

Veiliger internetten met de Raspberry Pi

Pi-hole, squid, squidGuard

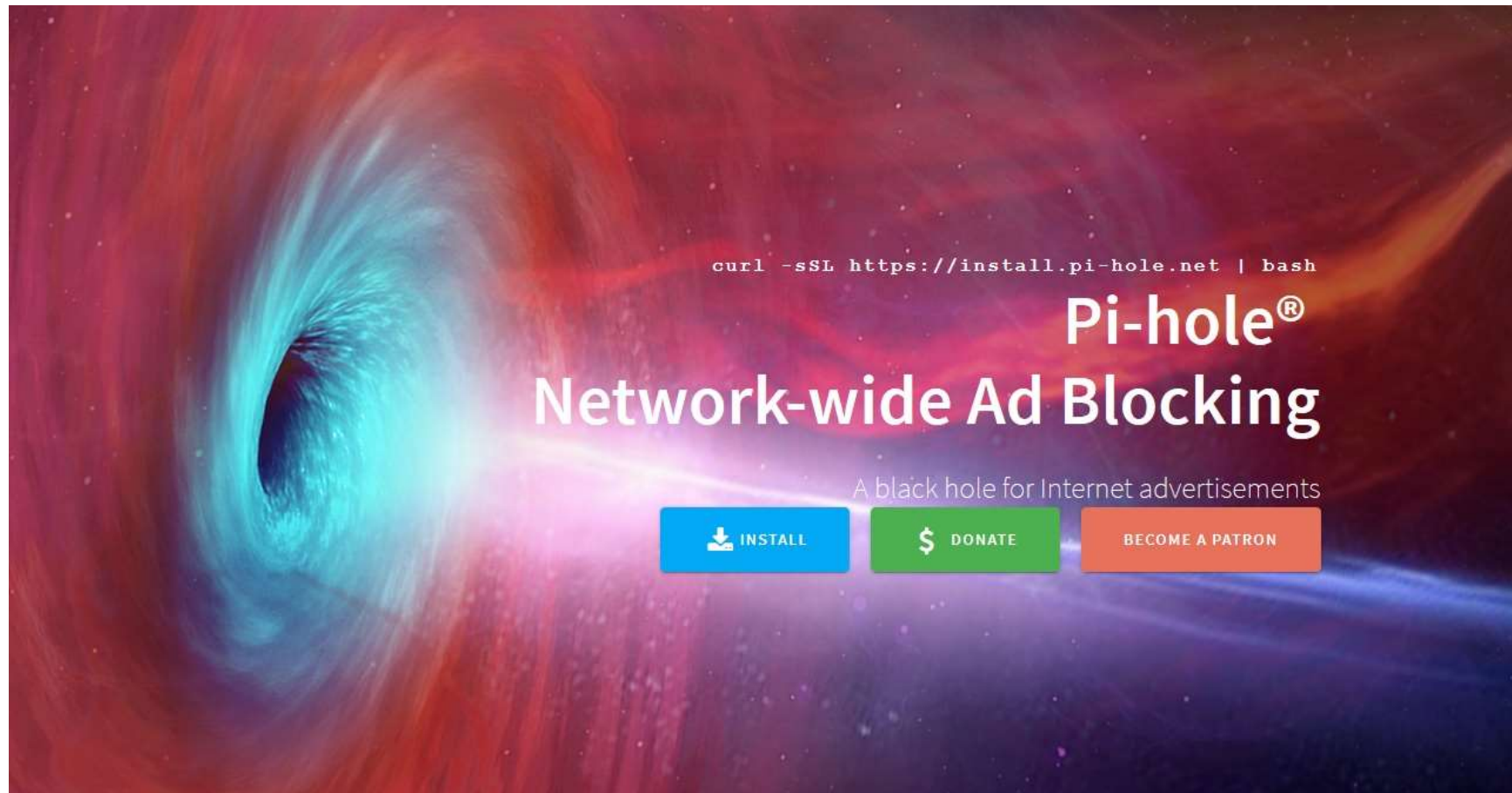
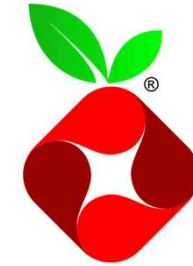
Marcel Runte, maart 2021,

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



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 \leftrightarrow 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)
- Kan 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

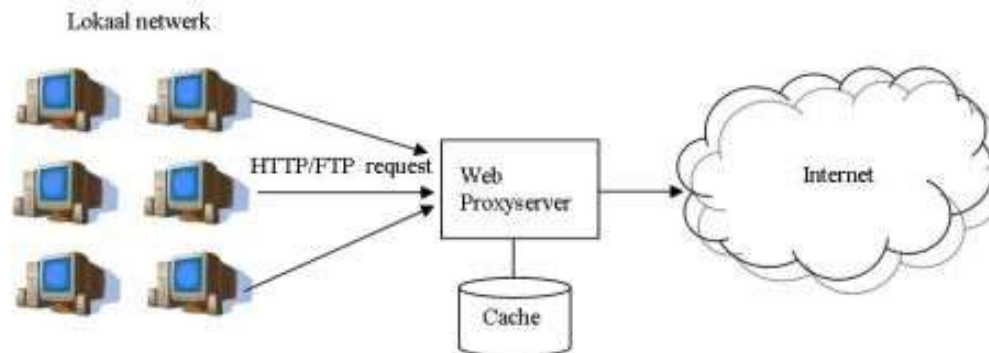
Agenda

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

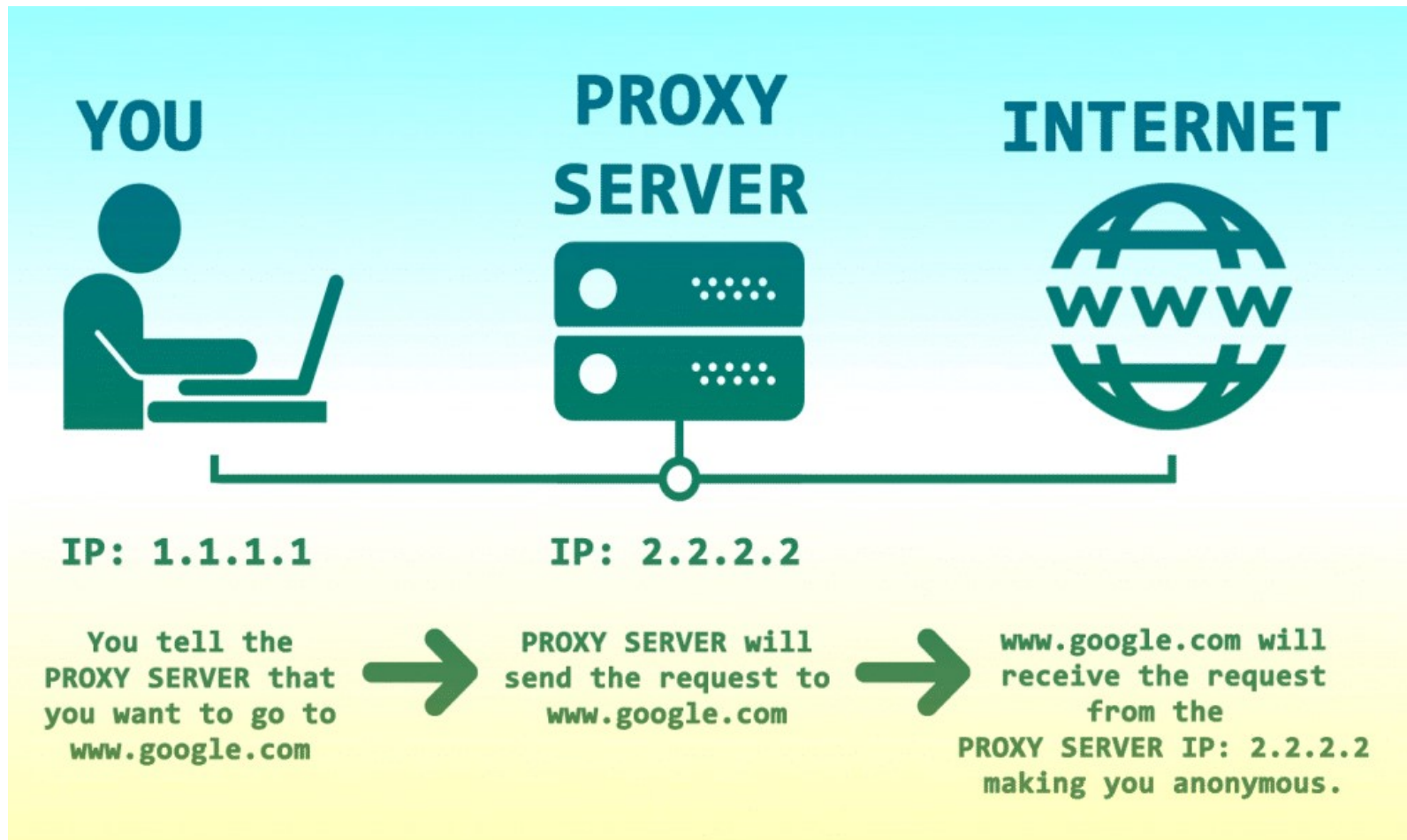
squid proxy

Wat is een proxyserver?

- Een server tussen de computer van een gebruiker en de computer waarop de door de gebruiker gewenste informatie staat
- Het Engelse 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 proxy servers.

- **Web proxy**
De meest voorkomende server.
Alle clients in een lokaal netwerk gaan via een proxy server het internet op.
Al het HTTP- en/of FTP-verkeer wordt gecached
Snelheidsvoordeel voor de clients in het netwerk die webpagina's opvragen uit de cache (of tussenbuffer) van de proxy server.
- **Open proxy**
Een **open proxy** is een proxy server 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 proxy server werkt hier van buiten naar binnen, dus andersom. Dit wordt ook wel "web server acceleration" genoemd. Hierbij wordt de proxy server 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
- Proxify
- 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

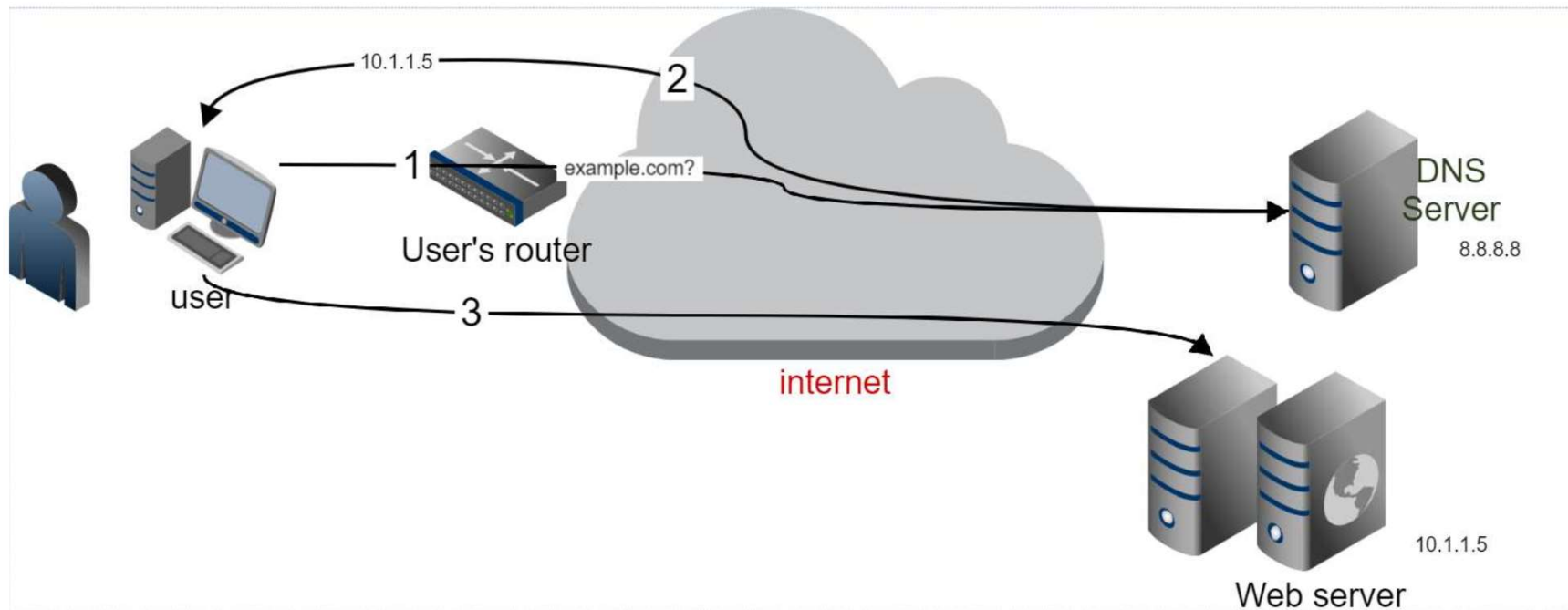
Wat is squidGuard?

- 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
 - Stuur client door naar info pagina
- Toegangsregels op basis van dag/tijdstip

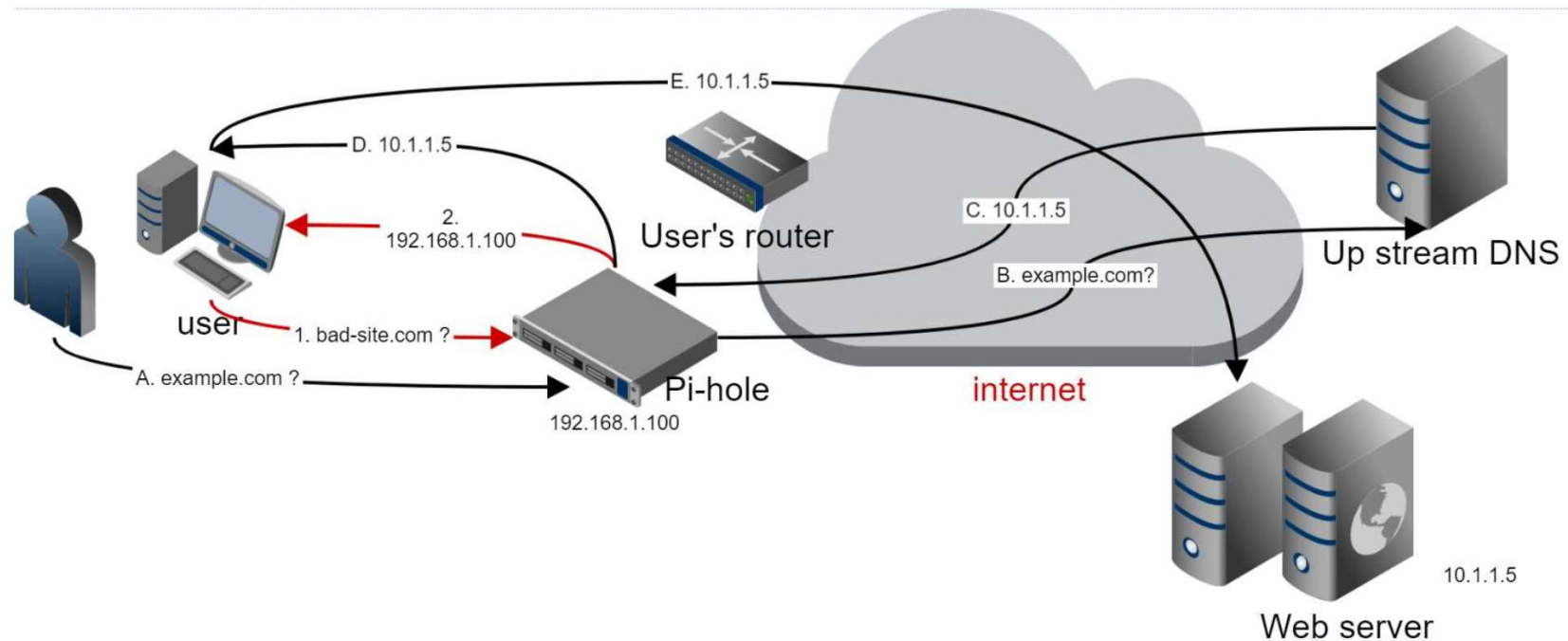
Waarom squidGuard

- 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 tijdzone 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

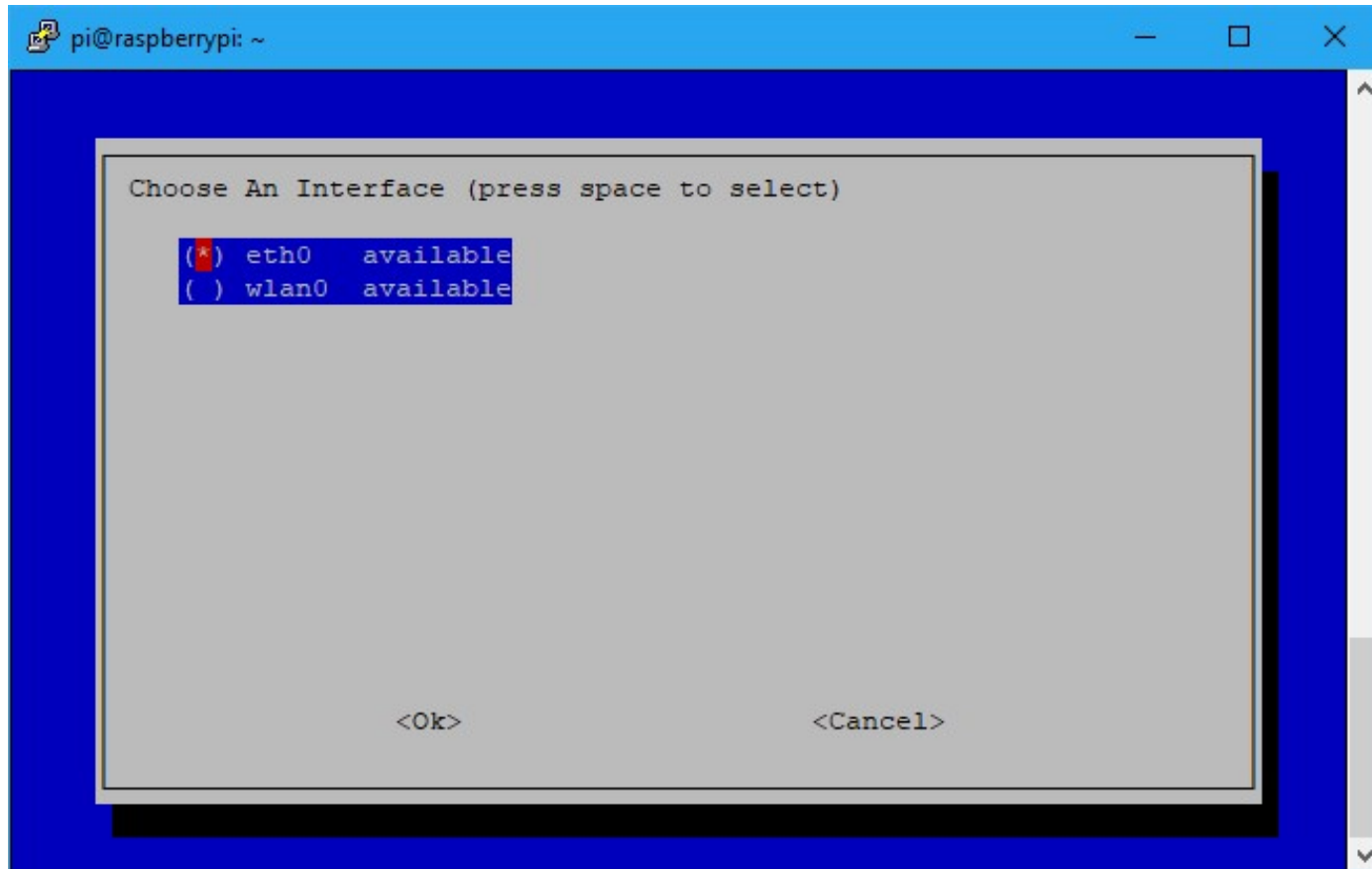
Pi-hole installatie

- Installeer Pi-hole:

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

- ...en volg de wizard

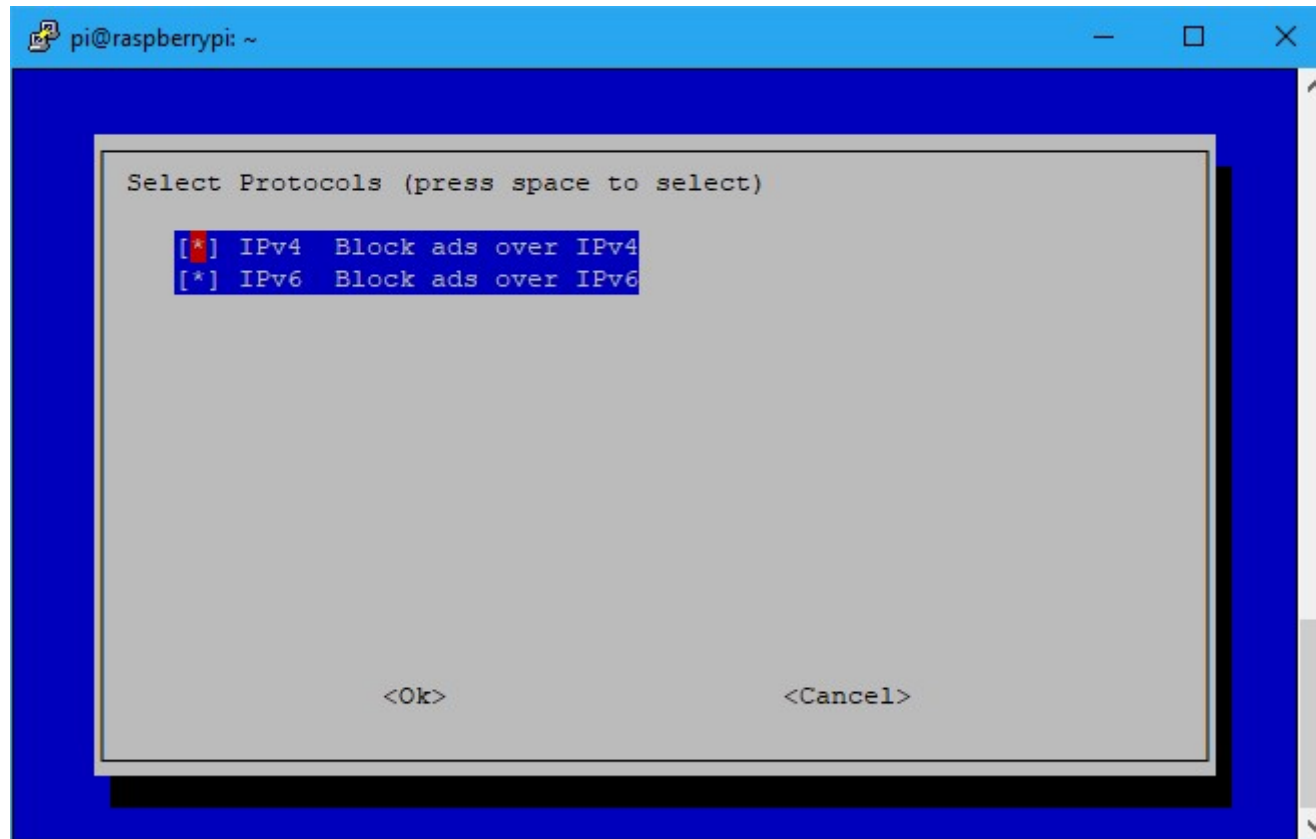
Kies eth0



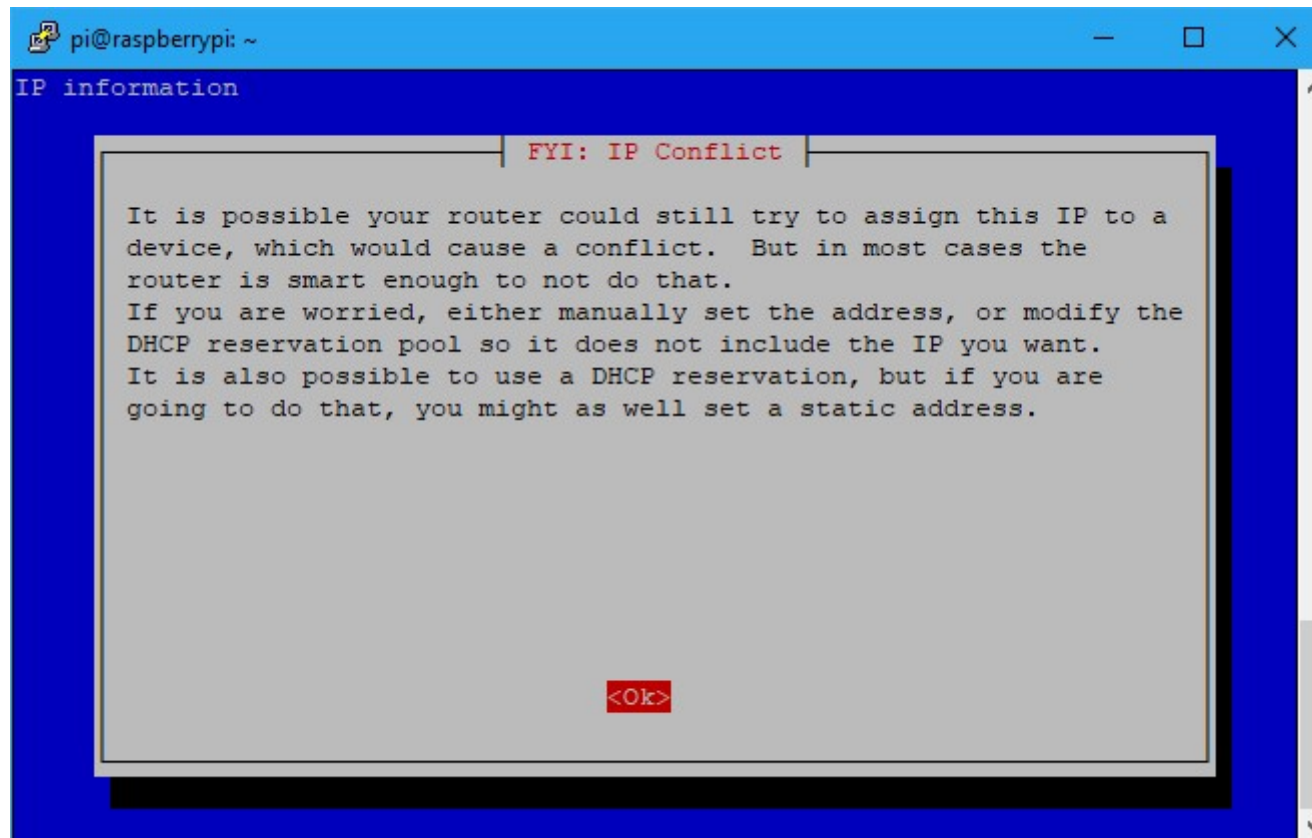
Laat alles aan

```
pi@raspberrypi: ~  
  
Pi-hole relies on third party lists in order to block ads.  
  
You can use the suggestions below, and/or add your own after  
installation  
  
To deselect any list, use the arrow keys and spacebar  
  
[*] StevenBlack  StevenBlack's Unified Hosts List  
[*] MalwareDom   MalwareDomains  
[*] Cameleon     Cameleon  
[*] ZeusTracker  ZeusTracker  
[*] DisconTrack  Disconnect.me Tracking  
[*] DisconAd     Disconnect.me Ads  
[*] HostsFile    Hosts-file.net Ads  
  
<Ok>                <Cancel>
```

Pi-hole installatie

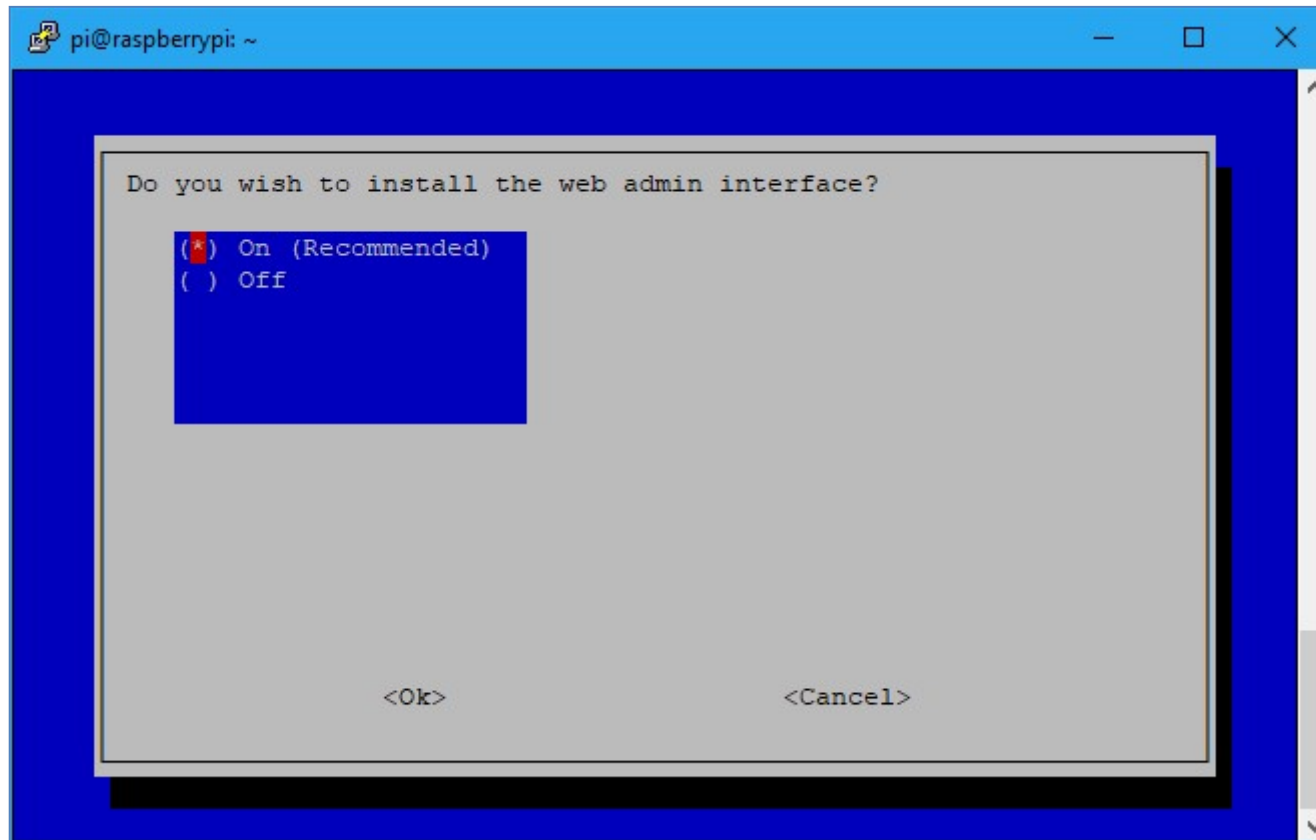


Pi-hole installatie

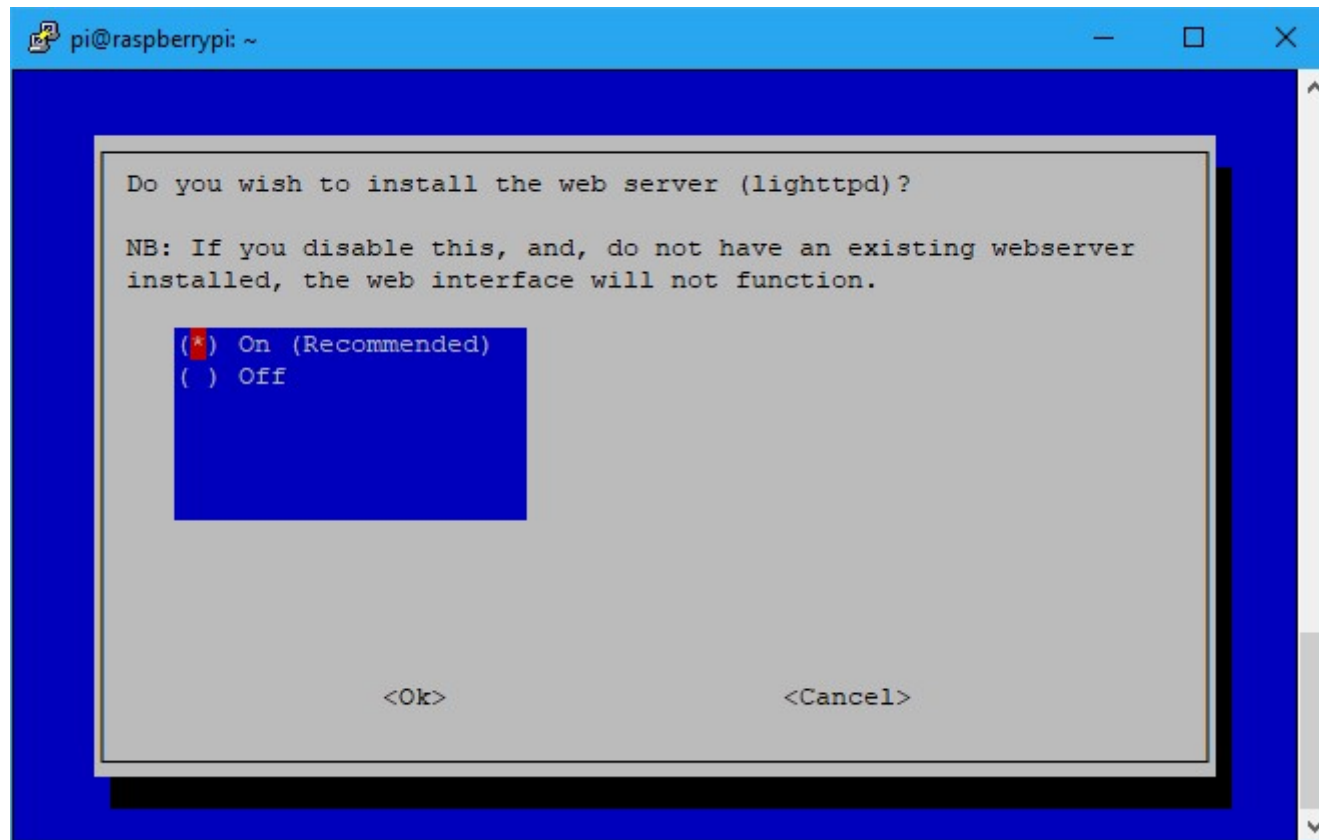


```
pi@raspberrypi: ~  
IP information  
FYI: IP Conflict  
It is possible your router could still try to assign this IP to a  
device, which would cause a conflict. But in most cases the  
router is smart enough to not do that.  
If you are worried, either manually set the address, or modify the  
DHCP reservation pool so it does not include the IP you want.  
It is also possible to use a DHCP reservation, but if you are  
going to do that, you might as well set a static address.  
<Ok>
```

Pi-hole installatie

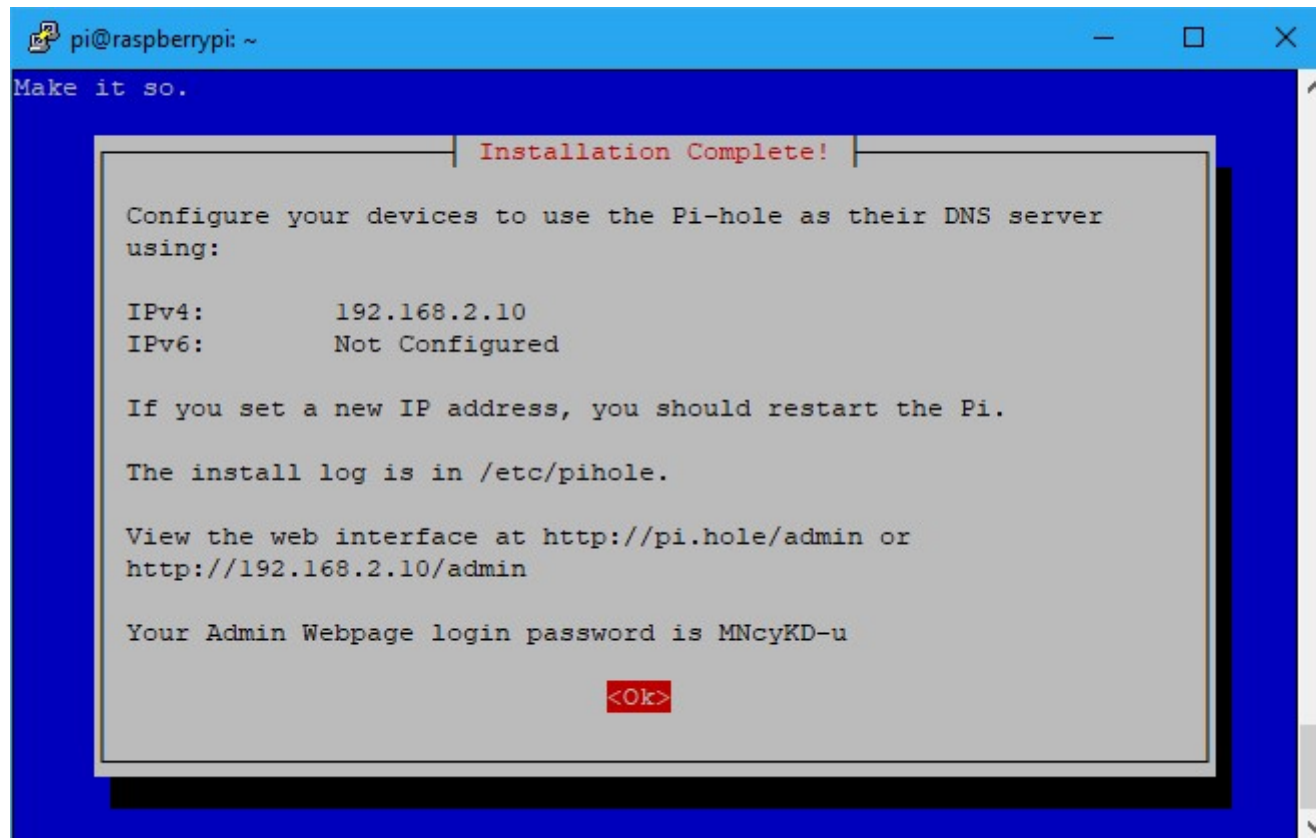


Let op!



Noteer het wachtwoord!

Wijzigen: `pihole -a -p`

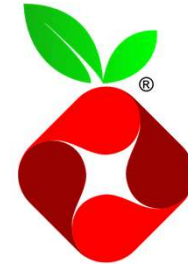


```
pi@raspberrypi: ~  
Make it so.  
Installation Complete!  
Configure your devices to use the Pi-hole as their DNS server  
using:  
IPv4:      192.168.2.10  
IPv6:      Not Configured  
If you set a new IP address, you should restart the Pi.  
The install log is in /etc/pihole.  
View the web interface at http://pi.hole/admin or  
http://192.168.2.10/admin  
Your Admin Webpage login password is MNcyKD-u  
<Ok>
```

Pi-hole opties

```
pi@raspberrypi: ~  
Installation Complete!  
pi@raspberrypi:~ $ sudo pihole  
Usage: pihole [options]  
Example: 'pihole -w -h'  
Add '-h' after specific commands for more information on usage  
  
Whitelist/Blacklist Options:  
-w, whitelist      Whitelist domain(s)  
-b, blacklist      Blacklist domain(s)  
--wild, wildcard   Wildcard blacklist domain(s)  
--regex, regex     Regex blacklist domains(s)  
                   Add '-h' for more info on whitelist/blacklist usage  
  
Debugging Options:  
-d, debug          Start a debugging session  
                   Add '-a' to enable automated debugging  
-f, flush          Flush the Pi-hole log  
-r, reconfigure    Reconfigure or Repair Pi-hole subsystems  
-t, tail           View the live output of the Pi-hole log  
  
Options:  
-a, admin          Web interface options  
                   Add '-h' for more info on Web Interface usage  
-c, chronometer    Calculates stats and displays to an LCD  
                   Add '-h' for more info on chronometer usage  
-g, updateGravity  Update the list of ad-serving domains  
-h, --help, help   Show this help dialog  
-l, logging        Specify whether the Pi-hole log should be used  
                   Add '-h' for more info on logging usage  
-q, query          Query the adlists for a specified domain  
                   Add '-h' for more info on query usage  
-up, updatePihole Update Pi-hole subsystems  
                   Add '--check-only' to exit script before update is performed.  
-v, version        Show installed versions of Pi-hole, Web Interface & FTL  
                   Add '-h' for more info on version usage  
uninstall          Uninstall Pi-hole from your system  
status            Display the running status of Pi-hole subsystems  
enable            Enable Pi-hole subsystems  
disable           Disable Pi-hole subsystems  
                   Add '-h' for more info on disable usage  
restartdns        Restart Pi-hole subsystems  
checkout          Switch Pi-hole subsystems to a different Github branch  
                   Add '-h' for more info on checkout usage  
pi@raspberrypi:~ $
```

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

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 2 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 254

Obtain DNS server address automatically

Use the following DNS server addresses:

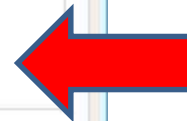
Preferred DNS server: 192 . 168 . 2 . 53

Alternative DNS server: | . . .

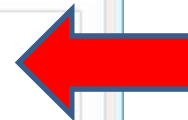
Validate settings upon exit

Advanced...

OK Cancel



IP adres Router



IP adres Raspberry Pi

Client - Proxy instellen

Connection Settings

Configure Proxy Access to the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy 192.168.2.53 Port 3128

Use this proxy server for all protocols

SSL Proxy 192.168.2.53 Port 3128

FTP Proxy 192.168.2.53 Port 3128

SOCKS Host 192.168.2.53 Port 3128

SOCKS v4 SOCKS v5

Automatic proxy configuration URL

192.168.2.0/24

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Enable DNS over HTTPS

Use provider Cloudflare (Default)

OK Cancel Help

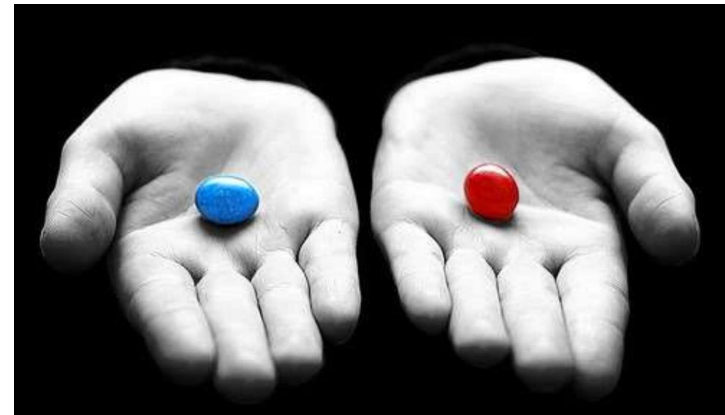
Geen Proxy voor LAN

DNS cache leegmaken

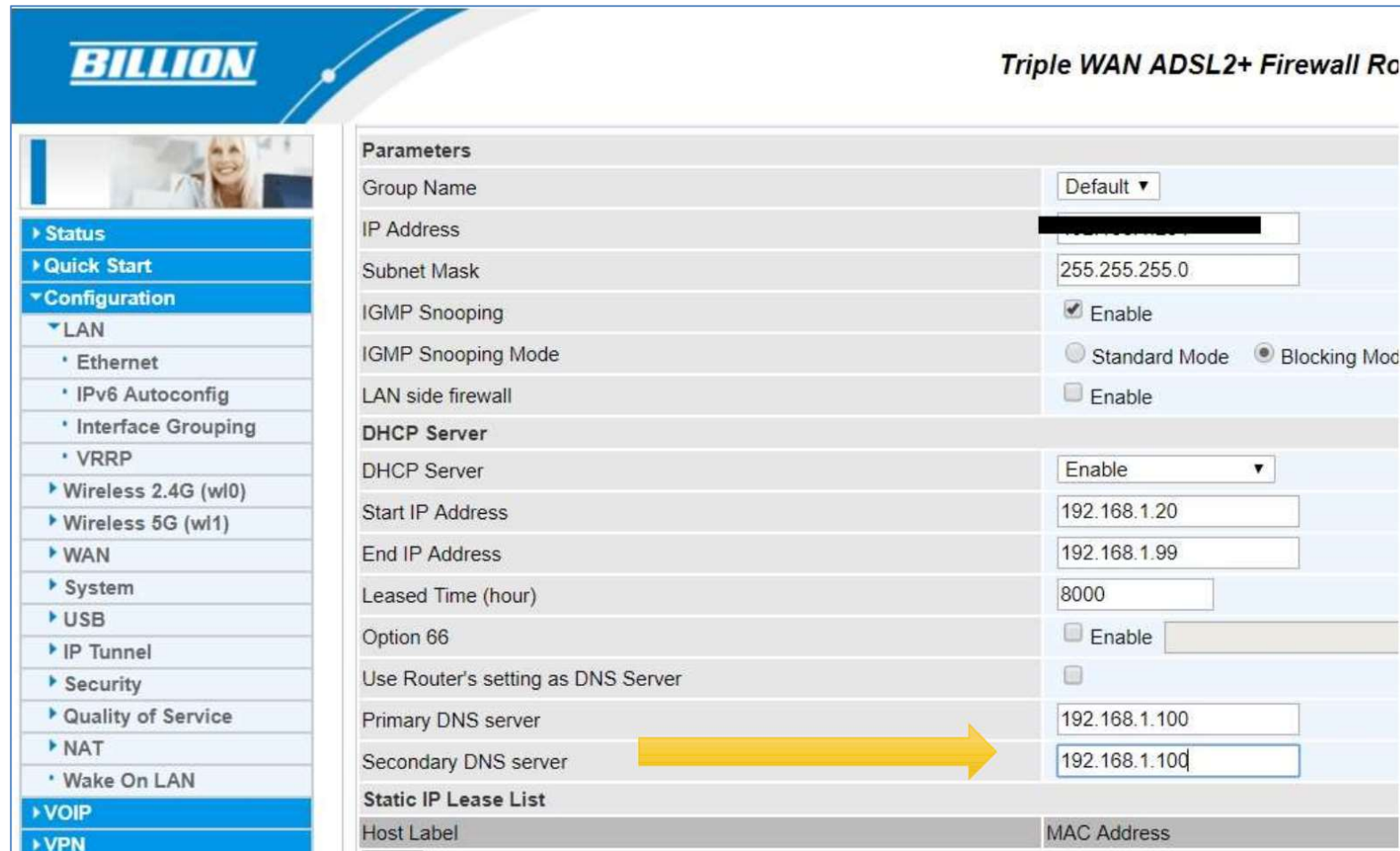
- Omdat het opvragen van websites in de DNS cache bewaard wordt, moet je de DNS cache leegmaken zodat de DNS gegevens ververs worden
 - Er wordt dan op de client een schone DNS opgebouwd (van Pi-hole i.p.v. van de router)
- **ipconfig /flushdns**

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



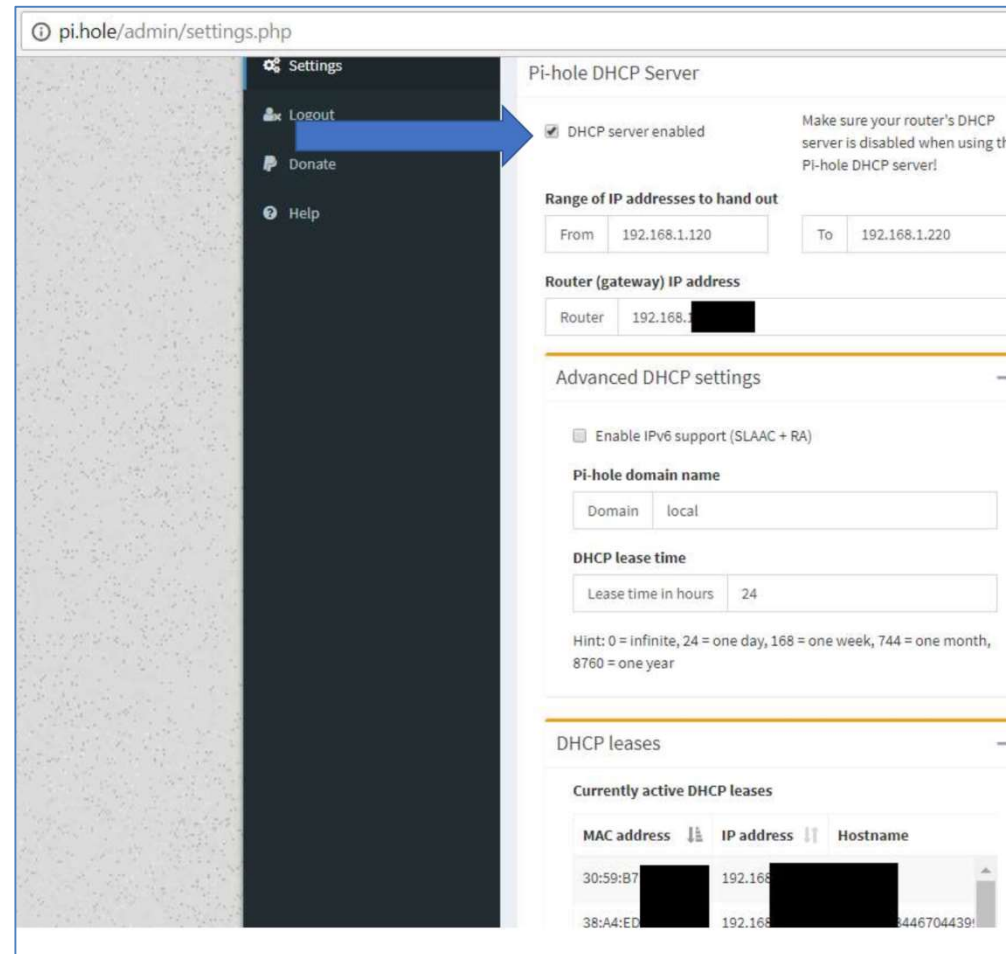
The screenshot shows the configuration interface for a Billion Triple WAN ADSL2+ Firewall Router. The left sidebar contains a navigation menu with options like Status, Quick Start, Configuration, LAN, WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN, VOIP, and VPN. The main content area is titled 'Triple WAN ADSL2+ Firewall Router' and displays the 'Parameters' section. Under 'DHCP Server', the 'Primary DNS server' is set to 192.168.1.100 and the 'Secondary DNS server' is set to 192.168.1.100. A yellow arrow points from the 'Secondary DNS server' field to the 'Primary DNS server' field. Other settings include Group Name (Default), IP Address (redacted), Subnet Mask (255.255.255.0), IGMP Snooping (Enabled), IGMP Snooping Mode (Blocking Mode), LAN side firewall (Disabled), DHCP Server (Enabled), Start IP Address (192.168.1.20), End IP Address (192.168.1.99), Leased Time (8000), Option 66 (Disabled), and Use Router's setting as DNS Server (Disabled).

Parameters	
Group Name	Default
IP Address	[Redacted]
Subnet Mask	255.255.255.0
IGMP Snooping	<input checked="" type="checkbox"/> Enable
IGMP Snooping Mode	<input type="radio"/> Standard Mode <input checked="" type="radio"/> Blocking Mode
LAN side firewall	<input type="checkbox"/> Enable
DHCP Server	
DHCP Server	Enable
Start IP Address	192.168.1.20
End IP Address	192.168.1.99
Leased Time (hour)	8000
Option 66	<input type="checkbox"/> Enable
Use Router's setting as DNS Server	<input type="checkbox"/>
Primary DNS server	192.168.1.100
Secondary DNS server	192.168.1.100
Static IP Lease List	
Host Label	MAC Address

Of...DHCP op router uitzetten...

The screenshot shows the configuration interface for a Billion Triple WAN ADSL2+ Firewall Router. The left sidebar contains a navigation menu with options like Status, Quick Start, Configuration, LAN, Ethernet, IPv6 Autoconfig, Interface Grouping, VRRP, Wireless 2.4G (w10), Wireless 5G (w11), WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN, VOIP, VPN, and Advanced Setup. The main content area is titled 'Configuration' and shows the 'LAN' settings. Under the 'DHCP Server' section, the 'DHCP Server' dropdown menu is set to 'Disable', which is highlighted by a blue arrow. Other settings include Group Name (Default), IP Address (192.168.1.1), Subnet Mask (255.255.255.0), IGMP Snooping (Enable), IGMP Snooping Mode (Blocking Mode), LAN side firewall (Disable), and IP Alias (Disable). The 'Apply' and 'Cancel' buttons are at the bottom of the configuration area.

...en DHCP aan op Pi-hole



The screenshot shows the Pi-hole admin interface at `pi.hole/admin/settings.php`. The left sidebar contains navigation links: Settings, Logout, Donate, and Help. A blue arrow points from the 'Settings' link to the 'Pi-hole DHCP Server' section. The main content area is titled 'Pi-hole DHCP Server' and includes the following settings:

- DHCP server enabled. Note: Make sure your router's DHCP server is disabled when using the Pi-hole DHCP server!
- Range of IP addresses to hand out**
 - From: 192.168.1.120
 - To: 192.168.1.220
- Router (gateway) IP address**
 - Router: 192.168.1.1
- Advanced DHCP settings**
 - Enable IPv6 support (SLAAC + RA)
 - Pi-hole domain name**
 - Domain: local
 - DHCP lease time**
 - Lease time in hours: 24
 - Hint: 0 = infinite, 24 = one day, 168 = one week, 744 = one month, 8760 = one year
- DHCP leases**
 - Currently active DHCP leases**

MAC address	IP address	Hostname
30:59:B7:...	192.168.1.120	
38:A4:ED:...	192.168.1.121	446704439...

Block lists instellen

The screenshot shows the Pi-hole Admin Console interface. The browser address bar indicates the URL is `pi.hole/admin/settings.php`. The left sidebar contains navigation options: Blacklist, Disable, Tools, Settings, Donate, and Help. The main content area is titled 'Blocklists' and is divided into three sections:

- Pi-hole hostname:** A text input field containing 'raspberrypi'.
- Pi-hole DHCP Server:** A section with a checkbox for 'DHCP server enabled' (checked). Below it, 'Range of IP addresses to hand out' is set from 'From 10.0.2.201' to 'To 10.0.2.251'. The 'Router (gateway) IP address' is set to '10.0.2.1'. There are expandable sections for 'Advanced DHCP settings' and 'DHCP leases'.
- Lists used to generate Pi-hole's Gravity:** A list of URLs with checkboxes and delete icons. The list includes:
 - <https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts>
 - <https://mirror1.malwaredomains.com/files/justdomains>
 - <http://sysctl.org/cameleon/hosts>
 - <https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist>
 - https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt
 - https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt
 - https://hosts-file.net/ad_servers.txt
 - https://s3.amazonaws.com/lists.disconnect.me/simple_malvertising.txt

A large yellow arrow points to the 'Save' button located at the bottom right of the settings area.

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 **pijljestoetsen**
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/squidguard`
- `ls`
- `sudo cp squidGuard.conf squidGuard.conf.org`
- `cd`
- `sudo squidGuard -C all`
 - Test of het compileren werkt voordat je squidGuard.conf aanpast

- `sudo chown -R proxy:proxy /var/lib/squidguard/db`
- `sudo chown -R proxy:proxy /var/log/squidguard`
- `sudo chown -R proxy:proxy /usr/bin/squidGuard`

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

```
pi@raspberrypi: ~  
pi@raspberrypi:~ $ sudo squidGuard -C  
squidGuard: option requires an argument -- 'C'  
Usage: squidGuard [-u] [-C block] [-t time] [-c file] [-v] [-d] [-P]  
Options:  
-v          : show version number  
-d          : all errors to stderr  
-b          : switch on the progress bar when updating the blacklists  
-c file     : load alternate configfile  
-t time     : specify startup time in the format: yyyy-mm-ddTHH:MM:SS  
-u          : update .db files from .diff files  
-C file|all : create new .db files from urls/domain files  
              specified in "file".  
-P          : do not go into emergency mode when an error with the  
              blacklists is encountered.  
pi@raspberrypi:~ $ █
```

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

```
GNU nano 2.7.4 File: squidGuard
)
dest local {
}

dest white {
    domainlist    BL/white/domains
    urllist       BL/white/urls
    redirect      http://192.168.2.53/blocked.html
}

#dest adult {
#    domainlist    BL/adult/domains
#    urllist       BL/adult/urls
#    expressionlist BL/adult/expressions
#    redirect      http://admin.foo.bar.de/cgi-bin/blocked.cgi?cli
#}

dest adv {
    domainlist    BL/adv/domains
    urllist       BL/adv/urls
    redirect      http://192.168.2.53/blocked.html
}

dest alcohol {
    domainlist    BL/alcohol/domains
    urllist       BL/alcohol/urls
    redirect      http://192.168.2.53/blocked.html
}
```

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.g`
`z`
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`

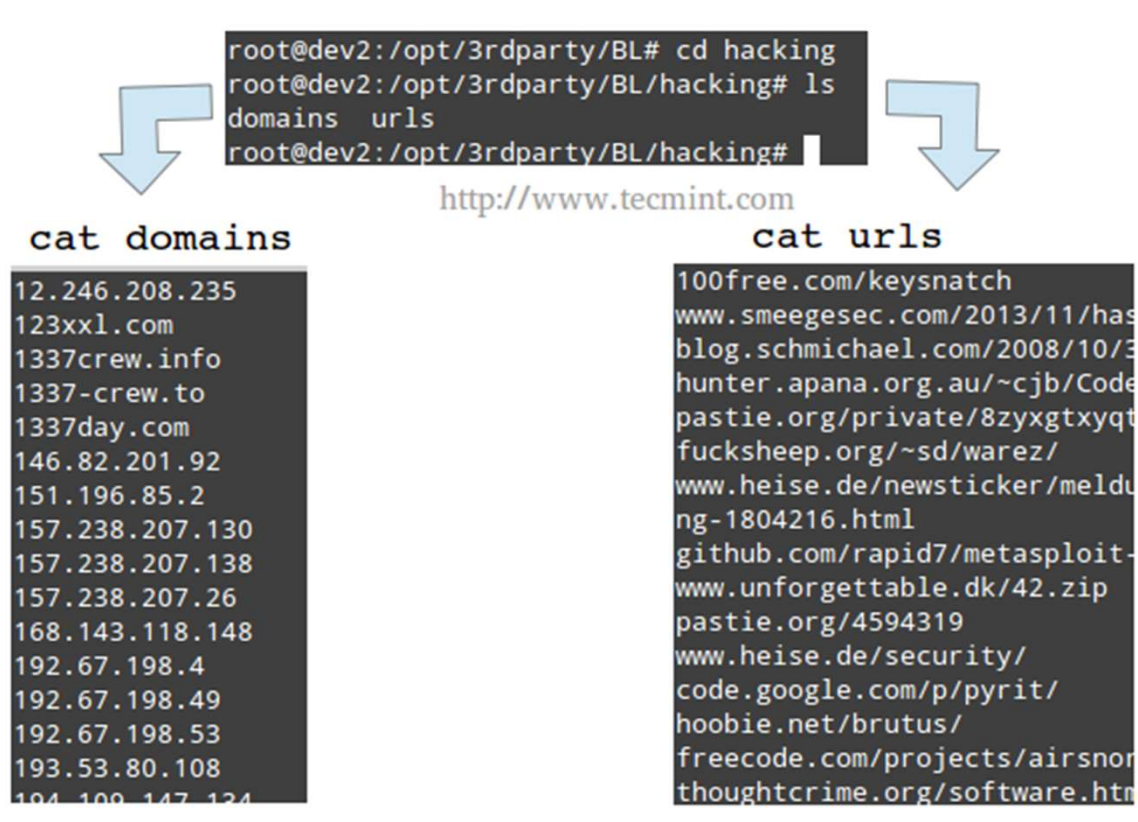
Shallalist installeren

- `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

```
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 $
```

Shallalist uitleg



```
root@dev2:/opt/3rdparty/BL# cd hacking
root@dev2:/opt/3rdparty/BL/hacking# ls
domains urls
root@dev2:/opt/3rdparty/BL/hacking#
```

<http://www.tecmint.com>

cat domains

```
12.246.208.235
123xxl.com
1337crew.info
1337-crew.to
1337day.com
146.82.201.92
151.196.85.2
157.238.207.130
157.238.207.138
157.238.207.26
168.143.118.148
192.67.198.4
192.67.198.49
192.67.198.53
193.53.80.108
194.109.147.124
```

cat urls

```
100free.com/keysnatch
www.smeegesec.com/2013/11/has
blog.schmichael.com/2008/10/3
hunter.apana.org.au/~cjb/Code
pastie.org/private/8zyxgtxyqt
fucksheep.org/~sd/warez/
www.heise.de/newsticker/meldu
ng-1804216.html
github.com/rapid7/metasploit-
www.unforgettable.dk/42.zip
pastie.org/4594319
www.heise.de/security/
code.google.com/p/pyrit/
hoobie.net/brutus/
freecode.com/projects/airsnor
thoughtcrime.org/software.htm
```

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

```
pi@PROXY: /etc/squidguard
GNU nano 2.7.4 File: squidGuard.conf
# domainlist BL/adult/domains
# urllist BL/adult/urls
# expressionlist BL/adult/expressions
# redirect http://admin.foo.bar.de/cgi-bin/blocked.cgi?clientaddr=%a&clie$
#}

dest adv {
    domainlist BL/adv/domains
    urllist BL/adv/urls
    redirect http://192.168.2.53/blocked.html
}

dest alcohol {
    domainlist BL/alcohol/domains
    urllist BL/alcohol/urls
    redirect http://192.168.2.53/blocked.html
}

dest dating {
    domainlist BL/dating/domains
}

^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
```

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

```
pi@PROXY: ~  
GNU nano 2.7.4 File: /var/lib/squidguard/db/BL/white/domains  
.live.com  
filehippo.com  
.apple.com  
wrox.com  
aliexpress.com  
marktplaats.nl  
mediamarkt.nl  
mediamarkt.pl  
mediamarkt.de  
banggood  
specsavers.nl  
bol.com  
fnac.be  
fnac.fr  
alternate.nl  
alternate.de  
amazon.com  
amazon.de  
.skype.com  
skype.net  
skype.org  
starstable.com  
.facebook.com  
.whatsapp.com  
.whatsapp.net  
twitter.com  
ninite.com  
abnamro.nl  
rabobank.nl  
asn.nl  
[ Wrote 40 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 Spell   ^_ Go To Line
```

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 websites.txt
# Websites te blokkeren
.nu.nl
.youtube.com
.starstable.com
.google.com
```

Geen internet op bepaalde tijd

```
pi@PROXY: /etc/squid
GNU nano 2.7.4 File: squid.conf
acl CONNECT method CONNECT

# Toegevoegd acl voor IPAD restrictietijden
acl ip-group1 src "/etc/squid/ipad.txt"

# In website1.txt zet je de domainnamen die niet bezocht mogen worden.
acl website1 dstdomain "/etc/squid/website1.txt"
acl weekeve time MTWHF 19:00-23:00 # Tussen deze tijden geen IPAD gebruiken
acl weekmrrn time MTWHF 06:00-08:30 # idem
+
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
^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
```

Geen internet op bepaalde tijd

```
pi@PROXY: /etc/squid
GNU nano 2.7.4 File: squid.conf
# one who can access services on "localhost" is a local user
http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow localnet

# Toegevoegd
# doordeweeks geen IPAD gebruiken gedurende bepaalde uren voor bepaalde websites
http_access allow ip-group1 websites1 !weekeve !weekmrn

# Toegevoegd
# Deny the CONNECT method to prevent outside people from trying to connect to t$
http_access deny CONNECT

#
# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

^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
```

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

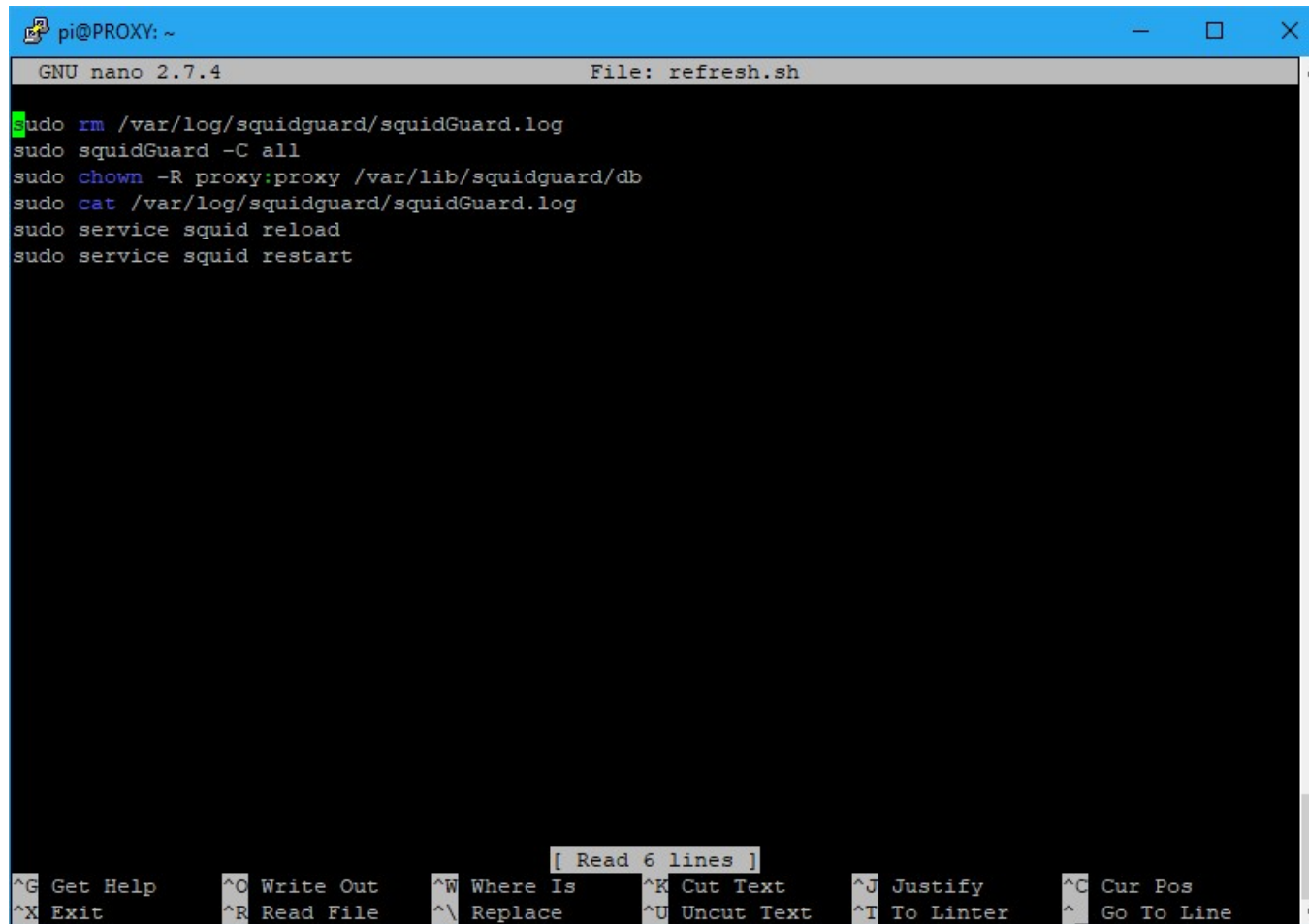
Eigen scripts voor snel beheer

edit_white.sh

```
pi@PROXY: ~
GNU nano 2.7.4 File: edit white.sh
sudo nano /var/lib/squidguard/db/BL/white/domains

[ File 'edit white.sh' is unwritable ]
^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
```

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
```

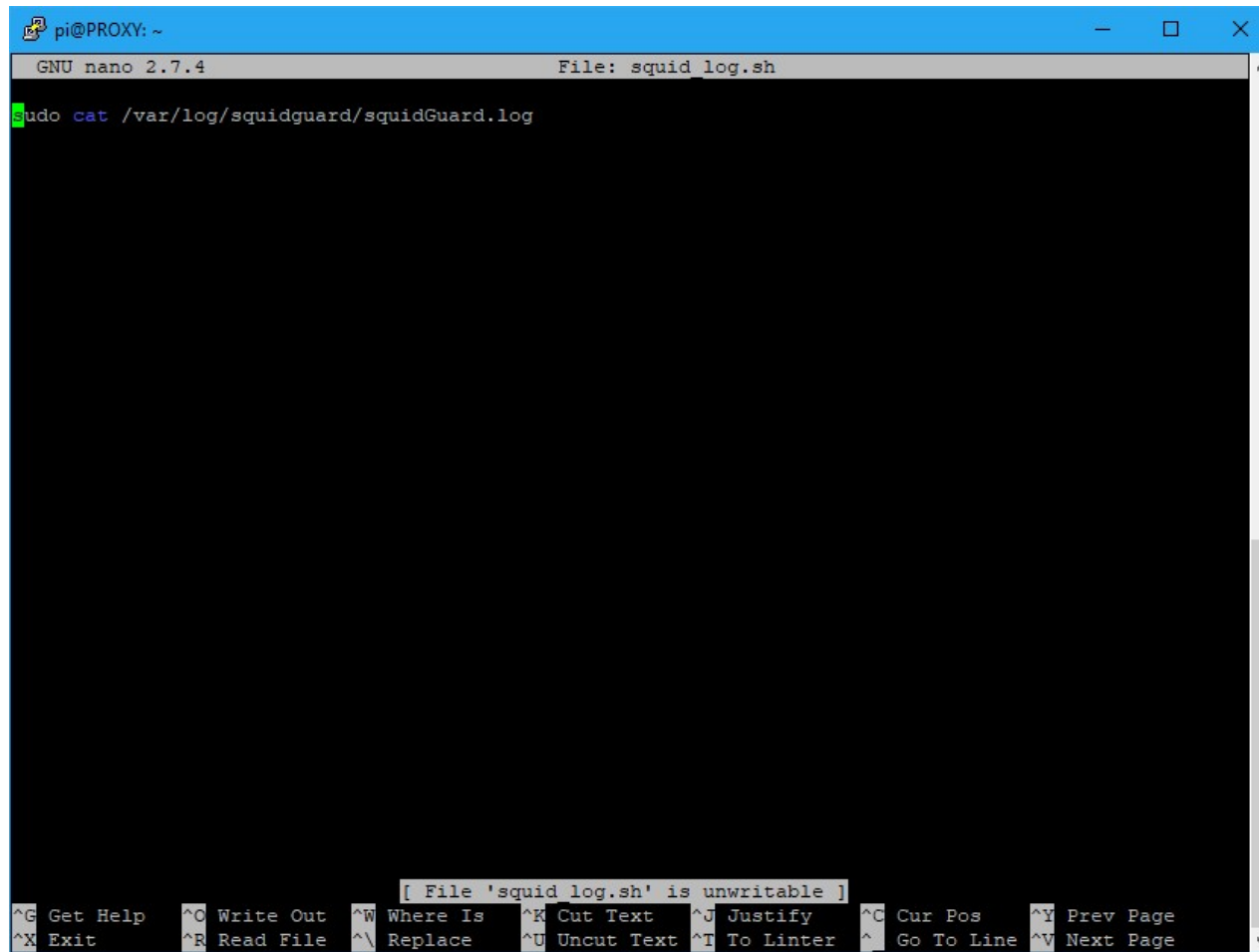
update_shallalist.sh

```
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 "Backupping 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



The image shows a terminal window titled "pi@PROXY: ~" with a blue header bar. The window contains the GNU nano 2.7.4 editor editing a file named "squid_log.sh". The command "sudo cat /var/log/squidguard/squidGuard.log" is entered at the prompt. A message "[File 'squid_log.sh' is unwritable]" is displayed in a light grey box. The bottom of the window shows the nano editor's help menu with various keyboard shortcuts.

```
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  ^G 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

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
aaaaaaaaaaaaaaaa Increase screen height to see graphical statistics aaaaaaaaaaaaaaaaaa
Press d to enable detailed statistics
Press i to enable additional information
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/why-you-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?

