration de Tor :

http://blog.pastoutafait.fr/billets/installer-serveur-tor-ubuntu [8]

Licence Creative Commons by-sa 3.

URL source: https://coagul.org/drupal/publication/installer-passerelle-tor-sur-son-serveur

Liens:
[1] https://coagul.org/drupal/rubrique/serveurs
[2] https://coagul.org/drupal/tag/d%C3%A9bian
[3] https://coagul.org/drupal/tag/tor
[4] https://www.eff.org/torchallenge
[5] https://fr.wikipedia.org/wiki/Tor_%28r%C3%A9seau%29
[6] http://www.toulouseinfos.fr/index.php/actualites/societe/8127-tor-un-internet-parallele-incontrolable-finance-par-le-gouvernementamericain.html
[7] http://fr.flossmanuals.net/comment-contourner-la-censure-sur-internet/
[8] http://blog.pastoutafait.fr/billets/installer-serveur-tor-ubuntu