

# Table des matières

- Le filtrage des Pubs** ..... 2
  - Sur La Box:** ..... 2
  - Installation** ..... 2
  - Configuration** ..... 3
  - Service** ..... 4
  - Script PUB** ..... 5
    - Filtre Perso ..... 5
    - Création script ..... 5



## Le filtrage des Pubs

Le but est de déporter ces deux services de notre « BOX INTERNET » sur un « mini PC » (RaspberryPi) et nous permettre de filtrer le contenu d'internet automatiquement. Ce system ce mettra à jour automatiquement en téléchargeant un fichier de définitions (« de serveurs de spams et pubs à inhiber ») à la manière d'un antivirus.



### **Explication du fonctionnement:**

Votre Tablette ou Ordinateur vois votre SSID Wifi ex:(BBOX2456-56G) si connecte, votre BOX Internet renvoie la demande à votre Mini Pc, qui lui attribura une adresse Ip avec DNS de la même façon que votre BOX. À la seule différence que votre Mini Pc contiendra une Blacklist de tout les serveurs « **dit dangereux sur Internet** » afin de les bloquer dès leur accès à « TOUS VOS EQUIPEMENTS RÉSEAUX WIFI ET FILAIRE« . Vous pourrez aussi Blacklister les sites que vous souhaitez ne pas voir accessible par vos enfants.

## Sur La Box:

- Arrêter le service DHCP sur la BOX Internet la laisser en IP Fixe.

(ce ne sera plus elle qui vous donnera ip et dns) nécessite un redémarrage de la box.

- La partie Wifi ne bouge pas (votre SSID et CLÉ psk)Côté Pc:

## Installation

Sur une machine Linux de préférence, dans un terminal jusqu'a la fin du tutaux.

```
sudo apt-get update && apt-get upgrade
sudo apt-get install dnsmasq dnsmasq-utils
```

Une fois installer le fichier de conf se situe dans /etc/dnsmasq.conf Convertir le fichier de configuration de base en sauvegarde.

```
cp /etc/dnsmasq.conf /etc/dnsmasq.sav
```

# Configuration

Editer un nouveau fichier de configuration et compléter en fonction de vos besoins.

```
nano /etc/dnsmasq.conf
```

Voici un exemple fonctionnel de fichier avec réservation d'ip en fonction de la Mac Address:

```
#####Pour éviter de fournir du trafic DHCP/DNS inutile du coté internet
domain-needed
bogus-priv
#####Pour permettre à dnsmasq de suivre vos changements d'IP:
##commentez cette ligne si vous avez une IP qui change
#no-poll
#####Pour limiter l'écoute de requêtes DHCP du coté réseau local
interface=eth0
#####DOMAINE pour dnsMasq#####
domain=Reseau.lan
#Cache DNS
cache-size=64
#Ajoute automatiquement le domain définit dans la configuration aux noms de
machines présents dans /etc/hosts
#expand-hosts
#####DHCP CONF#####
dhcp-authoritative
dhcp-leasefile=/tmp/dhcp.leases
#Activez le serveur DHCP:
###Adresse Passserelle & Routeur##
dhcp-option=3,192.168.0.1
###Désactive l'IP forwarding 19,0 ou active l'IP Forwarding 19,1.Util sous
les routers.
dhcp-option=19,0
###Plage DHCP & Baux en h ou min possible
dhcp-range=192.168.0.50,192.168.0.80,255.255.255.0,48h

###Plage IP FIXES ET RESA IP
#-----#
#DYNAMIC ASSIGNEMENT
# \\
###iPhone 5s ###
dhcp-host=18:af:61:xx:xx:xx,iPhone5s,192.168.0.xxx
###iPhone 5c ###
dhcp-host=0c:30:21:xx:xx:xx,iPhone5c,192.168.0.xxx
###iPad 2###
dhcp-host=a4:67:06:xx:xx:xx,iPad2,192.168.0.xxx \\
#-----#
#STATIC ASSIGNEMENT
#
###SYNOLOGY NAS###
dhcp-host=00:08:9b:xx:xx:xx,Syno,192.168.0.xxx
```

```
###Raspberrypi###
dhcp-host=b8:27:eb:xx:xx:xx,Razorback,192.168.0.xxx

##Route Suite...
# Indique qui est le server wins (netbios) sur le réseau
#dhcp-option=44,192.168.1.200
# indique qui possède en mémoire le datagram du réseau netbios (le contenu
du voisinage réseau sous windows)
#dhcp-option=45,192.168.1.200
# Le type de node à utliser pour le TCP/IP sur NetBIOS. Si vous utilisez
samba comme serveur wins, laissez-le à 8.
#dhcp-option=46,8
# Active le Scope TCP/IP sur NetBios. Si vous utilisez samba comme serveur
wins.
#dhcp-option=47
```

Adapter le à votre plan d'adressage Ip et enregistrer le « CTRL+o »

## Service

Faire un test et observer que tout est ok:

```
sudo service dnsmasq restart
sudo service dnsmasq status
```

Retour écran:

```
● dnsmasq.service – dnsmasq – A lightweight DHCP and caching DNS server
Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; vendor
preset: enabled)
Drop-In: /run/systemd/generator/dnsmasq.service.d
└─50-dnsmasq-$named.conf, 50-insserv.conf-$named.conf
Active: active (running) since mer. 2015-08-12 02:35:32 CEST; 12h ago
Process: 23416 ExecStop=/etc/init.d/dnsmasq systemd-stop-resolvconf
(code=exited, status=0/SUCCESS)
Process: 23476 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf
(code=exited,
status=0/SUCCESS)
Process: 23472 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited,
status=0/SUCCESS)
Process: 23469 ExecStartPre=/usr/sbin/dnsmasq -test (code=exited,
status=0/SUCCESS)
Main PID: 23475 (dnsmasq)
CGroup: /system.slice/dnsmasq.service
└─23475 /usr/sbin/dnsmasq -x /var/run/dnsmasq/dnsmasq.pid -u dnsmasq -r
/var/run/dnsmasq/resolv.conf -7
/e...
```

## Script PUB



### Si vous souhaitez simplement Filtrer vos dns

Installer DSNMASQ et modifier le DNS de Votre serveur DHCP de votre box internet pas celle du serveur DNSMasq.

Copier simplement la configuration liée au DNS (ne pas ajouter la partie DCHP)

## Filtre Perso

```
touch /home/pi/BlackListURI/perso.uri
```

```
nano /home/pi/BlackListURI/perso.uri
```

### Coller vos entrer perso:

```
127.0.0.1      localhost
::1           localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
#--Mes Entrees Perso--#
127.0.0.1     youtube.com
127.0.0.1     tiktok.com
#--Fin de mes Entrees Perso--#

#--Entrees yoyo.org--#
```

## Création script

```
nano /home/pi/Scripts/MajBlackListURI.sh
```

### Copier / Coller le Script ci dessous

```
#####
# SCRIPT DE MISE A JOUR DES REGIES PUB      #
#           Powered by ME ;o)              #
#                                           #
#                                           #
#####
#!/bin/sh
#Suppression du fichier host avant sa nouvelle mise à jour.
rm -rf /etc/hosts
#Ajout des entrées DNS PERSO depuis la liste perso dynmique
/home/pi/blacklistURI/perso.uri
```

```

#Exemple j'interdit le domaine youtube.com dans ce fichier perso.
cat /home/pi/BlackListURI/perso.uri >> /etc/hosts
#Supprimer l'ancien fichier source HOSTS.TXT
rm /home/pi/BlackListURI/hosts.uri
#Télécharger le nouveau fichier HOSTS.TXT depuis pgl.yoyo.org
wget -O /home/pi/BlackListURI/hosts.uri
https://pgl.yoyo.org/adserver/serverlist.php?hostformat=hosts
# ajout de la blacklist dans le fichier hosts courant
#sed -e 's/^.*172.0.0.1//' /home/pi/BlackListURI/hosts.uri >> /etc/hosts
#Recherche dans HOSTS.txt les lignes contenant 127.0.0.1
grep -w "127.0.0.1" /home/pi/BlackListURI/hosts.uri | sed -e "/^<td>/d" >>
/etc/hosts
sed -e "/^<td>/d" /etc/hosts
#redémarrage de Dnsmasq
service dnsmasq restart
sleep 2

###-----Formatage du message à envoyer-----###

echo Nous sommes le $(date) >> /tmp/message
echo >> /tmp/message
echo "SALUT MINOS! ☐" >> /tmp/message
echo "VOICI LE RAPPORT DU GESTIONNAIRE DE PUB DE MAZINGER" >> /tmp/message
echo "|----->^<-----|" >> /tmp/message
echo "|-----C(☐.)-----|" >> /tmp/message
echo "|-----((☐))-----|" >> /tmp/message
echo "|-----><-----|" >> /tmp/message
echo >> /tmp/message
echo "La taille du fichier Hosts fait:" $(du -sh /etc/hosts | awk {'print
$1'}) "et contient" $(wc -l /etc/hosts | awk {'print $1'}) lignes >>
/tmp/message
echo "La dernière date de modification du fichier est" $(ls -l /etc/hosts |
awk {'print "le "$6,$7, "à "$8'}) >> /tmp/message
echo "Le service DNSMASQ est en status:" $(service dnsmasq status | grep
Active | awk {'print $3, "depuis " $7, "soit " $9,$10'}) >>/tmp/message
echo >> /tmp/message
echo >> /tmp/message
echo
"☐YOUR BOT FRIEND ROBOTZINGER™☐" >> /tmp/message
echo
"Powered By You For You!☐" >> /tmp/message
echo >> /tmp/message
echo MAZINGER™ THE BEST OR NOTHING! >> /tmp/message
echo >> /tmp/message
#Valide seulement dans un shell ne marche pas dans un script.
#mail -s "UPADTE Hosts & BlackList Ok!" uers@me.com <<<"STATUS HOSTS UPDATE
& DNSMASQ : $(ll /etc/hosts) $(service dnsmasq status)$(cat
/tmp/dhcp.leases)"
mail -s "UPADTE Hosts & BlackList Status!" kogool@hotmail.com<
/tmp/message
rm /tmp/message

```

## exit

### Option



\$(du -sh /etc/hosts) = Contrôle du poids du fichier hosts

\$(service dnsmasq status | grep Active) = renvoie l'état du service DNSMASQ

\$(cat /tmp/dhcp.leases) = que si vous avez activé DNSMASQ pour du DHCP

### NOTE:

| sed -e "/^<td>/d" permet de supprimer une ligne contenant 127.0.0.1 d'une input box situé dans la page Web, afin que l'entrée <td>....</td> ne soit pas dans le fichier host.

### Enregistrer votre Script "ctrl+o" et ajouter lui les droits.

```
sudo chmod o+x /home/pi/Scripts/MajBlackListURI.sh
```

### Exécuter le:

```
/home/pi/Scripts/MajBlackListURI.sh
```

### ou directement depuis le repertoire source:

```
./MajBlackListURI.sh
```

Contôler l'opération:

```
sudo ll /etc/hosts
—  root 3633110 août 12 02:35
```

ou

```
du -sh /etc/hosts
```

### On voit bien que notre fichier hosts a été mis à jour fait une taille de ~3,6mo.

Automatiser la mise à jour de la BlackList:

```
sudo crontab -e
30 23 * * * /home/pi/Scripts/MajBlackListURI.sh
```

### qui correspond à exécuter tout les soirs à 23h30 le Script qui télécharge le fichier et met à jour hosts.



Note Explicative: Dnsmasq est donc un serveur DNS et DHCP, il a la particularité de s'appuyer sur le fichier hosts pour sa propre résolution de nom. Idéale quand on a pas envie d'installer Bind9. Tester la différence:

Faite le test en 3/4G sur un site avec des iad ou pub, switcher en wifi sur votre SSID, rafraichissez votre page Web!! Et hop! By la Pub!!



**L'option Mail est facultative dans ce script**

— [sylvain](#) 2020/02/15 12:26

Mise à jour — [sylvain](#) 2022/08/01 16:10

From:

<https://wiki.mazinger.fr/wiki/> - **My Personal Wiki**

Permanent link:

<https://wiki.mazinger.fr/wiki/doku.php?id=tutaux:linux:dnsmaq>

Last update: **2024/03/03 12:56**

