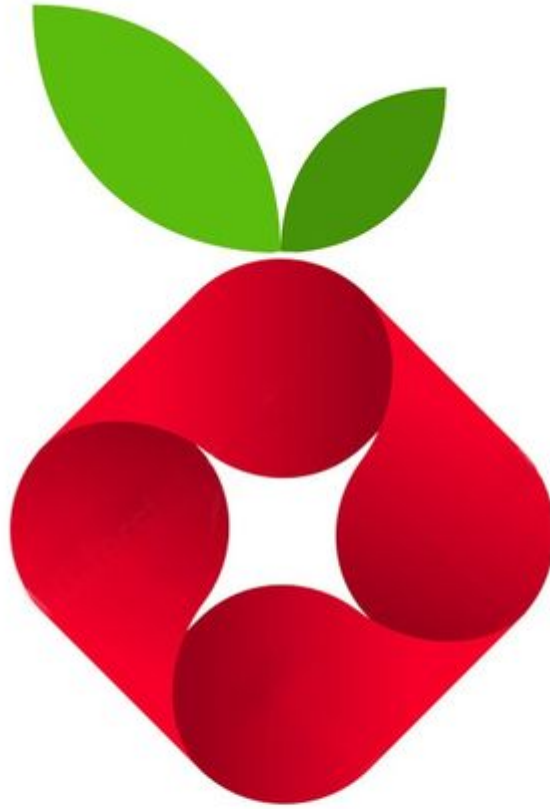


Edilson Carlos - Lucas Alazary - Ayoub Djebli



Pi-Hole

Sommaire

1. <i>Présentation</i>	<i>p.3</i>
<ul style="list-style-type: none">● Explication du Pi-Hole● Définition du DNS menteur● Définition DHCP	
2. <i>Contexte</i>	<i>p.4</i>
<ul style="list-style-type: none">● Le concepte du Pi-Hole● Définition blocklists● But du Pi-Hole	
3. <i>Procédure</i>	<i>p.5 à 6</i>
<ul style="list-style-type: none">● Etape par étape● Image	
4. <i>Résultats technique attendus</i>	<i>p.7</i>
<ul style="list-style-type: none">● Liste de tous les résultats	
5. <i>Teste de la fonctionnalité</i>	<i>p.8</i>
6. <i>Image relatif au projet</i>	<i>p.9 à 11</i>
<ul style="list-style-type: none">● Tableau et schéma du Pi-Hole	

1. Présentation

Pi-hole est un bloqueur de publicité au niveau du réseau qui agit comme un DNS menteur.

(Les DNS menteurs fonctionnent comme le DNS mais au lieu de renvoyer un code d'erreur standard « ce domaine n'existe pas » quand on entre le nom de domaine avec des lettres comme (google.com), amènent l'utilisateur vers une page de recherche sponsorisée proposant des suggestions de noms de domaines validés. Bien souvent, ces systèmes sont avant tout mis en place pour pouvoir placer des liens publicitaires sur les pages d'erreur)

Et éventuellement comme un serveur Dynamic Host Configuration Protocol.

(Le DHCP est un protocole réseau chargé de la configuration automatique des adresses IP d'un réseau informatique. Il évite ainsi à l'utilisateur qui se connecte pour la première fois à un réseau, d'avoir à configurer la pile IP de son équipement)

Il est destiné à être utilisé sur un réseau privé. Il est conçu pour être installé sur des périphériques intégrés dotés de capacités réseau, tels que le Raspberry Pi, mais il peut être utilisé sur d'autres machines exécutant Linux ou dans des environnements virtualisés.

Pi-hole est en mesure de bloquer les publicités traditionnelles sur les sites Web ainsi que les publicités moins conventionnelles, telles que celles sur les téléviseurs intelligents et les publicités pour systèmes d'exploitation mobiles.

2. Contexte

Le concept du Pi-hole est simple. Pour commencer on installe un service sur une machine sur un réseau local (historiquement, une Raspberry Pi, mais depuis un moment ça gère aussi différentes versions de Linux et Docker), qui va se charger de bloquer pubs et autres trackers divers, directement au niveau des DNS. Et les résultats sont de ne plus avoir de pub sur les appareils de votre maison, y compris sur certains jeux Free 2 Play mobiles.

Pour mettre les choses au clair, Pi-hole ne peut pas tout bloquer. Même avec la 5.0 toute fraîche qui vient de débarquer. La raison est que Pi-hole utilise une technique liée aux DNS, et certains services comme YouTube utilisent les mêmes adresses pour balancer leurs pubs. Si vous bloquez les pubs, vous bloquez donc le contenu ! Pour ces derniers, il faut ruser et continuer à installer un autre bloqueur avec scripts sur vos navigateurs. Sur Android, on peut aussi passer par des apps comme l'excellent YouTube Vanced, mais c'est un autre sujet.

Une fois Pi-hole en place, deux options s'offrent à nous, laisser les machines trouver leur adresse IP via le DHCP Pi-hole qui va devenir le serveur DNS de votre réseau, ou « forcer » ce paramètre à la main dans vos différents OS, en rentrant comme DNS l'adresse IP de la machine qui fait tourner Pi-hole. Ça dépend de votre installation, et de vos besoins.

Le but est de changer le serveur DNS déclaré et de mettre le Pi-Hole qui lui appliquera les blacklists. Les blacklists permettent de bloquer des adresses au cas par cas. Ces adresses sont tout simplement ajoutées aux blocklists.

(Blocklists ou en français liste noire est une liste d'éléments d'un ensemble qui ne sont pas acceptés. Dans le domaine de la sécurité informatique, une liste de blocage peut être utilisée pour exclure l'ensemble à détecter, mettre en quarantaine, bloquer ou effectuer des analyses de sécurité. Cette liste est exclusive, confirmant que l'élément analysé n'est pas acceptable. C'est le contraire d'une liste de sécurité, qui confirme que les éléments sont acceptables. Une liste de blocage des e-mails, par exemple, n'autorise pas la réception d'e-mails provenant d'adresses e-mail spécifiques, telles que celles connues pour être malveillantes.)

Une fois qu'on aura bien chargé en blacklists, il sera nécessaire de mettre au cas par cas des adresses dans la whitelist (celle-ci prime sur la blacklist) exemple YouTube car cela bloque aussi la vidéo.

3. Procédure

Création de la machine virtuelle :

Télécharger Raspberry Pi OS

Lancer VirtualBox

Créez une nouvelle VM avec les caractéristiques suivante


Nom : Raspberry Pi-Hole
Machine : Dossier : C:\VMs
Type : Linux
Version : Debian (32 bits)
Taille de la mémoire : 1024 Mo

? X

← Crée une machine virtuelle

Nom et système d'exploitation

Veillez choisir un nom et un dossier pour la nouvelle machine virtuelle et sélectionner le type de système d'exploitation que vous envisagez d'y installer. Le nom que vous choisirez sera repris au travers de VirtualBox pour identifier cette machine.

Nom :	<input type="text" value="Raspberry Pi Desktop"/>
Dossier de la machine :	<input type="text" value="C:\VMs"/>
Type :	Linux 
Version :	Debian (32-bit)

Mode expert

Suivant >

Annuler

Disque dur : Créer un disque dur virtuel maintenant

Cliquez sur Créer

Nommez l'image du disque virtuel Raspberry Pi-Hole.vdi

Taille du fichier : 14 Go

Type de fichier du disque dur : VDI

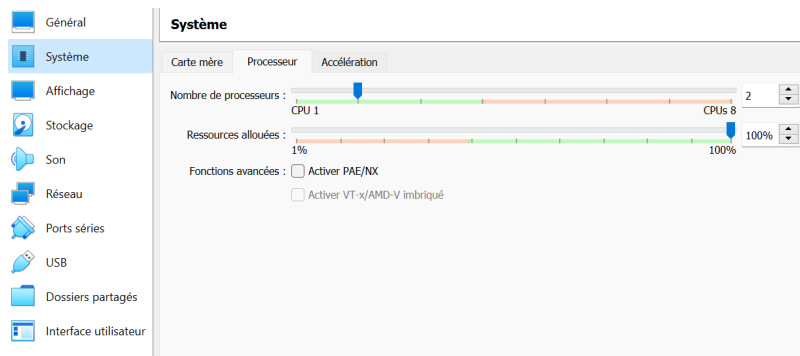
Stockage sur le disque dur physique : alloué dynamiquement

- | | |
|--|---|
| <input type="radio"/> Ne pas ajouter de disque dur virtuel | <input type="radio"/> VDI (VirtualBox Disk Image) |
| <input checked="" type="radio"/> Créer un disque dur virtuel maintenant | <input checked="" type="radio"/> VHD (Disque dur Virtuel) |
| <input type="radio"/> Utiliser un fichier de disque dur virtuel existant | <input type="radio"/> VMDK (Virtual Machine Disk) |

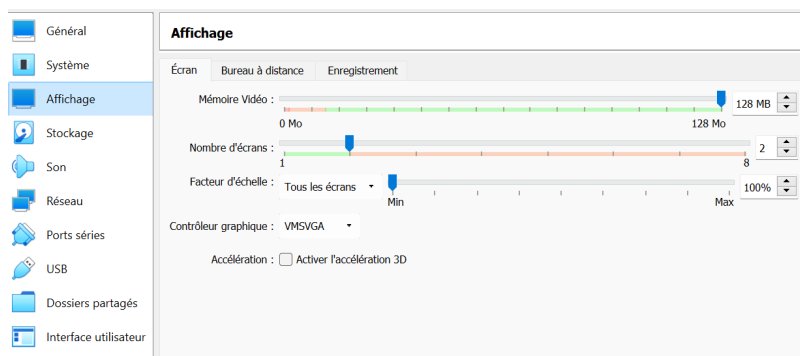
Cliquez sur Créer

Sélectionnez Système puis Processeur

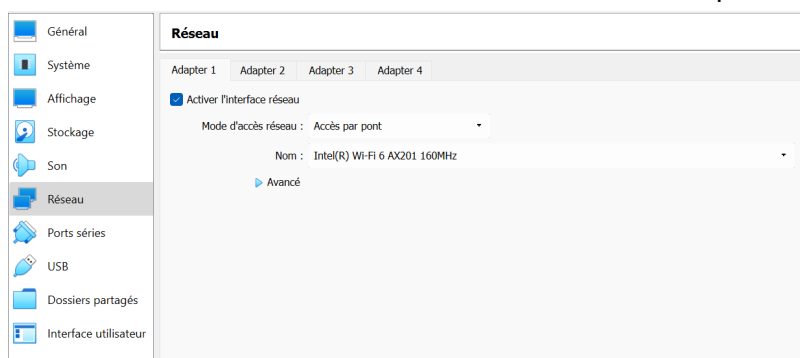
Donnez à la VM 2 processeurs



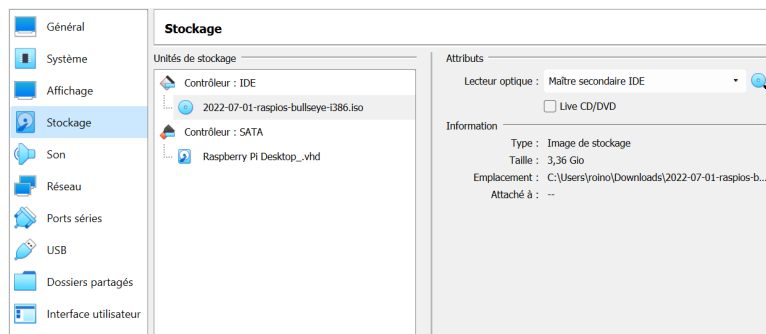
Sélectionnez Affichage
Mettre la mémoire vidéo à 128 Mo



Sélectionnez réseau
Définissez le menu déroulant Attaché à sur Adaptateur ponté



Sélectionnez Stockage
Cliquez sur le lecteur de CD-ROM



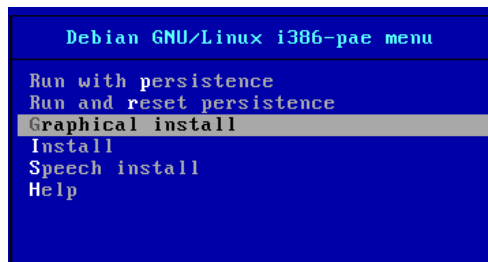
Sélectionnez le menu déroulant du disque à droite puis Choisissez un fichier de disque optique virtuel

Recherchez et sélectionnez le fichier .iso du bureau Raspberry Pi

Cliquez sur OK

Lancer la machine virtuelle Raspberry Pi-Hole

Sélectionnez l'installation graphique



Sélectionnez le langage du clavier puis Continuer

Sélectionnez Guidé utiliser tout le disque puis cliquez sur Continuer

Sélectionnez Oui pour confirmer l'écriture des modifications sur le disque puis cliquez sur Continuer

Attendez que Debian et le bureau Raspberry Pi soient installés

Sélectionnez Oui pour installer GRUB sur le secteur de démarrage principal puis cliquez sur Continuer

Sélectionnez /dev/sda > cliquez sur Continuer

Redémarrer la VM

Cliquez sur Suivant dans la boîte de dialogue de bienvenue

Définissez le pays, la langue et le fuseau horaire puis cliquez sur Suivant

Entrez et confirmez un mot de passe pour l'utilisateur pi puis cliquez sur Suivant

Cliquez sur Passer à la mise à jour du logiciel

Cliquez sur Terminer pour redémarrer la machine virtuelle et terminer la configuration

Installation des mises à jour et de Pi-Hole

Cliquez sur le bouton Applications puis Accessoires puis Terminal

Exécutez les commandes des suivantes pour installer les mises à jour

mise à jour `sudo apt`

`sudo apt upgrade -y`

`sudo apt propre`

`sudo redemarre maintenant`

Sélectionnez Périphériques puis Insérer l'image du CD des ajouts d'invités...

Si l'installation s'exécute automatiquement, sélectionnez Exécuter

Sur le bureau, faites un clic droit sur le disque Guest Additions puis Ouvrir dans le terminal

Dans la fenêtre du terminal, exécutez les commandes suivantes

`sudo sh ./VBoxLinuxAdditions.run`

`sudo redemarre maintenant`

La VM va redémarrer

Au redémarrage, vous pouvez maintenant afficher la machine virtuelle en plein écran et la résolution interne changera automatiquement pour correspondre à la taille de la fenêtre.

Cliquez sur le bouton Applications puis Accessoires puis Terminal

Exécutez la commande suivante pour installer Pi-Hole

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

Appuyez sur Entrée jusqu'à ce que la sélection DNS s'affiche

Sélectionnez un fournisseur DNS et appuyez sur Entrée
Appuyez sur Entrée dans le reste du programme d'installation de Pi-Hole, en sélectionnant les valeurs par défaut
Copiez le mot de passe administrateur généré aléatoirement (juste au cas où)
Appuyez sur Entrée pour terminer l'installation
Exécutez la commande suivante pour modifier le mot de passe administrateur Pi-Hole
`sudo pihole -a -p`
Entrez et confirmez le nouveau mot de passe
Cliquez sur le bouton Applications puis Internet puis Navigateur Web Chromium
Accédez à <http://DNSorIP/admin>
Cliquez sur Connexion
Authentifiez-vous avec le mot de passe administrateur
Tester le Pi-Hole
Cliquez avec le bouton droit sur la connexion réseau VM puis Paramètres réseau sans fil et filaire
Sélectionnez eth0 dans la liste déroulante de l'interface
Effacez les serveurs DNS et entrez l'adresse IP de la machine virtuelle
Cliquez sur Appliquer
Cliquez sur Périphériques puis Réseau puis Connecter l'adaptateur réseau pour désactiver la mise en réseau
Cliquez sur Périphériques puis Réseau puis Connecter l'adaptateur réseau pour réactiver la mise en réseau
Dans Chromium, ouvrez un nouvel onglet et accédez à <https://yahoo.com>
Revenez à l'onglet Pi-Hole et voyez que certaines requêtes DNS ont été bloquées
configuration à partir du client Windows
Cliquez sur le bouton Démarrer puis Panneau de configuration Type puis appuyez sur Entrée
Cliquez sur Afficher par puis Petites icônes
Cliquez sur Centre réseau et partage
Cliquez sur Modifier les paramètres de l'adaptateur
Clic droit sur la connexion réseau puis Propriétés
Sélectionnez Protocole Internet Version 4 (TCP/IPv4) puis Propriétés
Sélectionnez l'option radio à côté de Utiliser les adresses de serveur DNS suivantes
Entrez l'adresse IP de la machine virtuelle Pi-Hole
Cliquez sur OK dans les deux fenêtres de dialogue ouvertes
Cliquez avec le bouton droit sur le bouton Démarrer puis Invite de commandes (admin)
Tapez les commandes suivantes pour vider votre cache DNS et redémarrer les connexions réseau
`ipconfig /flushdns`

`ipconfig /release`

`ipconfig /renouveler`

4. Résultats techniques attendus

- Bloquer les pubs.
- bloquer les sites malveillants.
- site fonctionnel même après avoir bloqué la pub.
- Naviguer plus rapidement.
- aucune extension nécessaire.
- Surfez en toute tranquillité.

5. Teste de la fonctionnalité

je vais par exemple tenter de joindre le domaine <http://admin.gentbcn.org/> qui est sur la liste de abuse.ch parce qu'il est connu comme hébergement de malwares :

Si l'adresse est correcte, voici trois autres choses que vous pouvez essayer de faire :

- Réessayer ultérieurement.
- Vérifier votre connexion au réseau.
- Si vous êtes connecté au travers d'un pare-feu, vérifier que Firefox a la permission d'accéder au Web.

Réessayer

Visiblement, j'ai été bloqué quelque part, pour s'assurer que c'est bien le Pi-Hole qui a fait le job, nous pouvons consulter le journal de requêtes dans l'interface web "Query Log" pour voir que c'est bien un blocage issu d'une entrée de liste :

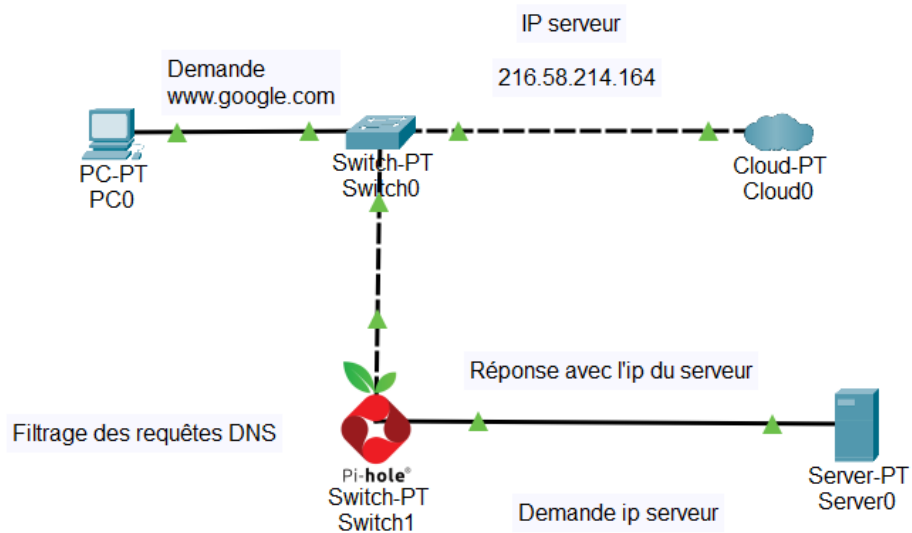
2021-11-07 11:55:43	A	admin.gentbcn.org	192.168.1.23	Blocked (gravity)	IP (0.1ms)
---------------------	---	-------------------	--------------	-------------------	---------------

6. Image relatif au projet

Voici le tableau de bord du pi-hole



Schéma du fonctionnement de pi hole



Panneau de configuration du dns

Pi-hole

hostname: raspberrypi

Status

Active Temp: 54.2 °C
Load: 0.16 0.17 0.11
Memory usage: 7.6%

MAIN NAVIGATION

Dashboard

Query Log

Long term data

Whitelist

Blacklist

Group Management

Disable

Tools

Network

Settings

Local DNS Records

Logout

Donate

Help

System Blocklists DNS DHCP API / Web interface Privacy Teleporter

Upstream DNS Servers

IPv4	IPv6	Name
<input type="checkbox"/>	<input type="checkbox"/>	Google (ECS)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	OpenDNS (ECS)
<input type="checkbox"/>	<input type="checkbox"/>	Level3
<input type="checkbox"/>	<input type="checkbox"/>	Comodo
<input type="checkbox"/>	<input type="checkbox"/>	DNS.WATCH
<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (filtered, DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (unfiltered, no DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (filtered + ECS)
<input type="checkbox"/>	<input type="checkbox"/>	Cloudflare

ECS (Extended Client Subnet) defines a mechanism for recursive resolvers to send partial client IP address information to authoritative DNS name servers. Content Delivery Networks (CDNs) and latency-sensitive services use this to give geo-located responses when responding to name lookups coming through public DNS resolvers. *Note that ECS may result in reduced privacy.*

Upstream DNS Servers

Custom 1 (IPv4)

Custom 3 (IPv6)

Custom 2 (IPv4)

Custom 4 (IPv6)

Interface listening behavior

☐ Listen on all interfaces
Allows only queries from devices that are at most one hop away (local devices)

☒ Listen only on interface eth0

☐ Listen on all interfaces, permit all origins

Note that the last option should not be used on devices which are directly connected to the Internet. This option is safe if your Pi-hole is located within your local network, i.e. protected behind your router, and you have not forwarded port 53 to this device. In virtually all other cases you have to make sure that your Pi-hole is properly firewalled.

Advanced DNS settings

☒ Never forward non-FQDNs

☒ Never forward reverse lookups for private IP ranges

Note that enabling these two options may increase your privacy slightly, but may also prevent you from being able to access local hostnames if the Pi-hole is not used as DHCP server

☐ Use DNSSEC

Validate DNS replies and cache DNSSEC data. When forwarding DNS queries, Pi-hole requests the DNSSEC records needed to validate the replies. If a domain fails validation or the upstream does not support DNSSEC, this setting can cause issues resolving domains. Use Google, Cloudflare, DNS.WATCH, Quad9, or another DNS