Point D’accès Tor

Ajouter Tor à notre point d’accès Wifi n'est pas très compliqué.

Tor sur notre point d’accès Wifi

Il est nécessaire d'avoir un point d’accès wifi fonctionnel, pour cela référez vous ici.

Installons tor avec la commande sudo **apt-get install tor**.

Nous allons maintenant modifier la configuration par default.

Éditons **/etc/tor/torrc** :

```
# fichier pour stocker les messages
Log notice file /var/log/tor/notices.log

# adresse virtuelle pour le partage
VirtualAddrNetwork 10.192.0.0/10

# on traite les .onion et .exit comme
# des machines dans le réseau Tor
AutomapHostsSuffixes .onion,.exit
AutomapHostsOnResolve 1

# on écoute sur le Wifi port 9040
TransListenAddress 192.168.2.254
TransPort 9040

# idem pour le DNS
DNSListenAddress 192.168.2.254
DNSPort 53
```

Voila à quoi peut ressembler votre fichier **torrc**.

VirtualAddrNetwork permet à Tor de fonctionner dans un contexte “partagé”. Lorsqu'on fournit le service à un réseau (ici 192.168.2.0 en Wifi), il faut spécifier des adresses virtuelles 10.192.0.0/10 ou 172.16.0.0/12.

TransListenAdress et **DNSListenAdress** précisent l'adresse sur laquelle Tor attend les connexions pour les communications et rêquetes DNS. Il existe un système qui permet d'envoyer ces demandes, et il se chargera de trouver les réponses tout en protégeant ces informations.

Nous avons plus qu'à redémarrer le service:

```
pi@raspberrypi ~ $ sudo service tor restart
[ ok ] Stopping tor daemon...done.
[ ok ] Starting tor daemon...done.
```

Pour s'assurer que tout fonctionne (**tail /var/log/tor/notices.log**):

```
pi@raspberrypi ~ $ tail /var/log/tor/notices.log
May 31 18:37:34.000 [notice] Tor 0.2.4.27 (git-412e3f7dc9c6c01a) opening new log file.
May 31 18:37:34.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
May 31 18:37:36.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
May 31 18:37:43.000 [notice] We now have enough directory information to build circuits.
May 31 18:37:43.000 [notice] Bootstrapped 80%: Connecting to the Tor network.
May 31 18:37:45.000 [notice] Bootstrapped 85%: Finishing handshake with first hop.
May 31 18:37:45.000 [notice] Bootstrapped 90%: Establishing a Tor circuit.
May 31 18:37:46.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
May 31 18:37:46.000 [notice] Bootstrapped 100%: Done.
```

Maintenant que Tor fonctionne sur notre point d'accès wifi, nous allons utiliser **iptables** pour rediriger les communications arrivant en Wifi dans le réseau Tor.

Définissons les règles **iptables** :

```
pi@raspberrypi ~ $ sudo iptables -t nat -A PREROUTING -i wlan0 \
> -p tcp --dport 22 -j REDIRECT --to-ports 22
pi@raspberrypi ~ $ sudo iptables -t nat -A PREROUTING -i wlan0 \
> -p udp --dport 53 -j REDIRECT --to-ports 53
pi@raspberrypi ~ $ sudo iptables -t nat -A PREROUTING -i wlan0 \
> -p tcp --syn -j REDIRECT --to-ports 9040
```

La premiere ligne permet de se connecter au ssh depuis **wlan0**.
La seconde ligne redirige le trafic DNS (port 53) vers le raspberrypi. Nous ne procédons pas à la résolution de nom au travers Tor, mais avec Tor lui-même.
La dernière ligne envoi tout le reste du trafic à Tor.

La dernière chose à faire est de rendre persistante les règles **iptables** après un redémarrage. Pour cela nous allons installer un paquet avec **apt-get install iptables-persistent** qui s'occupera de recharger les règles **iptables**.

Les règles seront enregistrer dans **/etc/iptables/rules.v4**. Pour apporter des modifications il vous faudra utiliser **iptables-save** en spécifiant le fichier en question.

Pour vérifier que tout fonctionne connectez vous au point d'accès Wifi et visitez la page **https://check.torproject.org**.

PRUDENCE

L'intérêt de disposer d'un point d'accès à Tor est évident : il n'y a plus rien a configurer et rien à installer de la part des utilisateurs.
Notez que cette solution n'est ni la seule ni la plus parfaite. Le project tor propose un navigateur dédié à installer sur votre ordinateur. C'est le Tor Browser. Une solution est aussi disponible sur smartphone avec l'application Android Orbot Proxy.

L'installation d'un point d'accès Tor ne suffit pas a assurer votre confidentialité. Un navigateur mal configurer pourrai révéler votre identité. Par exemple le Tor browser intègre des extensions Firefox bloquant Flash et Java, forçant l'utilisation de HTTPS ou encore permettant de régler précisément l'exécution des Javascript présent sur les pages web. Malgré tout, ce n'est pas une solution absolue. Vous pouvez très bien avoir un ordinateur infecté par un spyware qui compromettra votre tentative

d'anonymisation. N'oubliez pas que dans le cas d'un point d’accès comme celui que nous venons de créer, la communication entre les clients Wifi et le point d’accès n'est pas protégée.

Le principale rempart défendant votre vie privée est et sera toujours vous-même.

Source : Hackable Magazine