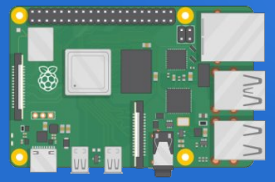
Using Raspberry Pi as a home/office server

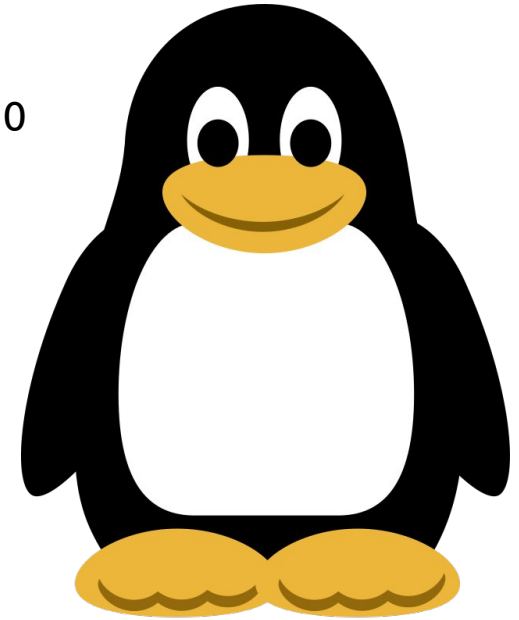
Michalis Zisis, GreekLUG

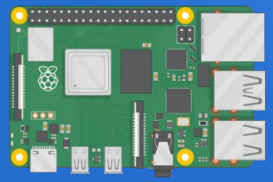


Using Raspberry Pi as a home/office server

whoami

- Member of the FOSS Community in Greece since around 2010
- Board Member of GreekLUG

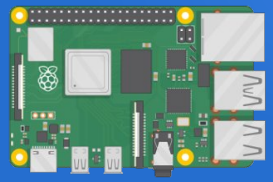




Using Raspberry Pi as a home/office server

The problem

- Security and Privacy
- Access our private network



Using Raspberry Pi as a home/office server

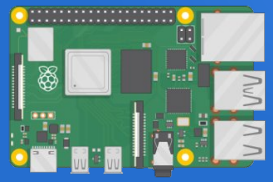
The solution

- VPN service

  allows us to remotely access our private network in a safe way

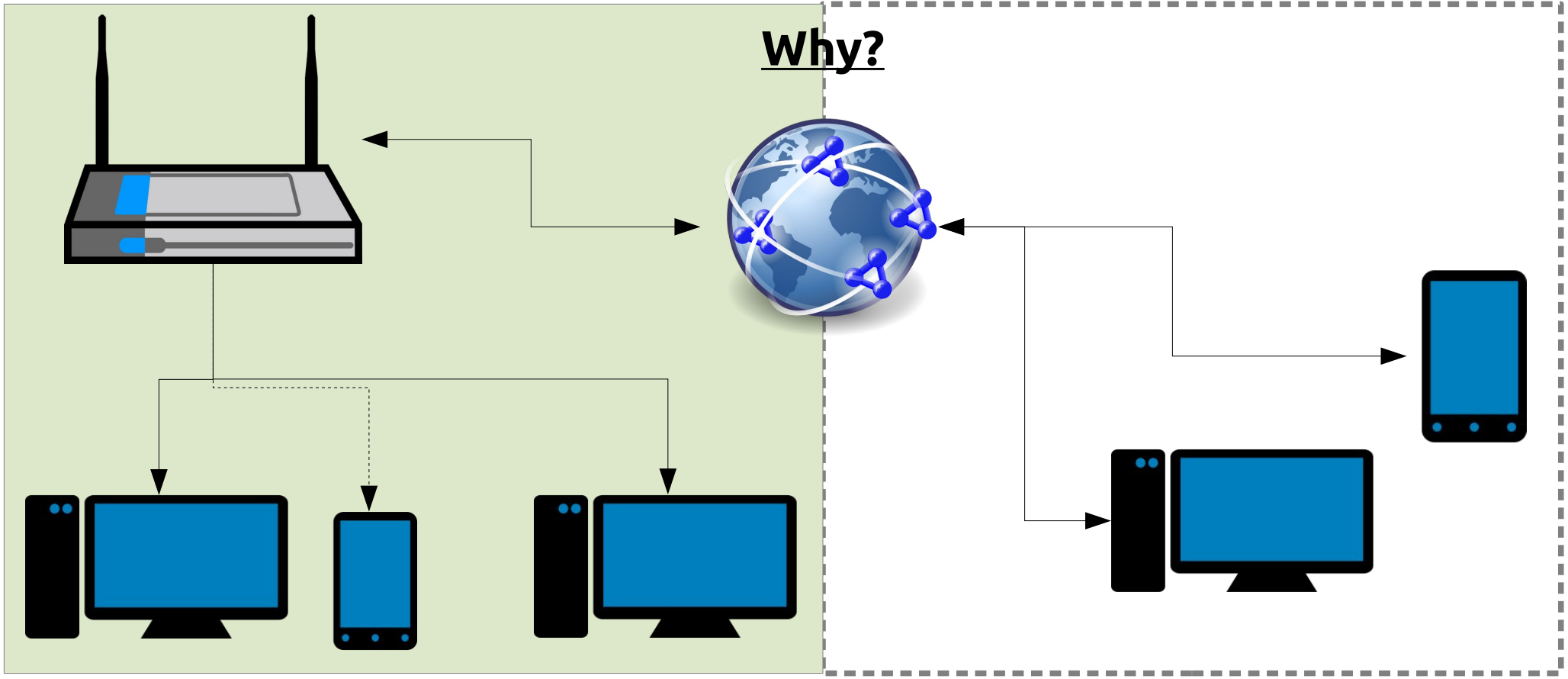
- Pi-Hole service

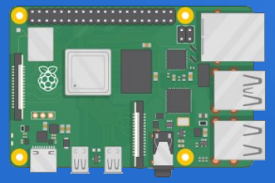
  allows us to filter unwanted content



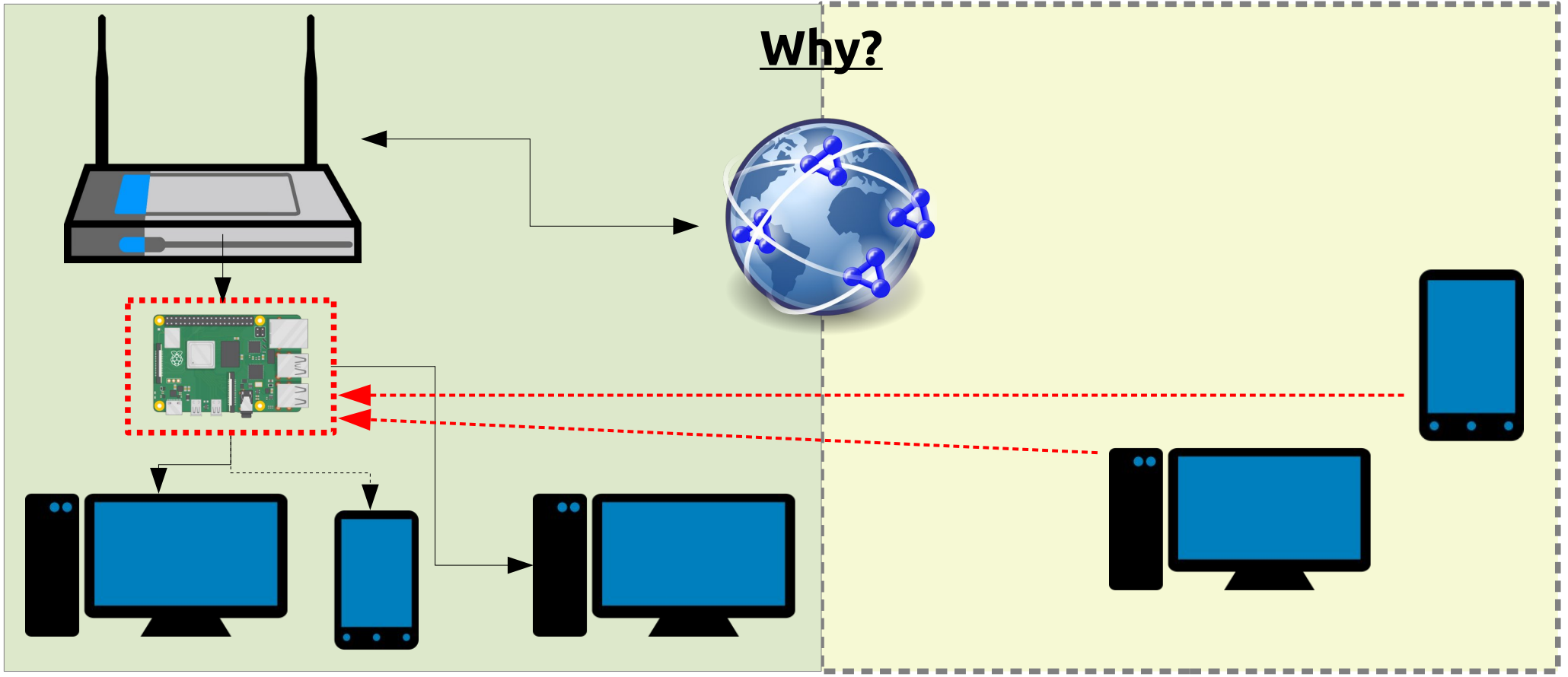
Using Raspberry Pi as a home/office server

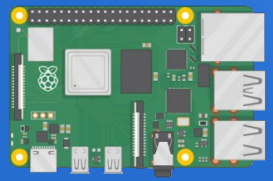
Why?





Using Raspberry Pi as a home/office server

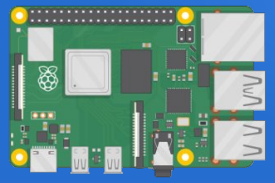




Using Raspberry Pi as a home/office server

Why?

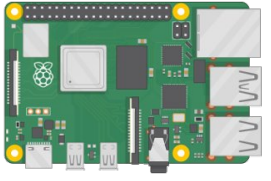
- Cost-effective
- Low energy footprint
- Easy to maintain
- Expandable

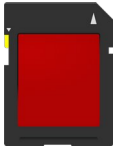


Using Raspberry Pi as a home/office server

What is Raspberry Pi

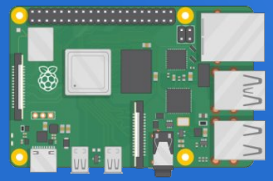
- The Raspberry Pi is a series of credit card-sized computers developed in the UK by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries.
  The original model became much more popular than expected, with uses such as robotics.





- https://www.raspberrypi.org/

https://en.wikipedia.org/wiki/Raspberry_Pi



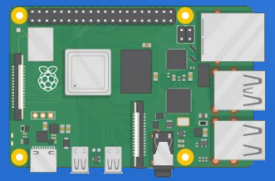
Using Raspberry Pi as a home/office server

What is OpenVPN

- OpenVPN is a virtual private network (VPN) system
  that implements techniques to create secure
  point-to-point or site-to-site connections
  in routed or bridged configurations and remote access facilities.
  It implements both client and server applications.

- License: GNU GPLv2
- https://openvpn.net/

https://en.wikipedia.org/wiki/OpenVPN



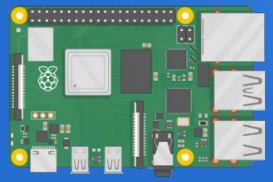
Using Raspberry Pi as a home/office server

What is Pi-Hole

- Pi-hole is a Linux network-level advertisement and Internet tracker blocking application which acts as a DNS sinkhole and optionally a DHCP server, intended for use on a private network.

- License: European Union Public Licence
- https://pi-hole.net/

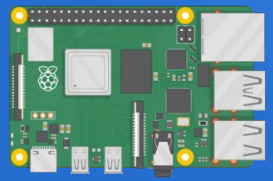
https://en.wikipedia.org/wiki/Pi-hole



Using Raspberry Pi as a home/office server

How

1) Install an OS, eg Raspberry Pi OS (formerly Raspbian)
2) Set a hostname and network settings to use a static local IP, eg 192.168.1.5
3) Install OpenVPN & Pi-Hole
4) Configure OpenVPN and Pi-Hole, in dual operation at the same time, LAN & WAN filtering via the VPN
5) Set the local router to provide the Pi-Hole DNS to local devices-clients
6) Port forward the needed port for OpenVPN
7) Configure Firewall



Using Raspberry Pi as a home/office server

Step1

1) Install with Raspberry Pi Imager

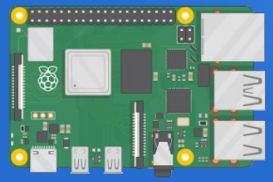
   or

2) Download Raspberry Pi OS (https://www.raspberrypi.org/software/operating-systems/) and write image to sd card, eg

```
unzip -p 2020-12-02-raspios-buster-armhf.zip | sudo dd of=/dev/sdX bs=4M conv=fsync
```

After 1st boot…

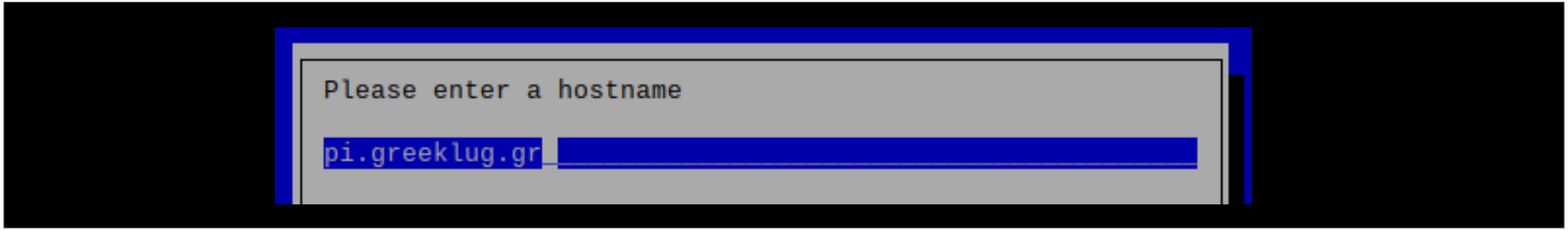
Enable SSH (and VNC) from Menu → Preferences → Raspberry Pi Configuration | Interfaces



Using Raspberry Pi as a home/office server

Step2

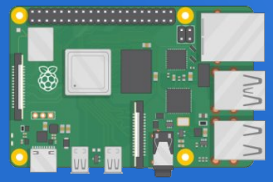
1) Set a hostname with raspi-config → 1 System Options → S4 Hostname



2) Set a static local IP, eg 192.168.1.5 (router IP 192.168.1.1) → edit /etc/dhcpcd.conf

```
interface eth0
static ip_address=192.168.1.5/24
static routers=192.168.1.1
static domain_name_servers=192.168.1.1 8.8.8.8
```

* Reboot needed!



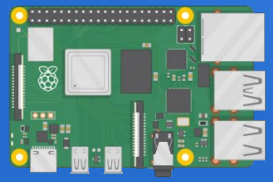
Using Raspberry Pi as a home/office server

Step3

1) Install OpenVPN

```
wget https://git.io/vpn -O openvpn-install.sh
chmod 755 openvpn-install.sh
./openvpn-install.sh
```

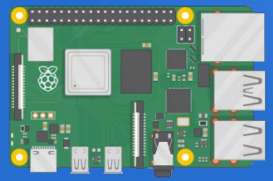
```
Welcome to this OpenVPN road warrior installer!

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [<External IP>]:

Which protocol should OpenVPN use?
  1) UDP (recommended)
  2) TCP
Protocol [1]:
```



Using Raspberry Pi as a home/office server

Step3

```
What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
   1) Current system resolvers
   2) Google
   3) 1.1.1.1
   4) OpenDNS
   5) Quad9
   6) AdGuard
DNS server [1]:

Enter a name for the first client:
Name [client]: myremotepc
OpenVPN installation is ready to begin.
```



Using Raspberry Pi as a home/office server

Step3

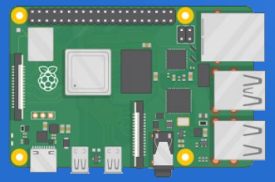
Important paths:

OpenVPN: /etc/openvpn/server/…

PKI dir: /etc/openvpn/server/easy-rsa/pki

CRL file: /etc/openvpn/server/easy-rsa/pki/crl.pem

The 1st vpn client configuration is available in: /root/myremotepc.ovpn



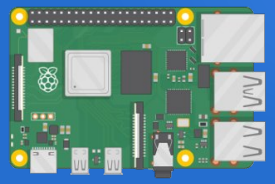
Using Raspberry Pi as a home/office server

Step3

2) Install Pi-Hole

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

```
[✓] Root user check

      .;;,.
      .ccccc:,.
       :cccclll:.      ..,,
        :ccccclll.   ;ooodc
         'ccll:;ll .oooodc
           .;cll.;;looo:.
               .. ','.
                .',,,,,,'.
              .',,,,,,,,,,.
            .',,,,,,,,,,,,....
          ....''',,,,,,,'.......
        ........  ....  .........
        ..........      ..........
        ..........      ..........
        ........  ....  .........
          ......,,,,,,,'......
            ....',,,,,,,,,,,,.
               .',,,,,,,,,'.
                .',,,,,'.
                  ..'''.

[i] Update local cache of available packages...
```



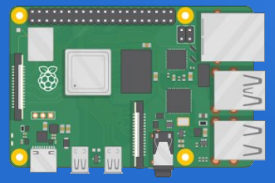
Using Raspberry Pi as a home/office server

Step3

```
Choose An Interface (press space to toggle selection)

    ( ) eth0   available
    ( ) wlan0  available
    (*) tun0   available
```

```
Select Upstream DNS Provider. To use your own, select Custom.

                    Google (ECS)                ↑
                    OpenDNS (ECS, DNSSEC)       ▮
```

```
                    Static IP Address

Do you want to use your current network settings as a static
address?
          IP address:    192.168.1.5/24
          Gateway:       192.168.1.1
```



Using Raspberry Pi as a home/office server

Step3

Installation Complete!

Configure your devices to use the Pi-hole as their DNS server using:

IPv4: 192.168.1.5
IPv6: fddd:1194:1194:1194::1

If you set a new IP address, you should restart the Pi.

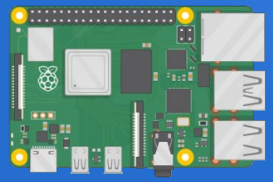
The install log is in /etc/pihole.

View the web interface at http://pi.hole/admin or http://192.168.1.5/admin

Your Admin Webpage login password is 3rFsWTJc

<Εντάξει>

* Reboot needed!



Using Raspberry Pi as a home/office server

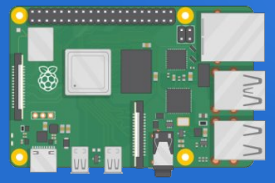
Step4

Configure OpenVPN and Pi-Hole, in dual operation at the same time, LAN & WAN filtering via the VPN

1) Configure OpenVPN → edit /etc/openvpn/server/server.conf

```
push "route 192.168.1.0 255.255.255.0"
push "dhcp-option DNS 192.168.1.5"
#push "dhcp-option DNS 192.168.1.1"
#push "dhcp-option DNS 8.8.8.8"
```

```
systemctl restart openvpn-server@server.service
```



Using Raspberry Pi as a home/office server

Step4

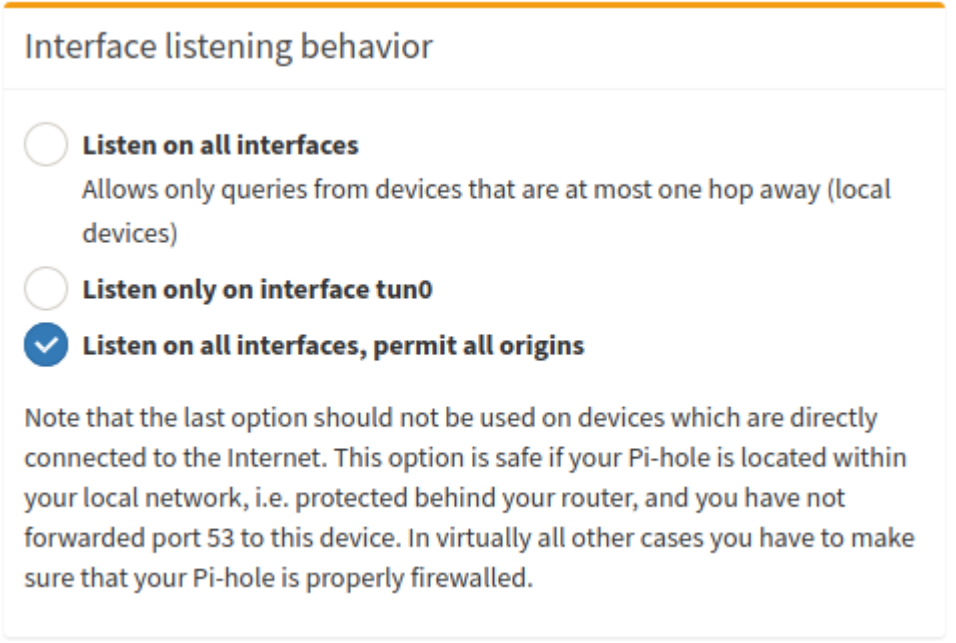
Configure OpenVPN and Pi-Hole, in dual operation at the same time, LAN & WAN filtering via the VPN

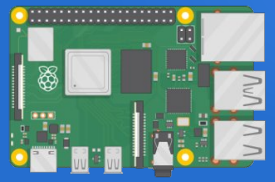
2) Configure Pi-Hole

```
pihole -a -i all
```

or

Go to admin web page http://192.168.1.5/admin/ then Settings → DNS tab





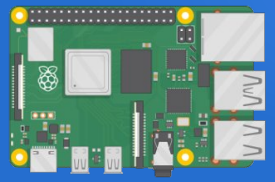
Using Raspberry Pi as a home/office server

Step5

▼ DHCP Server

DHCP Server	(•) On ( ) Off
LAN IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
DHCP Start IP Address	192 . 168 . 1 . 100
DHCP End IP Address	192 . 168 . 1 . 254
ISP DNS	( ) On (•) Off
Primary DNS	192 . 168 . 1 . 1
Secondary DNS	8 . 8 . 8 . 8
Lease Time Mode	Custom
Custom Lease Time	1814400 s

Apply Cancel



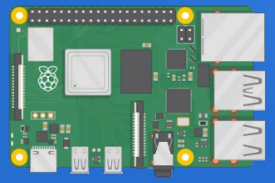
Using Raspberry Pi as a home/office server

Step5

▼ DHCP Server

DHCP Server	(•) On ( ) Off
LAN IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
DHCP Start IP Address	192 . 168 . 1 . 100
DHCP End IP Address	192 . 168 . 1 . 254
ISP DNS	( ) On (•) Off
Primary DNS	192 . 168 . 1 . 1
Secondary DNS	8 . 8 . 8 . 8
Lease Time Mode	Custom
Custom Lease Time	1814400 s

Apply Cancel



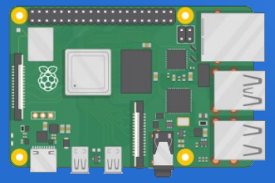
Using Raspberry Pi as a home/office server

Step5

▼ DHCP Server

DHCP Server	(•) On ( ) Off
LAN IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
DHCP Start IP Address	192 . 168 . 1 . 100
DHCP End IP Address	192 . 168 . 1 . 254
ISP DNS	( ) On (•) Off
Primary DNS	192 . 168 . 1 . 5
Secondary DNS	192 . 168 . 1 . 5
Lease Time Mode	Custom
Custom Lease Time	1814400 s

Apply Cancel



Using Raspberry Pi as a home/office server

Step6

- Status
- WAN
- Uplink Mode
- QoS
- Security
- Parental Control
- DDNS
- SNTP
- Port Binding
- Dynamic Routing
- Multicast

Firewall | Filter Criteria | Local Service Control | ALG | DMZ | Port Forward

Page Information

This page provides the function of port forwarding parameter(s) configuration.

Port Forwarding

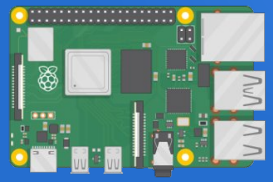
What should be noticed when configuring port forwarding?

pi-openvpn — On / Off

Name	pi-openvpn
Protocol	UDP
WAN Connection	PTM_DSL
WAN Host IP Range	0.0.0.0 ~ 0.0.0.0
MAC Mapping	On / Off
LAN Host IP Address	192.168.1.5
WAN Port Range	1194 ~ 1194
LAN Host Port Range	1194 ~ 1194

Apply | Cancel

Create New Item



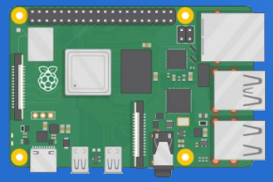
Using Raspberry Pi as a home/office server

Step7

Ports/IPTables

1) Accept SSH TCP 22 (and VNC TCP 5900), to access the SSH Service (or VNC)
2) Accept HTTP TCP 80 (or/and HTTPS TCP 443), to access Pi-Hole Web Interface
3) Accept VPN UDP or TCP 1194, to access VPN from remote devices (provided by vpn service)
4) Accept localhost traffic (loopback)
5) Accept traffic from the VPN nic, **tun0**
6) Change default policy of Chain INPUT to **DROP**

*** Don't forget about IPv6!**



Using Raspberry Pi as a home/office server

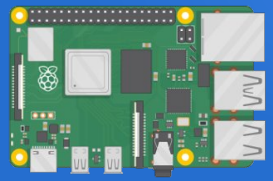
Step7

Ports/IPTables

Interfaces:

1) eth0 LAN interface
2) tun0 VPN/WAN interface

```
iptables -A INPUT -p tcp --destination-port 22 -j ACCEPT
iptables -A INPUT -p tcp --destination-port 80 -j ACCEPT
iptables -A INPUT -p tcp --destination-port 5900 -j ACCEPT        * if VNC is enabled
iptables -I INPUT -i tun0 -j ACCEPT
iptables -I INPUT -i lo -j ACCEPT
iptables -P INPUT DROP
```



Using Raspberry Pi as a home/office server

Step7

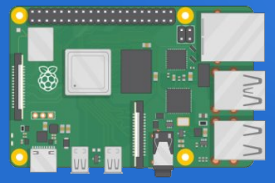
Ports/IPTables

OpenVPN iptables service → must be enabled

`systemctl status openvpn-iptables.service`

Provides:

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to <external_IP>

iptables -I INPUT -p udp --dport 1194 -j ACCEPT

iptables -I FORWARD -s 10.8.0.0/24 -j ACCEPT

iptables -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

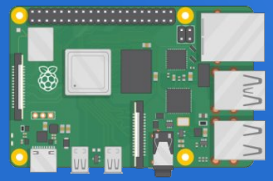


Using Raspberry Pi as a home/office server

Step7

iptables -L -n -v

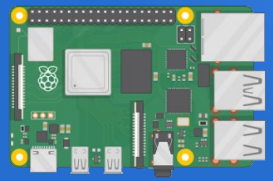
```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   96  5736 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  tun0   *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194
  136 14109 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   41  5900 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
  120 10394 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5900

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  *      *       10.8.0.0/24          0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```



Using Raspberry Pi as a home/office server

Ready!

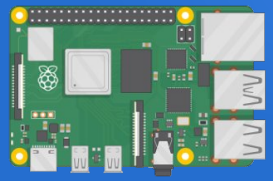
1) Copy the vpn configuration file from /root/myremotepc.ovpn to your remote pc
2) Run the script `./openvpn-install.sh` to create new configurations for other devices, eg your mobile phone
3) Use Pi-Hole web Admin panel to set up your filters
4) Use your installation!



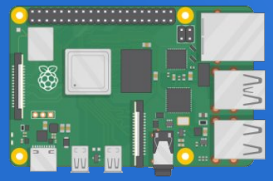
Using Raspberry Pi as a home/office server

Extra

1) Dynamic DNS, use a hostname to resolve
2) Use Pi-Hole DHCP capability, disable it from your router
3) Set up a Raspberry Pi as a routed wireless access point, disable it from your router



Thank you!



Greek Association of Free Software / Open Source Users | GreekLUG

https://www.greeklug.gr/