Version : dnscrypt-proxy 1.9.5

Web : la version 2.0.15 est sortie, mais Ubuntu 18.04 utilise encore la 1.9.5

Chat : l'URL/lien officiel est : #dnscrypt-proxy:matrix.org

Je suis une personne privée, et je n'aime pas que ma vie privée soit envahie. C'est une des principales raisons pour lesquelles j'utilise Linux.

Aujourd'hui, je vais vous montrer comment paramétrer DNSCrypt sur Ubuntu 18.04. Prenez ça, M. ISP, ainsi que toute autre personne essayant de suivre mon usage d'Internet !

Que vous aimiez ça ou non, vous êtes une marchandise ; vous êtes achetés et vendus partout dans le monde. Améliorez votre sécurité et le respect de votre vie privée en suivant ce guide.

DNSCrypt transforme le trafic DNS normal en trafic DNS chiffré, ce qui vous protège contre les attaques par écoute clandestine (eavesdropping) et « homme-au-milieu » (man-in-the-middle). De la même façon que HTTPS protège maintenant votre trafic sur Internet, DNSCrypt sécurise votre trafic DNS. (Cela dit, ce n'est pas une solution complète).

Laissez-moi vous en dire plus sur le protocole. Ceux d'entre vous qui n'y trouvent aucun intérêt peuvent passer à la section suivante. Je vous promets que cette section sera courte. DNSCrypt est un protocole qui authentifie les communications entre un client DNS et un « resolver » (une sorte de bibliothèque) DNS.

Le protocole DNSCrypt fonctionne avec les connexions TCP et UDP. Le port HTTPS par défaut est le 443, et DNSCrypt l'utilise aussi. Celui-là le laissera passer sans entrave à travers la plupart des pare-feux. Pour ceux d'entre vous qui sont intéressés, vous pouvez trouver une liste des ports ici : http://www.hostingreviewbox.com/rhel-tcp-and-udp-ports/

Le client comme le resolver génèrent initialement une paire de clés temporaires pour chaque système de chiffrage pris en charge. Chaque certificat comprend une période de validité, un numéro de série, une version qui définit un mécanisme d'échange de clés, un algorithme authentifié de chiffrage et ses paramètres, ainsi qu'une clé publique à courte durée de vie, appelée la clé publique du resolver.

Voilà… Depuis votre ordinateur ou portable (client), une session DNSCrypt commence quand le client envoie une requête DNS non authentifiée à un resolver activé pour DNSCrypt, tel que OpenDNS.

Cette requête DNS encode les versions de certificats prises en charge par le client, ainsi qu'un identifiant public du fournisseur demandé par le client.

Le serveur (resolver) répond avec un jeu de certificats publics signés, qui doivent être vérifiés par le client en utilisant une clé publique du fournisseur.

Chaque certificat comprend un « nombre magique » que le client doit préfixer sur toutes ses requêtes, pour que, avant de faire quoi que ce soit, le resolver sache quel certificat a été choisi par le client.

L'algorithme de chiffrage, la clé publique du resolver et le nombre magique du client tirés du certificat choisi sont ensuite utilisés par le client pour envoyer des requêtes chiffrées. Ces requêtes contiennent la clé publique du client.

En utilisant cette clé publique du client et en sachant quel est le certificat choisi par le client ainsi que la clé secrète correspondante, le resolver vérifie et déchiffre la requête et chiffre la réponse de la même façon.

DNSCrypt ne doit pas être confondu avec DoH (pas celui d'arkanoid), qui est un DNS sur HTTPS. Ceci est un projet de la fondation Mozilla.

Si vous ne maîtrisez pas la ligne de commande à 100 %, merci de sauvegarder les fichiers que vous voulez modifier, AVANT de les modifier !

Ouvrez un terminal et saisissez ce qui suit :

```
sudo apt-get install
dnscrypt-proxy
```

Entrez votre mot de passe et laissez l'action se terminer.