Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

7 nov, 2026 · @Gabriel

Objectif : *Installer et configurer* ***Pi-hole*** *sur un Raspberry Pi (ou un vieux PC) pour bloquer publicités, traqueurs et domaines malveillants pour* ***tous les appareils*** *de la maison (ordinateurs, smartphones, TV connectées), sans rien installer sur chacun d'eux.*

- ***Public visé :*** *Intermédiaire (quelques bases en ligne de commande sont utiles)*
- ***Temps estimé :*** *30 à 60 minutes*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *un Raspberry Pi (3, 4 ou 5), un vieux PC ou une machine virtuelle ; une carte microSD ou un disque ; la possibilité de modifier le DNS distribué par votre box (ou de régler chaque appareil)*
- ***Fiches associées :*** *N°6 (DNS), N°20c (AdGuard Home, alternative sur YunoHost), N°20a (WireGuard), N°30 (sécuriser la box)*

1. Qu'est-ce que Pi-hole ? (Le problème qu'il résout)

1.1. Le problème

Situation	Conséquence
Publicités partout	Dans le navigateur, les applications mobiles, la TV connectée
Traqueurs invisibles	Sites et applications vous suivent en arrière-plan
Appareils impossibles à protéger	TV, consoles et objets connectés n'acceptent pas de bloqueur
Protection appareil par appareil	uBlock Origin dans le navigateur ne protège ni les applications ni la TV

Le bénéfice : un seul réglage protège tout le réseau.

1.2. La solution : Pi-hole

Pi-hole est un serveur DNS qui répond « ce domaine n'existe pas » aux demandes vers des domaines publicitaires ou de pistage connus.

Caractéristique	Explication
Niveau réseau	Tous les appareils qui l'utilisent comme DNS sont protégés
Rien à installer sur les appareils	Il suffit de changer le DNS (dans la box ou sur l'appareil)
Listes de blocage	Listes maintenues par la communauté (des centaines de milliers de domaines)
Libre	Code ouvert, gratuit
Léger	Fonctionne sur un Raspberry Pi d'entrée de gamme

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

Caractéristique	Explication
Statistiques	Interface web pour voir ce qui est bloqué

Depuis **Pi-hole v6** (février 2025), le serveur web est intégré : lighttpd et PHP ne sont plus nécessaires, et la configuration est regroupée dans `/etc/pihole/pihole.toml`.

1.3. Ce que Pi-hole bloque

Catégorie	Exemples
Publicités	doubleclick.net, régies publicitaires
Traqueurs	Outils de mesure d'audience et pixels de suivi
Domaines malveillants	Hameçonnage, logiciels malveillants (avec des listes adaptées)
Télémétrie	Une partie de la télémétrie des systèmes et applications (avec des listes adaptées)

💡 **Pi-hole ne bloque pas :** les publicités servies depuis le même domaine que le contenu (YouTube, certaines applications), ni les appareils qui contournent le DNS de la box (DNS chiffré intégré au navigateur ou à l'appareil).

2. Prérequis matériels

2.1. Options

Solution	Avantages	Inconvénients	Coût
Raspberry Pi 3, 4 ou 5	Peu énergivore, silencieux	À acheter	40 à 100 €
Vieux PC	Gratuit si vous en avez un	Consomme davantage	0 €
Machine virtuelle ou conteneur	Utilise un serveur existant	Dépend de ce serveur	0 €
VPS	Rien chez soi	⚠️ Un DNS ouvert sur Internet est dangereux ; à réserver à un accès par VPN	Quelques euros par mois

2.2. Recommandation

Pour un usage familial : un Raspberry Pi 3 ou 4 + une carte microSD de 16 Go, branché en Ethernet.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

2.3. Raspberry Pi ou vieux PC ?

Critère	Raspberry Pi	Vieux PC
Consommation	Quelques watts (environ 10 €/an)	Plusieurs dizaines de watts
Bruit	Silencieux	Ventilateur
Taille	Carte de crédit	Boîtier
Fiabilité	Bonne (attention à l'usure des cartes microSD)	Disque mécanique susceptible de lâcher

3. Avant de commencer

- ☐ Vérifiez si votre box permet de changer le **serveur DNS distribué par le DHCP** (beaucoup de box d'opérateurs français ne le permettent pas : voir section 5).
- ☐ Prévoyez une **adresse IP fixe** pour Pi-hole (réservation DHCP dans la box).
- ☐ Ayez un câble Ethernet.

4. Installation de Pi-hole

4.1. Option A : sur Raspberry Pi

Étape 1 : Préparez Raspberry Pi OS

1. Téléchargez **Raspberry Pi Imager** sur raspberrypi.com › **Software**.
2. Choisissez votre modèle, **Raspberry Pi OS Lite** (sans bureau) et votre carte microSD.
3. Dans la **personnalisation de l'OS** :
    - nom d'hôte : `pihole` ;
    - **nom d'utilisateur et mot de passe** (il n'y a plus d'utilisateur `pi` par défaut) ;
    - activez **SSH** ;
    - Wi-Fi seulement si vous ne pouvez pas brancher de câble.
4. Écrivez l'image.

Étape 2 : Démarrez le Raspberry Pi

1. Insérez la carte, branchez le câble Ethernet, puis l'alimentation.
2. Trouvez son adresse IP dans l'interface de votre box, ou avec `ping pihole.local`.
3. Dans la box, **réservez cette adresse IP** pour le Raspberry Pi.

Étape 3 : Connectez-vous en SSH

```
ssh votre_utilisateur@adresse_ip_du_pi
```

Étape 4 : Installez Pi-hole

```
curl -sSL https://install.pi-hole.net | bash
```


gabriel.ananda@mailo.com
CC BY SA

Si vous préférez relire le script avant de l'exécuter :

```
curl -sSL https://install.pi-hole.net -o installer-pihole.sh
less installer-pihole.sh
sudo bash installer-pihole.sh
```

Étape 5 : Suivez l'assistant

- Interface réseau : `eth0` (Ethernet) ou `wlan0` (Wi-Fi).
- **Serveur DNS en amont :** choisissez un résolveur respectueux de la vie privée, par exemple **Quad9** (filtre aussi les domaines malveillants).
    - Évitez Google.
    - Rappel : le DNS public de Mullvad a fermé le 2 novembre 2026.
- Gardez la **liste de blocage** proposée par défaut.
- Activez l'**interface web** et la **journalisation des requêtes** (vous pourrez réduire le niveau de détail par respect pour les autres membres du foyer).
- **Notez le mot de passe** de l'interface affiché à la fin. Pour le changer : `sudo pihole setpassword`.

Vous devez voir :

- l'écran final de l'assistant avec l'adresse de l'interface web et le mot de passe.

4.2. Option B : sur un vieux PC (Debian ou Ubuntu)

```
sudo apt update && sudo apt upgrade -y
curl -sSL https://install.pi-hole.net | bash
```

Puis le même assistant qu'à l'étape 5.

4.3. Option C : avec Docker

Fichier `docker-compose.yml` (d'après la documentation officielle de Pi-hole v6) :

```
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "8080:80/tcp"
    environment:
      TZ: 'Europe/Paris'
      FTLCONF_webserver_api_password: 'MotDePasseFort'
      FTLCONF_dns_listeningMode: 'ALL'
    volumes:
      - './etc-pihole:/etc/pihole'
    restart: unless-stopped
```


gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

```
docker compose up -d
```

⚠️ Les anciennes variables (`WEBPASSWORD`…) de Pi-hole v5 ne fonctionnent plus en v6.

5. Faire utiliser Pi-hole par vos appareils

5.1. Méthode A : DNS distribué par la box (tout le foyer)

1. Connectez-vous à l'interface de la box (fiche N°30).
2. Dans les réglages **DHCP** ou **DNS du réseau local**, indiquez l'adresse IP de Pi-hole comme **serveur DNS**.
3. Enregistrez, puis reconnectez les appareils (ou redémarrez-les).

⚠️ **Toutes les box ne le permettent pas.** Si la vôtre ne le permet pas :

5.2. Méthode B : Pi-hole comme serveur DHCP

1. Dans l'interface de Pi-hole : **Settings** › **DHCP**, activez le serveur DHCP (plage d'adresses, passerelle = adresse de la box).
2. **Désactivez le DHCP de la box.**
3. Reconnectez les appareils : ils reçoivent leur adresse et leur DNS de Pi-hole.

⚠️ Si Pi-hole tombe en panne, plus aucun appareil n'obtient d'adresse : réactivez alors le DHCP de la box.

5.3. Méthode C : appareil par appareil

Windows : Paramètres › **Réseau et Internet** › votre connexion › **Attribution du serveur DNS** › **Modifier** › **Manuel** › IPv4 : adresse de Pi-hole.

Android : Paramètres › **Wi-Fi** › votre réseau › **Modifier** › **Options avancées** › **Paramètres IP : statique** › **DNS 1** : adresse de Pi-hole. Désactivez le **DNS privé** d'Android, sinon il contourne Pi-hole.

iPhone : Réglages › **Wi-Fi** › (i) à côté du réseau › **Configurer le DNS** › **Manuel** › supprimez les serveurs existants, ajoutez l'adresse de Pi-hole.

Navigateurs : désactivez le « DNS sécurisé » (DNS over HTTPS) de Firefox ou Chrome sur ces appareils, sinon ils contournent Pi-hole.

6. Configuration de Pi-hole

6.1. Interface web

- Ouvrez http://adresse_ip_du_pi/admin et saisissez le mot de passe.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

6.2. Ajouter des listes de blocage

Liste	Adresse	Ce qu'elle bloque
StevenBlack (unifiée)	`https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts`	Publicités et logiciels malveillants (liste par défaut)
OISD big	`https://big.oisd.nl`	Large couverture, peu de faux positifs
AdGuard DNS filter	`https://adguardteam.github.io/AdGuardSDNSFilter/Filters/filter.txt`	Publicités et traqueurs

1. **Lists** (Listes) › collez l'adresse › **Add blocklist**.
2. Mettez à jour la base : **Tools** › **Update Gravity**, ou `pihole -g`.

⚠️ Plus de listes ne veut pas dire mieux : trop de listes multiplient les faux positifs.

6.3. Mises à jour

- Les listes sont mises à jour automatiquement chaque semaine ; manuellement : `pihole -g`.
- Pi-hole lui-même : `pihole -up` (ou mise à jour de l'image Docker).

6.4. Débloquer un site (liste d'autorisation)

Si un site légitime ne fonctionne plus :

1. **Query Log** : repérez le domaine bloqué au moment du problème.
2. Cliquez sur **Allow** (Autoriser), ou ajoutez-le dans **Domains**.
3. En ligne de commande : `pihole allow domaine.fr`.

7. Utilisation au quotidien

7.1. Interface web

Rubrique	Contenu
Dashboard	Requêtes totales et bloquées
Query Log	Historique des requêtes DNS (appareil, heure, domaine)
Lists	Listes de blocage et d'autorisation
Domains	Domaines autorisés ou bloqués à la main

gabriel.ananda@mailo.com
CC BY SA

7.2. Commandes utiles

Commande	Action
`pihole -g`	Mettre à jour les listes
`pihole -up`	Mettre à jour Pi-hole
`pihole status`	État du service
`pihole -t`	Requêtes en temps réel
`pihole allow domaine.fr`	Autoriser un domaine
`pihole deny domaine.fr`	Bloquer un domaine
`sudo pihole setpassword`	Changer le mot de passe de l'interface
`pihole -d`	Diagnostic (dépannage)

7.3. Vérifier que Pi-hole fonctionne

1. Depuis un appareil qui utilise Pi-hole, ouvrez un site avec publicités.
2. Dans **Query Log**, regardez les requêtes de cet appareil.

Vous devez voir :

- des domaines publicitaires (par exemple doubleclick.net) avec le statut **Blocked**.

8. Dépannage

Symptôme	Cause possible	Action
Aucune requête dans Query Log	Les appareils n'utilisent pas Pi-hole	Vérifiez le DNS des appareils (`nslookup example.com` doit répondre depuis l'IP de Pi-hole)
Seuls certains appareils sont filtrés	DNS sécurisé du navigateur ou DNS privé d'Android	Désactivez-les, ou bloquez-les via les réglages de Pi-hole
Un site ou une application ne fonctionne plus	Faux positif	Autorisez le domaine (section 6.4)
Plus d'Internet du tout	Pi-hole arrêté	Redémarrez-le ; en attendant, remettez le DNS de la box
Erreur de port 53 sous Docker	Autre service DNS sur la machine (systemd-resolved)	Désactivez son écoute sur le port 53

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

9. À savoir avant de se lancer

Crainte fréquente	La réalité
« Je n'ai pas de Raspberry Pi. »	Un vieux PC, une machine virtuelle ou un conteneur conviennent.
« Ça va bloquer des sites légitimes. »	Rare avec les listes par défaut ; un clic suffit pour autoriser un domaine.
« C'est compliqué. »	L'installation prend quelques minutes ; le plus délicat est de faire utiliser Pi-hole par la box.
« Mon fournisseur d'accès voit-il mes requêtes ? »	Les requêtes transmises au résolveur amont ne sont pas chiffrées par défaut. Pour les chiffrer, ajoutez un résolveur local chiffré (Unbound, ou DNS over HTTPS avec un relais comme cloudflared ou dnscrypt-proxy).
« Pi-hole ralentit-il la connexion ? »	Non : les réponses sont mises en cache, et le blocage allège les pages.
« Et les publicités YouTube ? »	Pi-hole ne les bloque pas. Utilisez uBlock Origin (ordinateur) ou une application alternative comme NewPipe (Android).
« Et la vie privée des autres membres du foyer ? »	Le journal montre tous les sites consultés : prévenez-les, ou réduisez le niveau de détail de la journalisation.

10. Challenge 7 jours

Challenge : pendant 7 jours, faites passer votre réseau (ou vos appareils) par Pi-hole.

- **Jour 1 :** installez Pi-hole.
- **Jour 2 :** configurez la box ou vos appareils.
- **Jour 3 :** naviguez normalement et constatez la différence.
- **Jour 4 :** explorez le tableau de bord et les statistiques.
- **Jour 5 :** ajoutez une liste (OISD par exemple).
- **Jour 6 :** autorisez un domaine bloqué par erreur, s'il y en a un.
- **Jour 7 :** désactivez Pi-hole une heure (**Disable blocking**) et observez le retour des publicités.

Vous allez constater :

- moins de publicités et de traqueurs sur tous vos appareils ;
- une vision claire de ce que vos appareils contactent.

gabriel.ananda@mailo.com

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

11. Alternatives et approfondissements

Si vous avez besoin de…	Essayez plutôt…
Une solution sans matériel	**NextDNS** (service en ligne, gratuit jusqu'à 300 000 requêtes par mois) ou un résolveur filtrant comme Quad9 (fiche N°6)
Un équivalent avec interface plus moderne	**AdGuard Home** (fiche N°20c, aussi disponible sur YunoHost)
Être protégé en déplacement	Un VPN **WireGuard** vers votre réseau (fiche N°20a). PiVPN, souvent cité, a arrêté son développement en avril 2024
Chiffrer les requêtes vers l'extérieur	**Unbound** (résolveur local) ou un relais DNS over HTTPS
Bloquer les publicités YouTube	**uBlock Origin** (ordinateur), **NewPipe** (Android)

12. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Installer Pi-hole	Publicités et traqueurs bloqués sur tout le réseau	Section 4
Configurer la box ou le DHCP	Protection sans rien installer sur les appareils	Section 5
Ajouter des listes	Blocage plus complet (logiciels malveillants, télémétrie)	Section 6.2
Consulter les statistiques	Vous voyez ce que contactent vos appareils	Section 7

13. Conclusion

Si vous êtes…	Choisissez…
Particulier avec un Raspberry Pi	Pi-hole
Particulier sans matériel	NextDNS ou Quad9 (fiche N°6)
Utilisateur de YunoHost	AdGuard Home (fiche N°20c)
Souvent en déplacement	Pi-hole + WireGuard (fiche N°20a)

À retenir absolument

- **Pi-hole bloque publicités et traqueurs pour tout le réseau.**
- **Le plus délicat est de le faire utiliser par la box :** si elle ne le permet pas, passez par le DHCP de Pi-hole ou réglez chaque appareil.
- **Désactivez le DNS sécurisé des navigateurs** sur les appareils à protéger.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau V1.1

- **Pi-hole ne bloque pas les publicités YouTube.**

Test final :

1. Pi-hole installé et interface accessible (http://adresse_ip_du_pi/admin).
2. Un appareil configuré pour utiliser Pi-hole comme DNS.
3. Ouvrez un site avec publicités.
4. Dans **Query Log**, des domaines publicitaires apparaissent avec le statut **Blocked**.
5. Le site s'affiche avec moins de publicités.
6. Si tout fonctionne : vous avez un bloqueur pour toute la maison ✅

Références

- Pi-hole – Présentation de Pi-hole v6 (février 2025 : serveur web intégré, pihole.toml)
- Pi-hole – Documentation Docker (exemple docker-compose.yml v6)
- Linuxiac – PiVPN publie sa dernière version et arrête le projet (avril 2024)

gabriel.ananda@mailo.com
CC BY SA