SECURE PORTABLE ROUTE

Presented by :
Sai Nassim

CONTEXT AND PROBLEM

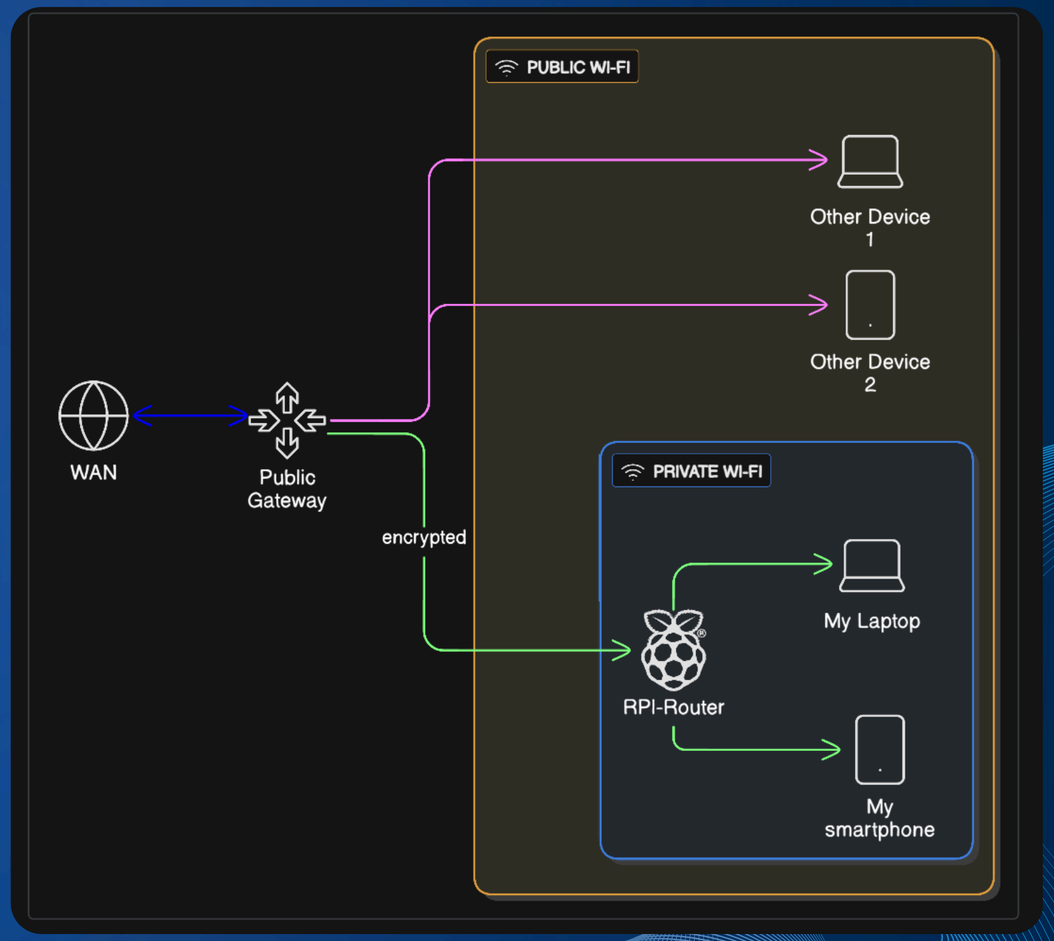
- Public Wi-Fi in cafés & restaurants is not secure by default
- Attackers can spy, steal data, or inject malicious traffic
- Techniques like packet sniffing, fake hotspots, and Man-in-the-Middle attacks make it easy
- Goal: understand the technique used & protect users and increase privacy on any public network

PROJECT OBJECTIVES

- Provide a portable security gateway using Raspberry Pi
- Runs OpenWRT firewall to control and monitor network traffic
- Secure connections with an encrypted VPN tunnel
- Block ads, trackers and malicious domains with Pi-hole
- Make it easy to use on any public Wi-Fi (cafés, restaurants, etc.)

PROJECT OVERVIEW & ARCHITECTURE

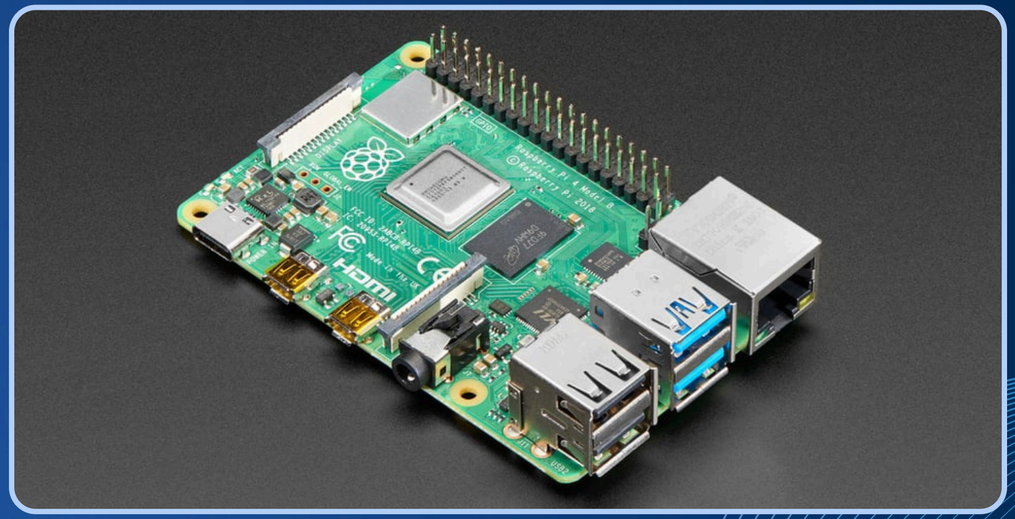
- Raspberry Pi acts as a secure router
- Connects to public Wi-Fi as WAN interface
- Creates a private, secure Wi-Fi hotspot for users (LAN)



HARDWARE & SOFTWARE COMPONENTS

Hardware:

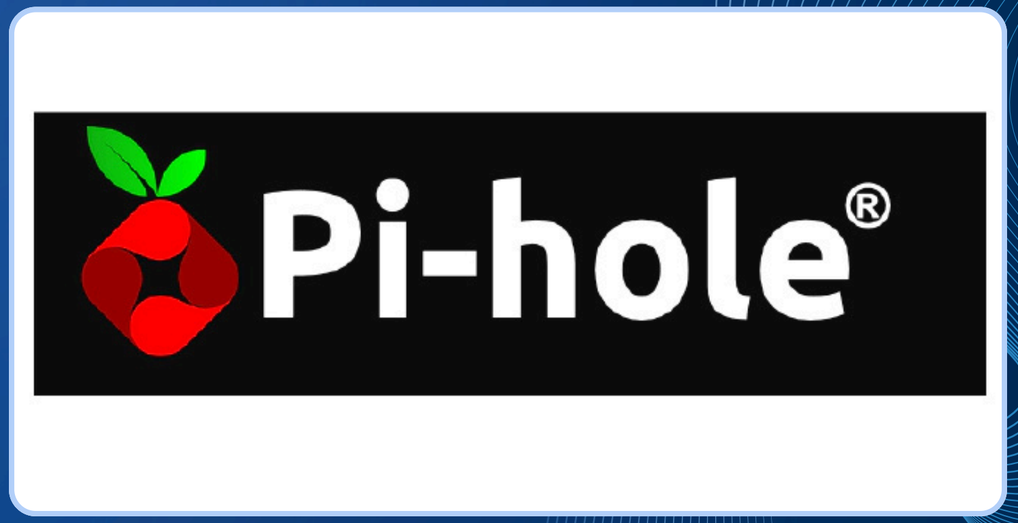
- Raspberry Pi 4 (main security gateway)
- microSD card (OpenWrt system & configs)
- Power supply / power bank (for portability)
- USB Wi-Fi adapter or Ethernet connection to public network



HARDWARE & SOFTWARE COMPONENTS

Software:

- OpenWrt (router OS & firewall)
- VPN client (OpenVPN)
- Pi-hole (DNS filtering & ad blocking)
- Cowrie (SSH & Telnet honeypot)



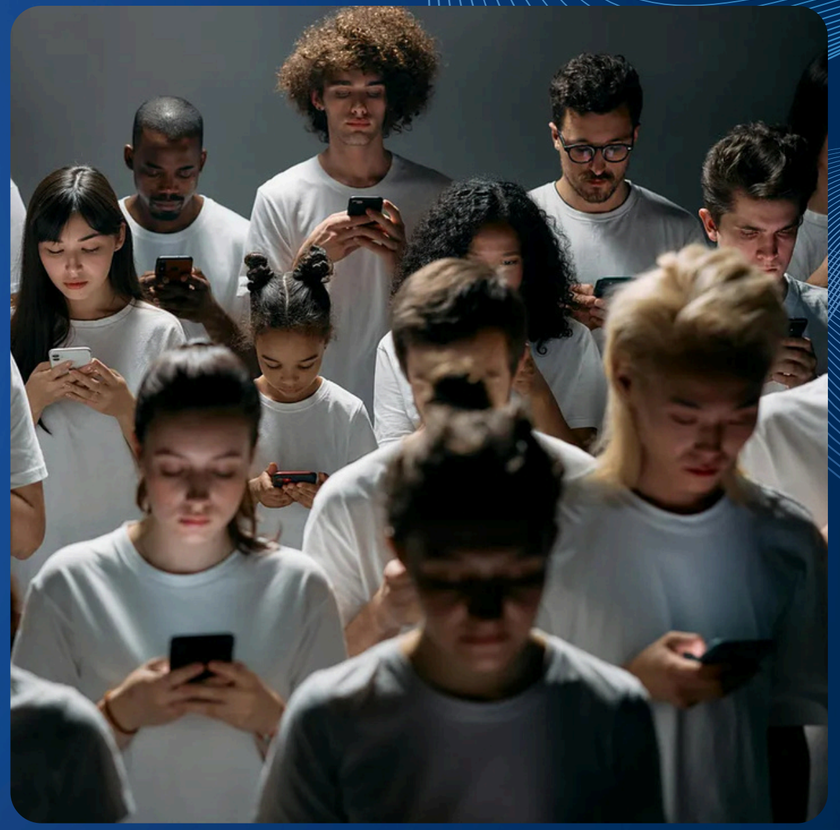
BENEFITS FOR USERS & REAL-WORLD APPLICATIONS

Benefits for Users:

- Encrypted traffic on any public Wi-Fi
- Protection against sniffing ,spoofing & MITM attacks
- Less tracking & ads thanks to Pi-hole
- Improved anonymity with VPN
- Easy to use: just connect to the Pi Wi-Fi

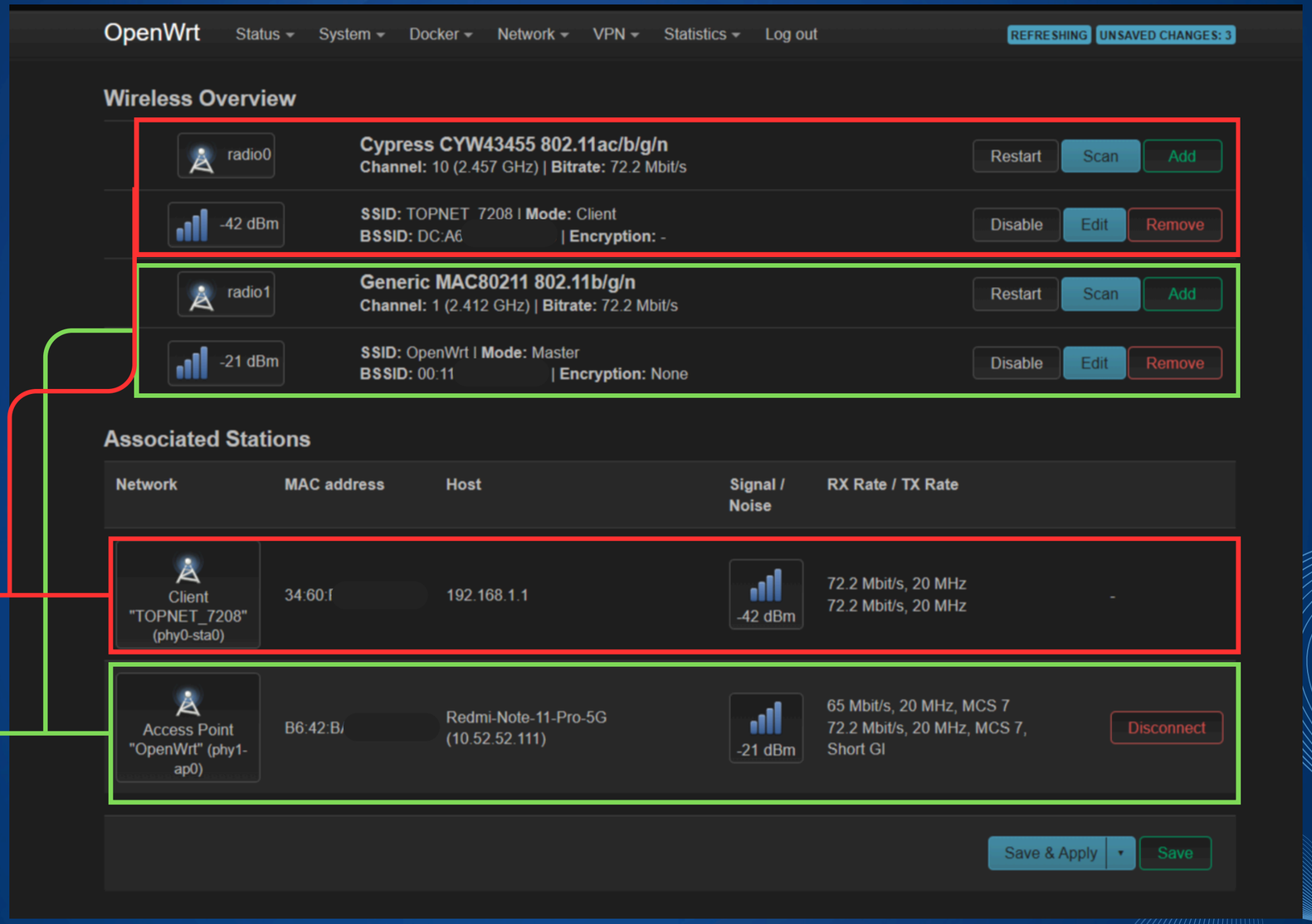
Real-World Applications:

- Using Wi-Fi in cafés, restaurants, airports, hotels
- Protecting students on university or shared networks
- Safe remote work for employees & freelancers
- Temporary secure network for events or trainings
- Portable security kit for cybersecurity demonstrations



DEMO

Wireless Interfaces

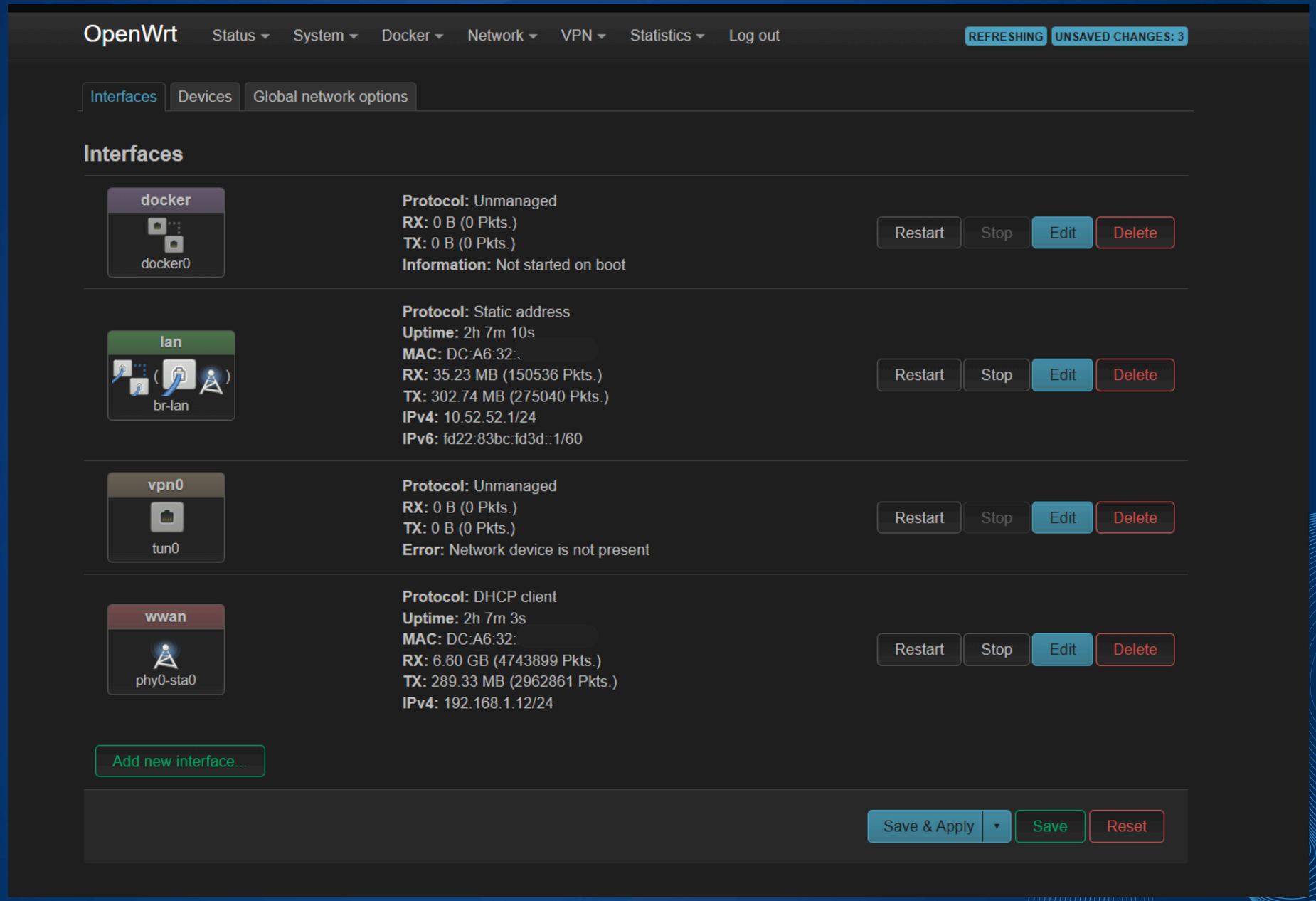


Public

Local

DEMO

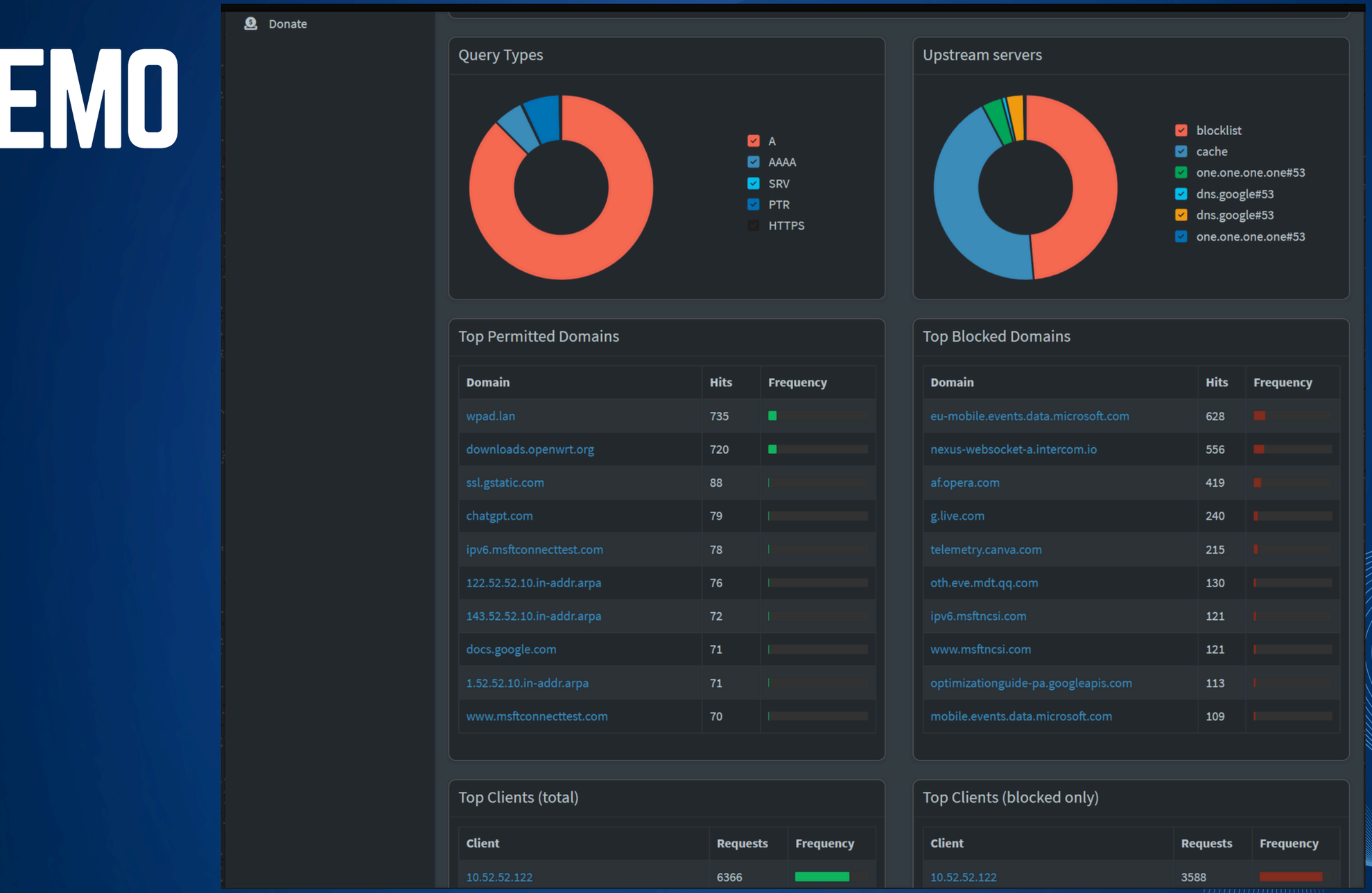
Network Interfaces



DEMO

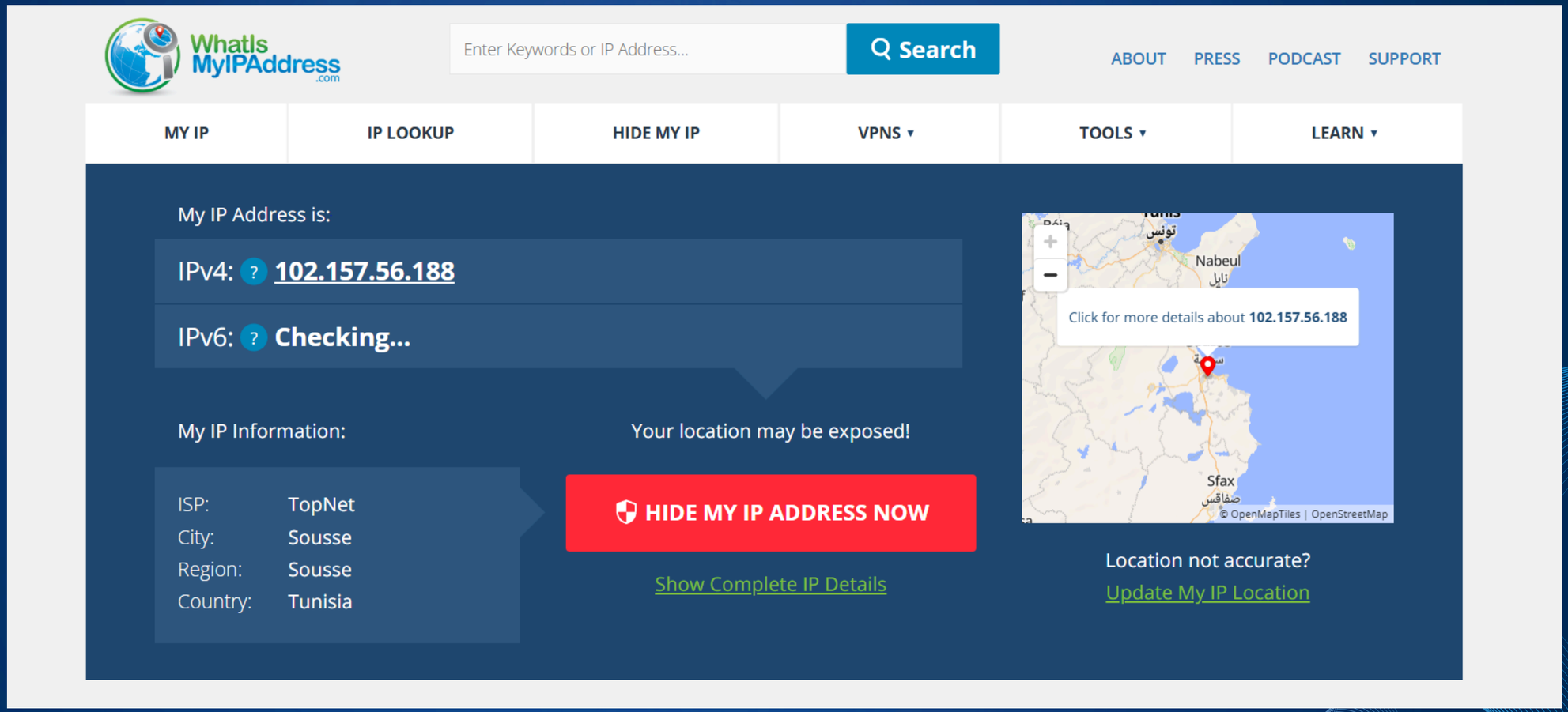

Pi-hole
hostname: OpenWrt
Status
Active
46 q/min
Load: 0.06 / 0.06 / 0.01
Memory usage: 4.3 %
MAIN
Dashboard
Query Log
GROUP MANAGEMENT
Groups 1
Clients 0
Domains 0 0
Lists 106,206 2
DNS CONTROL
Disable Blocking
SYSTEM
Settings
Tools
DONATE
Donate
Total Queries
8,648
8 active clients
Queries Blocked
4,161
List blocked queries
Percentage Blocked
48.1%
List all queries
Domains on Lists
106,206
Manage lists
Total queries
600
500
400
300
200
100
0
02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00
Client activity
600
500
400
300
200
100
0
02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00
Query Types
A
AAAA
SRV
PTR
HTTPS
Upstream servers
blocklist
cache
one.one.one.one#53
dns.google#53
dns.google#53
one.one.one.one#53

DEMO


Donate
Query Types
A
AAAA
SRV
PTR
HTTPS
Upstream servers
blocklist
cache
one.one.one.one#53
dns.google#53
dns.google#53
one.one.one.one#53
Top Permitted Domains
Domain Hits Frequency
wpad.lan 735
downloads.openwrt.org 720
ssl.gstatic.com 88
chatgpt.com 79
ipv6.msftconnecttest.com 78
122.52.52.10.in-addr.arpa 76
143.52.52.10.in-addr.arpa 72
docs.google.com 71
1.52.52.10.in-addr.arpa 71
www.msftconnecttest.com 70
Top Blocked Domains
Domain Hits Frequency
eu-mobile.events.data.microsoft.com 628
nexus-websocket-a.intercom.io 556
af.opera.com 419
g.live.com 240
telemetry.canva.com 215
oth.eve.mdt.qq.com 130
ipv6.msftncsi.com 121
www.msftncsi.com 121
optimizationguide-pa.googleapis.com 113
mobile.events.data.microsoft.com 109
Top Clients (total)
Client Requests Frequency
10.52.52.122 6366
Top Clients (blocked only)
Client Requests Frequency
10.52.52.122 3588

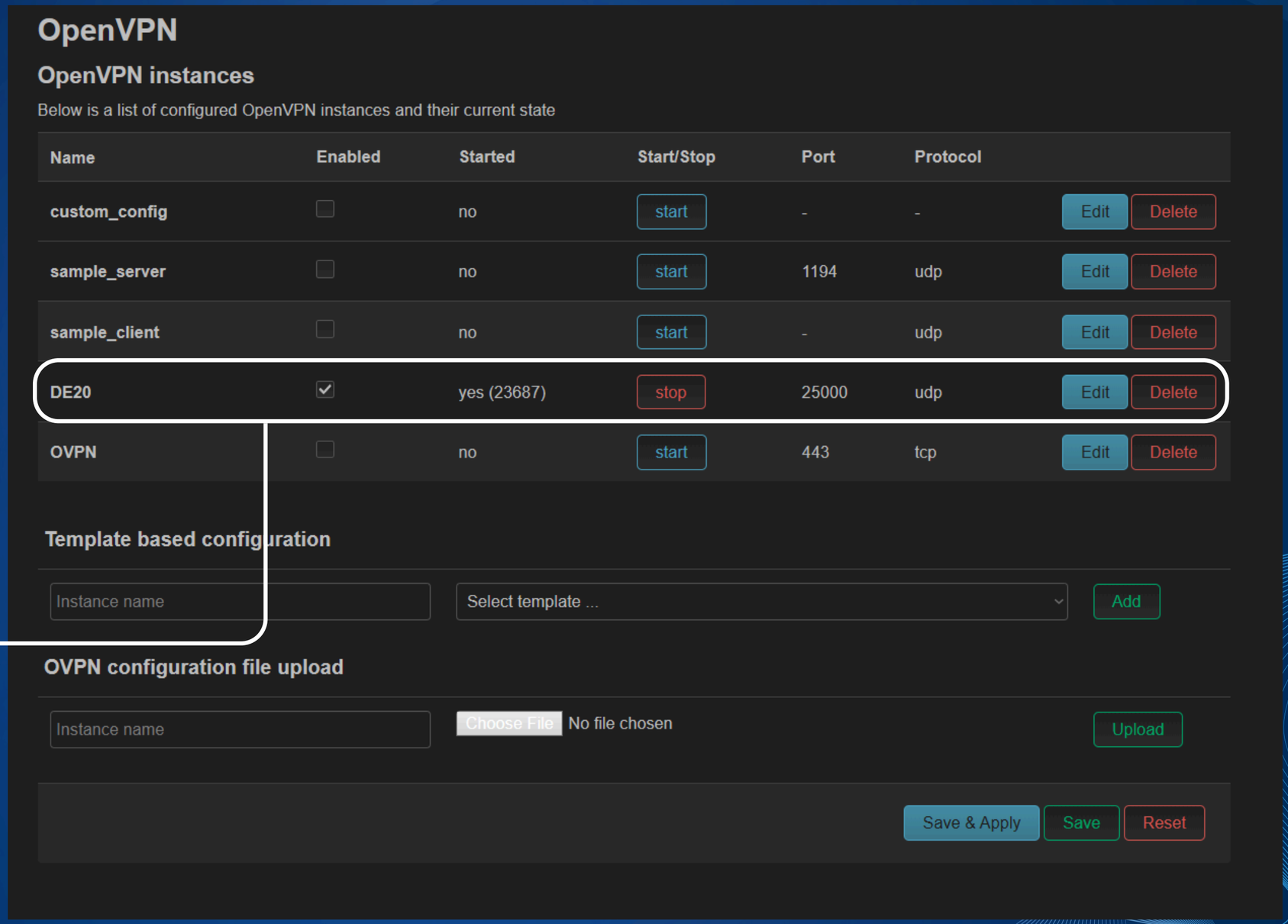
DEMO

Before


WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
PODCAST
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
My IP Address is:
IPv4: 102.157.56.188
IPv6: Checking...
My IP Information:
ISP: TopNet
City: Sousse
Region: Sousse
Country: Tunisia
Your location may be exposed!
HIDE MY IP ADDRESS NOW
Show Complete IP Details
Nabeul
Click for more details about 102.157.56.188
Sfax
© OpenMapTiles | OpenStreetMap
Location not accurate?
Update My IP Location

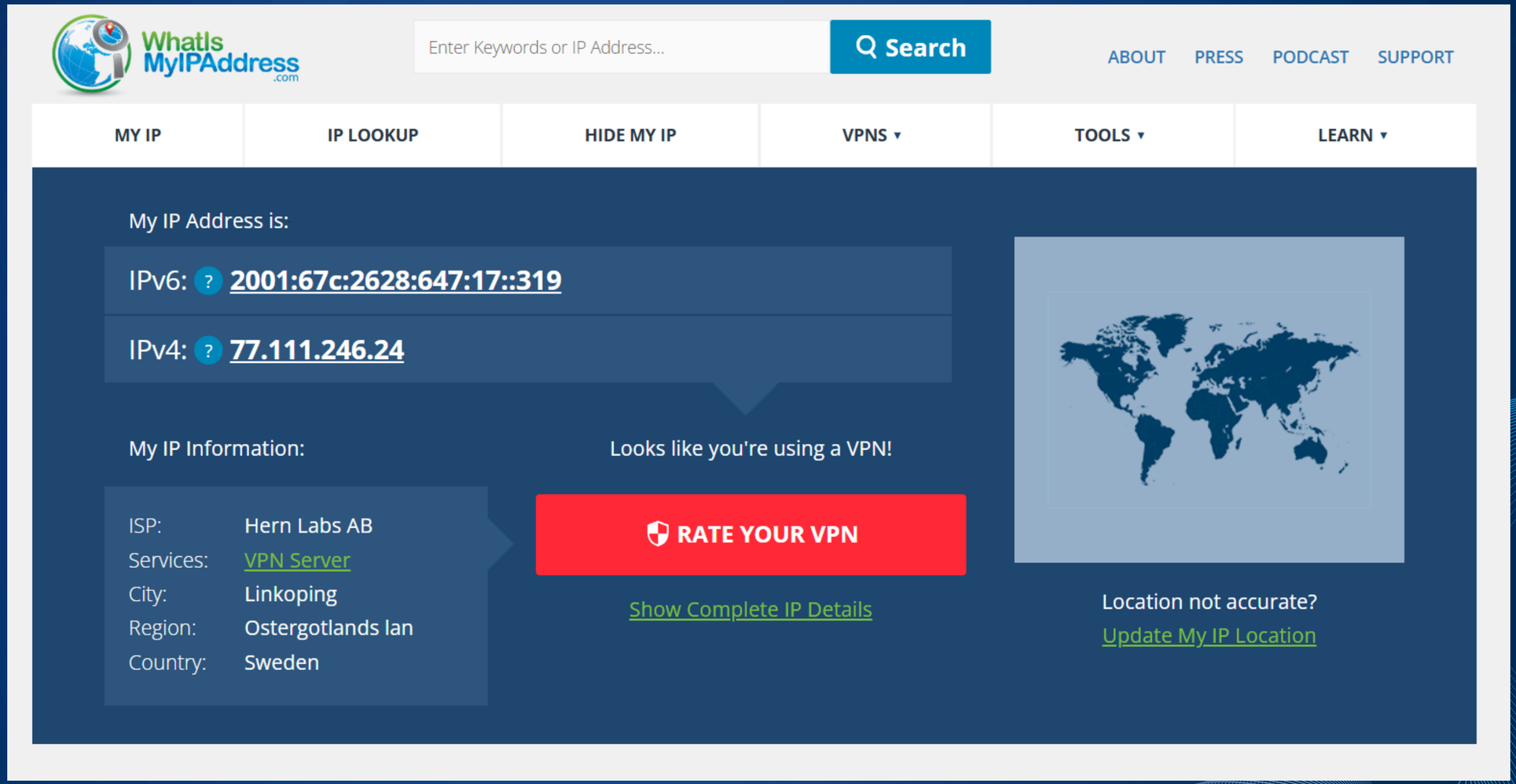
DEMO

VPN Tunnel



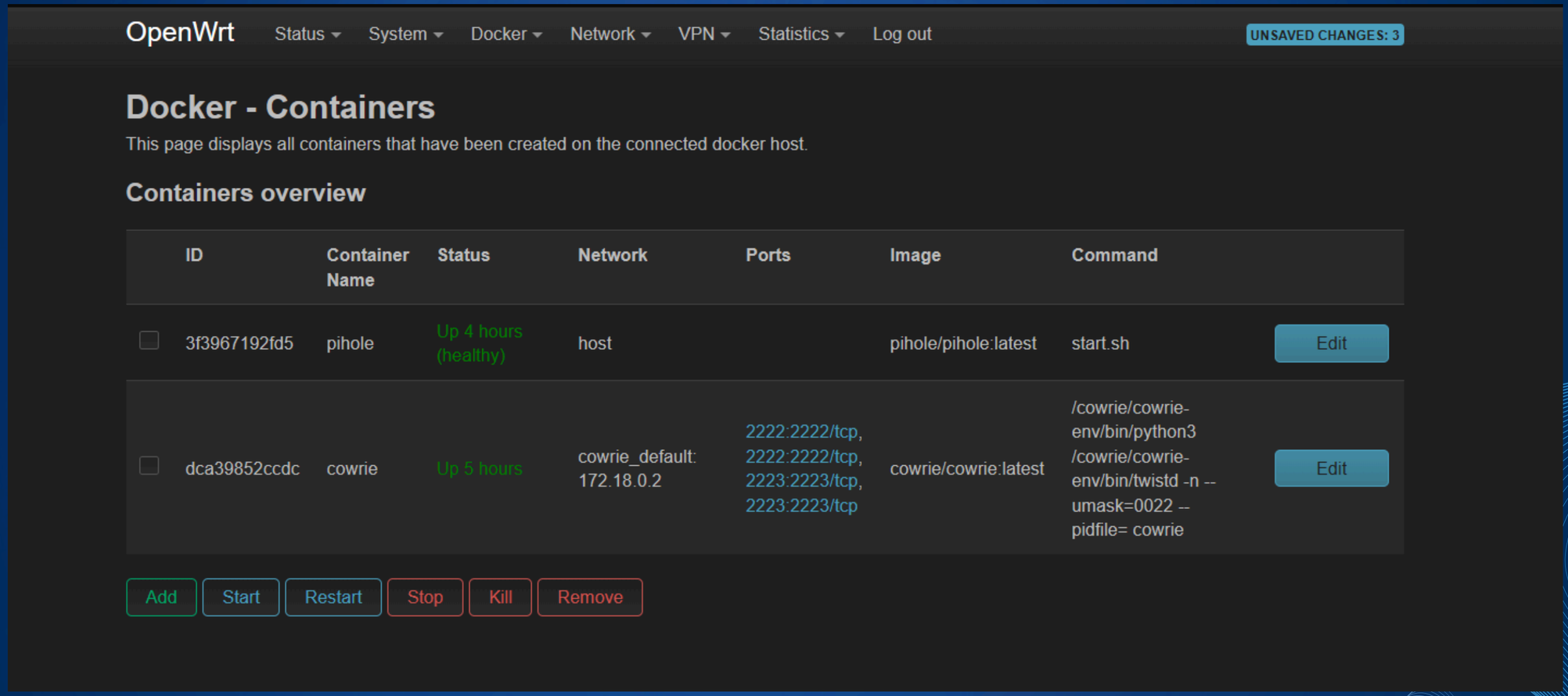
DEMO

After

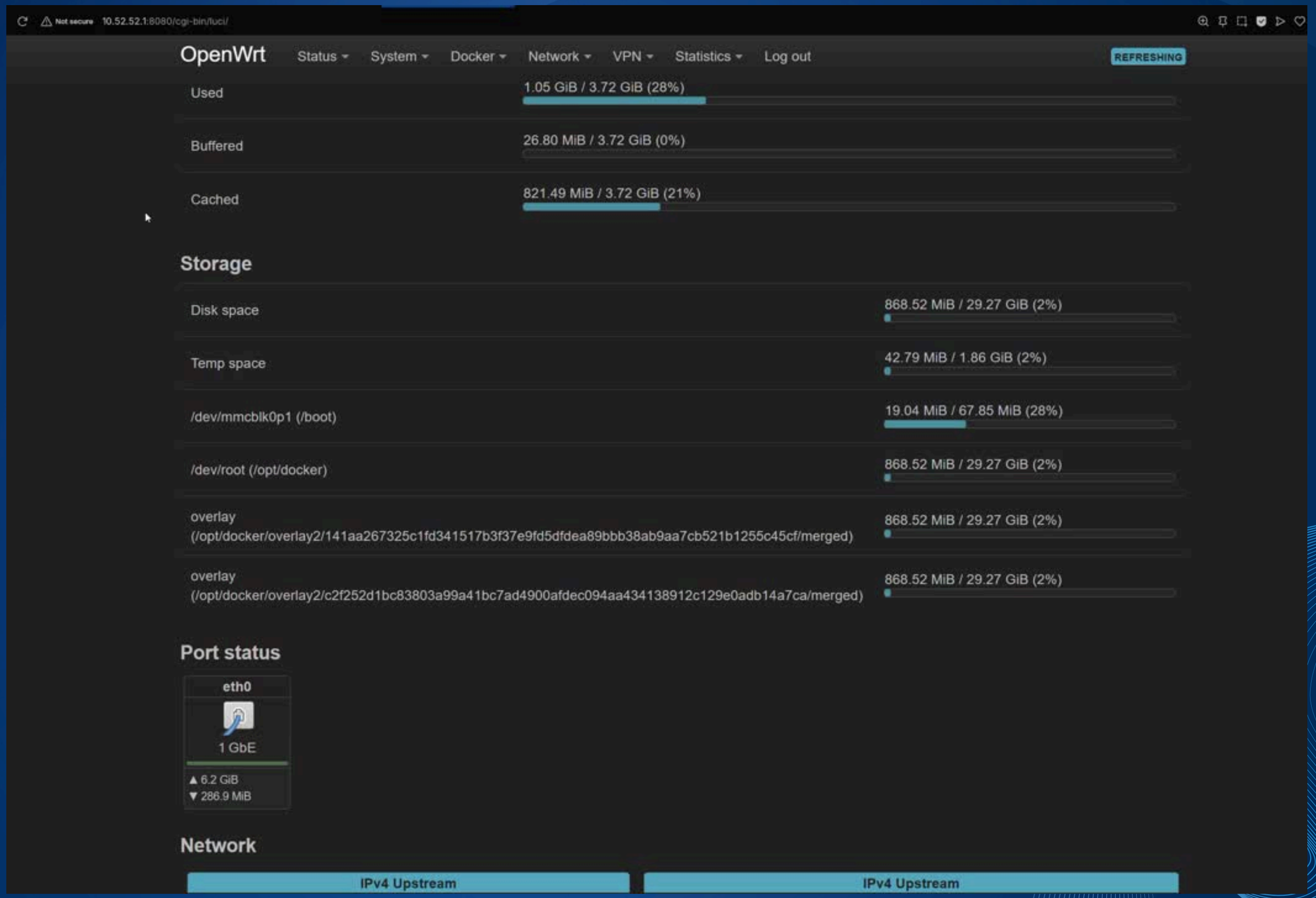

WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
PODCAST
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
My IP Address is:
IPv6: 2001:67c:2628:647:17::319
IPv4: 77.111.246.24
My IP Information:
ISP: Hern Labs AB
Services: VPN Server
City: Linkoping
Region: Ostergotlands lan
Country: Sweden
Looks like you're using a VPN!
RATE YOUR VPN
Show Complete IP Details
Location not accurate?
Update My IP Location

DEMO

Docker Containers



DEMO


Not secure 10.52.52.1:8080/cgi-bin/luci/
OpenWrt
Status
System
Docker
Network
VPN
Statistics
Log out
REFRESHING
Used
1.05 GiB / 3.72 GiB (28%)
Buffered
26.80 MiB / 3.72 GiB (0%)
Cached
821.49 MiB / 3.72 GiB (21%)
Storage
Disk space
868.52 MiB / 29.27 GiB (2%)
Temp space
42.79 MiB / 1.86 GiB (2%)
/dev/mmcblk0p1 (/boot)
19.04 MiB / 67.85 MiB (28%)
/dev/root (/opt/docker)
868.52 MiB / 29.27 GiB (2%)
overlay
(/opt/docker/overlay2/141aa267325c1fd341517b3f37e9fd5dfdea89bbb38ab9aa7cb521b1255c45cf/merged)
868.52 MiB / 29.27 GiB (2%)
overlay
(/opt/docker/overlay2/c2f252d1bc83803a99a41bc7ad4900afdec094aa434138912c129e0adb14a7ca/merged)
868.52 MiB / 29.27 GiB (2%)
Port status
eth0
1 GbE
▲ 6.2 GiB
▼ 286.9 MiB
Network
IPv4 Upstream
IPv4 Upstream

CONCLUSION & KEY TAKEAWAYS

- Public Wi-Fi = high risk (snooping, fake hotspots, MITM)
- Secure Portable Route = Secure Connection
- Combines OpenWrt + VPN + Cowrie + Pi-hole for layered protection
- Encrypts traffic, improves privacy, blocks malicious domains, Trap for the attacker
- Simple solution that can be used anywhere, by any user

THANK YOU