Veiliger internetten met de Raspberry Pi

Pi-hole, squid, squidGuard

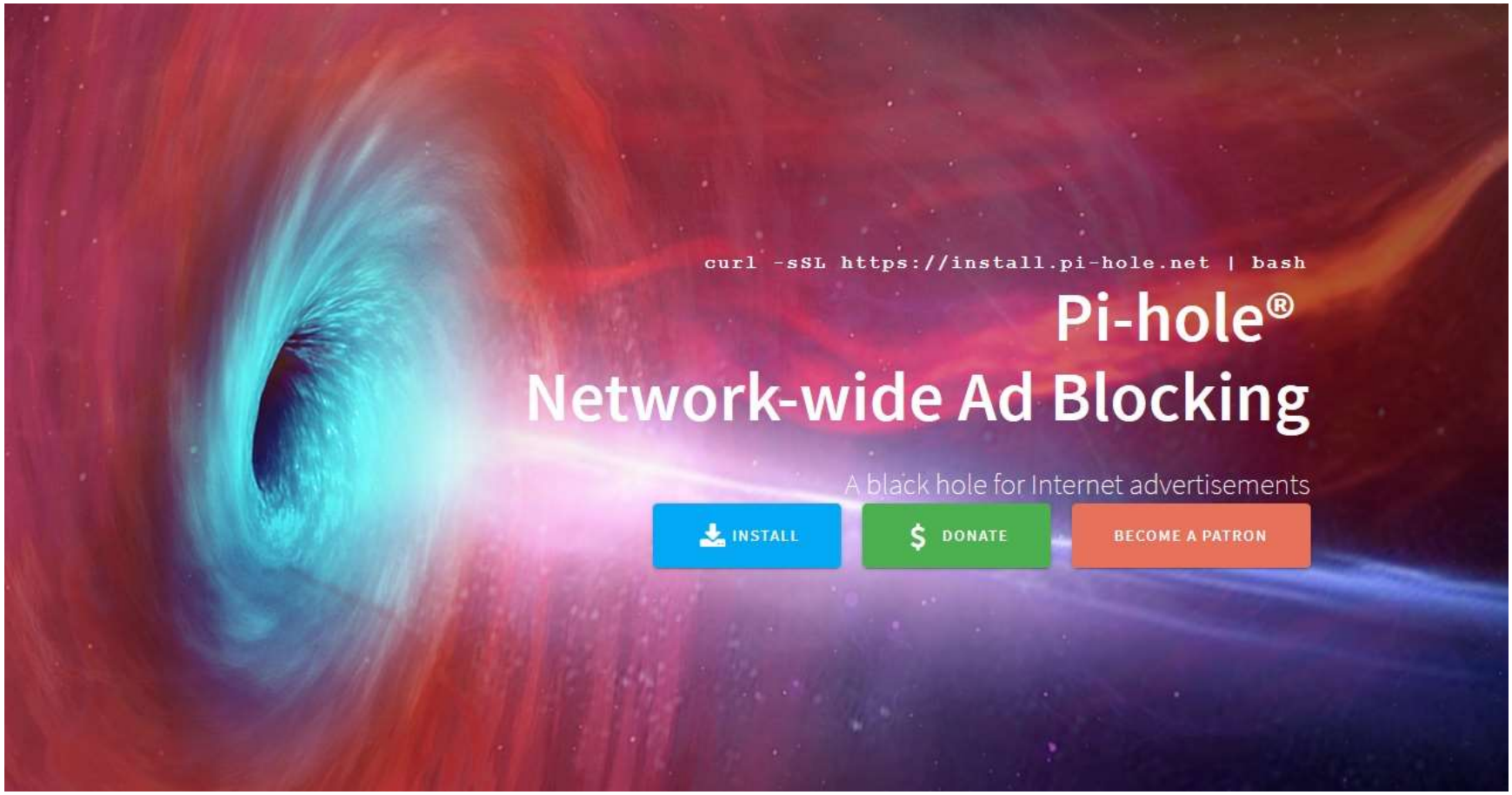
Marcel Runte, maart 2021,

m.runte@kader.hcc.nl

Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo’s
9. Extra’s: webmin

Pi-hole


curl -sSL https://install.pi-hole.net | bash
Pi-hole®
Network-wide Ad Blocking
A black hole for Internet advertisements
INSTALL
DONATE
BECOME A PATRON

Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

Wat is Pi-hole?

- Gemaakt door Jacob Salmela (Open Source - GitHub)
- Blokkeert DNS verzoeken
- Werkt als je eigen DNS server ←→ DNS provider
- Blokkeert advertenties, tracking domeinen, banners
- Maakt gebruik van lijsten (block lists)
  - Als domeinnaam in de lijst staat, wordt die geblokkeerd
- Draait naast of onafhankelijk van je router
- Extra block lists zijn toe te voegen

Wat is Pi-hole?

- Blokkeert advertenties en trackers op apparaten die achter Pi-hole hangen
  - Behalve Youtube en Facebook
- Eenvoudige installatie en configuratie
- Geen browser plug-in of software installatie op clients nodig
- 2e lijns bescherming (naast anti-virus)
- Kàn als DHCP server dienen

- Pi-hole is **geen** netwerkverkeer filter
- Pi-hole blokkeert **geen** websites!!!

Waarom Pi-hole

- Webpagina's laden sneller

Want geen last van :

- Pop-up en pop-under ads die je internet browser kapen
- Ads die je op alle andere apparaten volgen omdat je een bepaald product hebt gezocht (tracking)
- Ads die jouw locatie traceren en een profiel opbouwen
- Ads die laten weten dat je een grote prijs hebt gewonnen
- Ads die melden dat alle vrouwen bij je in de buurt met je uit willen (geo-caching)
- Ads die een zogenaamde foutmelding tonen en willen dat je hun helpdesk belt
- Ads die valse software updates van bijvoorbeeld Adobe Flash installeren
- Ads die melden dat je zogenaamd een virus hebt

Toepassingen

Blokkeert:

- Advertenties
- Pop-ups
- Trackers
- Phishing
- Geo-blocking
- Malware

Pi-hole samenwerking

Pi-hole kan gecombineerd worden met:

- Website filter (proxy)
  - squid, squidGuard, pfSense
- Domotica
  - Domoticz
- VPN server
  - OpenVPN
- Webserver
- E-mail server

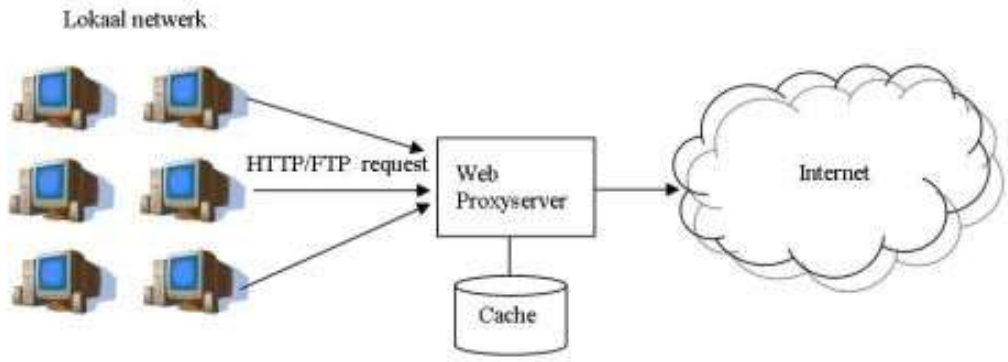
Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo’s
9. Extra’s: webmin

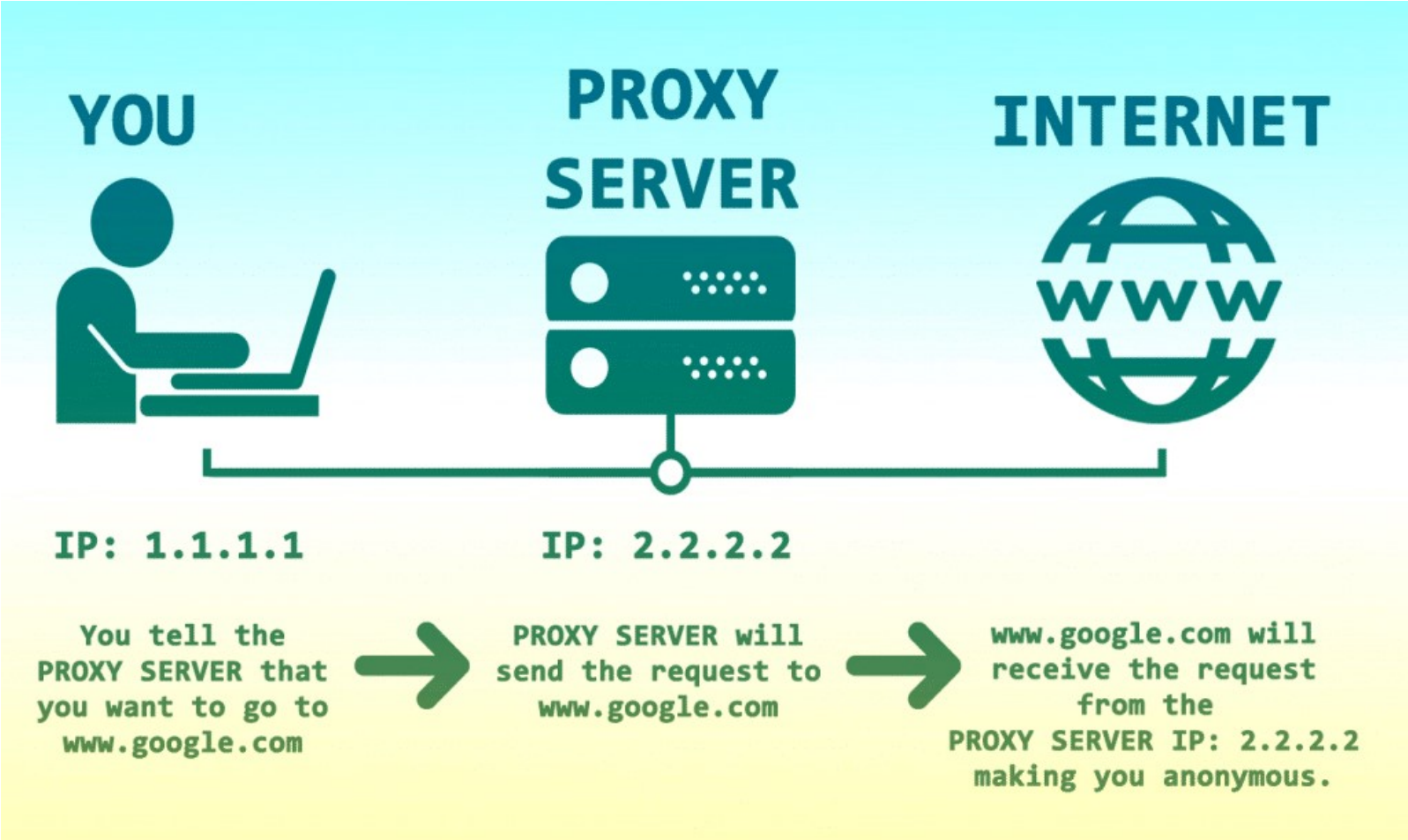
squid proxy

Wat is een proxyserver?

- Een server tussen de computer van een gebruiker en de computer waarop de door de gebruiker gewenste informatie staat
- Het Englese woord “proxy” betekent: *gevolmachtigd tussenpersoon*
- Wil iemand op een computer, waarop een proxyserver is ingesteld, een andere computer bereiken via deze proxyserver (en niet rechtstreeks)
- Het doel van deze tussenstap is afhankelijk van het type proxyserver.



Wat is een proxyserver?



Type proxyserver3

Er zijn globaal gezien drie typen proxyservers.

- **Web proxy**

  De meest voorkomende server.

  Alle clients in een lokaal netwerk gaan via een proxyserver het internet op.

  Al het HTTP- en/of FTP-verkeer wordt gecachet

  Snelheidsvoordeel voor de clients in het netwerk die webpagina's opvragen uit de cache (of tussenbuffer) van de proxyserver.

- **Open proxy**
- Een **open proxy** is een proxyserver die verbindingen toestaat van clients en ze voorziet van willekeurige IP-adressen. Deze open, transparante proxy's worden bijvoorbeeld gebruikt door mensen die hun privacy om welke reden dan ook willen beschermen, of om bij een website te kunnen komen die ontoegankelijk is vanaf het netwerk waarvan zij gebruikmaken. Open proxy's kunnen ook misbruikt worden door spammers en mensen die op andere manieren misbruik maken van het internet.

- **Reverse proxy**
- De proxyserver werkt hier van buiten naar binnen, dus andersom. Dit wordt ook wel "web server acceleration" genoemd. Hierbij wordt de proxyserver ingezet om de belasting vanuit het internet naar de webserver(s) gelijkmatiger te verdelen, zowel om beveiligings- als om "loadbalancing"-redenen.
- Voor ons is alleen de Web proxy functie interessant.

Doel proxyserver

- Beveiliging (kwaadaardige code detecteren)
- Sneller internetten (Caching)
- Bespaart bandbreedte
- Logging (Maar denk aan de AVG!)

Optioneel:

- Websites blacklisten (filteren van websites)

Voorbeelden proxyservers

- squid cache
- Apache HTTP server
- Provixy
- Microsoft ISA Server

Wat is squid?

- Proxy server
- Open Source
- Ontwikkeld voor Linux omgevingen
- Ondersteunt diverse protocollen: HTTP, HTTPS en FTP
- Cachen van opgevraagde webpagina's op Internet

Kan werken als

- web-proxyserver
- transparante proxyserver
- reverse proxyserver
- content filterserver

Waarom squid

- Verkleint de bandbreedte
- Verbetert reactietijden (caching)
- Ondersteunt de meeste besturingssystemen
  - Windows, MacOS, Android, iOS, Windows Mobile
- Het is gelicenseerd onder de GNU GPL
- Optimaliseert de gegevensstroom tussen client en server

squid kan samenwerken met

- squidGuard
- Pi-hole
- Domoticz
  - Domotica software
- VPN server
  - OpenVPN
- Webserver
- E-mail server

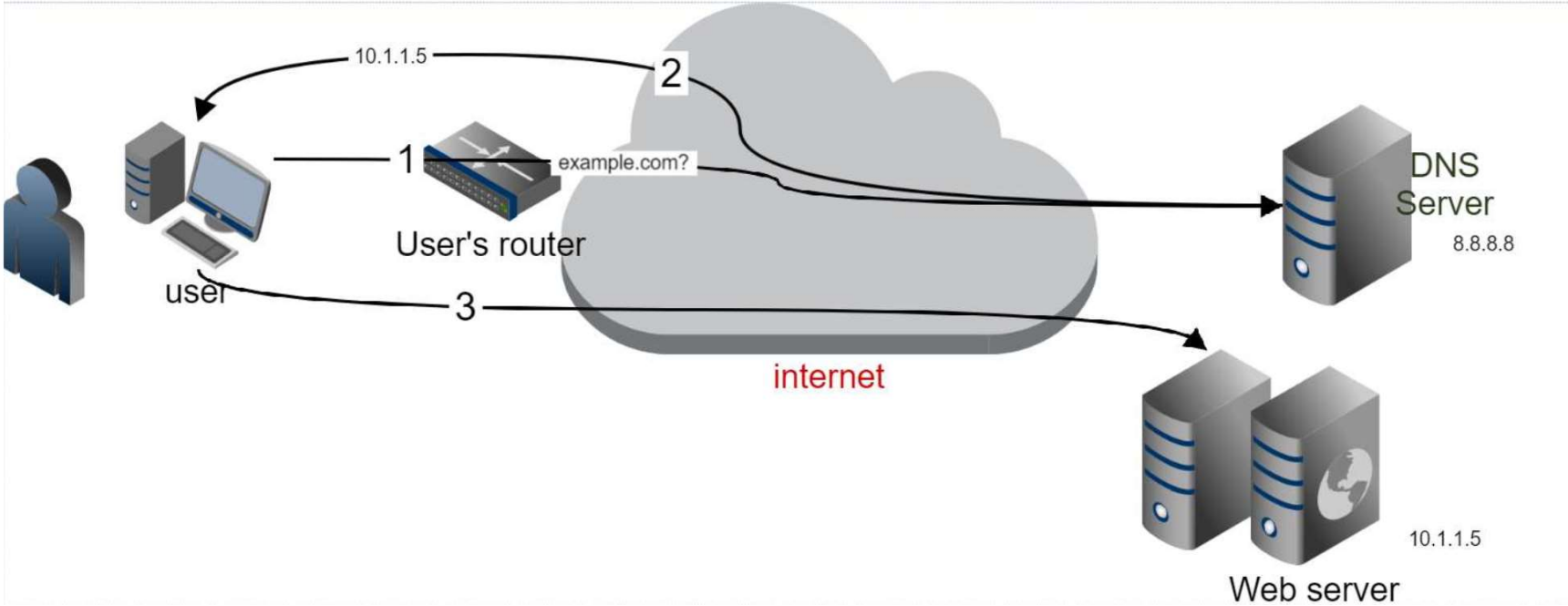
Wat is squidGuard?

- Blokkeert websites op basis van blocklists
- Blocklists worden in database gezet
- Uitbreiding op squid-cache
- Draait alleen op Linux
- Open Source
- URL-redirector voor squid
  - Stuurt client door naar info pagina
- Toegangsregels op basis van dag/tijdstip

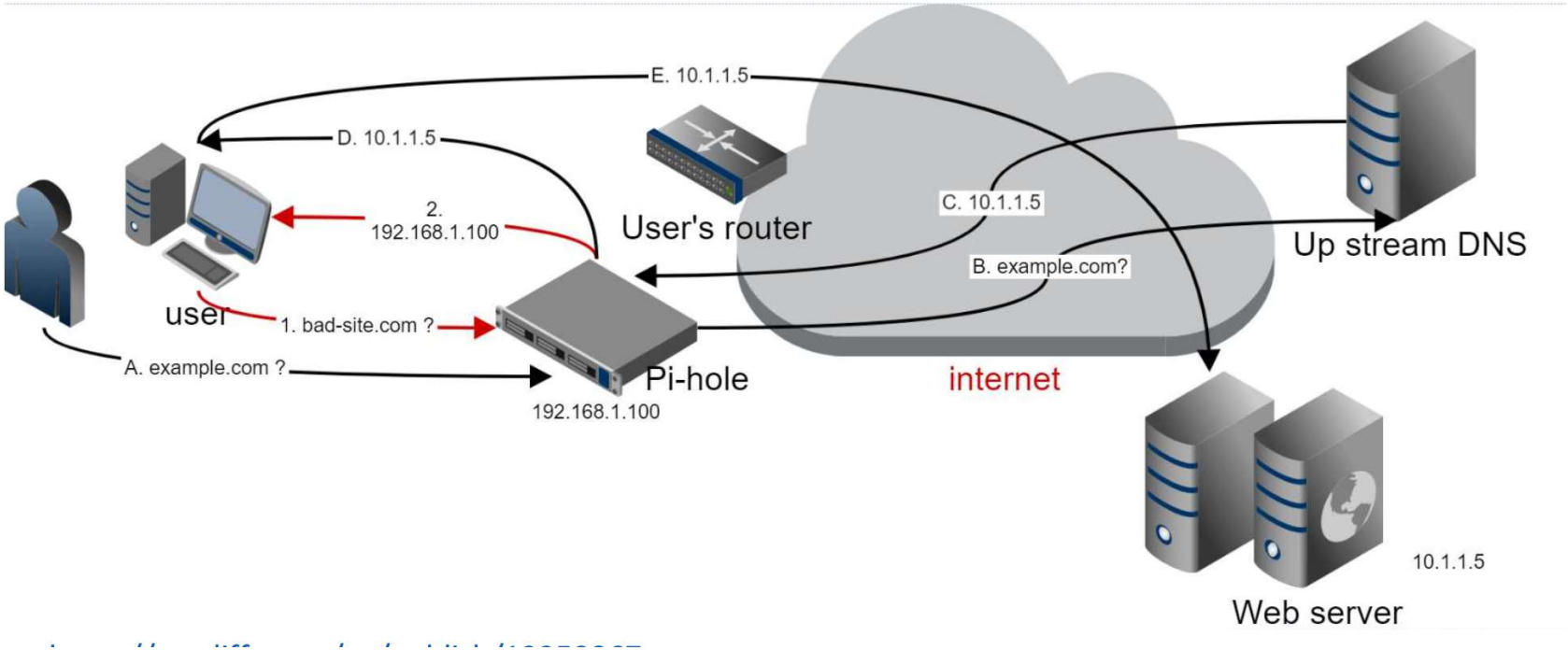
Waarom squidGuard

- Blokkeren van ongewenste websites
- Geen internet op bepaalde tijden
- Geen YouTube op bepaalde tijden
- Veiliger internetten
- Beheerbaar vanaf 1 locatie
- Configuratie eenvoudig te backuppen

Hoe werkt DNS via je router?



Hoe werkt DNS via Pi-hole?



Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

Quick Step Installatie

Wat heb je nodig

- Raspberry Pi (Model 2, 2B of hoger)
  - Geen Wi-Fi. Uitschakelen op Model 3.
- UTP kabel
- Laptop met PuTTy en WinSCP

Alleen voor 1e installatie:

- Monitor en toetsenbord

Nodig op laptop

- Raspbian image (‘Lite’ versie volstaat)
- Win32DiskImager

Verder:

- PuTTY – beheer op afstand
- WinSCP – om bestanden te kopiëren

Stappenplan (eenvoudig)

1. Download Raspbian Stretch Lite
   - http://www.raspberrypi.org/downloads (Buster)
   - http://downloads.raspberrypi.org/raspbian/images/ voor oudere versies
2. Zet image op microSD kaartje (8GB)
3. Maak in de bootpartitie een bestandje zonder extensie aan: 'ssh'
4. Stop het microSD kaartje in de RPi en zet hem aan
5. (Extra stap voor het 7" Touchscreen Display als de RPi power boven zit):
   1. 'sudo nano /boot/config.txt'
   2. Voeg onderaan toe: display_rotate=2
   3. 'sudo reboot'
6. Log in met PuTTy
7. 'sudo raspi-config'
   - Configureer toetsenbordindeling
   - Activeer automatisch opstarten met CLI
   - Wijzig het root wachtwoord
   - Stel hostname in
   - Stel tijdzonde in
   - Expand Filesystem

Stappenplan (vervolg)

1. sudo apt update && sudo apt upgrade -y
2. sudo reboot
3. sudo apt update
4. sudo apt --fix-broken install
5. sudo apt autoremove
6. sudo apt autoclean
7. sudo apt install mc && sudo apt install locate
8. sudo reboot
9. Maak een backup van microSD

Vervolg Stappenplan (optioneel)

1. Sluit de RPi af : ‘sudo shutdown –h now’
2. Maak een backup van het microSD kaartje

Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

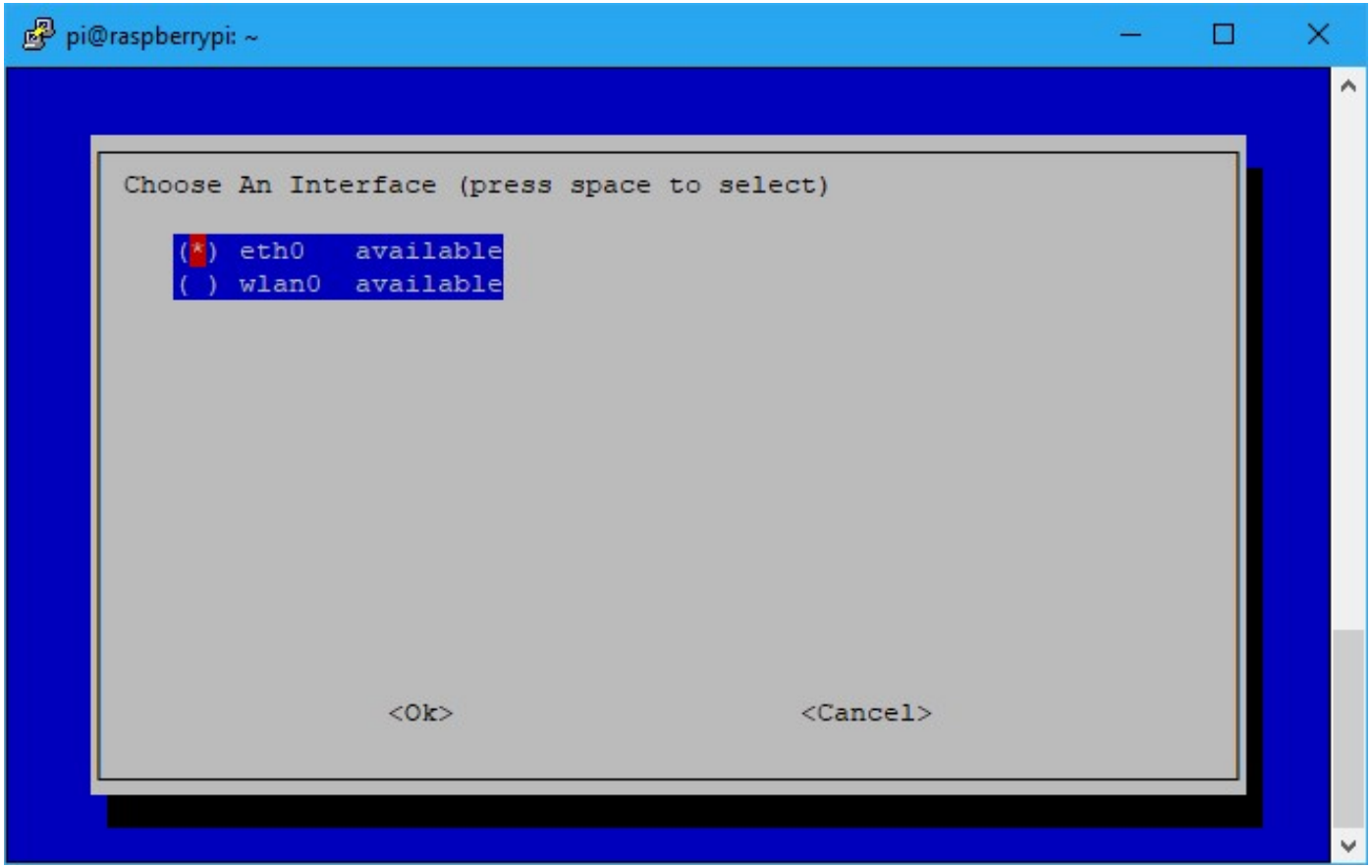
Pi-hole installatie

- Installeer Pi-hole:

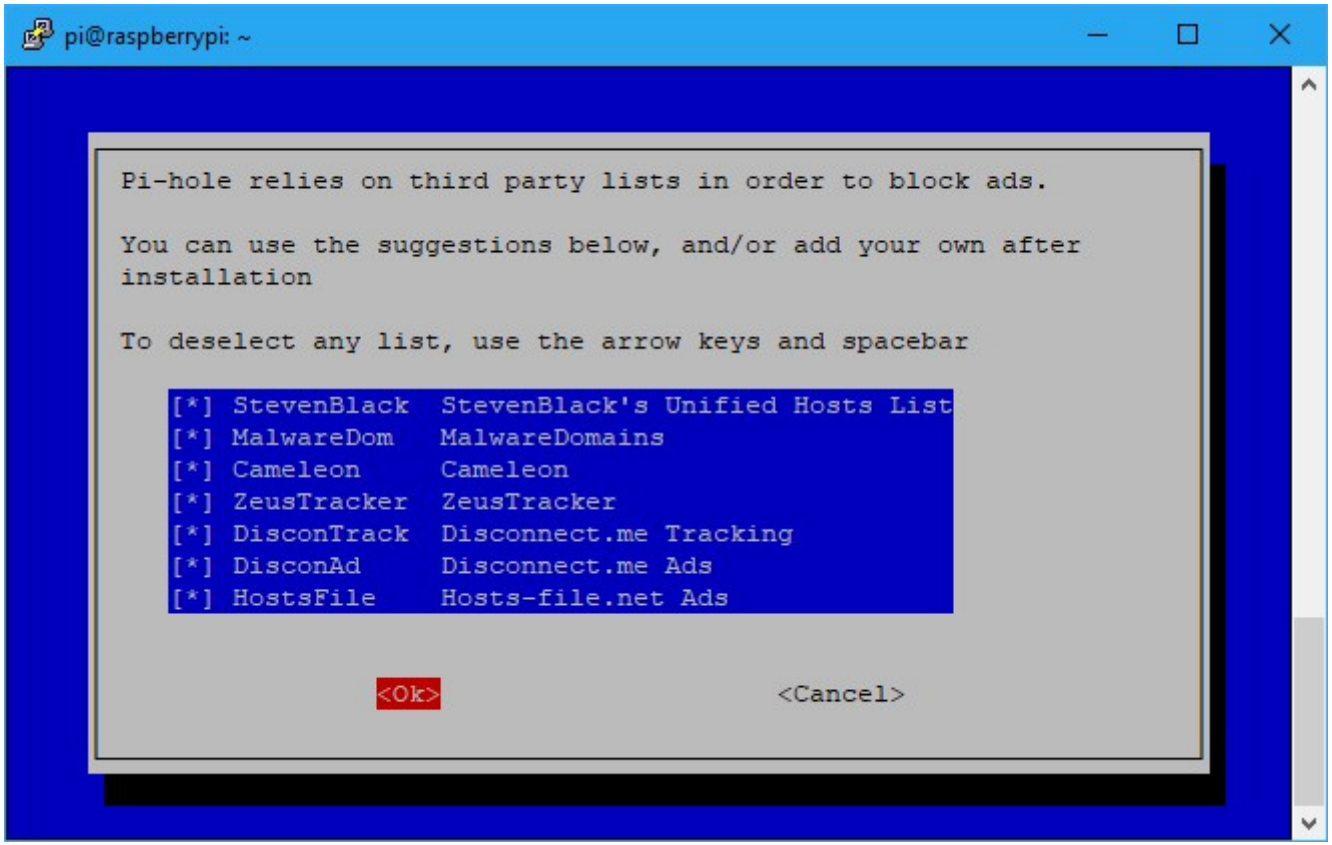
  sudo curl -sSL https://install.pi-hole.net | bash

- …en volg de wizard

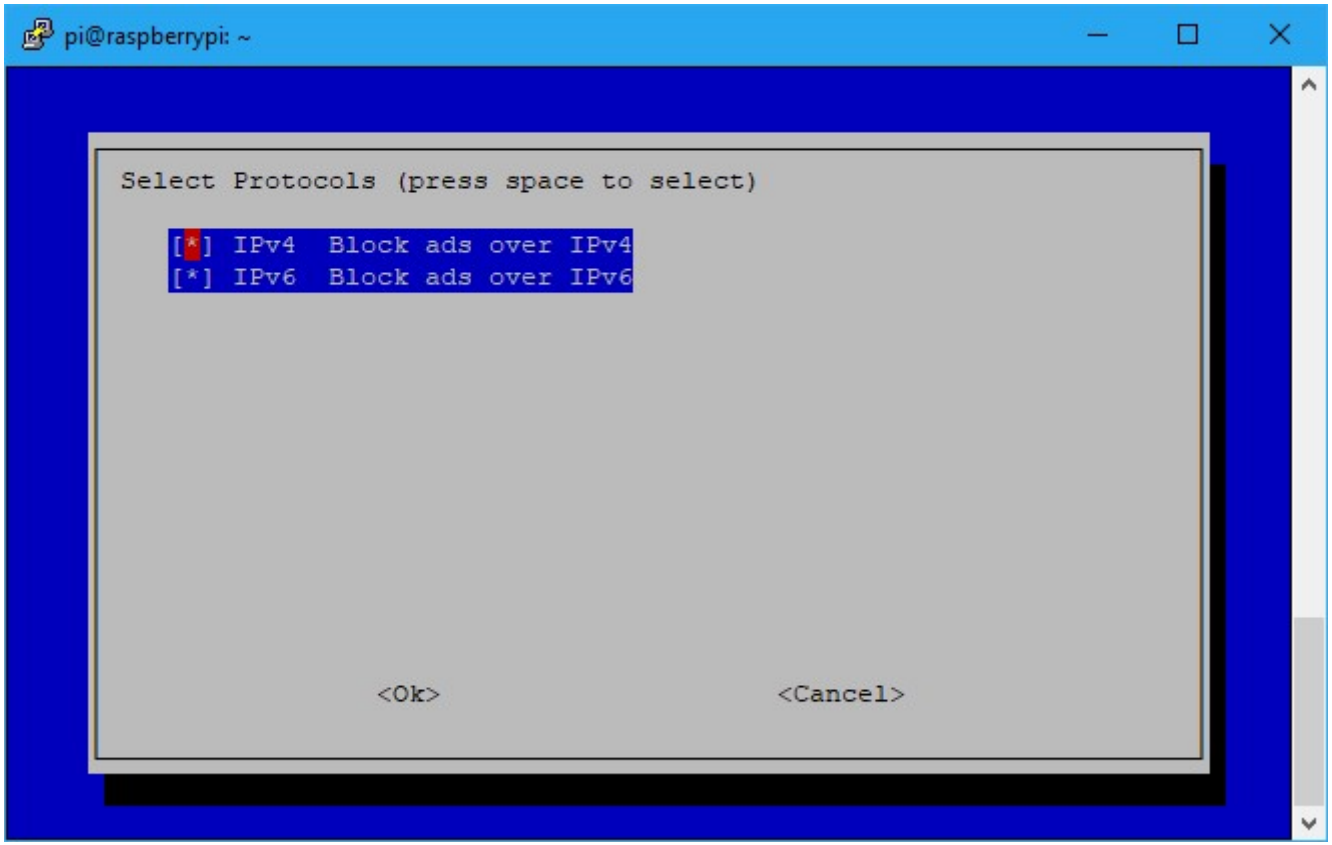
Kies eth0


pi@raspberrypi: ~
Choose An Interface (press space to select)
(*) eth0 available
( ) wlan0 available
<Ok>
<Cancel>

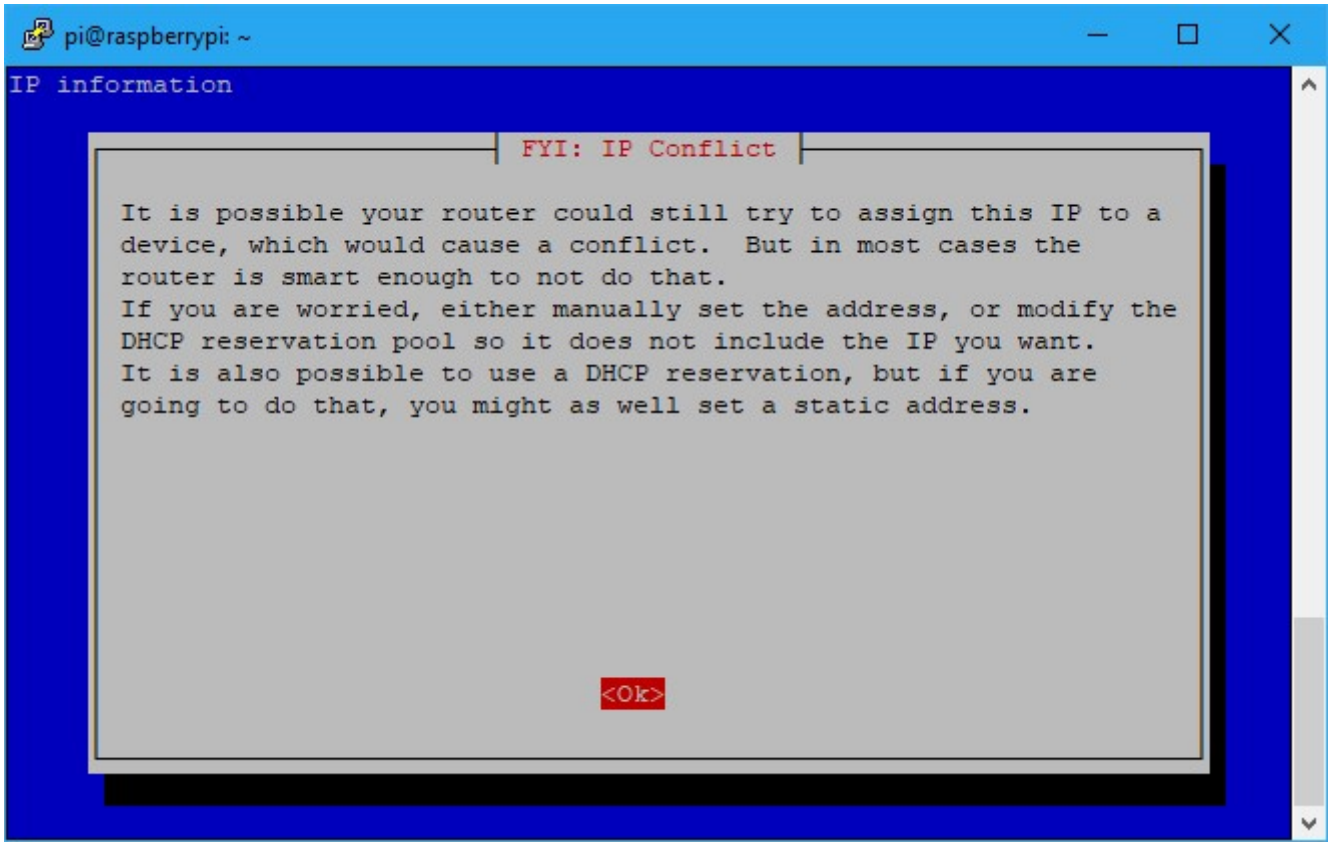
Laat alles aan



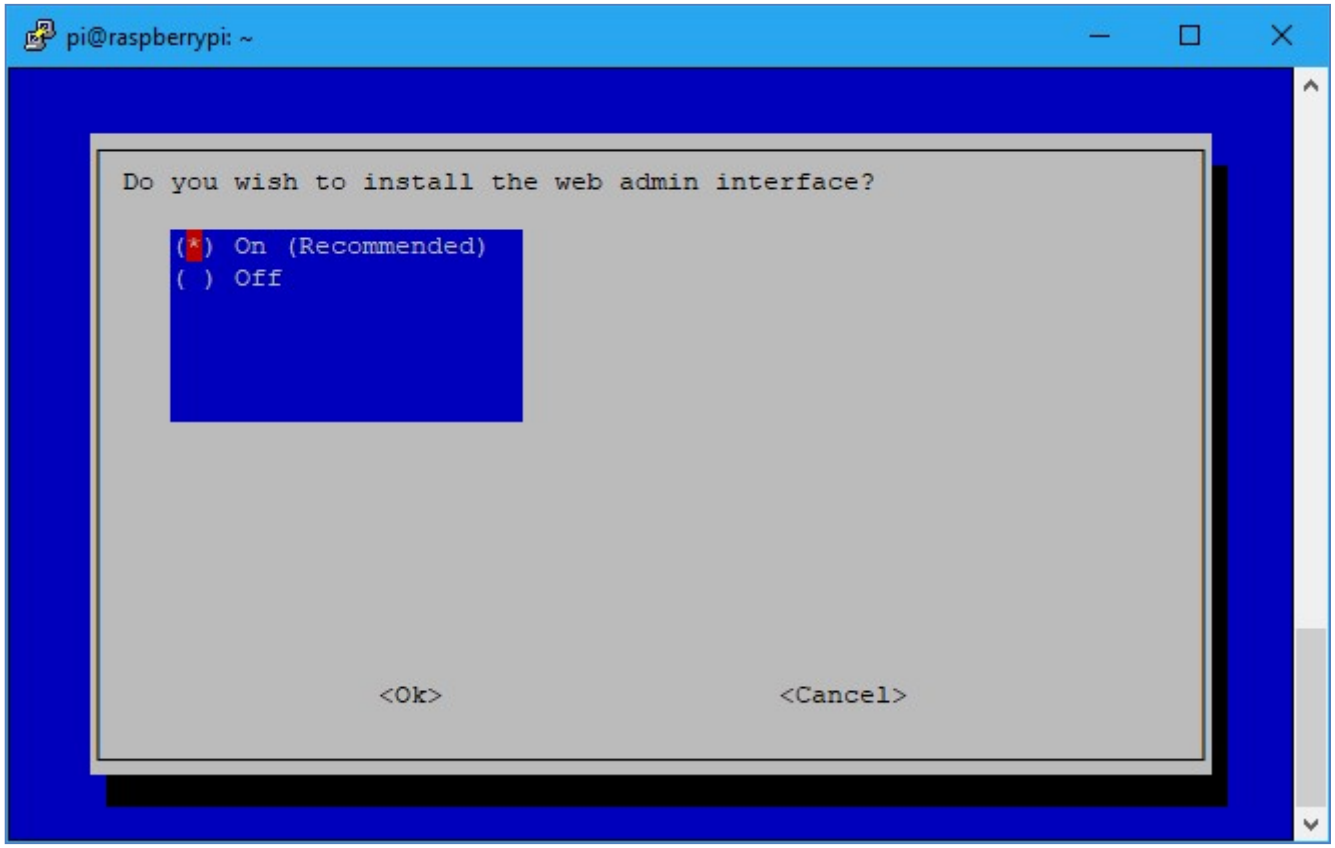
Pi-hole installatie



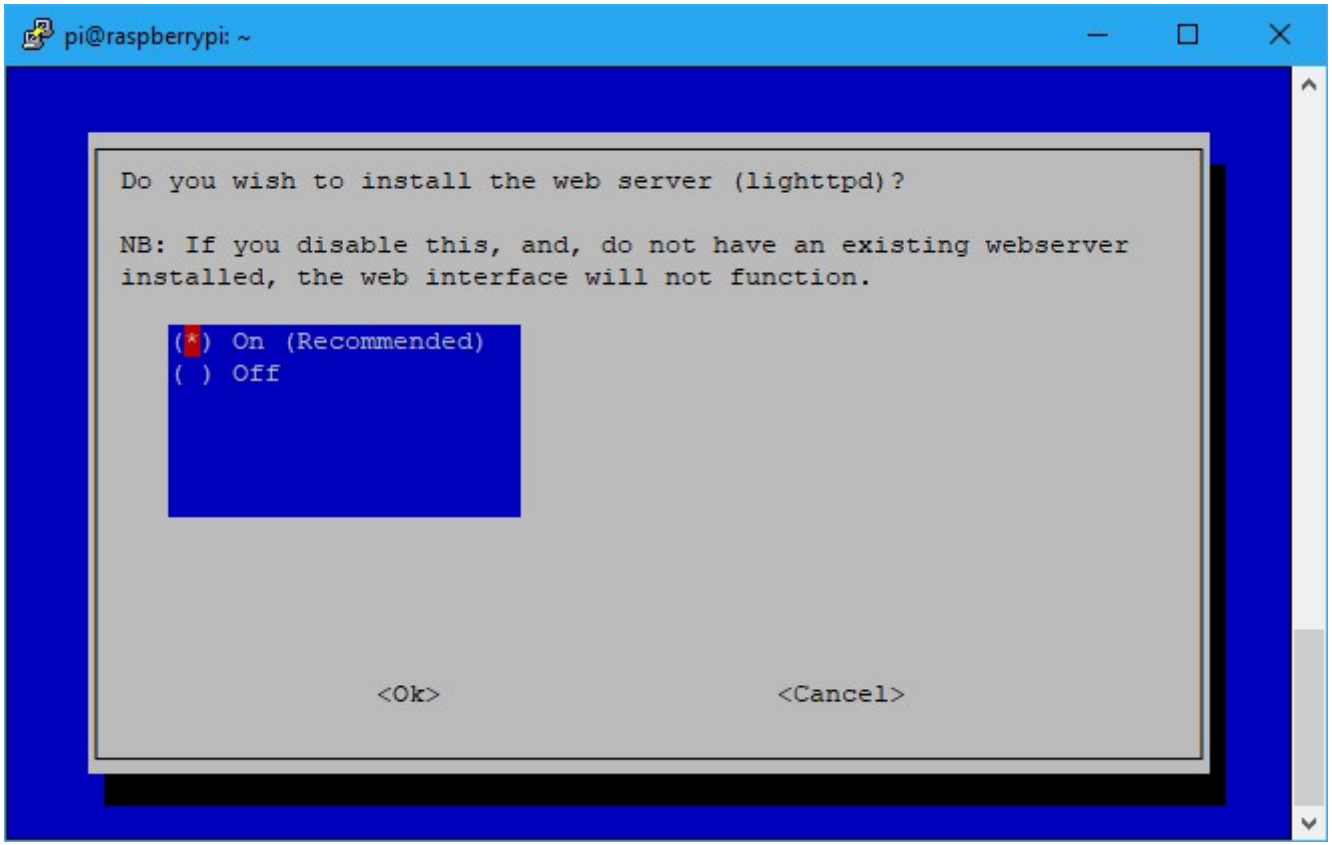
Pi-hole installatie



Pi-hole installatie

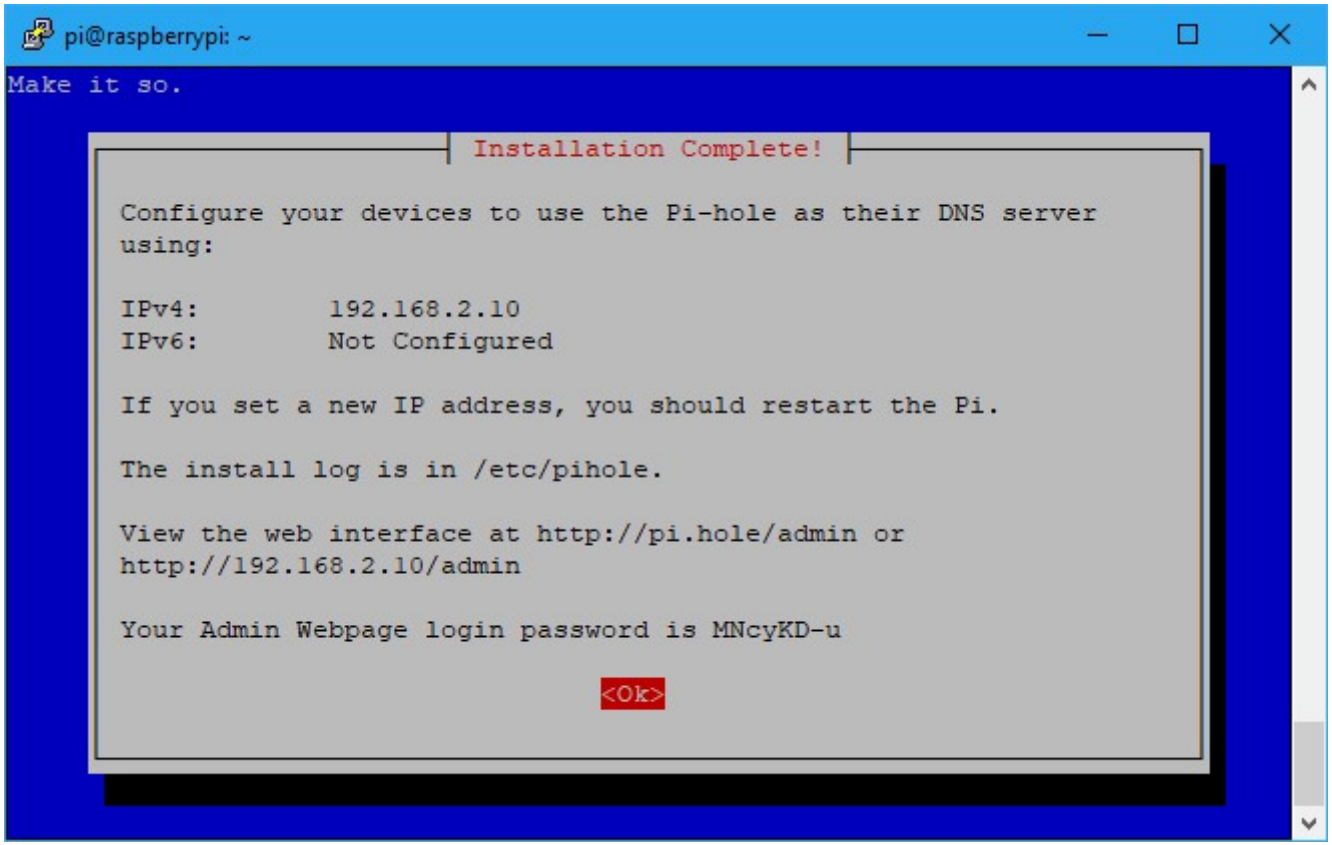


Let op!

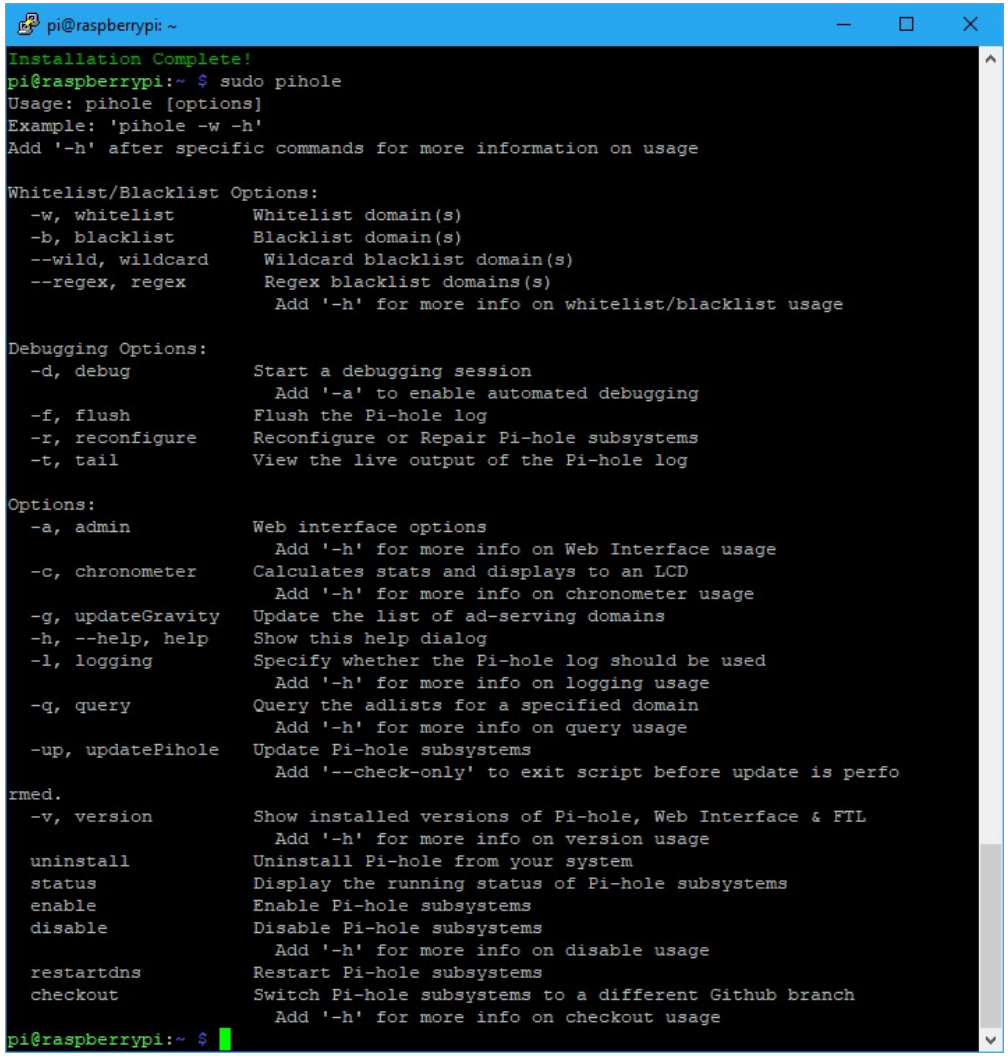

pi@raspberrypi: ~
Do you wish to install the web server (lighttpd)?
NB: If you disable this, and, do not have an existing webserver installed, the web interface will not function.
(*) On (Recommended)
( ) Off
<Ok>
<Cancel>

Noteer het wachtwoord!

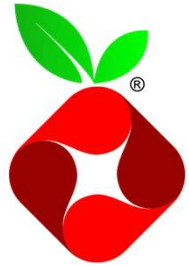
Wijzigen: pihole -a -p



Pi-hole opties



Pi-hole herinstalleren



- Foutje gemaakt / opnieuw installeren / ander IP adres instellen?:

  sudo pihole -r

- Pi-hole updaten:

  sudo pihole -up

- Overige opties:

  sudo pihole -a -p Wachtwoord opnieuw instellen

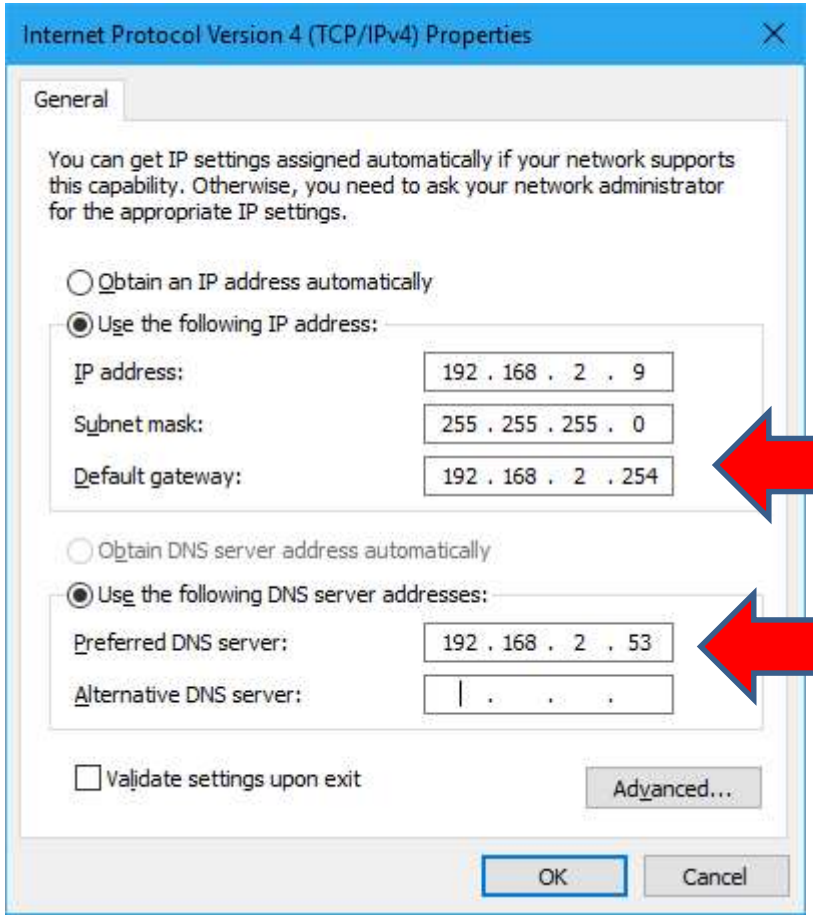
  sudo pihole -c (Chronometer)

Client instellen

- Test het eerst vanaf 1 client
- Stel het IP adres van Pi-hole in als de DNS van je client (laptop)
- Default Gateway = jouw router

- De Pi-hole moet direct aan de router hangen!

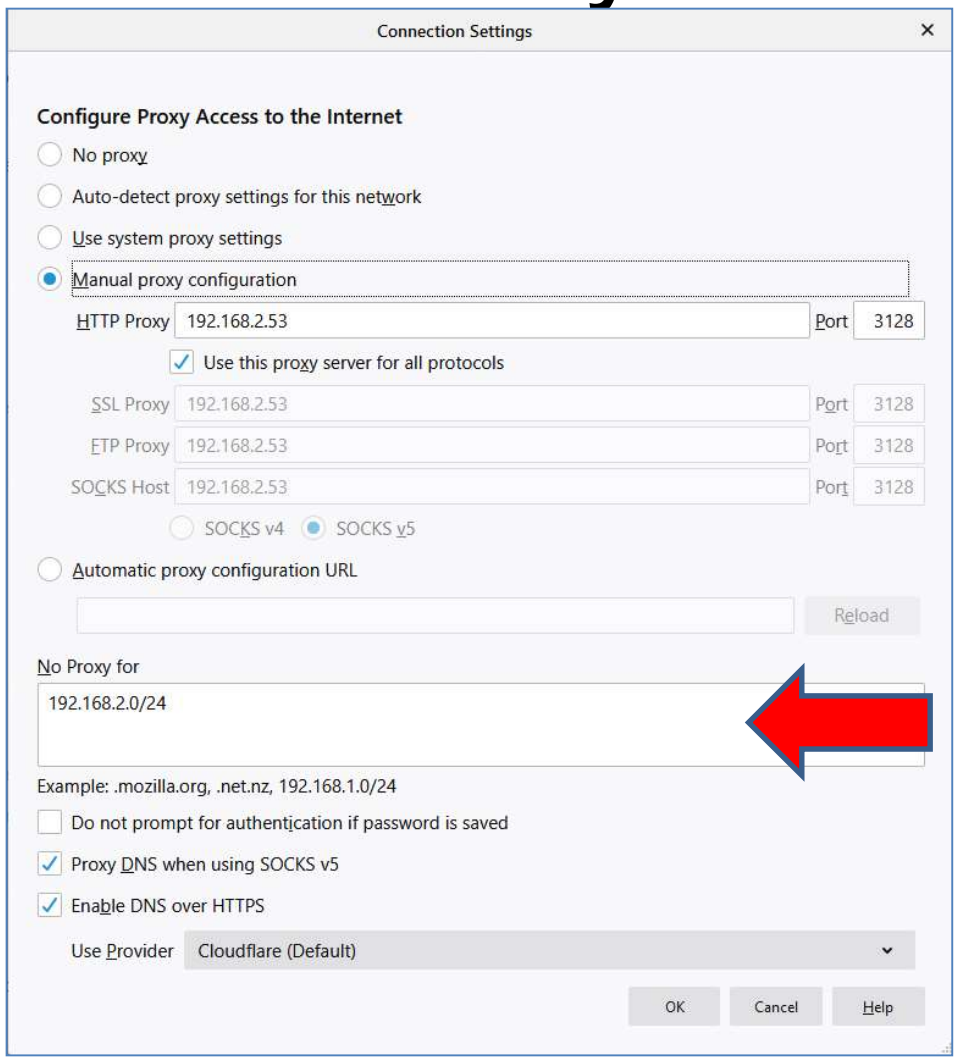
Client - Netwerkinstellingen



IP adres Router

IP adres Raspberry Pi

Client - Proxy instellen



Geen Proxy voor LAN

DNS cache leegmaken

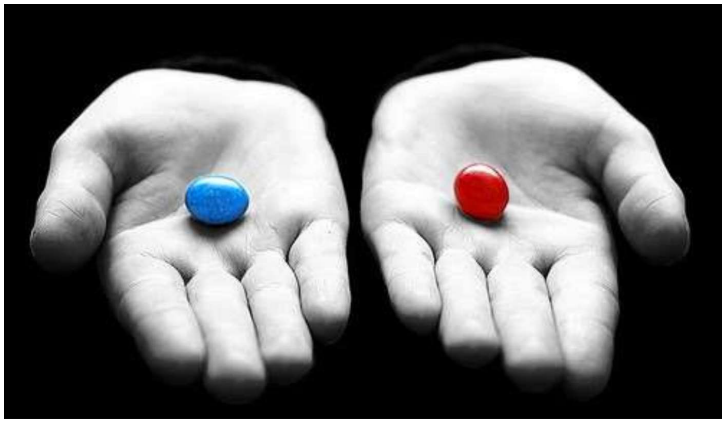
- Omdat het opvragen van websites in de DNS cache bewaard wordt, moet je de DNS cache leegmaken zodat de DNS gegevens ververst worden
- Er wordt dan op de client een schone DNS opgebouwd (van Pi-hole i.p.v. van de router)

➢ **ipconfig /flushdns**

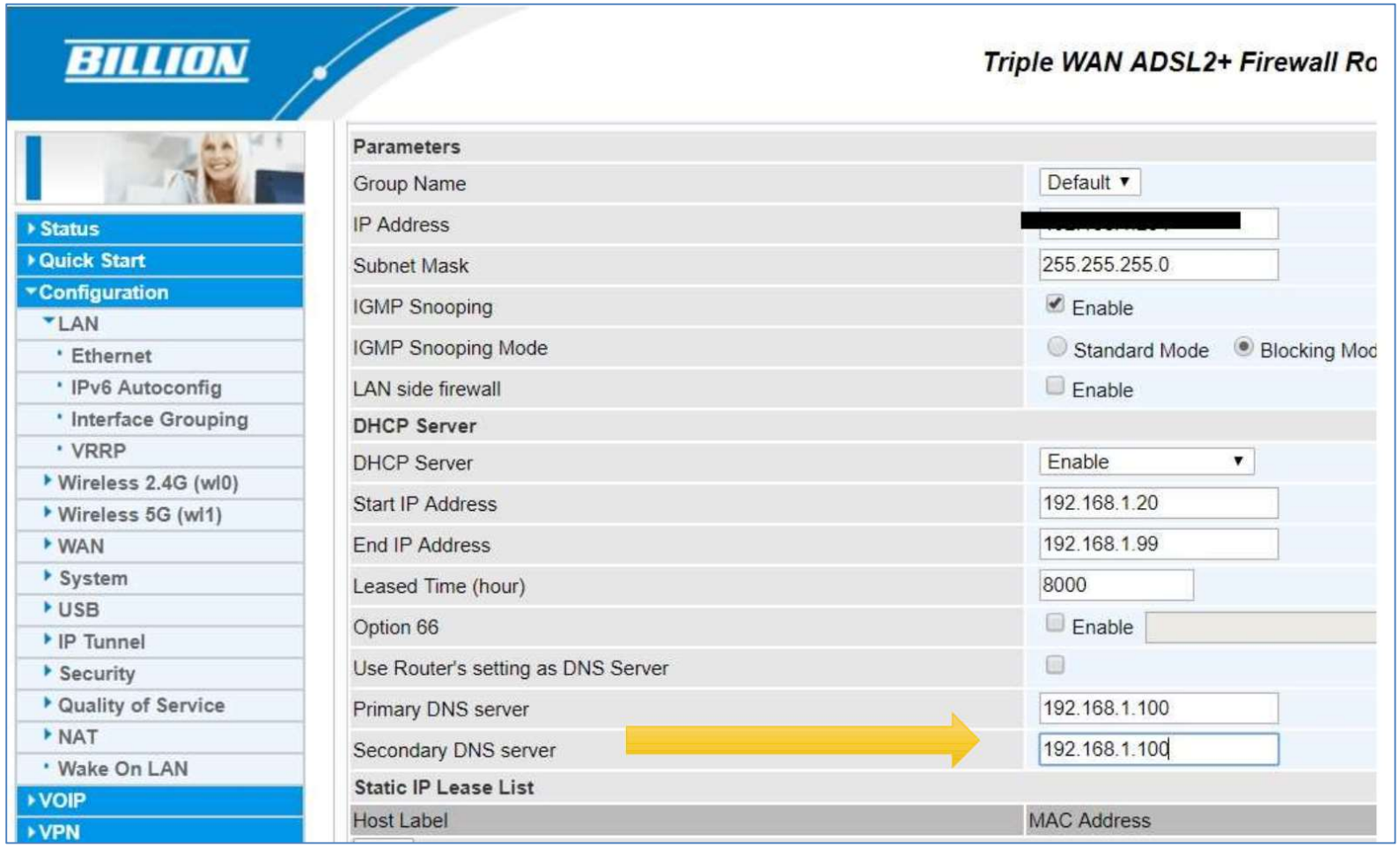
Router instellen: 2 keuzes

- Verander de DNS van de client(s)

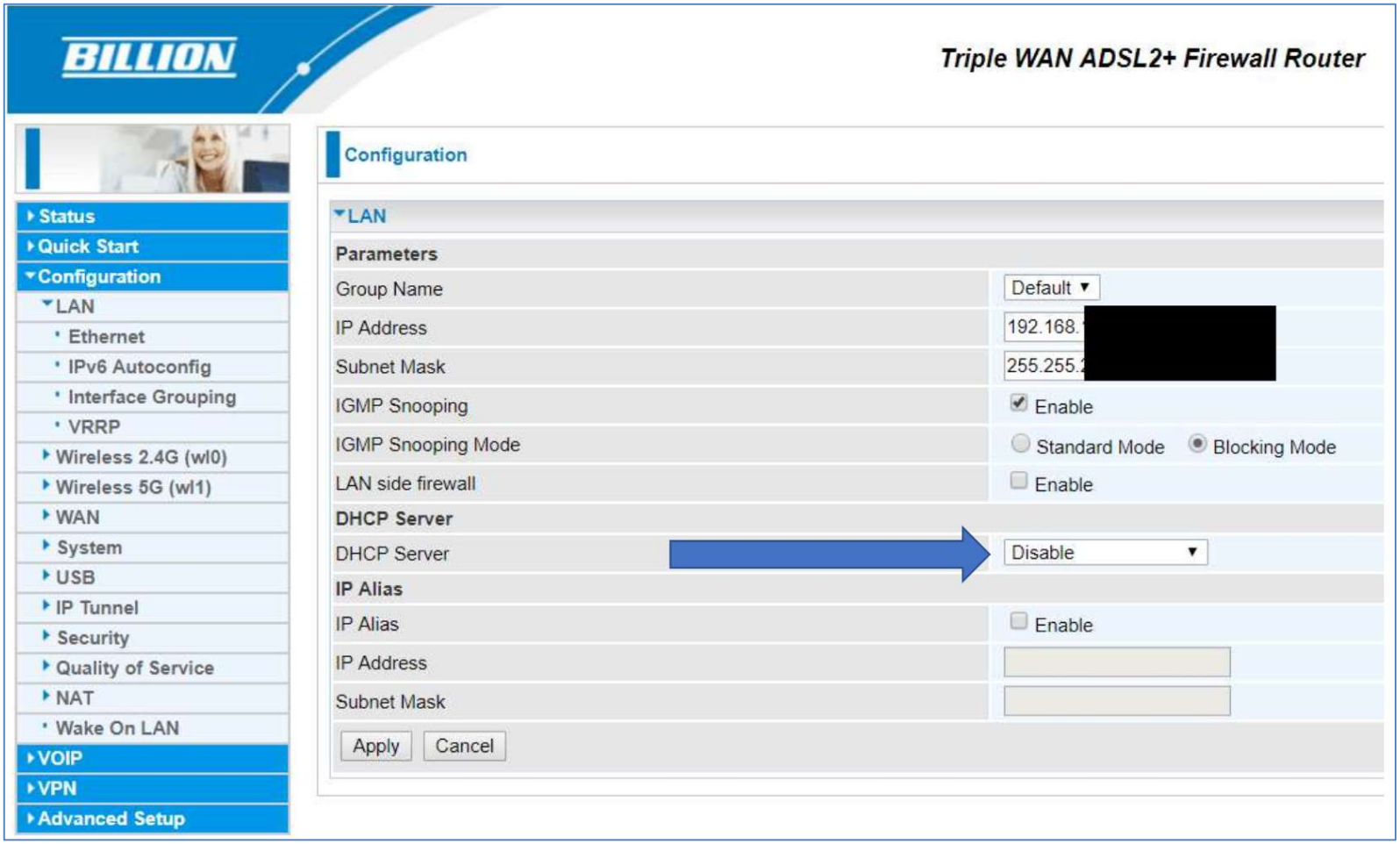
- of schakel DHCP op je router uit en laat Pi-hole DHCP-server spelen



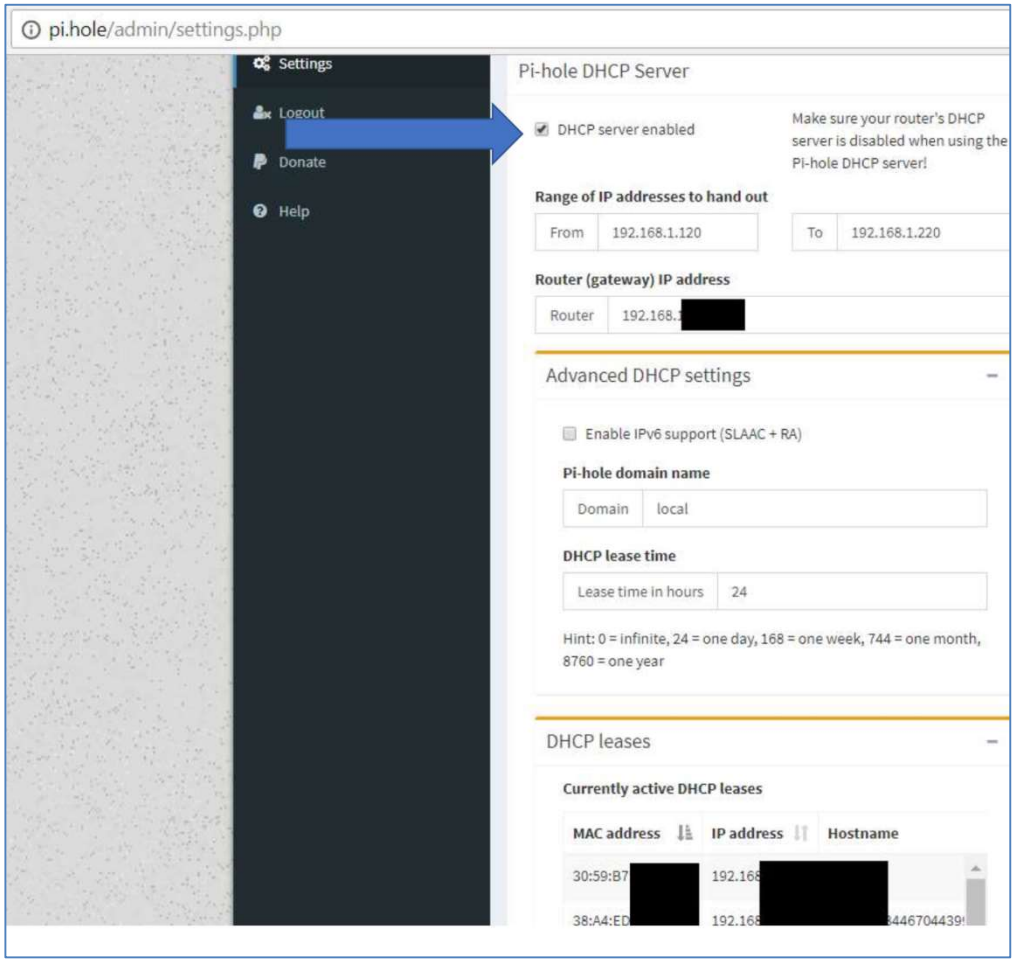
DNS aanpassen op Router



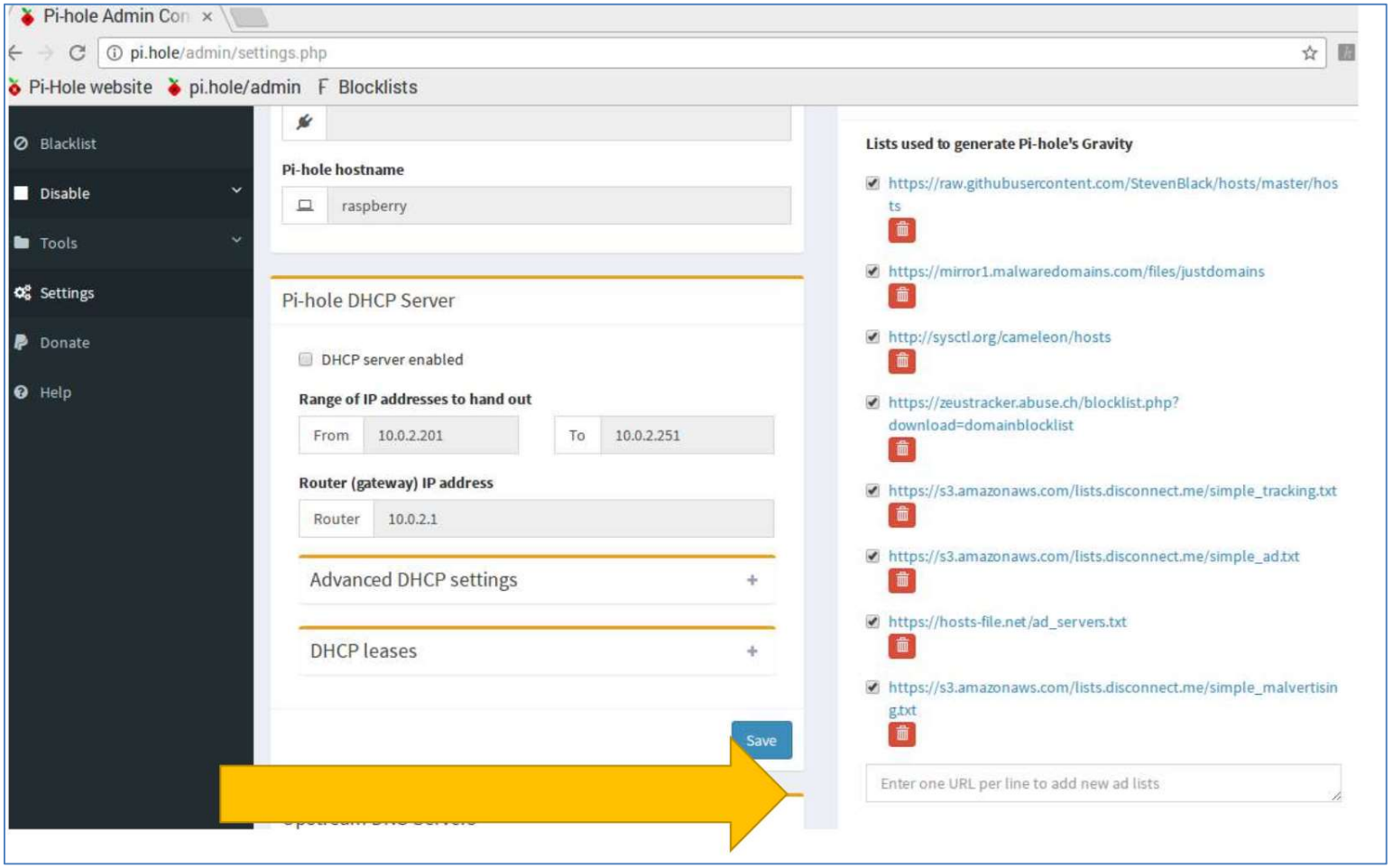
Of…DHCP op router uitzetten…



…en DHCP aan op Pi-hole



Block lists instellen



Websites met Block lists

Er zijn diverse block lists beschikbaar

- https://discourse.pi-hole.net/t/update-the-best-blocking-lists-for-the-pi-hole-dns-ad-blockers-interesting-combination/13620

- https://firebog.net/

Block lists installeren

- Worden opgeslagen als platte tekst in /etc/pihole

➢ Demo

nano - teksteditor

Even wat handige weetjes

nano sneltoetsen

Actie	Sneltoets	Alternatief
Help tonen	Ctrl+g	F1
Bestand sluiten	Ctrl+x	F2
Bestand opslaan	Ctrl+o	F3
Alinea uitlijnen	Ctrl+j	F4
Voeg ander bestand in	Ctrl+r	F5
Zoeken	Ctrl+w	F6
Verder zoeken	Alt+w	
Zoek en vervang	Ctrl+\	
Kopieer regel in klembord	Alt+^	Alt+6
Ga scherm omhoog	Ctrl+y	F7
Ga scherm omlaag	Ctrl+v	F8
Knip regel naar klembord	Ctrl+k	F9
Plak regel uit klembord	Ctrl+U	F10
Naar eerste regel	Alt+\	
Naar laatste regel	Alt+/	

nano tekst copy-paste

1. Plaats de cursor aan het begin van de tekst die je wilt kopiëren
2. Druk **Ctrl+6** (of **Alt+a**)
3. Markeer de tekst met de **pijtljestoetsen**
4. Druk **Alt+6** om de selectie te kopiëren
5. Druk **Ctrl+U** op de plaats waar je wilt plakken

Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

squid

squid installatie

- sudo apt-get update
- sudo apt-get install locate
  sudo updatedb

Install Squid, start it, and set it to start on boot:

- sudo apt-get install squid
- sudo apt-get install squid3
- sudo update-rc.d squid3 enable

squid installatie

- Kijk of squid op poort 3128 luistert:
- ➢ **sudo netstat –a ntp | grep squid**

- Squid gebruikt process id **proxy:proxy** voor de gebruiker en de groep
- ➢ **sudo ps -aux | grep squid**

squid installatie

- sudo apt install squidguard
- sudo update-rc.d squid enable

- sudo updatedb
- sudo nano /etc/squid3/squid.conf

squidGuard installatie

- cd /etc/squid**g**uard
- ls
- sudo cp squid**G**uard.conf squid**G**uard.conf.org
- cd
- sudo squid**G**uard -C all
  - Test of het compileren werkt voordat je squidGuard.conf aanpast

- sudo chown -R proxy:proxy /var/lib/squid**g**uard/db
- sudo chown -R proxy:proxy /var/log/squid**g**uard
- sudo chown -R proxy:proxy /usr/bin/squid**G**uard

squid configuratie

- Eerst een kopie maken:

➢ **sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.org**

➢ sudo nano -c /etc/squid/squid.conf

- Druk **Alt+/** om naar het einde te gaan en voeg toe:

  url_rewrite_program /usr/bin/squidGuard

➢ **sudo service squid restart**

squid configuratie

- squid.conf aanpassen:
- ➢ **sudo nano –c /etc/squid/squid.conf**
- uncomment the lines that start with
  #acl localnet src ...
- **acl localnet src 10.0.0.0/8**
  acl localnet src 172.16.0.0/12
  acl localnet src 192.168.0.0/16
- En pas ze aan voor jouw netwerk
- On line 1209 uncomment the line #http_access allow localnet:
  http_access allow localnet
- On line 1613 make sure http_port 3128 is uncommented:
  http_port 3128
- 'sudo service squid restart'

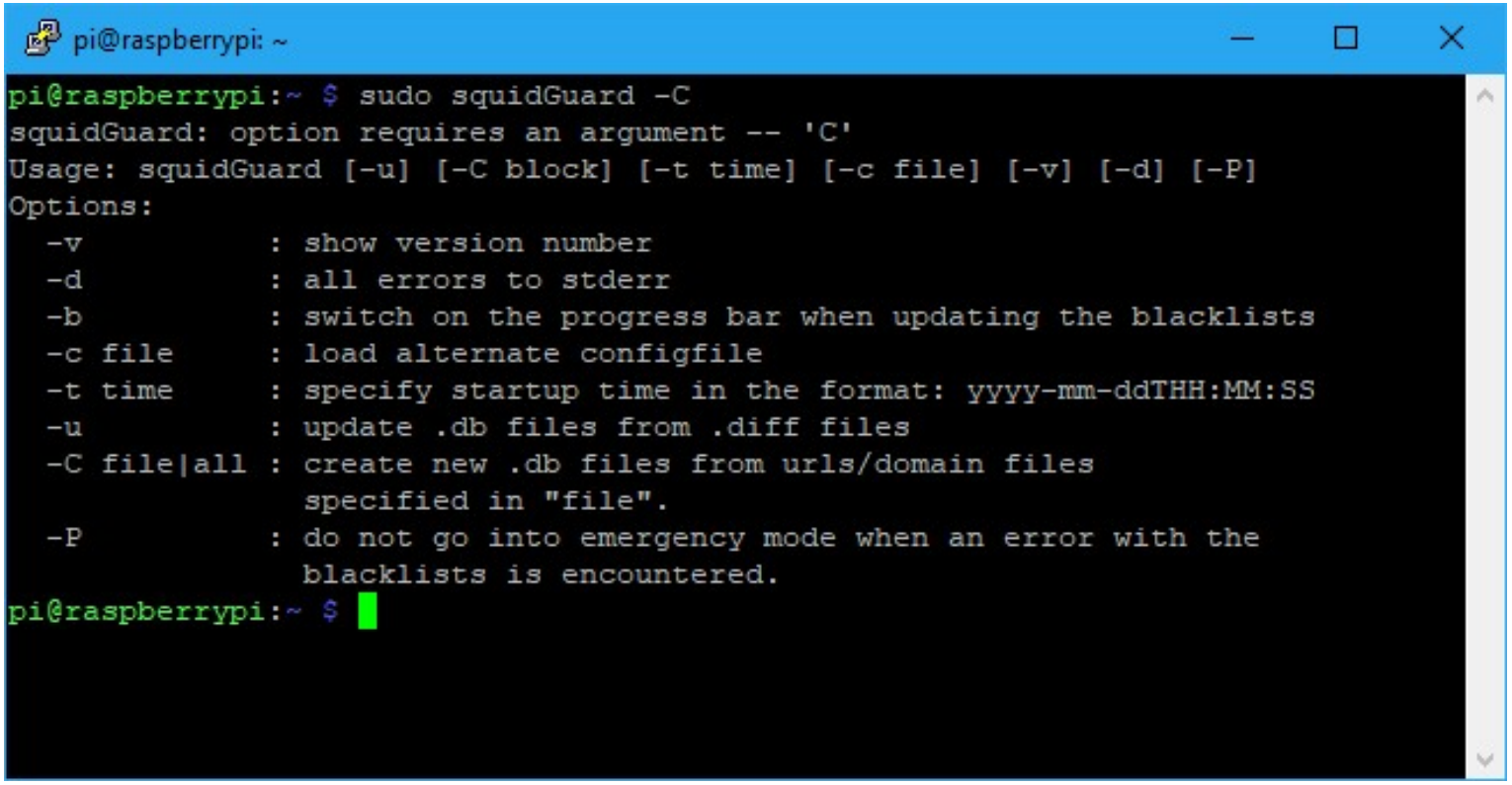
- ➢ Zoeken : **CTRL+w**

squid testen

- Stel client in als proxy client :
- IP-adres van de Raspberry Pi
- Poortnummer: 3128

- Monitoren van access.log:
- sudo tail -f /var/log/squid/access.log

squid opties



Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

Installatie squidGuard

squidGuard installeren

1. sudo apt-get install squidguard
2. sudo update-rc.d squid enable
3. sudo updatedb
4. cd /etc/squidguard
5. sudo cp squidGuard.conf squidGuard.conf.org
6. cd
7. sudo squidGuard -C all

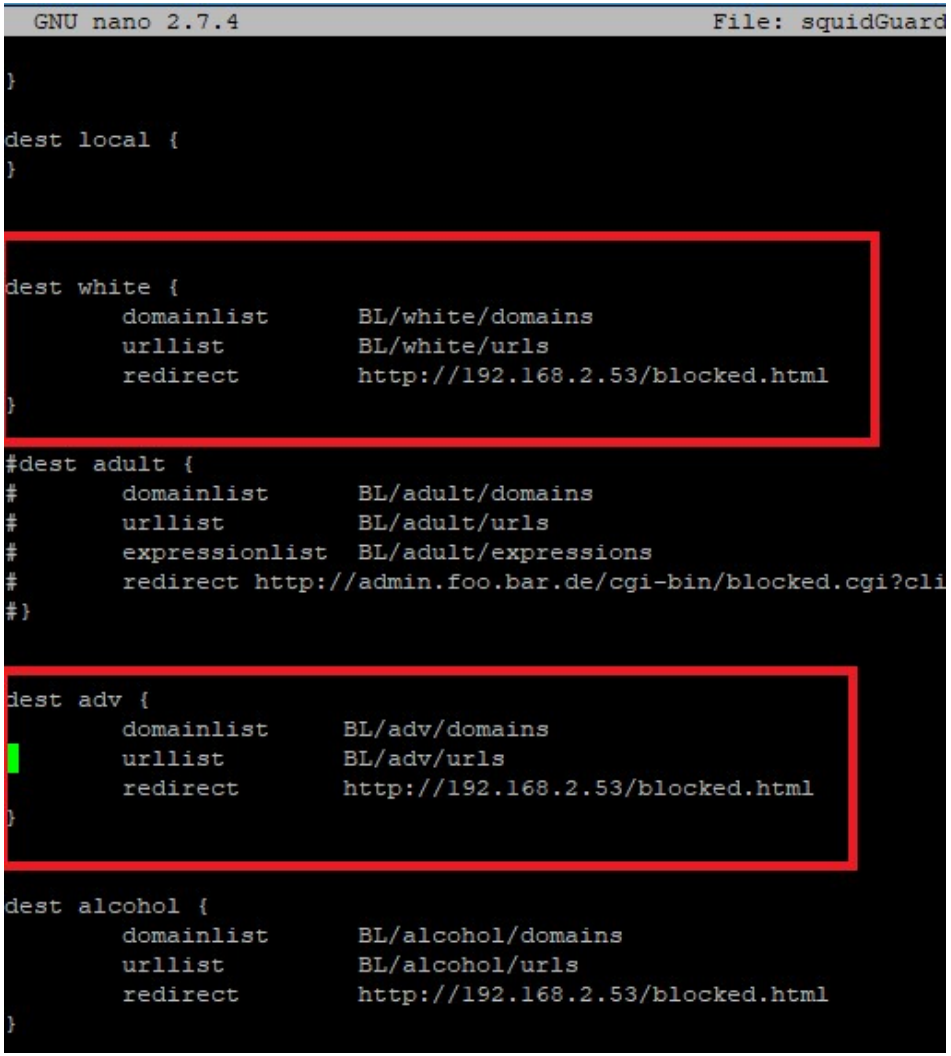
Hiermee test je eerst of het compileren werkt voordat je squidGuard.conf aanpast

8. sudo chown -R proxy:proxy /var/lib/squidguard/db
9. sudo chown -R proxy:proxy /var/log/squidguard
10. sudo chown -R proxy:proxy /usr/bin/squidGuard

Aanpassen squid.conf

11. cd /etc/squid
12. sudo cp squid.conf squid.conf.org
13. sudo nano /etc/squid/squid.conf
14. Voeg onderaan toe: url_rewrite_program /usr/bin/squidGuard
15. sudo service squid reload

Configuratie squidGuard



Configuratie squidGuard

```
#
# ACL RULES:
#

acl {
        admin {
                pass     any
        }

        foo-clients within workhours {
                pass     good !in-addr any
        } else {
                pass any
        }

        bar-clients {
                pass    local none
        }

        default {
#               pass     local none
                pass white !porn !adv  !finance !recreation  !urlshortener !fortunetelling
                redirect http://127.0.0.1/blocked.html
        }
}
```

Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

Installatie squidGuard Blacklists

Blacklist installeren

Installeer Shallalist :

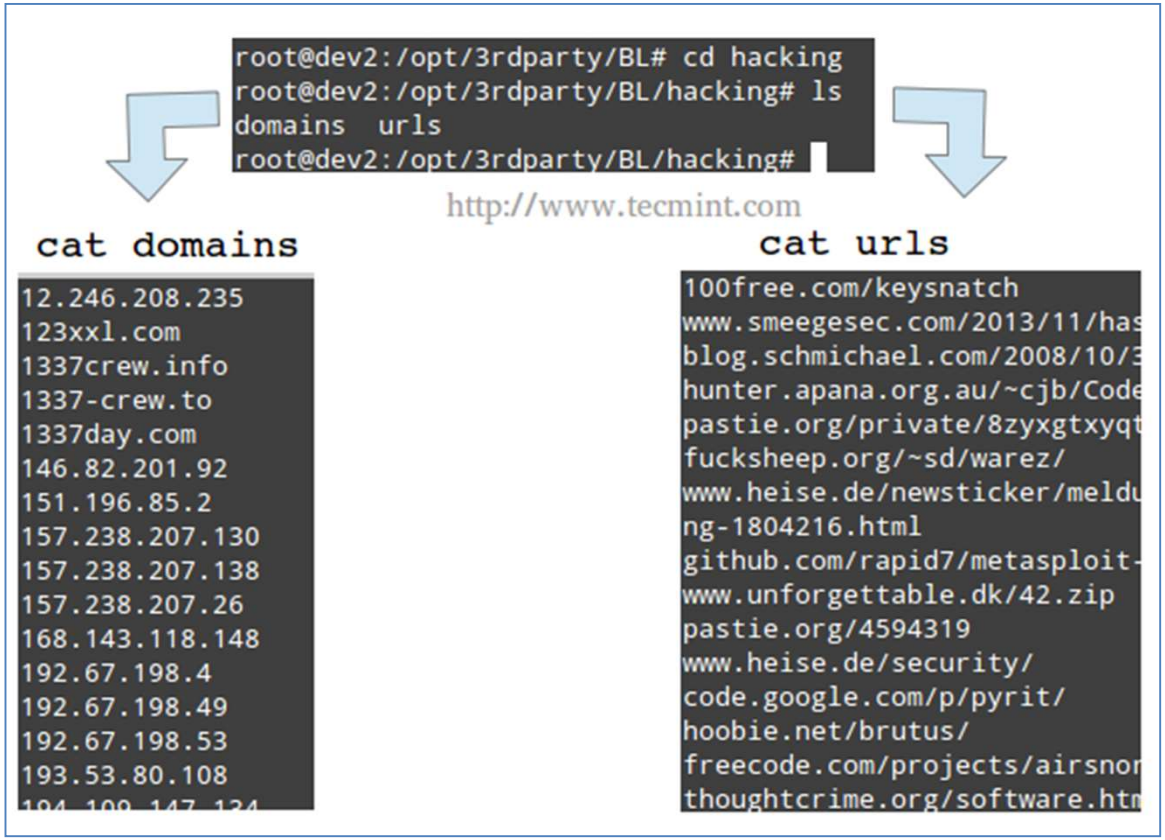
1. sudo mkdir Downloads
2. cd Downloads
3. sudo wget http://www.shallalist.de/Downloads/shallalist.tar.gz
4. sudo tar -xzf shallalist.tar.gz
5. sudo cp BL -R /var/lib/squidguard/db
6. cd /var/lib/squidguard/db # om te controleren
7. sudo chmod -R 755 /var/lib/squidguard/db/BL
8. cd /var/lib/squidguard/db/BL

Shallalist installeren

- sudo chown -R proxy:proxy /var/lib/squidguard/db
  - Dit is belangrijk, anders worden wijzigingen van de blacklist(s) niet gelezen door squid.
- sudo service squid restart
- sudo service squid status

Shallalist categoriën

Shallalist uitleg



Shallalist uitleg

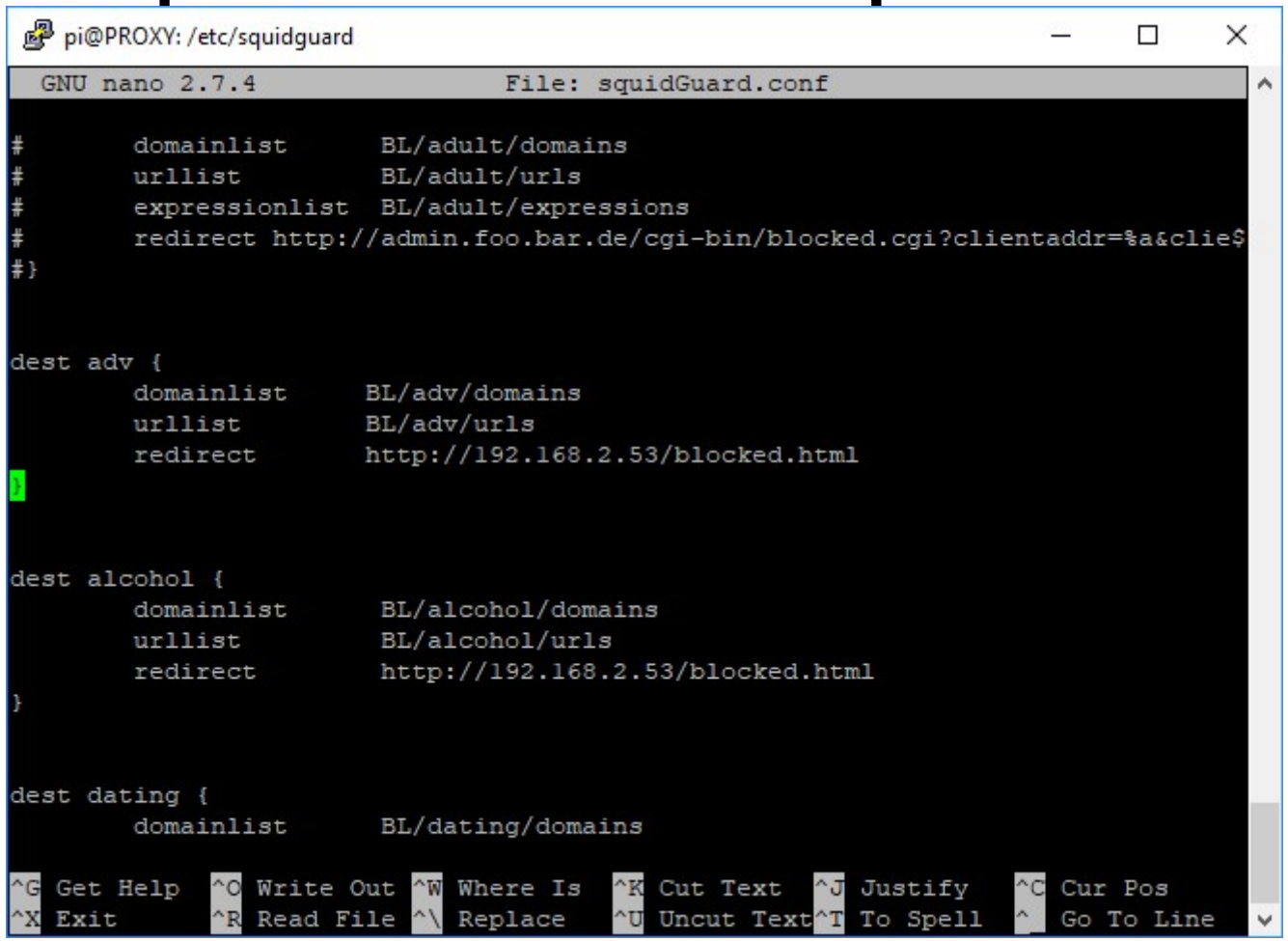
- Sommige blocklists zijn vrij groot!
- Bijv. de blocklist in porn, 15MB groot is!

- Online Games zit in de categorie ‘hobby’

- Om een domain naam in alle squidGuard categorieren te zoeken:

➢ grep -d recurse "how" *

squidGuard aanpassen



squidGuard aanpassen

pi@PROXY: /etc/squidguard

```
 GNU nano 2.7.4                    File: squidGuard.conf

        urllist         BL/webtv/urls
        redirect        http://192.168.2.53/blocked.html
}



#
# ACL RULES:
#

acl {
        admin {
                pass     any
        }

        foo-clients within workhours {
                pass     good !in-addr any
        } else {
                pass any
        }

        bar-clients {
                pass    local none
        }

        default {
#               pass     local none
                pass white !porn !adv  !finance !recreation  !urlshortener !fortunetel$

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Test Client instellen

- Test het eerst vanaf 1 apparaat
- Stel het IP adres van Pi-hole in als de DNS van je client (laptop)

Block lists bekijken

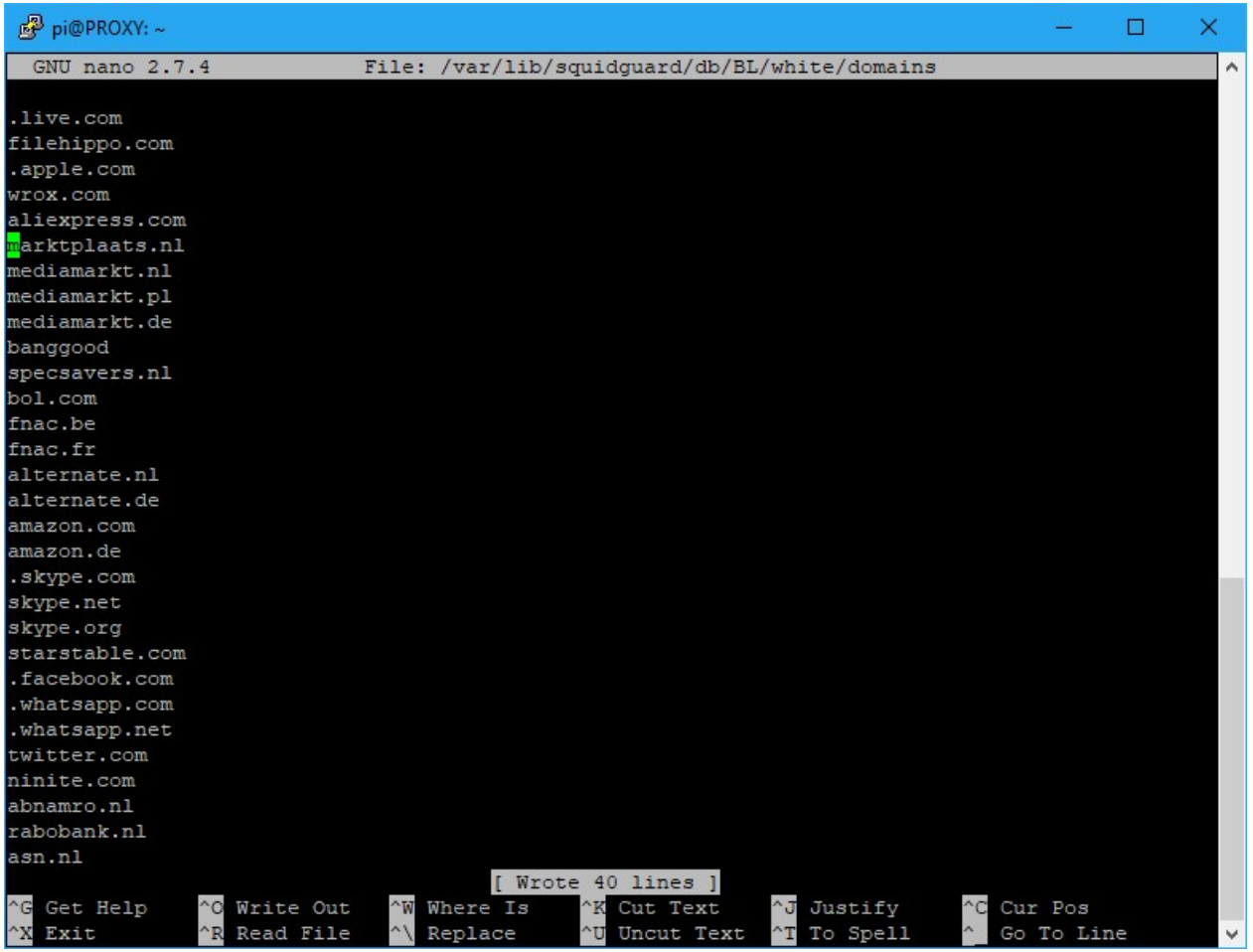
```
pi@PROXY:~ $ ls
blocked.html  CronOutput          edit_white.sh       restore_prev_shallalist.sh
check_log.sh  domoticz            installed-packages  squid_log.sh
CronJobs      Downloads           refresh.sh          uit.sh
cron_log.txt  edit_squidGuard.sh  refresh_white.sh    update_shallalist.sh
pi@PROXY:~ $ cat edit_white.sh
sudo nano /var/lib/squidguard/db/BL/white/domains
pi@PROXY:~ $
```

Whitelist maken

- cd /var/lib/squidguard/db/BL
- sudo mkdir white
- cd white
- sudo nano domains
- sudo nano urls

Whitelist maken

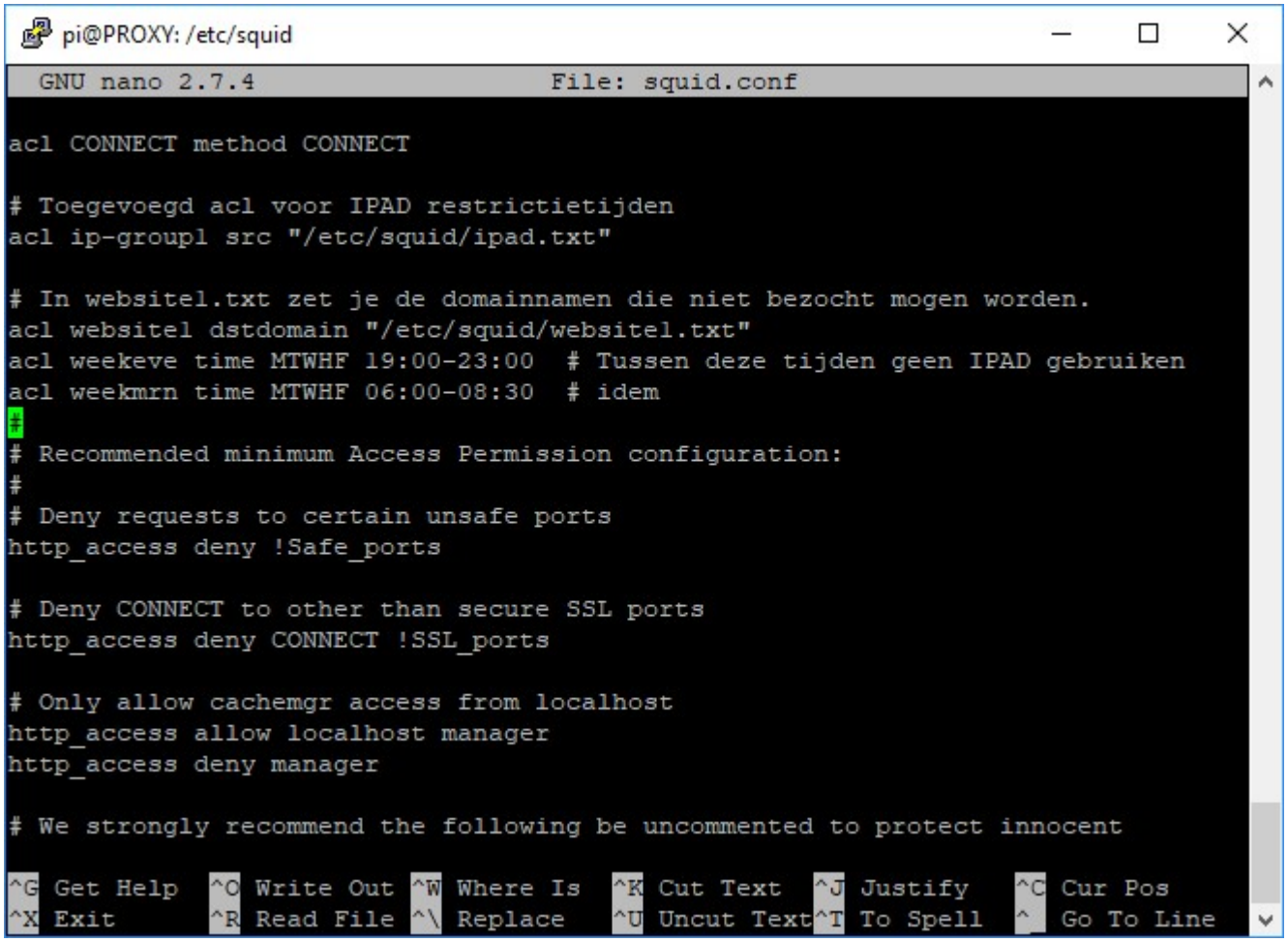
sudo nano domains



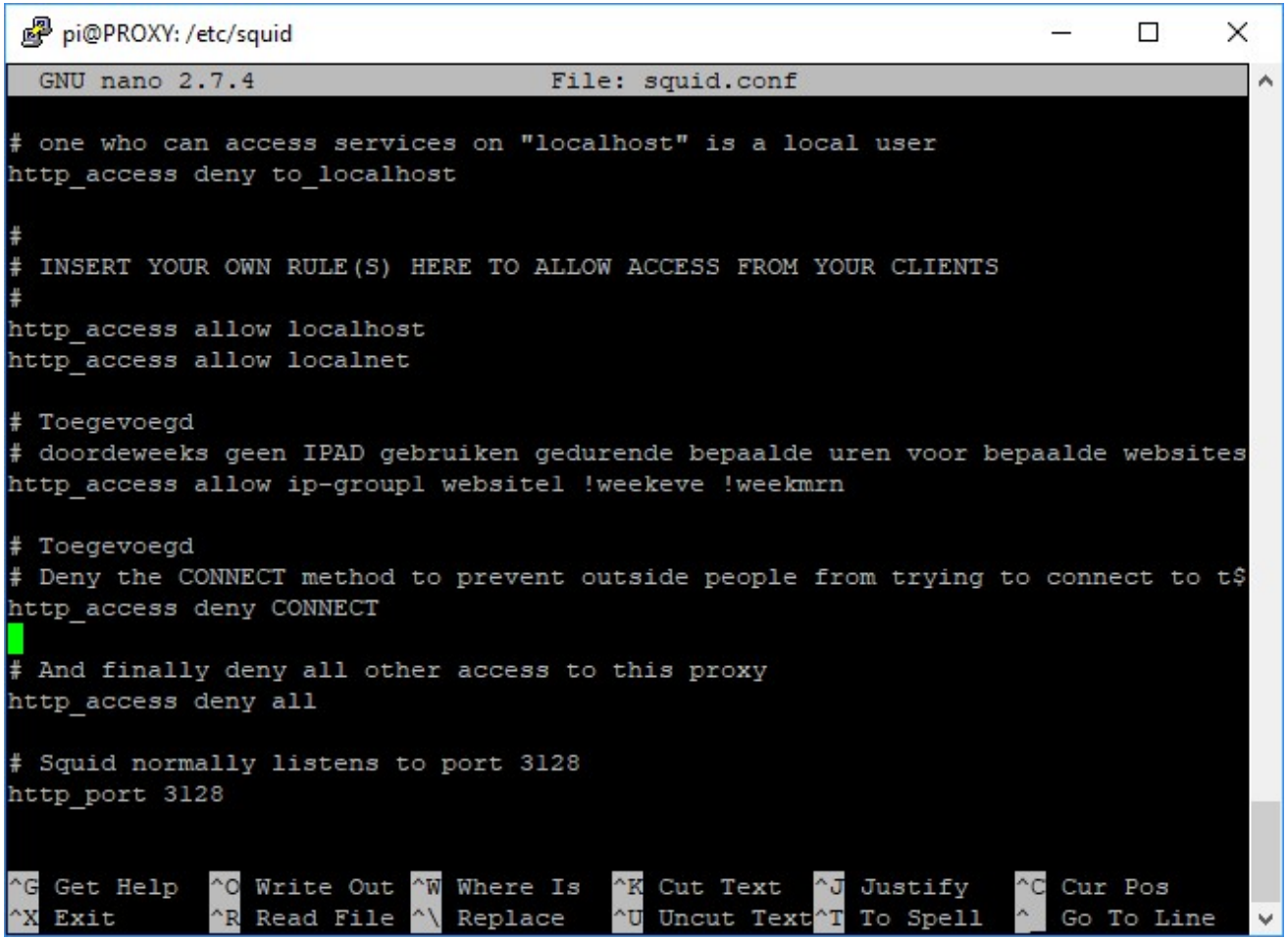
Geen internet op bepaalde tijd

```
pi@PROXY:/etc/squid $ cat time.txt
07:00-08:30
19:00-22:00
pi@PROXY:/etc/squid $ cat ipad.txt
# IP adres van iPAD
192.168.2.8
pi@PROXY:/etc/squid $ cat website1.txt
# Websites te blokkeren
.nu.nl
.youtube.com
.starstable.com
.google.com
```

Geen internet op bepaalde tijd



Geen internet op bepaalde tijd



Demo

- Pi-hole installatie
- Pi-hole configureren
- Blocklist toevoegen
- Whitelist toevoegen
- Extra blacklists toevoegen
- Pihole commando opties

Opdracht

1. Maak een eigen blacklist
2. Zorg dat die niet overschreven wordt door shallalist
3. Denk dus goed na over de mapnaam!
4. Zet daar een eigen url en domain in
5. Test bijvoorbeeld met ‘www.sheerenloo.nl’
6. Pas squidGuard.conf aan
7. Refresh squidGuard

➢ Als voorbeeld kun je onze eigen ‘white’ list gebruiken

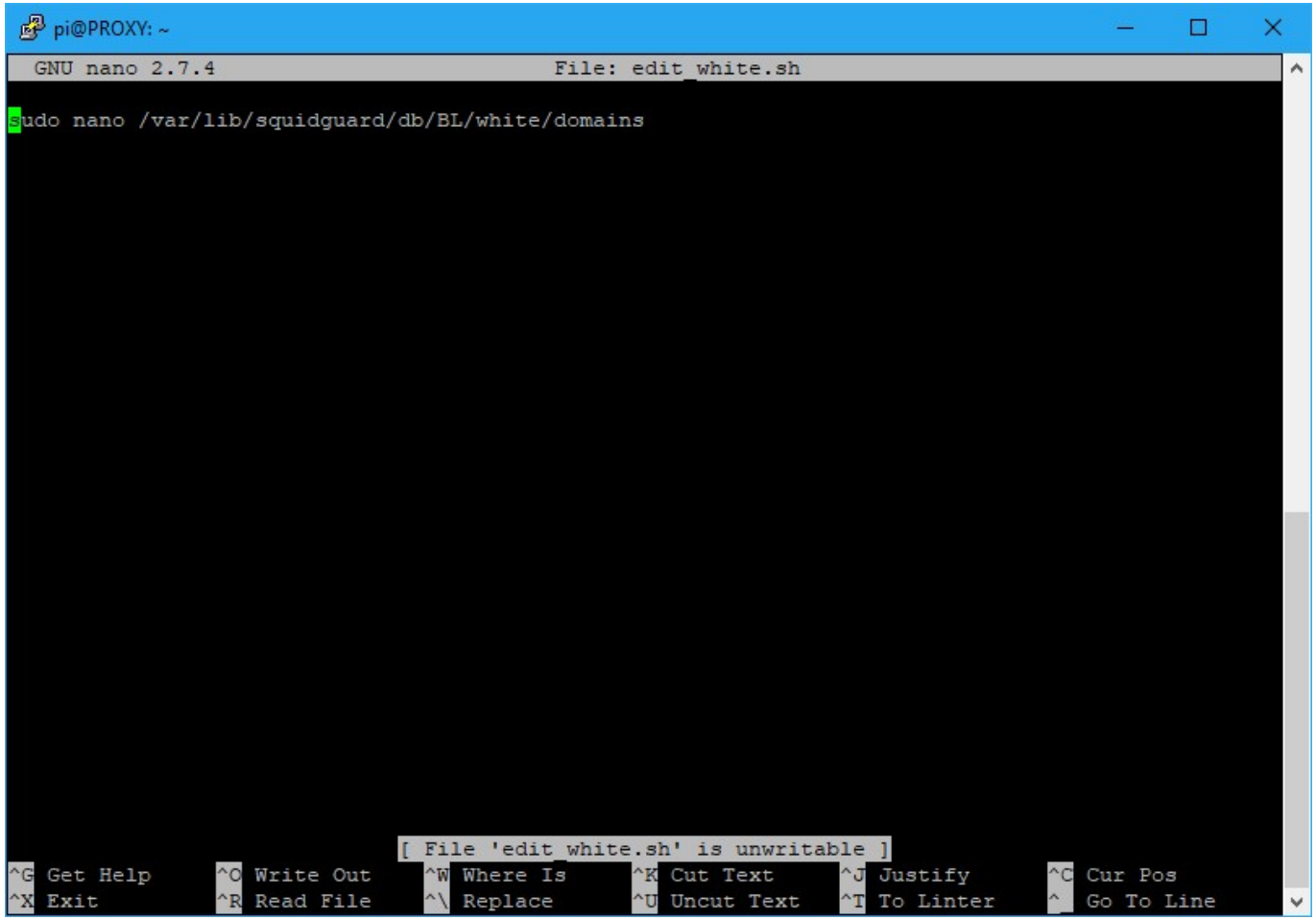
Agenda

1. Uitleg Pi-hole, squid en squidGuard
2. Benodigde hardware en software
3. Installatie en configuratie Pi-hole (Ad-blocker)
4. Installatie en configuratie squid (proxy)
5. Installatie en configuratie squidGuard (website blocker)
6. Installatie squidGuard blacklist (shallalist)
7. Onderhoud squid en squidGuard
8. Demo's
9. Extra's: webmin

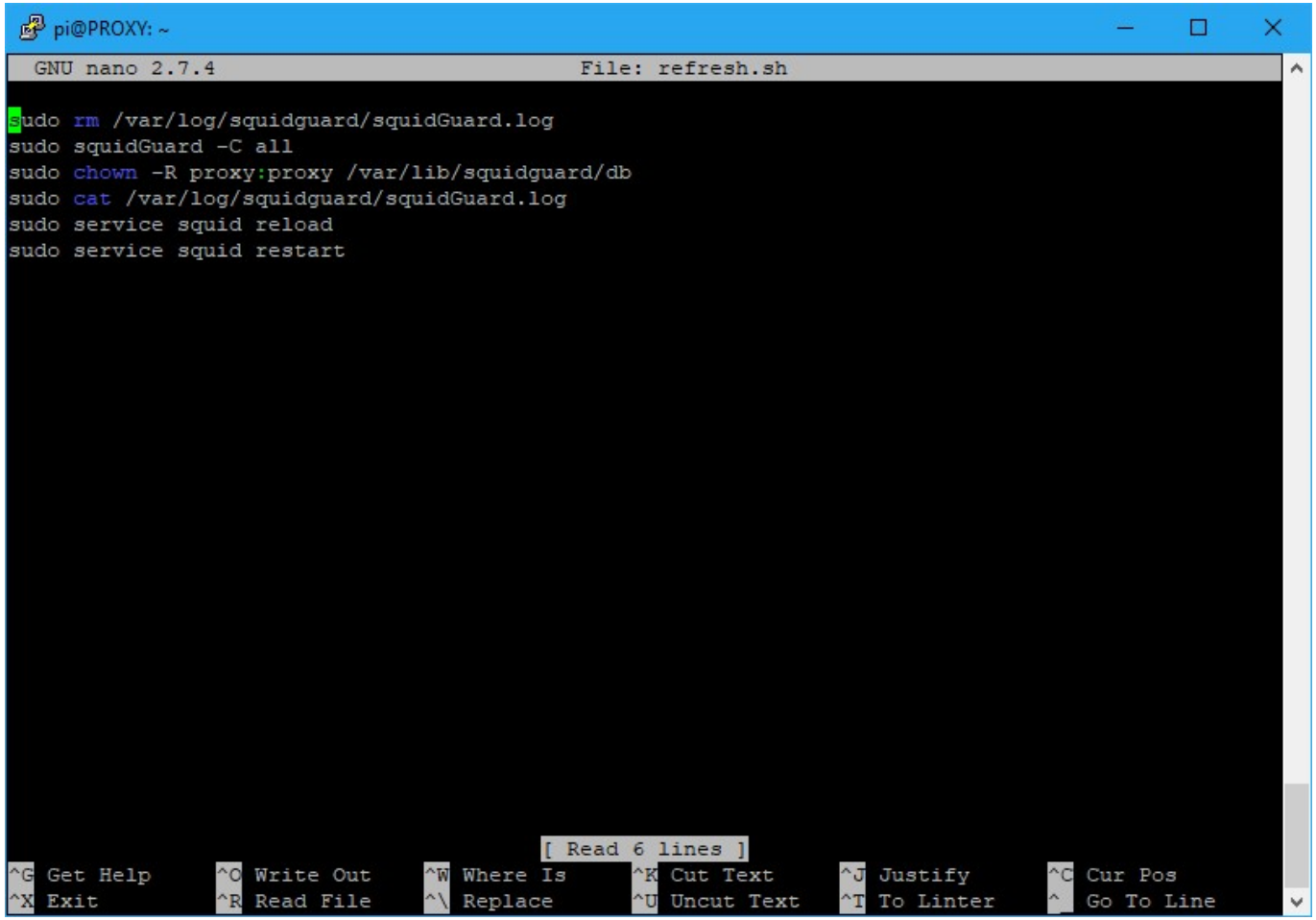
Handige scripts

Eigen scripts voor snel beheer

edit_white.sh



Refresh.sh


pi@PROXY: ~
GNU nano 2.7.4 File: refresh.sh
sudo rm /var/log/squidguard/squidGuard.log
sudo squidGuard -C all
sudo chown -R proxy:proxy /var/lib/squidguard/db
sudo cat /var/log/squidguard/squidGuard.log
sudo service squid reload
sudo service squid restart
[Read 6 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line

update_shallalist.sh

pi@PROXY: ~

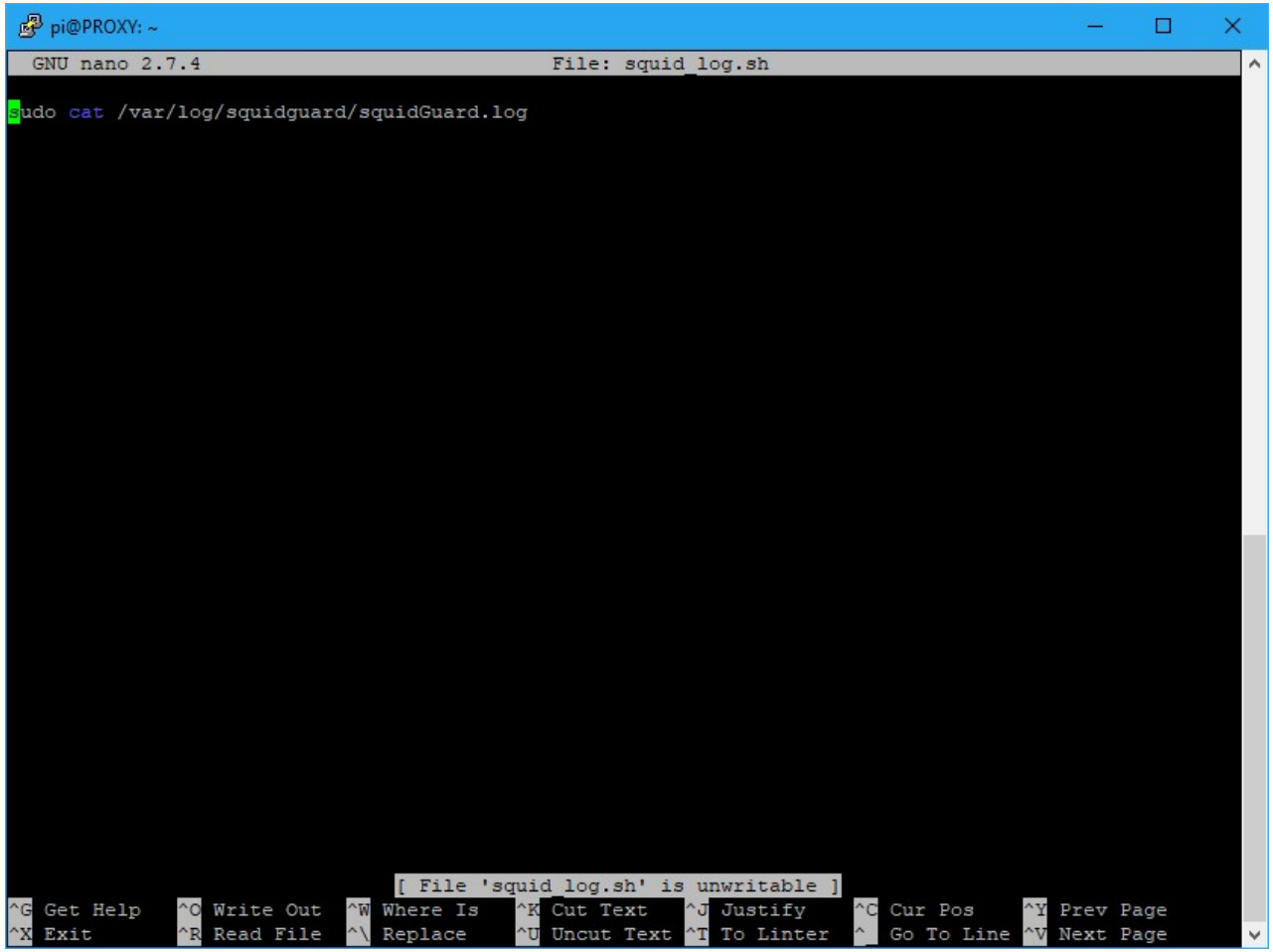
GNU nano 2.7.4 File: update_shallalist.sh

```
#!/bin/sh
# set -x  # Uitvoer naar scherm aanzetten
# set +x  # Uitvoer naar scherm uitzetten
cd
cd Downloads
echo "Backuping shallalist..."
sudo cp shallalist.tar.gz shallalist.tar.gz.old
sudo rm shallalist.tar.gz

echo "Downloading shallalist..."
sudo wget http://www.shallalist.de/Downloads/shallalist.tar.gz
echo "Extracting shallalist..."
sudo tar -xzf shallalist.tar.gz
echo "Copying shallalist to squidguard database files..."
sudo cp BL -R /var/lib/squidguard/db
echo "Assigning rights to the Blacklists"
sudo chmod -R 755 /var/lib/squidguard/db/BL
echo "Removing squidGuard.log..."
sudo rm /var/log/squidguard/squidGuard.log
echo "Building databases..."
sudo squidGuard -C all
echo "Database builds complete!"
sudo chown -R proxy:proxy /var/lib/squidguard/db
sudo squid -k reconfigure
echo "Squid Proxy Server reconfigured"
echo "Reloading squid..."
sudo service squid reload
echo "Restarting squid..."
sudo service squid restart
echo "Done!"
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line ^V Next Page

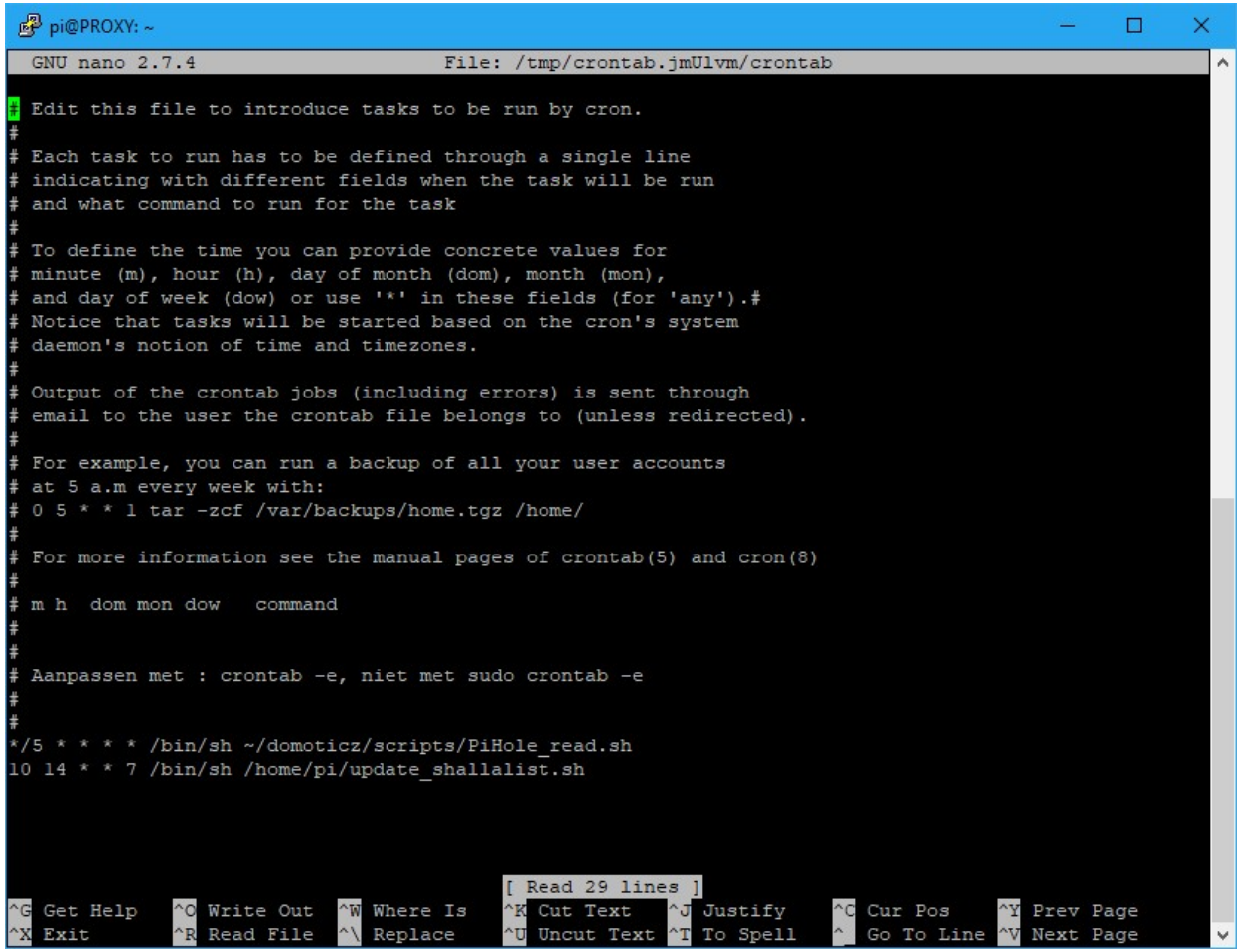
squid_log.sh


pi@PROXY: ~
GNU nano 2.7.4
File: squid_log.sh
sudo cat /var/log/squidguard/squidGuard.log
[File 'squid_log.sh' is unwritable]
^G Get Help
^O Write Out
^W Where Is
^K Cut Text
^J Justify
^C Cur Pos
^Y Prev Page
^X Exit
^R Read File
^\ Replace
^U Uncut Text
^T To Linter
^_ Go To Line
^V Next Page

crontab

Automatisch taken uitvoeren

crontab


pi@PROXY: ~
GNU nano 2.7.4 File: /tmp/crontab.jmUlvm/crontab
Edit this file to introduce tasks to be run by cron.
#
Each task to run has to be defined through a single line
indicating with different fields when the task will be run
and what command to run for the task
#
To define the time you can provide concrete values for
minute (m), hour (h), day of month (dom), month (mon),
and day of week (dow) or use '*' in these fields (for 'any').#
Notice that tasks will be started based on the cron's system
daemon's notion of time and timezones.
#
Output of the crontab jobs (including errors) is sent through
email to the user the crontab file belongs to (unless redirected).
#
For example, you can run a backup of all your user accounts
at 5 a.m every week with:
0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
For more information see the manual pages of crontab(5) and cron(8)
#
m h dom mon dow command
#
#
Aanpassen met : crontab -e, niet met sudo crontab -e
#
#
*/5 * * * * /bin/sh ~/domoticz/scripts/PiHole_read.sh
10 14 * * 7 /bin/sh /home/pi/update_shallalist.sh
[Read 29 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line ^V Next Page

squid_log.sh

- crontab -e

Voert het script elke zondag uit om kwart over 10:

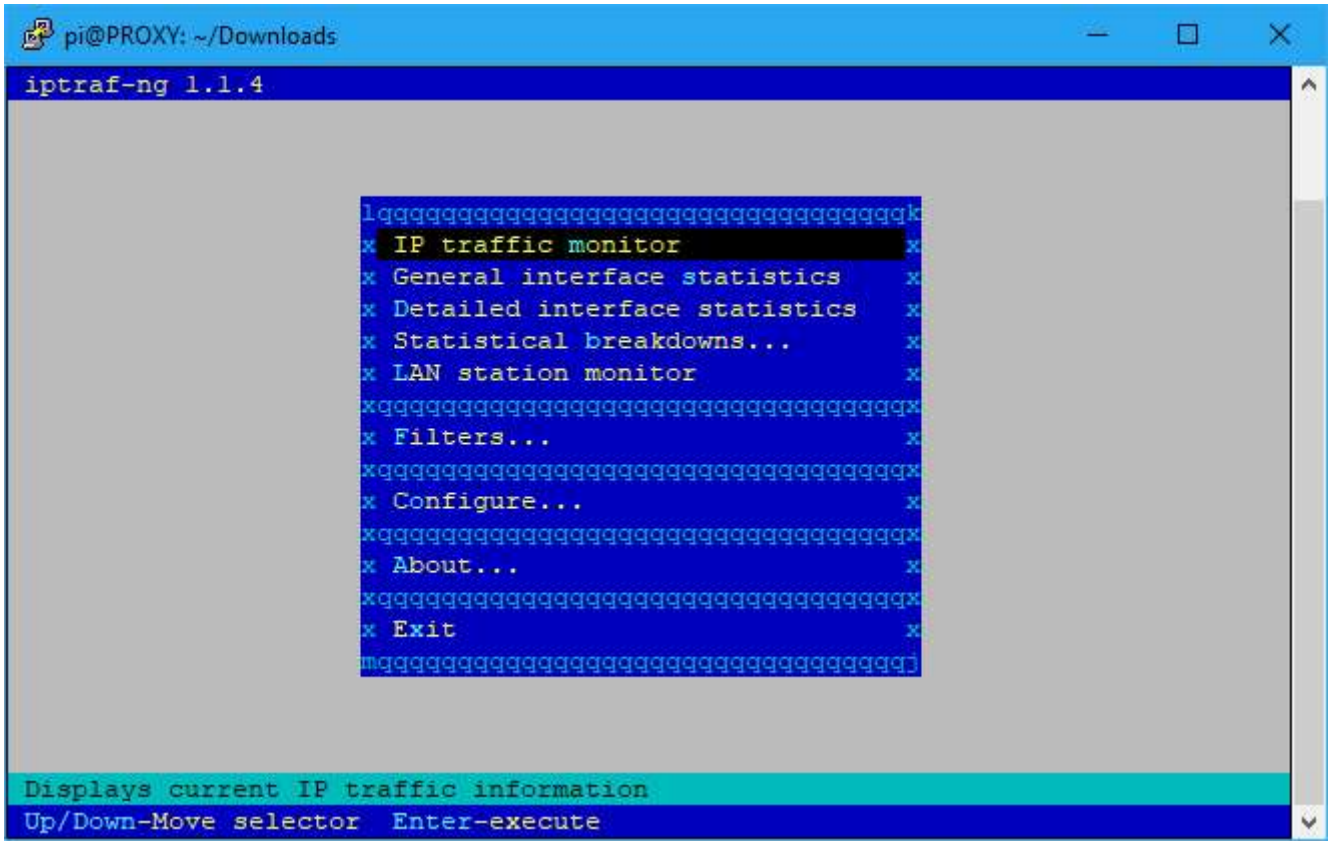
➢ 10 15 * * 7 /bin/sh /home/pi/update_shallalist.sh

Monitoren

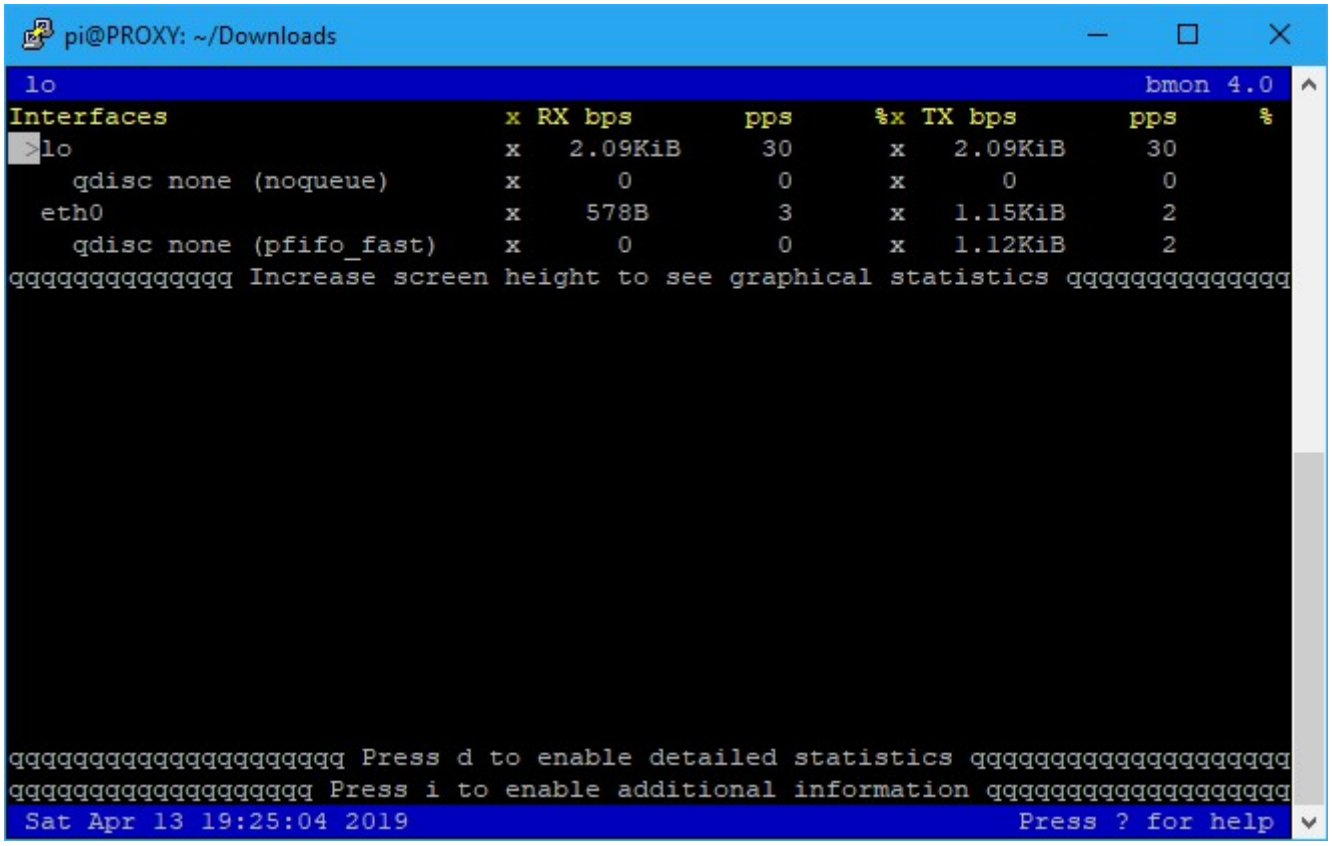
Netwerkverkeer bekijken

- iptraf-ng
  - sudo apt-get install iptraf-ng
- bmon
  - sudo apt-get install bmon
- vnstat
  - sudo apt-get install vnstat
- sarg (Squid Analysis Report Generator)
  - sudo apt-get install sarg

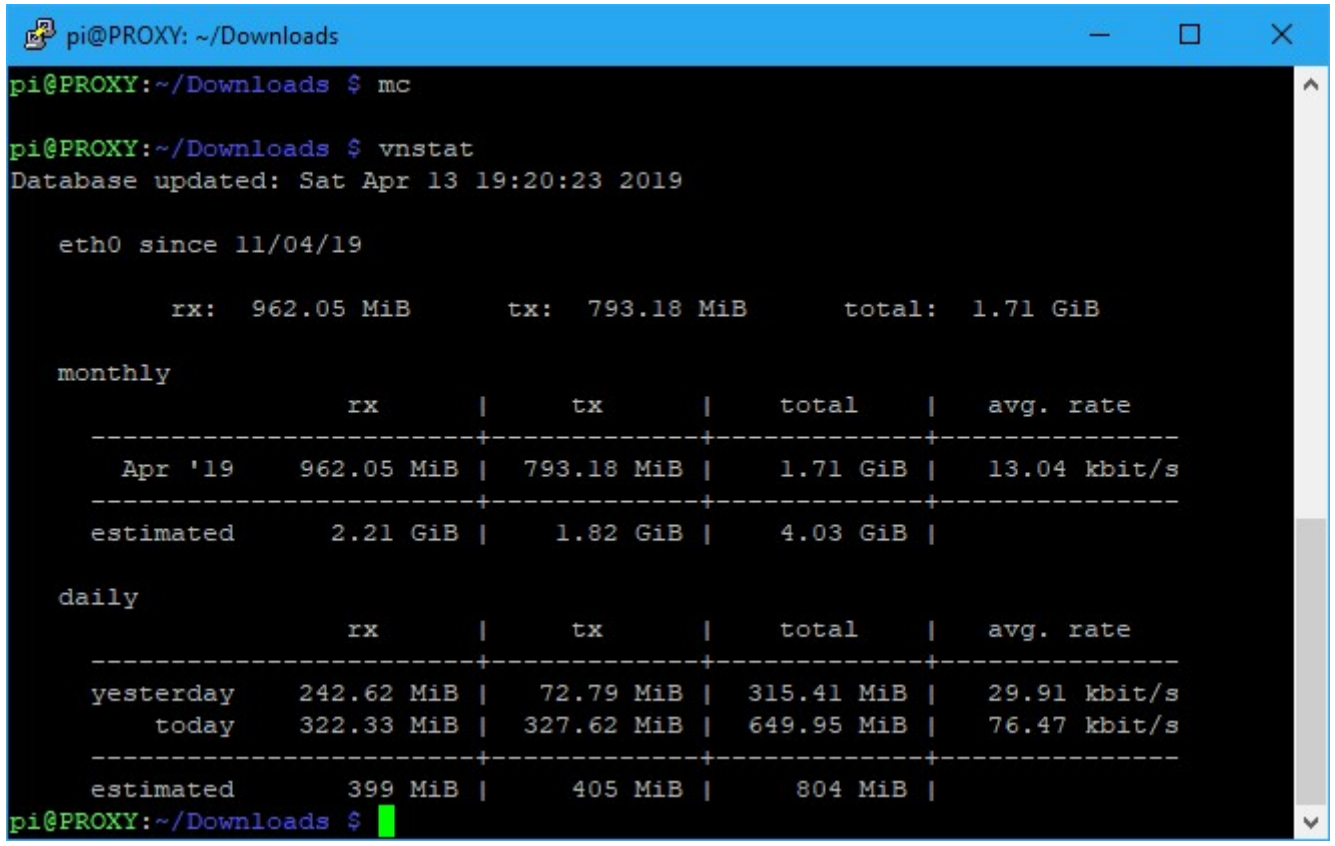
iptraf-ng


pi@PROXY: ~/Downloads
iptraf-ng 1.1.4
IP traffic monitor
General interface statistics
Detailed interface statistics
Statistical breakdowns...
LAN station monitor
Filters...
Configure...
About...
Exit
Displays current IP traffic information
Up/Down-Move selector Enter-execute

bmon


pi@PROXY: ~/Downloads
lo
bmon 4.0
Interfaces x RX bps pps %x TX bps pps %
>lo x 2.09KiB 30 x 2.09KiB 30
qdisc none (noqueue) x 0 0 x 0 0
eth0 x 578B 3 x 1.15KiB 2
qdisc none (pfifo_fast) x 0 0 x 1.12KiB 2
qqqqqqqqqqqqqq Increase screen height to see graphical statistics qqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqq Press d to enable detailed statistics qqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqq Press i to enable additional information qqqqqqqqqqqqqqqqqqqq
Sat Apr 13 19:25:04 2019
Press ? for help

vnstat


pi@PROXY: ~/Downloads
pi@PROXY:~/Downloads $ mc
pi@PROXY:~/Downloads $ vnstat
Database updated: Sat Apr 13 19:20:23 2019
eth0 since 11/04/19
rx: 962.05 MiB tx: 793.18 MiB total: 1.71 GiB
monthly
rx | tx | total | avg. rate
Apr '19 962.05 MiB | 793.18 MiB | 1.71 GiB | 13.04 kbit/s
estimated 2.21 GiB | 1.82 GiB | 4.03 GiB |
daily
rx | tx | total | avg. rate
yesterday 242.62 MiB | 72.79 MiB | 315.41 MiB | 29.91 kbit/s
today 322.33 MiB | 327.62 MiB | 649.95 MiB | 76.47 kbit/s
estimated 399 MiB | 405 MiB | 804 MiB |
pi@PROXY:~/Downloads $

Extra informatie

- https://pi-hole.net/
- https://jacobsalmela.com/2015/06/16/block-millions-ads-network-wide-with-a-raspberry-pi-hole-2-0/
- http://users.telenet.be/MySQLplaylist/pi-hole.pdf
- https://blog.cryptoaustralia.org.au/whyou-need-network-wide-ad-blocker-pi-hole/
- https://blog.cryptoaustralia.org.au/instructions-for-setting-up-pi-hole/
- https://discourse.pi-hole.net/t/how-do-i-show-hostnames-instead-of-ip-addresses-in-the-dashboard/3530
- https://docs.pi-hole.net/ftldns/dns-cache/
- https://docs.pi-hole.net/guides/vpn/overview/
- https://en.wikipedia.org/wiki/Pi-hole

Vragen?