Bien se servir des VPN

Nothing2Hide Decentralized Festival @TetaLab

Bien se servir des VPN

le sujet

- présentation basée sur la chronique "How-to: bien se servir des VPN", épisode 231 de l'émission C.P.U. sur Radio FMR

- plan
  - ce qu'un VPN fait vraiment
  - avez-vous besoin d'un VPN sponsor YouTube ?
  - votre propre VPN pour aller chez vous depuis dehors
  - votre VPN pour aller dehors

Bien se servir des VPN

ce qu’un VPN fait vraiment

- *Virtual Private Network*
- Internet est un réseau de réseaux
  - ces « réseaux » sont ceux de vos fournisseurs d’accès
  - et votre réseau local à la maison, protégé du monde extérieur
- simuler un réseau local à cheval sur plusieurs réseaux publics
  - *réseau privé* = accès réservé, sécurisé par chiffrement
  - *virtuel* car pas d’existence physique, utilise l’existant

Bien se servir des VPN

avez-vous besoin d'un VPN sponsor YouTube ?

- VPN pour surfer sur Internet anonymisé, et changer de pays
- VPN = simple serveur -> pas bien cher, bonne marge
  - d'autant plus lucratif plus vous avez de clients
- le problème ? argumentaire fallacieux
  - sécurité redondante (avec HTTPS) (installez plutôt consent-o-matic)
  - sécurité à côté de la plaque (si vous ouvrez toutes les P.J.)
  - des utilisations légitimes : contrer les prix basés sur le pays
    - incitation à violer les C.G.U. par exemple géoblocage
  - vous montrez tout votre traffic (iront-ils en prison à votre place ?)
    - commencez par utiliser un DNS chiffré : 9.9.9.9 (fondation suisse quad9.net)

Bien se servir des VPN

votre propre VPN pour aller chez vous depuis dehors

- pour accéder à votre NAS, votre Home Assistant, …
- à faire soi-même sur un serveur Linux (une Raspberry Pi)
  - nécessite un brevet de sysadmin :-(
- fonction incluse dans certains *routeurs*
  - par exemple GL.iNet, tourne sous OpenWRT
  - les protocoles populaires : *OpenVPN*, *WireGuard*, …
  - WireGuard facile à configurer et meilleur débit qu'OpenVPN
    - marche sur Linux, Windows, MacOS, iOS, Android, UNIX, …
- /!\ la sécurité repose sur la **bonne gestion des clés** /!\ (et les màj)

Bien se servir des VPN

votre VPN pour aller dehors : *TOR* the Onion Router

- votre traffic rebondit sur plein de machines et se mélange au traffic des autres utilisateurs de TOR

  == pelures d'onion

- les serveurs ont du mal à distinguer les nombreux utilisateurs arrivant d'un même « *TOR exit node* »
  - il y a des TOR exit nodes partout dans le monde
- à l'intérieur de TOR le traffic est chiffré et anonymisé
  - contrairement à *IP* l'Internet Protocol, chaque routeur TOR ne connait ni la source ni la destination de votre traffic
  - seulement le rebond précédent et le rebond suivant

Bien se servir des VPN

est-ce que *TOR* est sûr ?

- plus il y a d'utilisateurs, plus chaque utilisateur est planqué dans la masse
  - TOR a été créé par l'*US Navy* pour faire du renseignement sur Internet sans se faire repérer
    - *Naval Research Lab* créé en 1923 par Thomas Edison, il ne semble pas que ce soit une manœuvre d'infiltration
- il ne faut pas qu'un même opérateur possède beaucoup de noeuds du réseau *TOR*
  - donc plus il y a d'indépendants qui contribuent des routeurs, plus c'est sûr

Bien se servir des VPN

TOR en pratique

- plutôt que payer un VPN à youtubeur, financez des TOR exit nodes
  - TetaNeutral en a un
- utiliser TOR
  - basique : naviguer avec le *TOR browser* basé sur *Firefox*
  - avancé : passer tout le traffic de votre ordinateur dans TOR
  - niveau expert : ajouter des TOR exit nodes
    - légal mais risqué sur votre connexion à la maison
      à faire sur un serveur loué chez un hébergeur off-shore - comme un VPN youtubeur !!
- Si vous voulez vraiment un OuestVPN : Proton VPN Mozilla Opera
  - le VPN de Free.fr : peu d'intérêt