



BLOQUER LES PUBLICITÉS ET LES MOUCHARDS SUR TOUT LE RÉSEAU GRÂCE À PI-HOLE

Aujourd'hui, presque tout le monde a un appareil connecté chez soi. Que ce soit une télé, un ordinateur, un téléphone, et même un robot-cuiseur, vu tout ce qu'on peut faire avec Internet, c'est presque devenu indispensable. Mais, ce que l'on oublie le plus souvent, c'est que vos données personnelles peuvent être enregistrées et n'importe qui peut vous espionner. À cause de cela, ils vous font perdre votre vie privée et peuvent même revendre vos données pour des publicités ciblées... Dans ce tutoriel, je vais vous montrer comment bloquer les publicités et les pisteurs sur tous les appareils connectés grâce à Pi-hole !

Merci à Yann Jaulin pour cet article. Allez visiter son site : <https://protege-moi-sur-internet.com>

LEXIQUE

***DNS :** Le Domain Name System abrégé DNS est un service qui traduit un nom de domaine en adresse IP. En outre, quand vous allez sur un site Internet comme wikipedia.org par exemple, votre navigateur va demander à votre fournisseur DNS l'adresse numérique du site derrière ce nom de domaine et vous y redirige immédiatement. Bien entendu les DNS sont les éléments les plus sensibles sur vos appareils connectés, car ils peuvent facilement être modifiés.





INFOS [Pi-hole]

Où le trouver ? [<https://pi-hole.net/>]

Difficulté :

➤ Blocage de publicité

Préservez votre vie privée sur tout votre réseau, c'est possible grâce à Pi-hole !

POUR QUI ?

Les personnes inquiètes de l'utilisation de leurs données

POUR QUOI FAIRE ?

Pour bloquer en amont les pubs et les mouchards

CE QU'IL VOUS FAUT...

Pour ce tutoriel, il vous faudra du matériel, mais aussi des logiciels et des listes de blocage DNS. Pour éviter de surcharger l'article, voici tous les liens vers ces éléments :

- Un Raspberry Pi
- Une carte microSD d'au moins 8 Go

[Raspbian Buster Lite]

Où le trouver ?
[<https://www.raspberrypi.org/downloads/raspbian/>]

[Pi-hole]

Où le trouver ?
[<https://pi-hole.net/>]

[Etcher]

Où le trouver ?
[<https://etcher.io>]

[Angry IP Scanner]

Où le trouver ?
[<https://angryip.org>]

[Putty]

Où le trouver ?
[<https://www.putty.org/>]

- Les résolveurs DNS récuratifs ouverts de chez FDN

Où le trouver ?
[<https://www.fdn.fr/actions/dns/>]

- Les listes de blocage DNS

Où les trouver ?
[<https://firebog.net/>]
[<https://blocklist.site/>]
[<https://filterlists.com/>]
[<https://energized.pro/>]



HACKING

En se connectant sur Internet, on perd forcément sa confidentialité. Car tout ce qu'on fait est enregistré et nos données peuvent être utilisées pour des publicités ciblées. Certes, avoir des objets connectés, c'est super pratique, car on peut communiquer avec ses amis, se divertir en regardant des vidéos à volonté, cuisiner sans effort, et même contrôler sa maison à distance ! Malgré tous ces avantages, il ne faut pas oublier qu'un objet dit connecté/intelligent est synonyme de surveillance, car depuis plusieurs années, se développe la surveillance sur Internet, connue grâce aux révélations d'Edward Snowden, leur but est simple : récolter un maximum de données sur vous, que ce soit votre historique de recherche, l'historique de localisation voire même les publications aimées afin de vous créer un profil pour les publicités ciblées (et pas que...). Comment ils le font ? C'est simple, quand vous chargez une page Web, certains pisteurs sont dissimulés dans le code afin de vous espionner numériquement et matériellement (<https://frama.link/robotcuiseurespion>). Bien sûr, vos données peuvent être vendues et ça peut aller encore plus loin, car ils peuvent exécuter du code malveillant... Bien qu'il existe plusieurs solutions pour bloquer tout cela comme uBlock origin et privacy badger

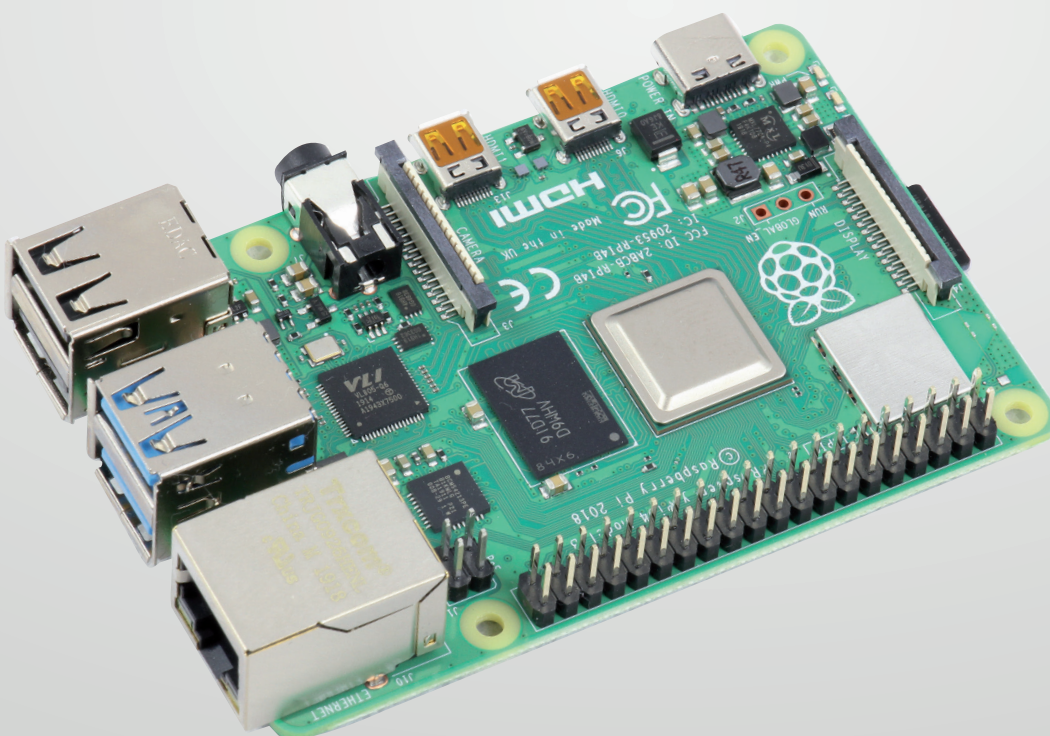
sur navigateur, ils ne sont pas compatibles partout et ils en existent très peu voire pas du tout sur d'autres appareils connectés comme les télévisions. L'avantage de Pi-hole, c'est que lui, il s'applique sur tout le réseau et donc pas besoin d'installer de logiciel !

PI-HOLE, LE BLOQUEUR DE PUBLICITÉ UNIVERSEL !

Pi-hole est un bloqueur de publicité matériel gratuit et open source qui se place entre le réseau et les appareils connectés. Pour cela, nous allons l'installer sur un seul appareil : le Raspberry Pi. Bien sûr, vous n'êtes pas limité à ce nano-ordinateur bon marché : un système d'exploitation comme Ubuntu, Debian, Fedora, CentOS et Docker fera l'affaire. Après avoir été configurée, quand vous ferez une requête, elle passera par Pi-hole qui interroge le résolveur et filtre les pisteurs en fonction des listes de blocage, le site demandé ! En plus, Pi-hole offre une interface web qui vous permet de gérer les listes et vous fournit des statistiques d'utilisation grâce au moteur FTL créée par eux-mêmes. Bien sûr, d'autres fonctionnalités existent comme la possibilité de jumeler Pi-hole avec un VPN ! Enfin n'oubliez pas que Pi-hole est créé par une équipe 100 % distante pendant leur temps libre et donc le projet est alimenté par vos dons et votre support.



POUR MOINS DE 40 €, LE RASPBERRY PI EST LA SOLUTION IDÉALE POUR IMPLÉMENTER PI-HOLE. PETIT ET PEU ÉNERGIVORE, IL PREND PLACE IDÉALEMENT À CÔTÉ DE VOTRE BOX...



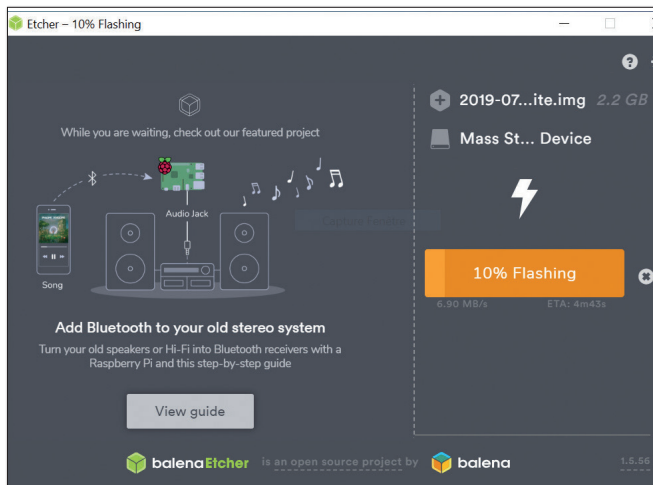
INSTALLATION ET CONFIGURATION DE PI-HOLE !

PRATIQUE



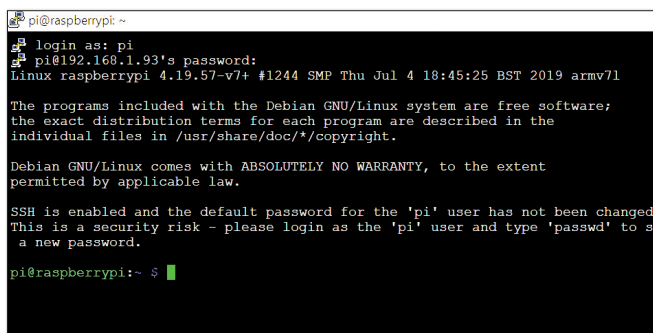
01 > INSTALLATION ET DÉMARRAGE DE RASPBIAN

Pour fonctionner, Pi-hole doit être installé sur un système d'exploitation supporté comme Raspbian par exemple. Pour cela, allez sur le site de raspberry pi et téléchargez le fichier zip de Raspbian Buster Lite. Après l'avoir téléchargé, dézippez-le afin d'obtenir l'image. Une fois l'image obtenue, branchez votre carte microSD sur votre pc, ouvrez Etcher, sélectionnez votre image et flashez ! Une fois terminé, créez le fichier ssh sur la carte, retirez-la et mettez-la dans votre Raspberry Pi, branchez-la et ça démarre !



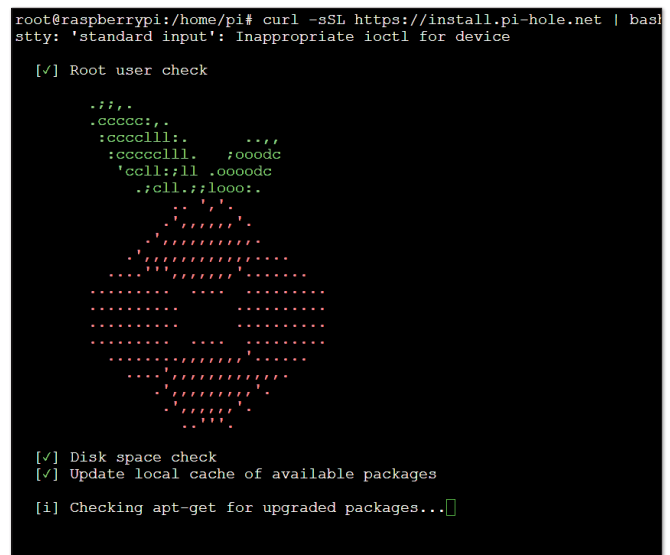
02 > DÉTECTION DE SON ADRESSE IP ET ACCÈS AU RASPBERRY PI

Ouvrez Angry IP Scanner et cliquez sur Démarrer. Une fois fini, cherchez votre Raspberry Pi dans les Noms d'hôte et copiez son adresse IP. Pour mon cas, ça sera 192.168.1.93. Collez cette adresse dans Host Name sur PuTTY et cliquez sur **Open**. Si c'est votre première connexion, PuTTY vous fera une alerte sur la clé d'empreinte du Raspberry pi, cliquez sur oui pour accepter, ensuite le nom d'utilisateur sera **pi** et le mot de passe **raspberry**. Ça y est, vous êtes connecté sur Raspbian !



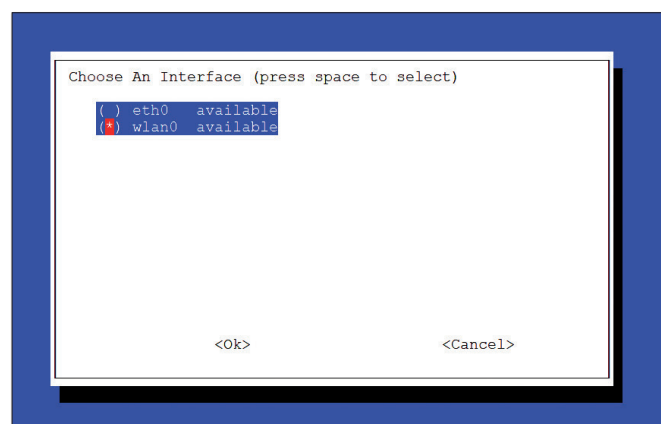
03 > PARAMÉTRAGE DE RASPBIAN ET INSTALLATION DE PI-HOLE

Une fois connecté, on vous demandera de changer le mot de passe, tapez **passwd** et remplacez le par le vôtre, ensuite activez le mode administrateur en tapant **sudo su**. Enfin, mettez Raspbian à jour en tapant **apt-get update**, **apt-get upgrade** et **apt-get dist-upgrade**. Après cela, installez Pi-hole avec la commande : **curl -sSL https://install.pi-hole.net | bash**



04 > CONFIGURATION DE PI-HOLE : CHOISIR SON INTERFACE RÉSEAU

Ça y est, on va configurer Pi-hole ! Il va y avoir plusieurs étapes avant qu'il fonctionne, suivez bien mon tutoriel ! Après l'avoir installé, on vous demande de choisir une interface réseau : soit eth0 (ethernet) ou wlan0 (WiFi). Mon Raspberry pi étant connecté en WiFi, je choisis **wlan0** en appuyant sur espace, mais si il est avec un câble Ethernet rester sur **eth0** et cliquez sur **entrée**.

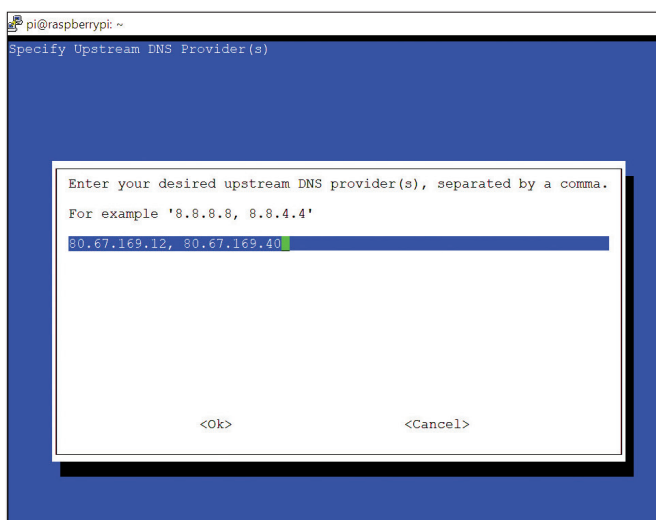




HACKING

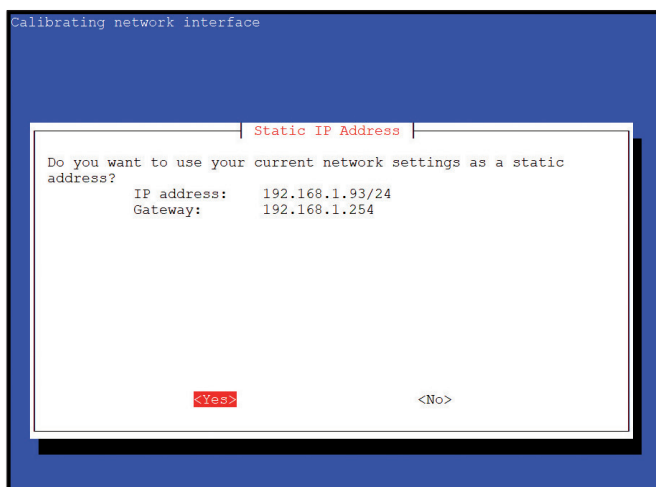
05 > CHOISIR SON FOURNISSEUR DNS

Après avoir choisi votre interface réseau, on vous demandera de choisir un fournisseur DNS. Bien évidemment, on va en choisir un qui ne nous censure pas et qui respecte notre vie privée contrairement à celui par défaut qui est sur notre box. Personnellement, je vous conseille les DNS de **French Data Network** qui est un fournisseur d'accès à Internet associatif qui propose un accès Internet propre, neutre et militant. Pour cela allez tout en bas de la liste et choisissez **Custom** et entrez comme adresse **80.67.169.12, 80.67.169.40**. Une fois cela fait, cliquez sur **entrée** et choisissez **Yes**.



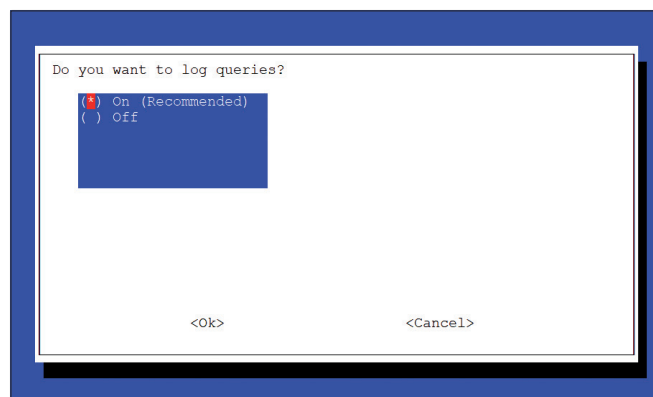
06 > CHOIX DES LISTES DE BLOCAGE, DES PROTOCOLES ET DE L'ADRESSE IP STATIQUE

Là, on va vous demander de choisir des listes de blocage, ceux sélectionnés par défaut sont bons, mais pas suffisants, on en rajoutera tout à l'heure, cliquez sur entrée. Ensuite, on vous demandera de choisir les protocoles à activer, pareil, cliquez sur entrée étant sélectionné par défaut et enfin, on vous demandera si vous voulez que le Raspberry Pi ait une adresse IP statique, cliquez sur **Yes**.



07 > INSTALLATION DE L'INTERFACE WEB, DE SON SERVEUR ET CONFIGURATION DU JOURNAL

Ensuite, Pi-hole va vous demander si vous voulez installer une interface Web, **On** étant sélectionné, faites **Entrée**. Pareil pour le serveur web lighttpd. Les paramètres suivants vont dépendre de vous, car Pi-hole va proposer d'enregistrer les requêtes, cela veut dire qu'il enregistre les domaines qui communiquent avec vos appareils afin de vous faire des statistiques sur les requêtes bloquées ou non par vos listes et dans le long terme vous aider à mieux les ajuster s'il y a des sites qui ne marchent pas correctement. Bien évidemment, tout est enregistré en local et personne n'y a accès sauf vous. Bien sûr, vous n'êtes pas obligé d'accepter et si vous ne voulez rien enregistrer, choisissez **Off** avec la barre d'espace, cliquez sur **entrée** et à la fin de la configuration de pi-hole, faites la commande **sudo pihole logging off**. Étant une des fonctionnalités principales de Pi-hole, je laisse sur **Yes**.



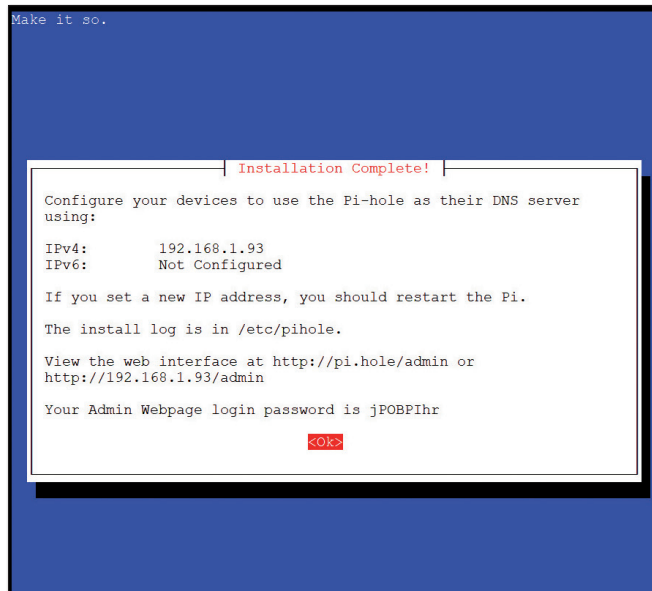
08 > CHOIX DU DÉTAIL DES DONNÉES À VISIONNER

Pi-hole vous demandera ensuite ce que vous voulez voir comme données que ce soit tout, aucun domaine, aucun domaine et appareils, tout anonymiser ou rien. Pour avoir plus de visibilité, je laisse **show everything**, mais si vous n'avez pas activé l'enregistrement du journal avant, choisissez **disabled statistics**.



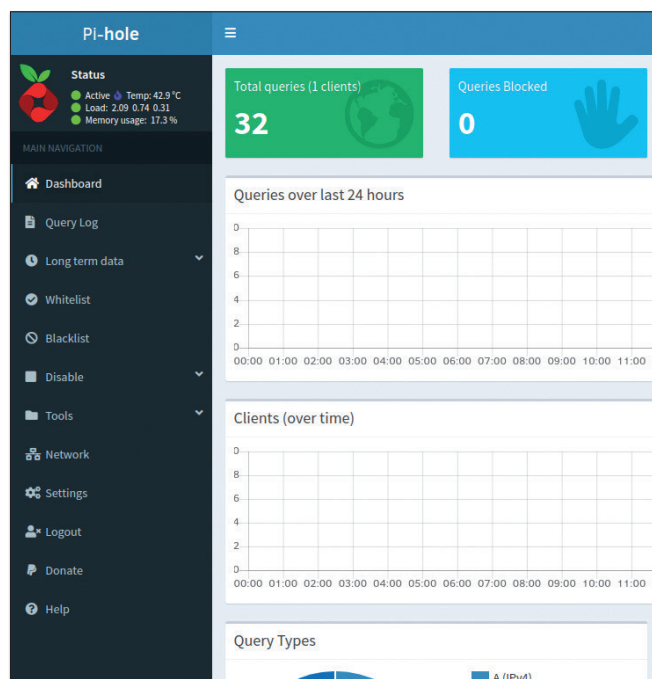
09 > RÉCUPÉRATION DU MOT DE PASSE ET ACCÈS AU SERVEUR WEB

Ça y est, Pi-hole est configuré, il installe et configure les dépendances afin de fonctionner correctement ! Une fois terminé, il vous affiche une page comme quoi tout est prêt et qu'on peut aller sur l'interface Web pour configurer les listes et voir les statistiques. **Enregistrez bien le mot de passe** et allez sur le lien donné !



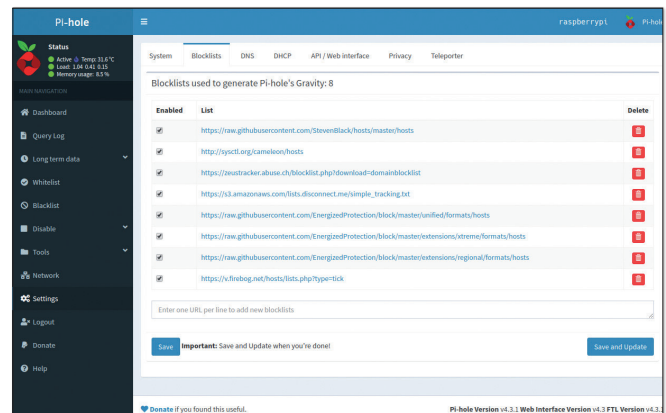
10 > DÉCOUVERTE DE L'INTERFACE WEB

Une fois sur l'interface Web, cliquez sur login, mettez le mot de passe. Vous avez accès à toutes les statistiques que ce soient les requêtes, le nombre de domaines bloqués, les listes, les clients, les types de requêtes, etc.



11 > AJOUT DE LISTES DE BLOCAGE

Maintenant que Pi-hole fonctionne, il ne bloquera pas toutes les publicités, car la liste de base n'est pas très complète. Alors allez dans **Settings > Blocklists** et ajoutez les listes que j'ai données dans les liens. Personnellement, je vous conseille en priorité les listes d'**energized.pro**, car elles sont très complètes !



12 > CONFIGURATION DES OPTIONS DHCP ET C'EST FINI !

Attention, lisez bien cette étape, car sans celle-ci, Pi-hole ne fonctionnera pas sur vos appareils ! Bien que pi-hole soit configuré et les listes ajoutées, tous les appareils doivent avoir Pi-hole comme fournisseur DNS en l'occurrence pour ma part, je dois mettre sur chaque appareil le DNS **192.168.1.93 qui est un IP fixe**. Pour aller plus vite, il y a une option sur votre box qui permet de le mettre par défaut, pour cela connectez vous sur votre box en **Ethernet** et allez dans les options **DHCP**, activez-les et mettez dans les **DNS statiques l'IP de Pi-hole** ! Si votre box ne prend pas en charge le DHCP / n'accepte pas de changer les DNS, vous pouvez activer le serveur DHCP intégré de Pi-hole dans **Settings > DHCP**. Bien évidemment, désactivez les options DHCP de votre box si vous faites ainsi. En dernier recours, vous pouvez toujours configurer manuellement chaque périphérique pour qu'il utilise Pi-hole comme serveur DNS. Bonne utilisation de Pi-hole !

