

INSTALLATION D'UN SERVEUR ADGUARD SOUS RASPBERRY PI

Raspberry Pi - Debian Buster
Configuration de base

Tutoriel **ADGUARD** - RASPBERRY PI

David GOÏTRÉ

Table des matières

Introduction	1
1. Pré requis	1
2. Paramétrage de connexion au serveur	2
3. Paramétrage du serveur	2
4. Installer AdGuard Home	3
5. Configurer AdGuard Home	3
6. Paramètres DNS (les serveurs)	6
7. Paramètres DNS (les listes DNS)	7
8. Paramètres DHCP	8
9. Paramètres de Chiffrement	8
10a. Réécriture DNS (IPv4)	10
10b. Réécriture DNS (IPv6)	11
11. Filtrage personnalisé	12
12. Gestion de AdGuard Home.....	12
13. Modifier la configuration de AdGuard Home	14
14. Supprimer la publicité sur Youtube	14
15. Tester AdGuard Home	14
16. Commandes RaspberryPi.....	15
17. Conclusion	15

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.

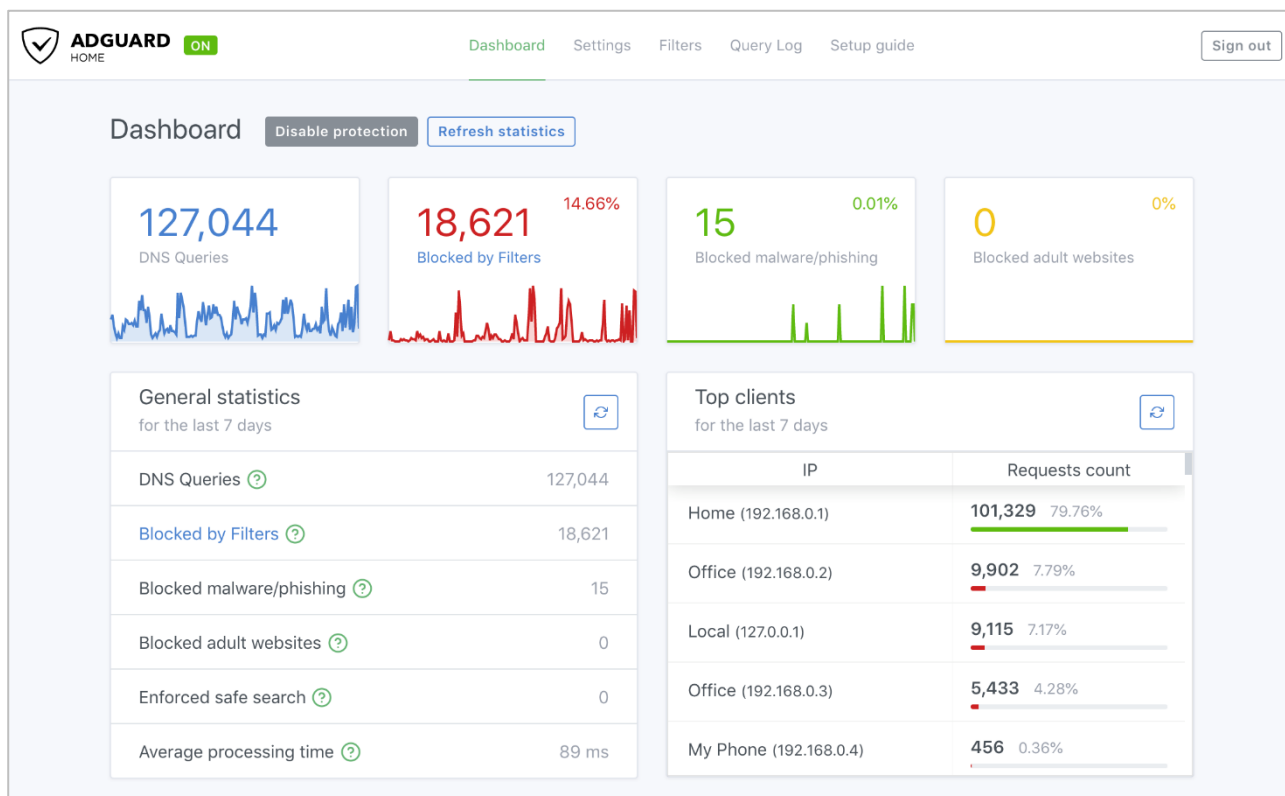
Il fournit le cryptage et l'anonymat, protège nos activités en ligne, nos achats en ligne, l'envoi d'e-mails et aide également à garder notre navigation Web anonyme.

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 de connexion au serveur

- a) 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**.
- b) Ouvrir **Putty** et se connecter au serveur AdGuard avec les identifiants (par défaut **pi/raspberry**) Pour entrer en mode admin, saisir la commande **sudo su**
- c) Exécuter la commande suivante pour mettre à jour et mettre à niveau les packages du système :

```
# apt-get update && apt-get upgrade
```

3. 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  
dns-nameservers 192.xxx.xxx.xxx
```

- d) Comme on n'utilise pas le **dhcpcd.conf** pour avoir une @IP fixe, il faut le désactiver

```
# sudo systemctl stop dhcpcd  
# sudo systemctl disable dhcpcd  
# sudo reboot
```

- e) Rebooter le serveur

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

f) Paramétrer le **DNS** du serveur

Le fichier **/etc/resolv.conf** peut être généré automatiquement au démarrage du système selon la configuration des interfaces réseaux. Ainsi, les modifications effectuées **manuellement** peuvent être **écrasées à chaque redémarrage**.

La génération dépend de la distribution Linux et du système utilisé (systemd, NetworkManager, etc)

```
# cat /etc/resolv.conf # ouvre le fichier resolv.conf
```

On peut déclarer les interfaces dans le fichier **/etc/network/interfaces** (voir page 2) ou modifier la ligne **#DNS=** en **DNS=192.XXX.XXX.XXX** du fichier **/etc/systemd/resolved.conf**

g) Paramétrage du système

Pour paramétrer le système **Raspian OS** via l'interface graphique, il suffit d'exécuter la commande

```
$ raspi-config # ouvre l'utilitaire de configuration
```

Vous trouverez plus de détails dans le fichier [Installation-ServeurRASPIANOS-Raspberry.pdf](#)

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) Une fois le serveur installé, ouvrir la page avec **@IPduServeur:3000** dans le navigateur et cliquer sur **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

eth0 - 192.168.1.197

Port

80

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

DNS server

Listen interface

eth0 - 192.168.1.197

Port

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


BackNext


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 (les serveurs)

C'est ici que l'on configure les serveurs DNS qu'AdGuard Home va utiliser pour résoudre les noms de domaine sur Internet ainsi que la manière dont il va les requêter (https, tls, udp, tcp etc...).

En cliquant sur **liste des fournisseurs DNS connus**, on peut voir un ensemble de fournisseurs de DNS utilisables. Ces fournisseurs ont des spécificités que l'on peut découvrir (blocage de site frauduleux, domaine connu pour du phishing etc...). Pour ajouter ceux de **AdGuard**, il faut copier l'adresse et la coller dans AdGuard Home.

Dans l'exemple ci-dessous, on a sélectionné l'adresse **DNS-over-HTTPS**. Le DNS-over-HTTPS permet de chiffrer les requêtes DNS en utilisant HTTPS. Pour que cela fonctionne, il faudra ouvrir le port 443 (HTTPS) sur le pare-feu depuis le serveur AdGuard Home vers Internet.

- a) Ouvrir l'interface Web d'AdGuard Home et cliquer sur le menu **Settings/Settings DNS**
- b) Dans la section **Serveurs DNS upstream**, coller la ou les adresses DNS-over-HTTPS, DNS IPv4, DNSCrypt IPv4, etc... (exemple de DNS Chiffrés ci-dessous)

```
tls://dns.adguard-dns.com
quic://unfiltered.adguard-dns.com
```

- c) Vérifier les tests **Secure DNS** et **DNSSEC** : <https://dnscheck.tools> et [Browsing Exp Security Check](#)
- d) Cocher une des cases ci-après selon votre besoin. Par défaut Equilibrage de charge et cocher.
- e) Dans la section **Serveurs DNS de repli**, coller une adresse DNS. Celle-ci sera utilisée en cas de panne sur les DNS ajoutés plus haut (encore plus important si l'on n'utilise qu'un seul fournisseur).

```
https://dns.google/dns-query
```

- f) Une fois la configuration terminée, on clique sur **Tester les upstreams** et sur **Appliquer**. Si les upstream sont bien ajoutés et le pare-feu configuré on doit voir ceci apparaître un message de réussite : **Les serveurs DNS spécifiés fonctionnent correctement**.
- g) Dans la section **Configuration du serveur DNS**, régler la **Limite de taux**. Elle définit le nombre de requête DNS qu'un client peut faire par seconde. S'il est défini trop bas, il peut **ralentir** la navigation sur Internet car le serveur ne répondra plus, s'il est trop élevé (ou sur 0), il peut être sujet aux attaques de type DNS Flooding (ou DDOS). Il faut donc l'ajuster en fonction de nos besoins.

Pour une utilisation à son domicile, la valeur de 20 est convenable. Cliquer sur **Enregistrer** pour appliquer les modifications.

DNS server configuration

Rate limit
The number of requests per second that a single client is allowed to make (setting it to 0 means unlimited)











☒ **Enable EDNS Client Subnet**
If enabled, AdGuard Home will be sending clients' subnets to the DNS servers.

7. Paramètres DNS (les listes DNS)

C'est ici que l'on configure les listes de **blocage** ou **autorisation** qu'AdGuard home va utiliser pour bloquer ou pas tel ou tel service ou site web.


a) Ouvrir l'interface Web d'AdGuard Home et cliquer sur le menu **Filters/DNS Blocklists** et ajouter des **listes de blocage DNS** comme dans la capture ci-dessous.

AdGuard Home understands basic adblock rules and hosts files syntax.

Activé	Nom	URL de la liste	Nombre des règles	Dernière mise à jour	Actions
<input checked="" type="checkbox"/>	AdGuard DNS filter	https://adguardteam.github.io/Ad...	36962	22 avril 2021 à 17:51	 
<input checked="" type="checkbox"/>	AdAway Default Blocklist	https://adaway.org/hosts.txt	8767	22 avril 2021 à 17:51	 
<input checked="" type="checkbox"/>	MalwareDomainList.com Hosts List	https://www.malwaredomainlist.c...	1	22 avril 2021 à 17:51	 
<input checked="" type="checkbox"/>	The Big List of Hacked Malware W...	https://raw.githubusercontent.co...	13822	22 avril 2021 à 17:51	 
<input checked="" type="checkbox"/>	Online Malicious URL Blocklist	https://curben.gitlab.io/malware-fi...	7053	22 avril 2021 à 17:51	 

Previous

Page / 7

5 rows 

Next

Add blocklist

Check for updates

b) Cliquer sur le bouton **Add blocklist**

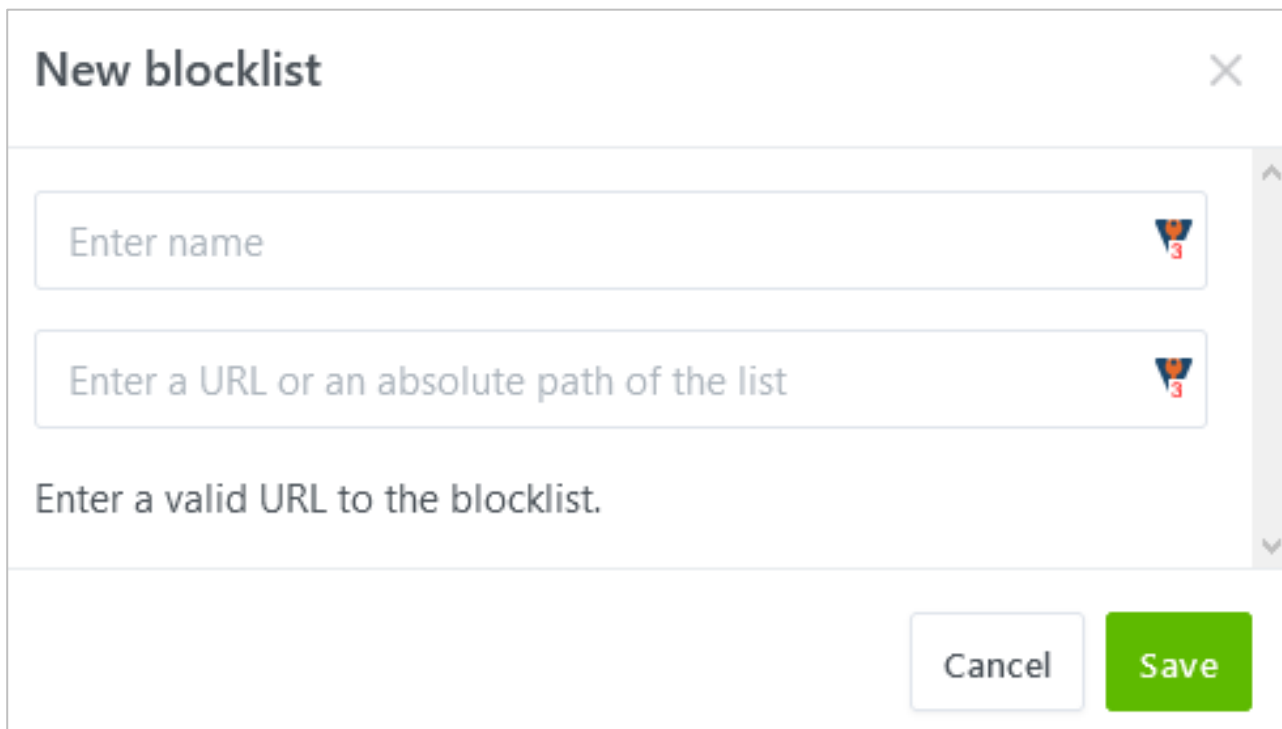
c) Cliquer sur le bouton **Choose from the list** pour ajouter une liste d'Adguard et cliquer sur le bouton **Add a custom list** pour ajouter une liste proposée par un site partenaire comme [Firebog](#).

New blocklist

Choose from the list

Add a custom list

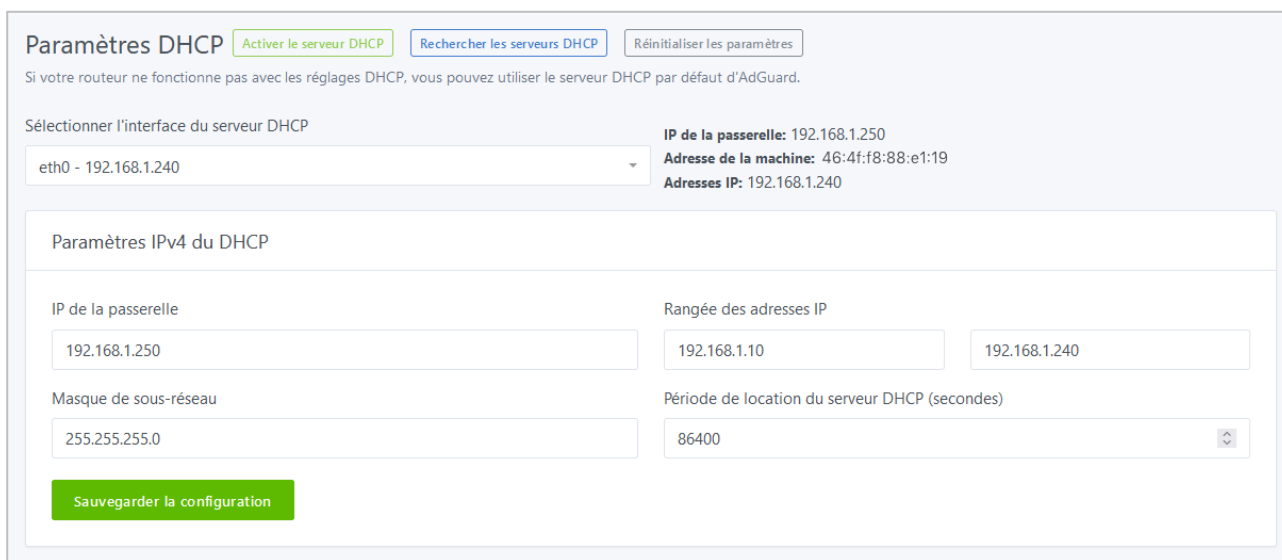
d) Copier le lien proposé par le site (ex : <https://v.firebog.net/hosts/static/w3kbl.txt>) et le coller, puis saisir un nom (voir ci-dessous) et valider.



The image shows a 'New blocklist' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Enter name' and 'Enter a URL or an absolute path of the list'. Below these fields is a text prompt: 'Enter a valid URL to the blocklist.' At the bottom right, there are two buttons: 'Cancel' and 'Save'.

8. Paramètres DHCP

Utiliser AdGuard Home comme serveur DHCP par défaut, paramétrer le DHCP comme ci-dessous :



The image shows the 'Paramètres DHCP' (DHCP Settings) interface. At the top, there are three buttons: 'Activer le serveur DHCP' (green), 'Rechercher les serveurs DHCP' (blue), and 'Réinitialiser les paramètres' (grey). Below these is a note: 'Si votre routeur ne fonctionne pas avec les réglages DHCP, vous pouvez utiliser le serveur DHCP par défaut d'AdGuard.' The main section is titled 'Sélectionner l'interface du serveur DHCP' and shows a dropdown menu with 'eth0 - 192.168.1.240' selected. To the right, there are three lines of information: 'IP de la passerelle: 192.168.1.250', 'Adresse de la machine: 46:4f:f8:88:e1:19', and 'Adresses IP: 192.168.1.240'. Below this is a section titled 'Paramètres IPv4 du DHCP' with two columns of settings. The left column has 'IP de la passerelle' (192.168.1.250) and 'Masque de sous-réseau' (255.255.255.0). The right column has 'Rangée des adresses IP' (192.168.1.10 and 192.168.1.240) and 'Période de location du serveur DHCP (secondes)' (86400). At the bottom left, there is a green button labeled 'Sauvegarder la configuration'.

9. Paramètres de Chiffrement

Il existe deux méthodes pour configurer l'accès au portail web de AdGuard home pour fonctionner en **https** avec un **certificat auto-signé** ou un **certificat SSL** à l'aide d'un nom de domaine.

a) Cliquer sur le menu **Paramètres/Paramètres de chiffrement** et cocher la case **Activer le chiffrement**

b) Saisir le nom du serveur : **adguard-home.test.fr**

Chiffrement avec un certificat auto-signé

On va créer un fichier de configuration avec le CN : **adguard-home.test.fr**

```
# sudo nano adguard-home.conf
```

a) Copier les lignes ci-dessous dans le fichier

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = FR (Initiale de la langue)
ST = Occitanie (région)
L = Toulouse (ville)
O = Home (organisation)
OU = IT (unité d'organisation)
CN = adguard-home.test.fr
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = DNS.1:adguard-home.test.fr
```

b) Saisir la commande pour générer le certificat et la clé privée

```
openssl req -x509 -days 365 -nodes -newkey rsa:2048 -config adguard-home.conf -keyout
adguard-key.pem -out adguard-cert.pem
```

c) Afficher le fichier du certificat et copier son contenu dans la **section Certificat**

```
cat adguard-cert.pem
```

On peut voir le message d'avertissement **Chaîne de certificat invalide** s'afficher en rouge car on utilise un certificat auto-signé.

d) Afficher le fichier de la clé privée et copier son contenu dans la **section Clé privée**

```
cat adguard-key.pem
```

e) On clique sur **sauvegarder la configuration**.

Chiffrement avec un certificat SSL

Si l'on veut créer un certificat SSL signé, 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 faudra donc créer un nom de domaine et y installer **Adguard Home**. Voir ce [tutorial](#) pour créer facilement un nom de domaine et pour tester la compatibilité du nom de domaine, voir ce [site](#).

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**

The screenshot shows the 'Encryption' settings page in AdGuard Home. At the top, it says 'Encryption (HTTPS/TLS) support for both DNS and admin web interface'. There is a checkbox labeled 'Enable Encryption (HTTPS, DNS-over-HTTPS, and DNS-over-TLS)' which is currently unchecked. Below this, a note states: '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.' The 'Server name' section has a text input field with the placeholder 'Enter your domain name' and a checkbox labeled 'Redirect to HTTPS automatically'. A note below the input field says: 'In order to use HTTPS, you need to enter the server name that matches your SSL certificate.' The 'DNS-over-TLS port' section has a text input field with the value '853'. A note below it says: 'If this port is configured, AdGuard Home will run a DNS-over-TLS server on this port.' The 'HTTPS port' section has a text input field with the value '443'. A note below it says: 'If HTTPS port is configured, AdGuard Home admin interface will be accessible via HTTPS.'

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**

10a. Réécriture DNS (IPv4)

Dans cette partie, on va définir la correspondance nom avec l'adresse IP du serveur AdGuard.

a) Cliquer sur le menu **Filtres/Réécritures DNS** et cliquer sur **Ajouter une réécriture DNS**.

b) Dans la nouvelle fenêtre, renseigner les informations suivantes :

- Saisir un domaine : **intranet.test.fr**
- Saisir l'adresse IP du serveur AdGuard : **192.168.1.250**

c) Cliquer sur **Enregistrer**

d) On peut maintenant accéder au serveur via l'url **https://intranet.test.fr**

10b. Réécriture DNS (IPv6)

La **version 0.107.46** de notre serveur **AdGuard Home** possède maintenant l'IPv6. On peut donc la déclarer dans les paramètres DNS IPv6 du routeur ou de la box. La réécriture DNS fonctionnera ainsi avec les deux protocoles d'IP. Si l'IPv6 n'est pas déclarée, la désactiver sur la carte réseau du système.

- Se connecter au serveur en **ssh**
- Saisir la commande **ip a**
- Le résultat s'affiche
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> ...
link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff
inet 192.xxx.xxx.xxx/24 brd 192.xxx.xxx.xxx scope global eth0
inet6 **fe80::xxxx:xxxx:xxxx:xxxx**/64 scope link
- Copier l'IPv6 de la **ligne inet6**, puis suivre l'une des méthodes ci-après

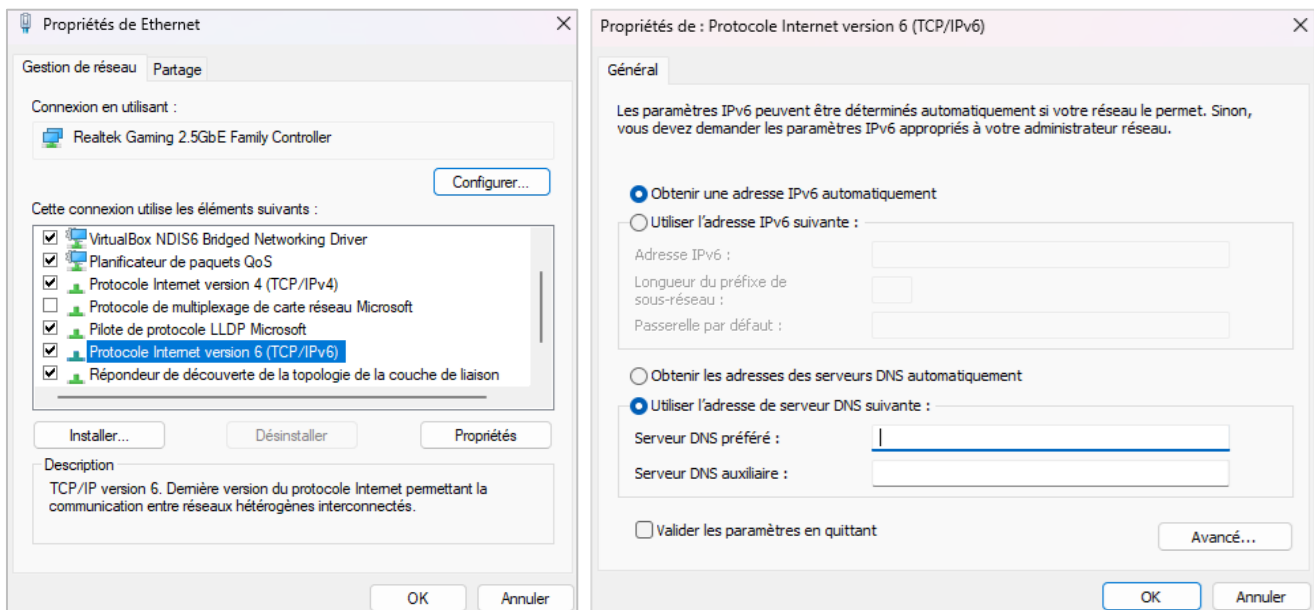
Méthode 1 : via la Box Internet (Sfr, Free, Orange...)

- Se connecter à l'administration de la box
- Ouvrir la **configuration IPv6**
- Activer l'utilisation de **serveurs DNS Personnalisés**
- Copier l'IPv6 dans le champ **Serveur DNS IPv6 Primaire**



Méthode 2 : via la carte réseau du PC

- Ouvrir les propriétés de la carte réseau, sélectionner **Protocole IPv6**
- Coller l'IPv6 dans le champ **Serveur DNS préféré**



- Cliquer sur le bouton **Ok** deux fois

11. Filtrage personnalisé

Cette section permet de gérer les règles de filtrage afin que **AdGuard Home** autorise ou non les sites ajouter à cette section.

Enter one rule on a line. You can use either adblock rules or hosts files syntax.

`@@||https://docs.google.com/^$important`

Apply

a) Ouvrir l'interface Web d'AdGuard Home et cliquer sur le menu **Filters/Custom filtering rules**

b) Descendre jusqu'à la section **Check the filtering** et saisir une url valide à vérifier

Check the filtering
Check if the host name is filtered

https://docs.google.com/

Check

https://docs.google.com/
Not found in your filter lists

Block

c) Cliquer sur le bouton **Check**, AdGuard Home vérifie l'url et nous propose de la bloquer si elle n'existe pas dans la liste. Le bouton **Block** ou **Unblock** s'affiche. Cliquer dessus pour appliquer le filtre.

d) L'url apparaît dans la liste avec le suffixe **||** si on n'autorise pas l'url et **@@||** si on autorise l'url

e) Cliquer sur le bouton **Apply** pour appliquer les règles

12. Gestion de AdGuard Home

a) Vérifier et/ou activer AdGuard Home

```
# sudo systemctl status AdGuardHome # vérifie le statut de AdGuardHome
# sudo systemctl enable AdGuardHome # Active AdGuardHome
# sudo systemctl start AdGuardHome # lance AdGuardHome
# sudo systemctl daemon-reload # relance le démon
```

b) Vérifier le fichier de service

```
# sudo nano /etc/systemd/system/AdGuardHome.service # vérifie le service
```

Résultat

```
[Unit]
Description=AdGuard Home: Network-level blocker
ConditionFileIsExecutable=/opt/AdGuardHome/AdGuardHome

[Service]
StartLimitInterval=5
StartLimitBurst=10
ExecStart=/opt/AdGuardHome/AdGuardHome -s run
WorkingDirectory=/opt/AdGuardHome
StandardOutput=file:/var/log/AdGuardHome.out
StandardError=file:/var/log/AdGuardHome.err
Restart=always
RestartSec=120

[Install]
WantedBy=multi-user.target
```

c) Réinstaller AdGuard Home

```
# sudo rm -r /opt/AdGuardHome
# sudo rm /etc/systemd/system/AdGuardHome.service
# cd /home/pi/AdGuardHome
# sudo ./AdGuardHome -s uninstall
# sudo ./AdGuardHome -s install
# sudo ./AdGuardHome -s status
# sudo reboot
```

d) Sauvegarder AdGuard Home

```
# cd /opt/AdGuardHome ou encore cd /var/snap/adguard-home/6450
# sudo cp -r Data Databackup # contient tous les filtres DNS
# sudo cp AdGuardHome.yaml AdGuardHome.yaml.backup # réglages de AdGuard
```

e) Mise à jour automatique de AdGuard Home

```
$ cd /home/pi/AdGuardHome
# sudo ./AdGuardHome --update
```

f) Mise à jour manuelle de AdGuard Home

```
$ mkdir /home/user/temp
# wget https://github.com/AdguardTeam/AdGuardHome/releases/download/v0.107.21/
AdGuardHome_linux_armv7.tar.gz
# sudo tar xzvf AdGuardHome_linux_armv7.tar.gz
# sudo cp /temp/*.* /AdGuardHome/
# sudo reboot
```

13. Modifier la configuration de AdGuard Home

AdGuardHome enregistre la configuration de l'interface d'écoute de l'**Admin WEB Interface** et du **DNS Server** dans le fichier **AdGuardHome.yaml**. Il suffit d'éditer ce dernier et modifier les valeurs.

a) Chercher et ouvrir le fichier

```
# sudo find / -type f -iname "*.yaml" # recherche les fichiers yaml dans tout le système
# sudo nano /path/AdGuardHome.yaml # Editer le fichier
```

b) Modifier le fichier comme ci-dessous pour corriger la configuration

```
bind_host : 192.168.XXX.XXX
bind_port : 80
.....
.....
dns:
  bind_hosts :
    - 192.168.XXX.XXX
ports : 53
.....
```

14. Supprimer la publicité sur Youtube

Pour supprimer la publicité sur Youtube, il faut activer le **DNS via HTTPS** du navigateur.

- Ouvrir les paramètres du navigateur tel que Firefox
- Chercher les **paramètres réseaux**
- Cocher la case **Activer le DNS via HTTPS**
- Dans le champ **Utiliser un fournisseur**, choisir **Personnalisé**
- Dans le champ **Personnalisé**, saisir l'**@IP** du serveur Adguard Home

15. Tester AdGuard Home

AdGuard est bien installé. Pour vérifier son bon fonctionnement, il suffit de le tester sur différents sites tel que :

- Test AdGuard : <https://adguard.com/fr/test.html>
- Test sites bloqués : <https://d3ward.github.io/toolz/adblock>
- Test services bloqués : <https://canyoublockit.com>
- Pubs supprimées : <https://www.speedtest.net/fr>
- Liste de filtres AdGuard : <https://adguard.com/kb/it/general/ad-filtering/adguard-filters>

On peut aussi vérifier en ligne de commande sur le poste client

```
$ ipconfig /all | findstr "DNS\ Servers"
$ nslookup google.fr
```

Attention pour que **AdGuard Home** bloque efficacement, il est nécessaire de désactiver l'iPv6 sur la carte réseau du ou des pc clients, si ce dernier n'est pas déclaré dans la box.

16. 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 # installe le bureau à distance RDP
# systemctl enable xrdp # active xrdp en tant que service système
# apt install openssh-server # installe le SSH
# systemctl enable sshd.service # active le service SSH au démarrage
##### Désactive la mise en veille #####
# systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target
```

b) Autre méthode d'installation de **AdGuard Home**

```
# curl -sSL https://raw.githubusercontent.com/AdguardTeam/AdGuardHome/master/
scripts/install.sh | sh
ou
# curl -s -S -L https://raw.githubusercontent.com/AdguardTeam/AdGuardHome/master/
scripts/install.sh | sh -s -- -v
```

17. Conclusion

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

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

Pour Debian

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

Pour Fedora

```
# sudo dnf install snapd
# sudo ln -s /var/lib/snapd/snap /snap
# sudo snap install adguard-home
```

Pour tout autre distribution, voir le lien : <https://snapcraft.io/adguard-home>