Installatie handleiding Pi-hole, squid en squidGuard

voor de Raspberry Pi

(Auteur: M. Runte, maart 2021)

Inhoud

Deze handleiding in bedoeld voor de Raspberry Pi maar kan eventueel ook op een andere Linux distributie worden uitgevoerd. Voor de Raspberry Pi is er ook een ISO die je in Virtualisatie software kunt installeren.

Deze handleiding helpt je om dankzij je Raspberry Pi, veiliger te kunnen internetten.
Hiervoor worden 3 diensten op de Raspberry Pi geïnstalleerd:

- Pi-hole : om advertenties te blokkeren
- Squid: om internetverkeer centraal te laten lopen. De RPi is dan de proxy server
- Squidguard: om domeinen en websites (urls) te blokkeren

Om hier vanaf de client(s) gebruik van te maken, moet je:

1. het IP adres van de Raspberry Pi als DNS server op je client(s) instellen
2. in de webbrowser(s) van je client(s), de proxy server instellen: IP adres van de Raspberry Pi en Poortnummer 3128

De installatie op de Raspberry Pi, voer je vanaf de CLI uit. Dit kan op afstand door met SSH (PuTTY) in te loggen.

Installatie Pi-hole (advertenties blokkeren)

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

En volg de wizard. In principe kun je steeds op ENTER drukken, maar lees wel de schermen even.

Het wachtwoord voor de Pi-hole webinterface aanpassen doe je met :

pihole -a -p

Overige opties bekijk je met :

pihole -h

Installatie squid (de proxy server)

1. sudo apt-get update
2. sudo apt-get install locate
3. sudo updatedb

Op sommige Linux distributies moet je *squid* gebruiken, op andere moet je *squid3* gebruiken. Kijk na uitvoer van het commando of je een foutmelding krijgt. Pas het woord *squid* of *squid3* dan aan door er wel of geen 3 achter te typen.

Installeer squid en laat de squid service opstarten na een reboot:

1. sudo apt-get install squid
2. sudo apt-get install squid3
3. sudo update-rc.d squid enable (of sudo update-rc.d squid3 enable)
4. sudo updatedb

Nu gaan we squid configureren. Hiervoor moet je het configuratie bestand aanpassen.
We maken natuurlijk eerst een kopie van het squid configuratiebestand:
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.org

Nu gaan we het squid configuratiebestand aanpassen.
Zoeken in nano doe je met: **CTRL+w** en hetzelfde nog eens zoeken doe je met: **ALT+w**

5. sudo nano /etc/squid/squid.conf
6. Zoek met CTRL+w naar **acl localnet src**
7. Activeer één van deze regels en pas hem aan voor jouw netwerk:

acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16

Voorbeeld voor KPN/Telfort: **acl localnet src 192.168.2.0/24**

(/24 geeft het subnet aan. Zie: https://nl.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

8. Zoek naar **http_access allow localnet** en haal het # ervoor weg: **http_access allow localnet**
9. Zoek naar **http_port 3128** en haal het # ervoor weg: **http_port 3128**
10. Druk op **Alt+/** om naar het einde van het bestand te gaan en voeg toe:

url_rewrite_program /usr/bin/squidGuard

11. Deze regel is voor squidguard, dat we hierna gaan installeren
12. Sla **squid.conf** op en sluit de nano editor af
13. sudo service squid start

Squid testen

1. Stel in de webbrowser van je client, de Proxy server in: IP-adres van squid, Poortnummer: 3128
2. Test of je kunt internetten
3. Je kunt squid monitoren met het commando: **sudo tail -f /var/log/squid/access.log**

Installatie squidGuard (de website en domein blokkeer service)

Let op: squid**g**uard is de directory; squid**G**uard is de service!

1. sudo apt install squidguard
2. sudo cp /etc/squidguard/squidGuard.conf /etc/squidguard/squidGuard.conf.org

Test of het compileren werkt voordat je squidGuard.conf aanpast:

3. sudo squidGuard -C all

Je zou vrij snel de cursor weer moeten zien.

Rechten geven aan de groep en de gebruiker ‘proxy’ op de mappen voor squidguard:

4. sudo chown -R proxy:proxy /var/lib/squidguard/db
5. sudo chown -R proxy:proxy /var/log/squidguard
6. sudo chown -R proxy:proxy /usr/bin/squidGuard

Installatie Blocklists (lijsten met domeinnamen en urls om te blokkeren)

Er zijn lijsten beschikbaar waar heel veel domeinnamen en urls in staan om te blokkeren. Eén daarvan heet **shallalist** en die gaan we hier installeren. Shallalist bevat lijsten van domeinen en urls, ingedeeld in categorieën. Zie het hoofdstuk **SquidGuard aanpassen** verderop.

Opmerking: *Als je deze installatie op een andere Linux distributie uitvoert, moet je de map /home/pi/Downloads hieronder aanpassen voor jouw distributie. De map Downloads moet je waarschijnlijk eerst aanmaken.*

Archief-bestand met blokkeerlijsten downloaden in de map **/home/pi/Downloads** (de map moet bestaan, anders aanpassen):

1. sudo wget http://www.shallalist.de/Downloads/shallalist.tar.gz -P /home/pi/Downloads

Archief-bestand uitpakken:

2. sudo tar -zxf /home/pi/Downloads/shallalist.tar.gz -C /home/pi/Downloads

Uitgepakte mappen en bestanden kopiëren naar de squidguard map:

3. sudo cp /home/pi/Downloads/BL -R /var/lib/squidguard/db

Rechten op de squidguard map wijzigen:

4. sudo chmod -R 755 /var/lib/squidguard/db/BL

De user en de groep 'proxy' eigenaar maken van de squidguard map en submappen:

5. sudo chown -R proxy:proxy /var/lib/squidguard/db

De lijsten opnemen in de squidGuard database:

6. sudo squid**G**uard -C all

squid proxy service opnieuw configureren:

7. sudo service squid start
8. sudo squid -k reconfigure

En de squid service herstarten:

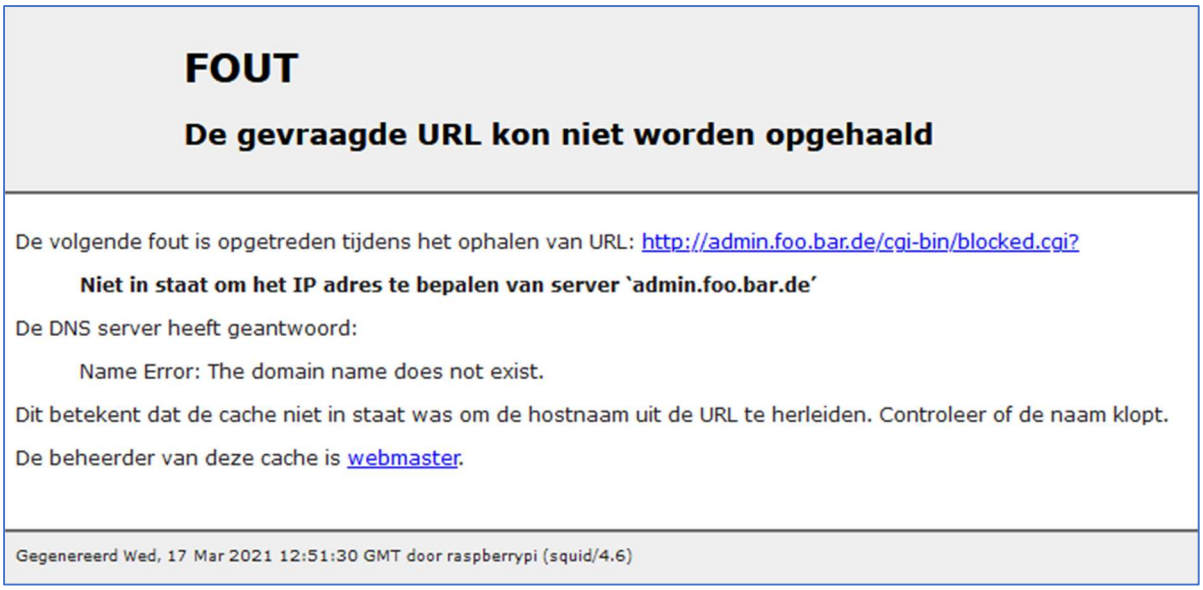
9. sudo service squid reload
10. sudo service squid restart

Het herstarten van de squid service duurt even…

Squid en squidGuard testen

1. Controleer dat je in de webbrowser van je client, de proxy server hebt ingesteld: IP-adres van squid, Poortnummer: 3128
2. Kijk of je naar website kunt en kijk of ze geblokkeerd worden. Tip: probeer websites van bekende winkels.
3. Als het goed is, worden sommige websites geblokkeerd. Bijvoorbeeld www.blokker.nl:

4.



FOUT

De gevraagde URL kon niet worden opgehaald

De volgende fout is opgetreden tijdens het ophalen van URL: http://admin.foo.bar.de/cgi-bin/blocked.cgi?

Niet in staat om het IP adres te bepalen van server 'admin.foo.bar.de'

De DNS server heeft geantwoord:

Name Error: The domain name does not exist.

Dit betekent dat de cache niet in staat was om de hostnaam uit de URL te herleiden. Controleer of de naam klopt.

De beheerder van deze cache is webmaster.

Gegenereerd Wed, 17 Mar 2021 12:51:30 GMT door raspberrypi (squid/4.6)

squidGuard aanpassen

Zie ook: http://www.squidguard.org/Doc/configure.html

In het configuratie bestand van squidGuard geef je enkele dingen aan zoals:

- het IP-adres waarop jouw proxy server draait (van de Raspberry Pi dus)
- de melding die men eventueel te zien krijgt als een website geblokkeerd wordt door de proxy server
- het soort website dat geblokkeerd wordt of juist wordt toegestaan
- verdere restricties voor bijvoorbeeld bepaalde device en/of tijden
- enzovoort

Globaal is het configuratiebestand als volgt opgebouwd:

- de definitie van de categorie: hierin geef je de map van het blok op en de bestanden voor 'domains' en 'urls'. Deze map en bestanden moeten bestaan (maar mogen nog leeg zijn)
- onderaan geef je de aangemaakte categorie op in de acl (Access Control List) en of je die categorie wilt blokkeren (door er '!' voor te zetten), of juist toestaat (door er geen '!' voor te zetten)
- Let goed op de structuur van het bestand: een type fout of een verkeerde opmaak zorgt ervoor dat het niet werkt. Maak daarom ALTIJD eerst een kopie van het bestand voordat je iets aanpast!!!
- Na de aanpassingen, neem je de wijzigingen in de squidGuard database op met het commando:

  sudo squidGuard -C all

Na elke wijziging moet je de volgende commando's geven:

1. sudo squidGuard -C all
2. sudo chown -R proxy:proxy /var/lib/squidguard/db
3. ~~sudo cat /var/log/squidguard/squidGuard.log (dit commando is optioneel maar dan zie je wat er gebeurt)~~
4. sudo service squid reload
5. sudo service squid restart

Om squidGuard naar je eigen wensen aan te passen, moet je dus het configuratiebestand aanpassen. We maken eerst een backup:

1. sudo cp /etc/squidguard/squidGuard.conf /etc/squidguard/squidGuard.conf.org
2. sudo nano /etc/squidguard/squidGuard.conf
3. In dit bestand pas je het IP adres aan voor dat van je Raspberry Pi
4. Vervolgens geef je de categorie aan van de websites die je wilt blokkeren. De websites van de shallalist blocklists moet je apart opgeven. Begin met 1 categorie en test of dat werkt
5. Zie hieronder enkele voorbeelden
6. Om bepaalde geblokkeerde websites die in shallalist staan juist toe te laten, kun je een aparte categorie en mappen aanmaken, bijvoorbeeld genaamd 'white'.
7. In die submap maak je een tekstbestand 'domains' en 'urls' voor respectievelijk de betreffende domain naam en de url. Elk domain op een aparte regel zetten!

Uitleg squidguard.conf

Most simple config uration: one category, one rule for all

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /usr/local/squidGuard/db
logdir /usr/local/squidGuard/logs

dest porn {
        domainlist porn/domains
        urllist porn/urls
        }

acl {
        default {
                pass !porn all
                redirect http://localhost/block.html
        }
 }
```

dbhome	Locatie van de blacklists
Logdir	Locatie van de logfiles
Dest	Definitie van een categorie om te blokkeren. Je kunt het domein en het URL bestand opgeven met een regular expressie lijst
Acl	De feitelijke blokkeer definitie. In our example only the default is displayed. Je kunt meer dan 1 acl opgeven. De categorie porn you die we in dest opgeven, wordt geblokkeerd door de expressie !porn. Je moet de indicator na de blocklist zetten, anders werkt het niet. De omleidingsmap is verplicht! Je moet squidGuard vertellen welke pagina moet worden getoond i.p.v. de geblokkeerde pagina.

Eerst de categorie definiëren:

Defining three categories for blocking

```
dest adv {
        domainlist      adv/domains
        urllist         adv/urls
}
dest porn {
        domainlist      porn/domains
        urllist         porn/urls
}
dest warez {
        domainlist      warez/domains
        urllist         warez/urls
}
```

Dan de acl (Access Control List) aangeven:

Defining a whitelist

```
dest white {
        domainlist      white/domains
        urllist         white/urls
}

acl {
        default {
                pass    white !adv !porn !warez all
                redirect http://localhost/block.html
                }
}
```

Na elke wijziging moet je de volgende commando's geven:

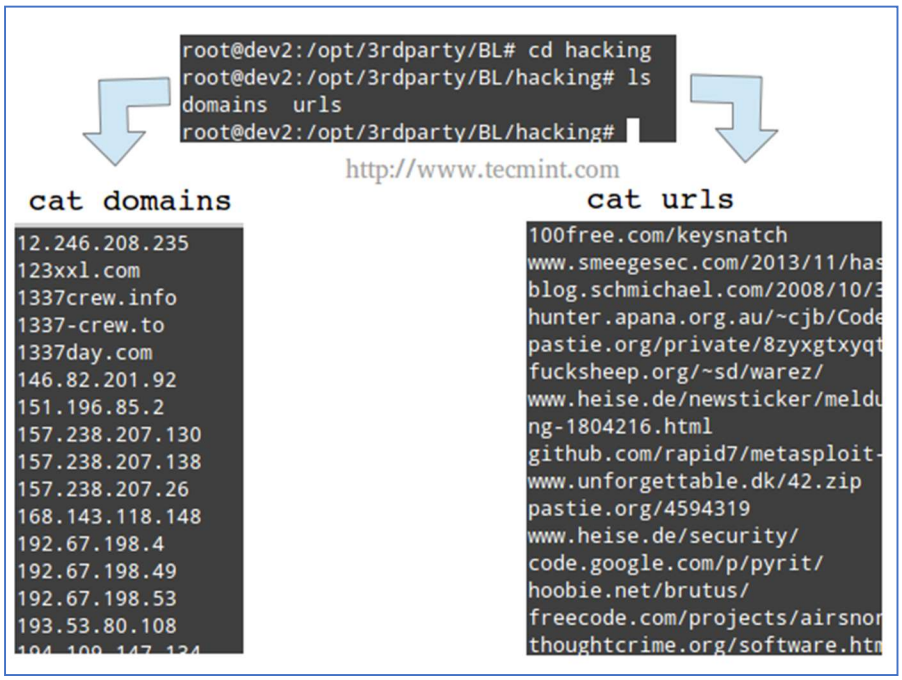
1. sudo squidGuard -C all
2. sudo chown -R proxy:proxy /var/lib/squidguard/db
3. sudo cat /var/log/squidguard/squidGuard.log (dit commando is optioneel maar dan zie je wat er gebeurt)
4. sudo service squid reload
5. sudo service squid restart

Als de uitvoer van **sudo squidGuard -C all** langer dan 1 minuut duurt, dan is er iets mis met de configuratie. Breek het proces dan af met CTRL+c, want het proces stopt niet vanzelf! Controleer vervolgens het configuratie bestand en probeer het opnieuw.

Hieronder zie je de categorieën van shallalist:

```
pi@PROXY: /var/lib/squidguard/db/BL
pi@PROXY:/var/lib/squidguard/db/BL $ ls
adv           downloads       government    military    recreation     socialnet     webphone
aggressive    drugs           hacking       models      redirector     spyware       webradio
alcohol       dynamic         hobby         movies      religion       tracker       webtv
anonvpn       education       homestyle     music       remotecontrol  updatesites   white
automobile    finance         hospitals     news        ringtones      urlshortener
chat          fortunetelling  imagehosting  podcasts    science        violence
COPYRIGHT     forum           isp           politics    searchengines  warez
costtraps     gamble          jobsearch     porn        sex            weapons
dating        global_usage    library       radiotv     shopping       webmail
pi@PROXY:/var/lib/squidguard/db/BL $
```

Deze zijn onderverdeeld in 2 bestanden:



Na compileren met **sudo squidGuard -all**, worden de bestanden in de squidGuard database opgenomen zodat er sneller gezocht wordt.

Bronnen

- https://pi-hole.net/
- https://computertotaal.nl/artikelen/overige-elektronica/zo-maak-je-een-professionele-ad-blocker-met-raspberry-pi/
- http://www.squid-cache.org/
- https://www.liquidweb.com/kb/install-squid-proxy-server-ubuntu-16-04/
- http://www.squidguard.org/
- http://www.squidguard.org/Doc/configure.html
- http://www.shallalist.de/