

INSTALLATION D'UN SERVEUR ADGUARD SOUS RASPBERRY PI

RaspberryPi - Debian Buster
Configuration de base

Tutoriel **ADGUARD** - RASPBERRYPI

David GOÏTRÉ

Table des matières

Introduction	1
1. Pré requis	1
2. Paramétrage du serveur	2
3. Paramétrage de connexion au serveur	3
4. Installer AdGuard Home	3
5. Configurer AdGuard Home	3
6. Paramètres DNS	6
7. Paramètres de Chiffrement	7
8. Commandes RaspberryPi.....	9
9. Conclusion	9

Introduction

AdGuard Home est un logiciel à l'échelle du réseau pour bloquer les publicités et le suivi. Une fois que vous l'avez configuré, il couvrira tous les appareils domestiques, et on n'a pas besoin de logiciel côté client pour cela. Il fonctionne comme un serveur DNS qui redirige les domaines de suivi vers un « trou noir », empêchant ainsi vos appareils de se connecter à ces serveurs.

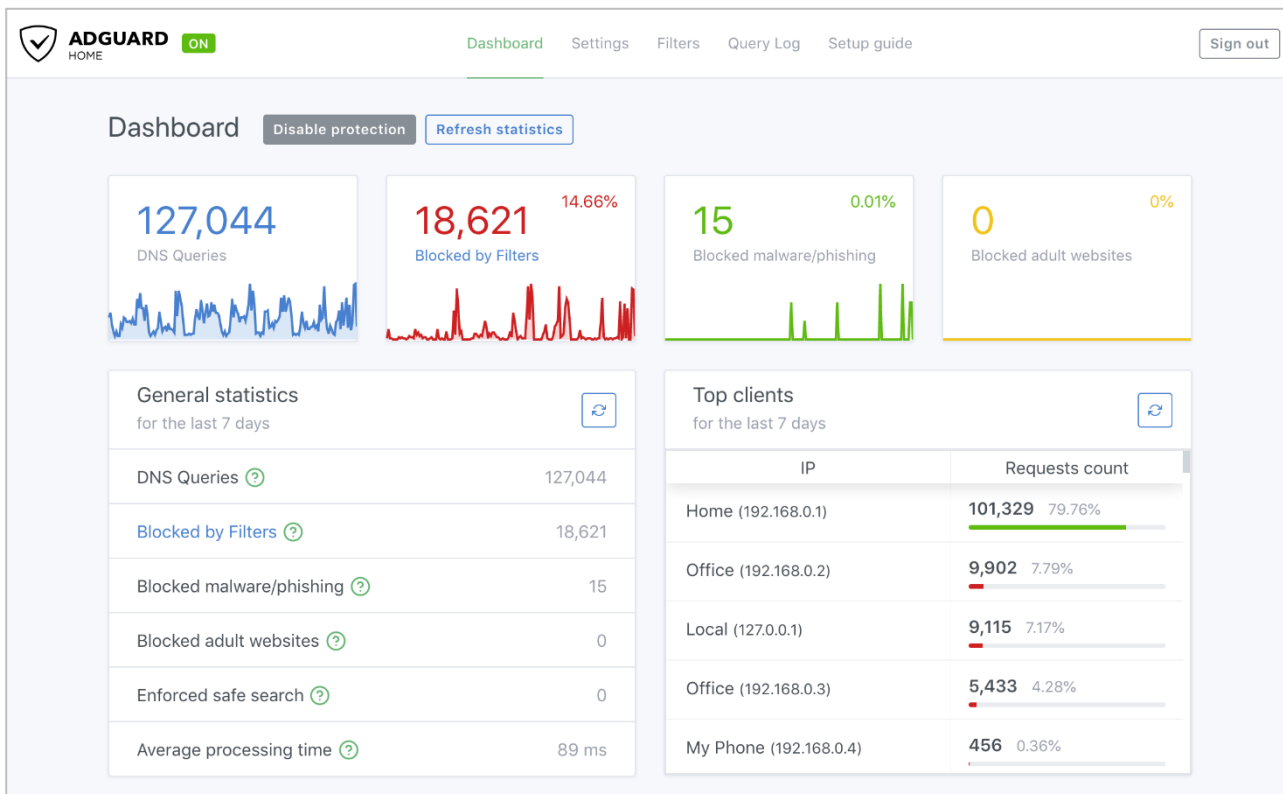
Il fournit le cryptage et l'anonymat, protège nos activités en ligne, nos achats en ligne, l'envoi d'e-mails et aide également à garder notre navigation Web anonyme.

1. Pré requis

On a besoin des différents matériels et logiciels pour la création d'un Serveur ADGUARD avec un RaspberryPi.

- Un ou des PC client sous Windows
- Une Box (Free, Orange, Sfr...)
- Un Raspberry 3B+ avec l'[OS Raspian Buster](#) installé avec [Etcher](#)
- Le logiciel [Putty](#) pour se connecter en SSH au serveur VPN
- Connaître l'interface réseau (eth0, br0, ens3...) via la commande : **ip a**
Pour notre test c'est **l'interface eth0** qui sera utilisée

Voici l'interface que l'on doit obtenir une fois le serveur **AdGuard** mise en place



2. Paramétrage du serveur

Avant d'aller plus loin, il nous faut connaître l'interface réseau de notre serveur **RaspberryPI** et lui attribuer une adresse IP fixe.

a) Lister les interfaces

```
$ ip link | awk '{ print $2}' # liste les interfaces
# ethtool <interface> | grep detected # détecte l'interface connectée
```

b) Définir une adresse IP fixe

```
# nano /etc/network/interfaces # ouvre le fichier des interfaces
```

c) Copier le texte ci-dessous dans le fichier **interfaces**

```
# Interface reseau de bouclage
auto lo
iface lo inet loopback
# Interface reseau principale
allow-hotplug eth0
iface eth0 inet static
address 192.xxx.xxx.xxx
netmask 255.255.255.0
gateway 192.xxx.xxx.xxx
```

d) Rebooter le serveur

```
# /etc/init.d/networking restart
# reboot
```

e) Paramétrer le serveur

```
$ raspi-config # ouvre l'utilitaire, sélectionner le menu System Options
```

```
┌─────────── Raspberry Pi Software Configuration Tool (raspi-config) ───────────┐
│ 1 System Options          Configure system settings                          │
│ 2 Display Options        Configure display settings                          │
└───────────┘
```

Sélectionner le menu **S3 Password** pour modifier le mot de passe et **S4 Hostname** pour modifier le nom du serveur.

```
┌─────────── Raspberry Pi Software Configuration Tool (raspi-config) ───────────┐
│ S1 Wireless LAN          Enter SSID and passphrase                          │
│ S2 Audio                  Select audio out through HDMI or 3.5mm jack        │
│ S3 Password              Change password for the 'pi' user                    │
│ S4 Hostname               Set name for this computer on a network            │
└───────────┘
```

3. Paramétrage de connexion au serveur

a) Une fois installé, ouvrir la page **127.0.0.1:3000** dans le navigateur pour effectuer la configuration initiale et apprendre à configurer les appareils pour utiliser **AdGuard Home**. On n'a pas besoin de lancer quoi que ce soit de manière explicite, le service AdGuard Home est déjà démarré après l'installation.

b) Activer le **SSH** sur le serveur. Pour ce faire, ouvrir le dossier **Boot**, de la carte SD du RaspberryPi via l'explorateur de Windows et créer un fichier **ssh** (sans extension) dans ce **dossier**.

c) Ouvrir **Putty** et se connecter au serveur AdGuard avec les identifiants (par défaut **pi/raspberry**)

b) Mettre à jour les packages du système vers la dernière version. Exécuter la commande suivante pour mettre à jour et mettre à niveau les packages de votre système :

```
# apt-get update -y  
# apt-get upgrade -y
```

4. Installer AdGuard Home

Par défaut, le paquet AdGuard n'est pas disponible dans le référentiel par défaut Debian 10. Il faut l'installer avec la commande suivante :


```
# sudo apt install snapd  
# sudo reboot  
# sudo snap install adguard-home
```

5. Configurer AdGuard Home

a) Sélectionner **Get Started** pour démarrer le processus de configuration



b) Remplacer l'interface d'écoute par l'adresse IP de votre Raspberry Pi.



Admin Web Interface

Listen interface Port

eth0 - 192.168.1.197 ▾

80

Your AdGuard Home admin web interface will be available on the following addresses:
<http://192.168.1.197>

DNS server

Listen interface Port

eth0 - 192.168.1.197 ▾

53

You will need to configure your devices or router to use the DNS server on the following addresses:
192.168.1.197

Static IP Address

AdGuard Home is a server so it needs a static IP address to function properly. Otherwise, at some point, your router may assign a different IP address to this device.

We have detected that a dynamic IP address is used — **192.168.1.197/24**. Do you want to use it as your static address?


Set a static IP address

Back

Next

Step 2/5

c) Spécifier un **nom d'utilisateur** et un **mot de passe**



Authentication


It is highly recommended to configure password authentication to your AdGuard Home admin web interface. Even if it is accessible only in your local network, it is still important to protect it from unrestricted access.

Username

Password


Confirm password


d) L'écran suivant vous montrera comment configurer différents appareils





Configure your devices


To start using AdGuard Home, you need to configure your devices to use it.
AdGuard Home DNS server is listening on the following addresses:
192.168.1.198



Router


Windows


macOS


Android


iOS


DNS Privacy

e) Cliquer sur le bouton **Suivant**, puis ouvrir le tableau de bord. Connectez-vous lorsque vous y êtes invité.

f) **AdGuard Home** est maintenant configuré et installé. Noter que l'on n'utilisera plus le **port 3000** lors de la navigation vers le portail Web. Une fois le processus de configuration terminé, on pourra accéder au portail de gestion en utilisant uniquement l'adresse IP (car il utilise le port 80).

g) Cliquer sur **Paramètres Généraux** pour les choix suivants :

- **Bloquer les domaines à l'aide des filtres...** permet de bloquer via les règles de filtrage
- **Utiliser le service de sécurité...** permet de vérifier le domaine
- **Utiliser le contrôle parental...** permet de vérifier les contenus pour adulte
- **Renforcer la recherche sécurisée...** permet de bloquer certains contenus comme les vidéos sur Youtube (à cocher si nécessaire)

6. Paramètres DNS

Cette section permet de bloquer les publicités sur Internet sur tous les périphériques connectés au DNS de Adguard.

a) Ouvrir l'interface Web d'AdGuard Home et cliquer sur le menu **Settings/Settings DNS**

b) Descendre jusqu'à la section **Configuration du serveur DNS** et cocher les lignes comme dans la capture ci-dessous (Désactiver IPV6 n'est pas obligatoire) :

Configuration du serveur DNS

Limite de taux
Le nombre de requêtes par seconde qu'un seul client est autorisé à faire (le réglage 0 fait illimité)

20

Activer le sous-réseau du client EDNS
Si activé, AdGuard Home enverra les sous-réseaux des clients aux serveurs DNS.

Activer DNSSEC
Définir l'indicateur DNSSEC dans les requêtes DNS sortantes et vérifier le résultat (résolveur compatible DNSSEC requis)

Désactiver IPv6
Si cette fonctionnalité est activée, toutes les requêtes DNS visant des adresses IPv6 (type AAAA) seront annulées.

Mode du blocage

- Par défaut : Répondre avec adresse IP zéro (0.0.0.0 pour A; :: pour AAAA) lorsque bloqué par la règle de style Adblock; répondre avec l'adresse de la règle du style /etc/hosts
- REFUSED: Répondre avec le code REFUSED
- NXDOMAIN : Répondre avec le code NXDOMAIN
- IP nulle : Répondre avec une adresse IP nulle (0.0.0.0 pour A; :: pour AAAA)
- IP personnalisée : Répondre avec une adresse IP définie manuellement

Par défaut

REFUSED

7. Paramètres de Chiffrement

Cela n'a pas beaucoup de sens de configurer le cryptage DNS à l'intérieur de son propre réseau local. Le but de la sécurisation du trafic DNS est de le sécuriser des tiers qui pourraient l'analyser ou le modifier.

Par exemple, auprès du FAI. Cela signifie que l'on aura besoin d'un serveur avec une **adresse IP publique dédiée**. Il existe de nombreux fournisseurs de serveurs cloud bon marché, tel que DigitalOcean, Vultr, Linode, etc.

Il faut donc créer un nom de domaine et y installer **Adguard Home**. Voir ce [tutorial](#) pour créer facilement un nom de domaine.

a) Obtenez un certificat SSL

Les deux **DNS-over-HTTPS** et **DNS-over-TLS** sont basés sur le cryptage TLS afin de les utiliser, on doit acquérir un certificat SSL. Un certificat SSL peut être acheté auprès d'une **autorité de certification (CA)**, une entreprise approuvée par les navigateurs et les systèmes d'exploitation pour inscrire des certificats SSL pour les domaines.

On peut également obtenir le certificat gratuitement auprès de la CA **Let's Encrypt**, une autorité de certification gratuite développée par Internet Security Research Group (ISRG).

b) Installer Certbot

```
# sudo snap install --classic certbot
```

c) Suivre le tuto [Intaller Certbot](#) pour créer un certificat. A la fin de l'installation, on obtient les deux fichiers (nécessaires pour configurer AdGuard Home) ci-dessous :

- **fullchain.pem** : certificat SSL encodé PEM
- **privkey.pem** : clé privée encodée PEM

d) Ouvrir l'interface Web d'AdGuard Home et cliquer sur le menu **Settings/Encryption settings**

Encryption

Encryption (HTTPS/TLS) support for both DNS and admin web interface

Enable Encryption (HTTPS, DNS-over-HTTPS, and DNS-over-TLS)

If encryption is enabled, AdGuard Home admin interface will work over HTTPS, and the DNS server will listen for requests over DNS-over-HTTPS and DNS-over-TLS.

Server name

Redirect to HTTPS automatically

If checked, AdGuard Home will automatically redirect you from HTTP to HTTPS addresses.

In order to use HTTPS, you need to enter the server name that matches your SSL certificate.

HTTPS port **DNS-over-TLS port**

If HTTPS port is configured, AdGuard Home admin interface will be accessible via HTTPS, and it will also provide DNS-over-HTTPS on '/dns-query' location. If this port is configured, AdGuard Home will run a DNS-over-TLS server on this port.

Certificates

In order to use encryption, you need to provide a valid SSL certificates chain for your domain. You can get a free certificate on letsencrypt.org or you can buy it from one of the trusted Certificate Authorities.

Copy/paste your PEM-encoded certificates here.

Private key

Copy/paste your PEM-encoded private key for your certificate here.

e) Cocher la case **Activer le chiffrement (HTTPS, DNS-over-HTTPS, and DNS-over-TLS)**

f) Copier le contenu du fichier **fullchain.pem** dans le champ **Certificats**

g) Copier le contenu du fichier **privkey.pem** dans le champ **Clé privée**

h) Saisir le nom de domaine dans le champ **Nom du serveur**

i) Cliquer sur le bouton **Sauvegarder la configuration**

8. Commandes RaspberryPi

a) Liste des commandes basique à la gestion du serveur RaspberryPi

```
# shutdown -h now # éteint le serveur en toute sécurité  
# shutdown -r now # redémarre le serveur en toute sécurité  
# apt install xrdp # install le bureau à distance RDP  
# systemctl enable xrdp # active xrdp en tant que service système
```

f) Autre méthode d'installation de **AdGuard**

```
$ curl -sSL https://raw.githubusercontent.com/AdguardTeam/AdGuardHome/master/  
scripts/install.sh | sh
```

9. Conclusion

AdGuard est installé et configuré avec succès sur le serveur **RaspberryPi Debian 10**. On peut désormais accéder à Internet en toute sécurité et protéger son identité.

Destiné au RaspberryPi (Raspbian), **PiVPN AdGuard** fonctionne aussi parfaitement sur une distribution Debian, Fedora ou une Ubuntu en mode VPS ou sur un ordinateur personnel.