

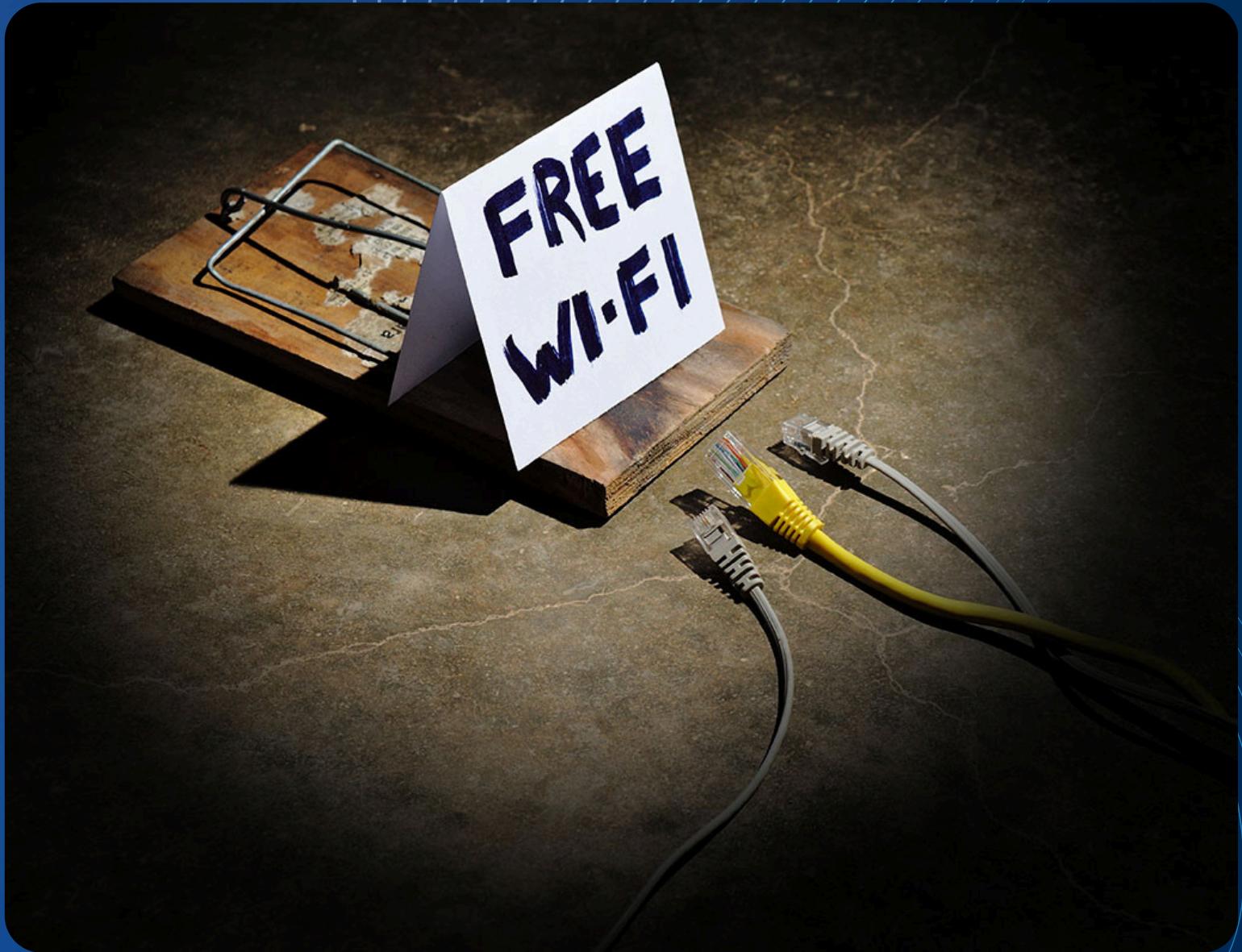
SECURE PORTABLE ROUTE

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

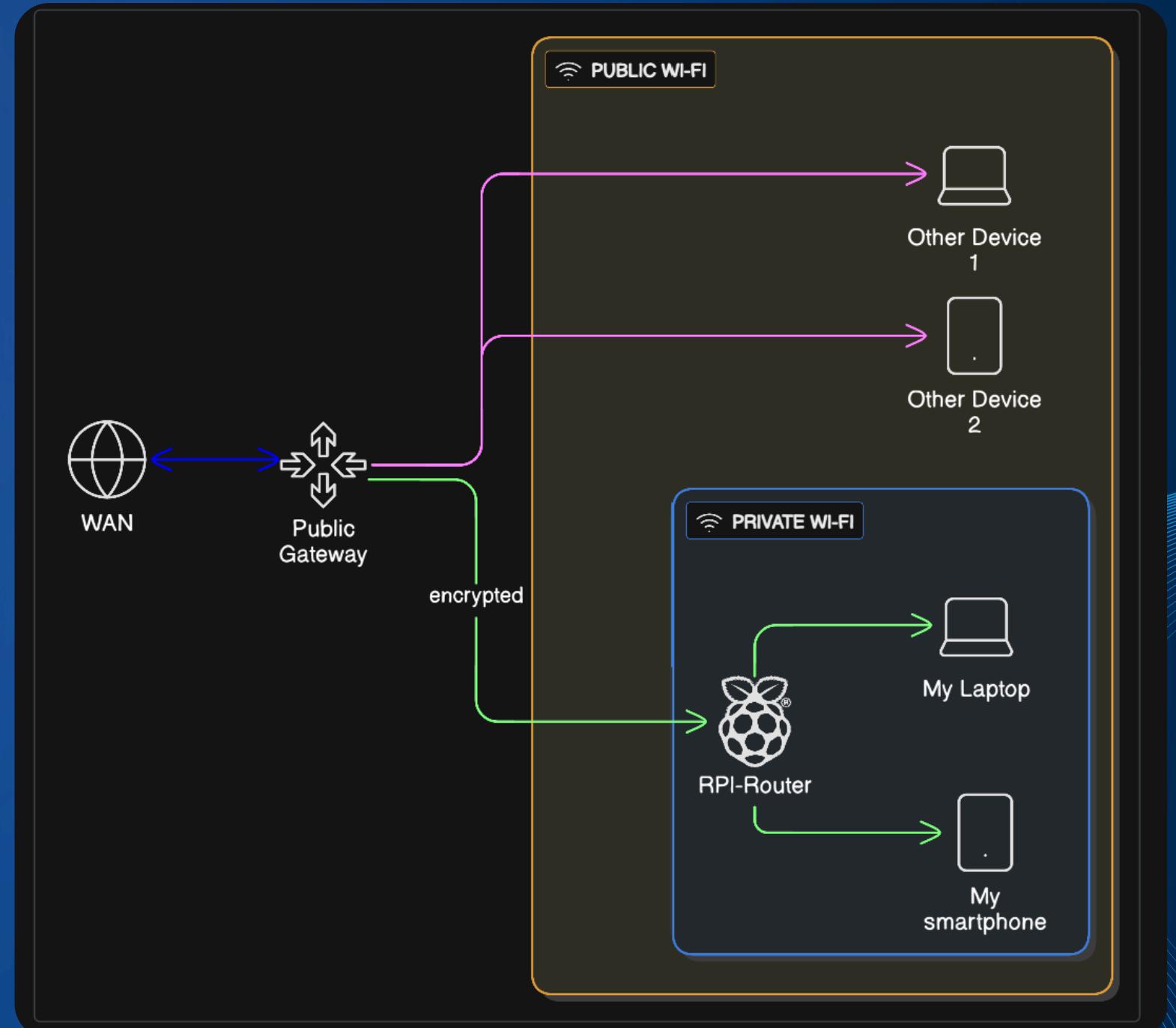


PROJECT OBJECTIVES

- 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

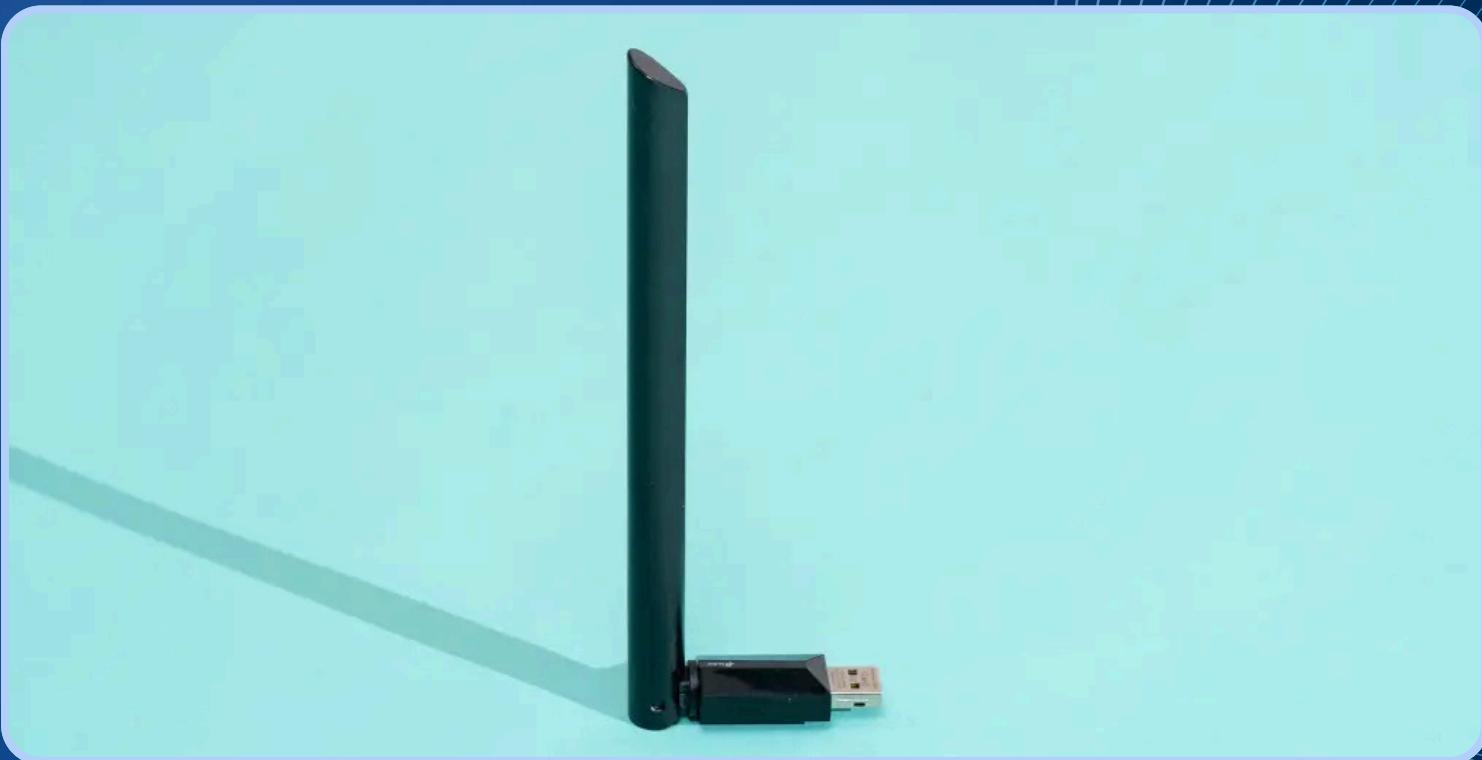
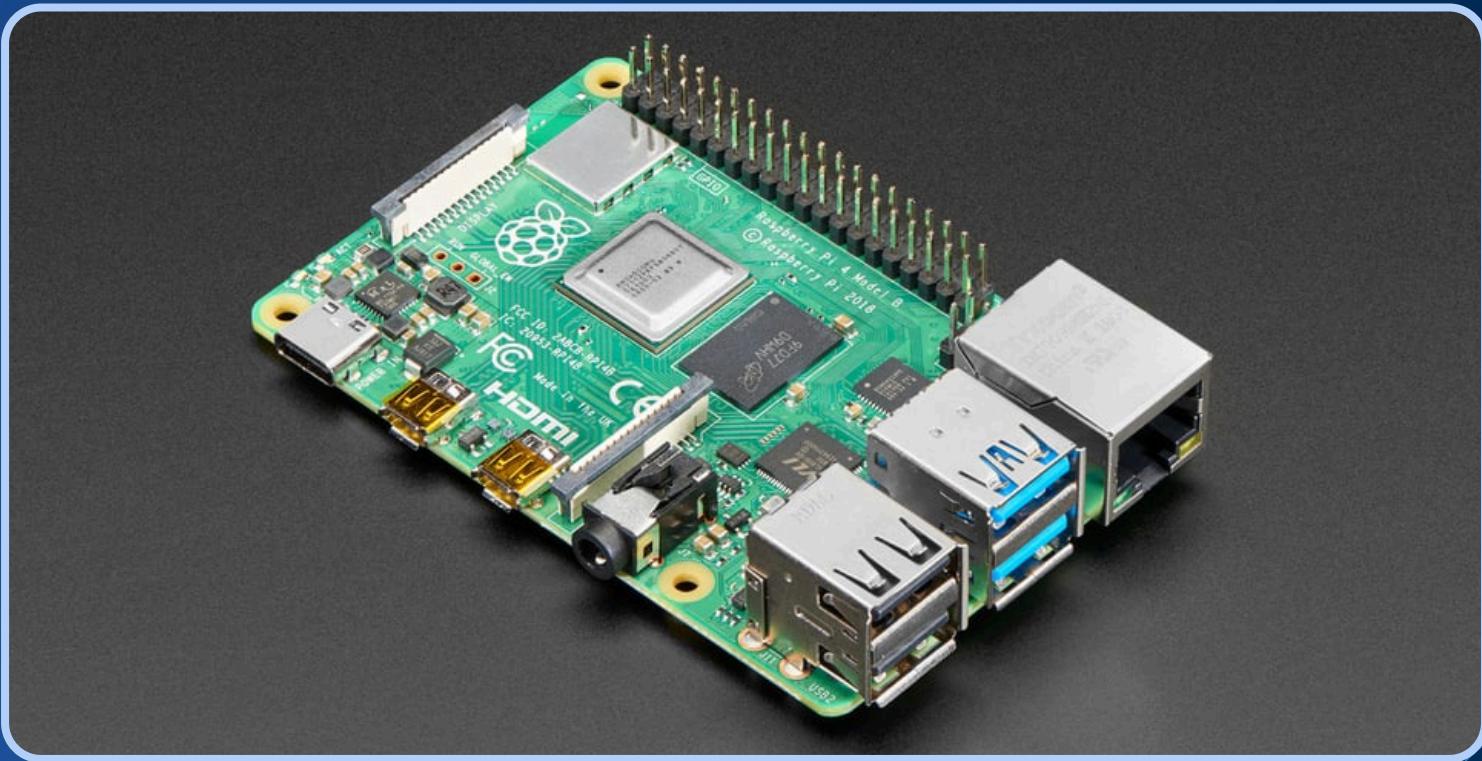
- Raspberry Pi acts as a secure router
- Connects to public Wi-Fi as WAN interface
- Creates a private, secure Wi-Fi hotspot for users (LAN)



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

OpenWrt Status System Docker Network VPN Statistics Log out REFRESHING UNSAVED CHANGES: 3

Wireless Overview

radio0	Cypress CYW43455 802.11ac/b/g/n Channel: 10 (2.457 GHz) Bitrate: 72.2 Mbit/s	<button>Restart</button> <button>Scan</button> <button>Add</button>
-42 dBm	SSID: TOPNET_7208 Mode: Client BSSID: DC:A6 Encryption: -	<button>Disable</button> <button>Edit</button> <button>Remove</button>
radio1	Generic MAC80211 802.11b/g/n Channel: 1 (2.412 GHz) Bitrate: 72.2 Mbit/s	<button>Restart</button> <button>Scan</button> <button>Add</button>
-21 dBm	SSID: OpenWrt Mode: Master BSSID: 00:11 Encryption: None	<button>Disable</button> <button>Edit</button> <button>Remove</button>

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
Client "TOPNET_7208" (phy0-sta0)	34:60:f	192.168.1.1	-42 dBm	72.2 Mbit/s, 20 MHz 72.2 Mbit/s, 20 MHz
Access Point "OpenWrt" (phy1-ap0)	B6:42:B	Redmi-Note-11-Pro-5G (10.52.52.111)	-21 dBm	65 Mbit/s, 20 MHz, MCS 7 72.2 Mbit/s, 20 MHz, MCS 7, Short GI

Save & Apply Save

Network Interfaces

DEMO

OpenWrt Status ▾ System ▾ Docker ▾ Network ▾ VPN ▾ Statistics ▾ Log out REFRESHING UNSAVED CHANGES: 3

Interfaces Devices Global network options

Interfaces

 Protocol: Unmanaged RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) Information: Not started on boot	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
 Protocol: Static address Uptime: 2h 7m 10s MAC: DC:A6:32: RX: 35.23 MB (150536 Pkts.) TX: 302.74 MB (275040 Pkts.) IPv4: 10.52.52.1/24 IPv6: fd22:83bc:fd3d::1/60	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
 Protocol: Unmanaged RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) Error: Network device is not present	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
 Protocol: DHCP client Uptime: 2h 7m 3s MAC: DC:A6:32: RX: 6.60 GB (4743899 Pkts.) TX: 289.33 MB (2962861 Pkts.) IPv4: 192.168.1.12/24	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>

Add new interface...

Save & Apply ▾ Save Reset

DEMO

Pi-hole

Status
● Active
● 46 q/min
● Load: 0.06 / 0.06 / 0.01
● Memory usage: 4.3 %

Total Queries **8,648** 8 active clients [List blocked queries](#)

Queries Blocked **4,161** [List all queries](#)

Percentage Blocked **48.1%** [Manage lists](#)

Domains on Lists **106,206**

MAIN

- Dashboard
- Query Log

GROUP MANAGEMENT

- Groups **1**
- Clients **0**
- Domains **0**
- Lists **106,206** **2**

DNS CONTROL

- Disable Blocking <

SYSTEM

- Settings <
- Tools <

DONATE

- Donate

Total queries

Client activity

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	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
downloads.openwrt.org	720	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
ssl.gstatic.com	88	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
chatgpt.com	79	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
ipv6.msftconnecttest.com	78	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
122.52.52.10.in-addr.arpa	76	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
143.52.52.10.in-addr.arpa	72	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
docs.google.com	71	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
1.52.52.10.in-addr.arpa	71	<div style="width: 100%; height: 10px; background-color: #808080;"></div>
www.msftconnecttest.com	70	<div style="width: 100%; height: 10px; background-color: #808080;"></div>

Top Blocked Domains

Domain	Hits	Frequency
eu-mobile.events.data.microsoft.com	628	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
nexus-websocket-a.intercom.io	556	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
af.opera.com	419	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
g.live.com	240	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
telemetry.canva.com	215	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
oth.eve.mdt.qq.com	130	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
ipv6.msftncsi.com	121	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
www.msftncsi.com	121	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
optimizationguide-pa.googleapis.com	113	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>
mobile.events.data.microsoft.com	109	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>

Top Clients (total)

Client	Requests	Frequency
10.52.52.122	6366	<div style="width: 100%; height: 10px; background-color: #00ff00;"></div>

Top Clients (blocked only)

Client	Requests	Frequency
10.52.52.122	3588	<div style="width: 100%; height: 10px; background-color: #ff0000;"></div>

DEMO

Before

What's MyIPAddress.com

Enter Keywords or IP Address...

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...

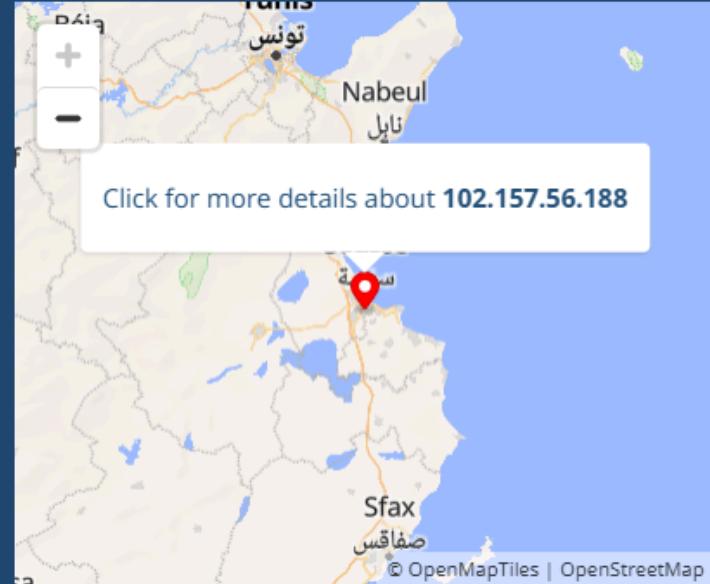
My IP Information:

ISP:	TopNet
City:	Sousse
Region:	Sousse
Country:	Tunisia

Your location may be exposed!

 [HIDE MY IP ADDRESS NOW](#)

[Show Complete IP Details](#)


Click for more details about 102.157.56.188

Location not accurate?
[Update My IP Location](#)

DEMO

VPN Tunnel

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Name	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	<input type="checkbox"/>	no	<button>start</button>	-	-	<button>Edit</button> <button>Delete</button>
sample_server	<input type="checkbox"/>	no	<button>start</button>	1194	udp	<button>Edit</button> <button>Delete</button>
sample_client	<input type="checkbox"/>	no	<button>start</button>	-	udp	<button>Edit</button> <button>Delete</button>
DE20	<input checked="" type="checkbox"/>	yes (23687)	<button>stop</button>	25000	udp	<button>Edit</button> <button>Delete</button>
OVPN	<input type="checkbox"/>	no	<button>start</button>	443	tcp	<button>Edit</button> <button>Delete</button>

Template based configuration

Instance name: Select template ... Add

OVPN configuration file upload

Instance name: Choose File: No file chosen Upload

Save & Apply Save Reset

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

OpenWrt Status ▾ System ▾ Docker ▾ Network ▾ VPN ▾ Statistics ▾ Log out UNSAVED CHANGES: 3

Docker - Containers

This page displays all containers that have been created on the connected docker host.

Containers overview

ID	Container Name	Status	Network	Ports	Image	Command
<input type="checkbox"/> 3f3967192fd5	pihole	Up 4 hours (healthy)	host		pihole/pihole:latest	start.sh <button>Edit</button>
<input type="checkbox"/> dca39852ccdc	cowrie	Up 5 hours	cowrie_default: 172.18.0.2	2222:2222/tcp, 2222:2222/tcp, 2223:2223/tcp, 2223:2223/tcp	cowrie/cowrie:latest	/cowrie/cowrie-env/bin/python3 /cowrie/cowrie-env/bin/twistd -n --umask=0022 --pidfile= cowrie <button>Edit</button>

Add Start Restart Stop Kill Remove

DEMO

Net secure 10.52.52.1:8080/cgi-bin/luci/ REFRESHING

OpenWrt Status System Docker Network VPN Statistics Log out

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

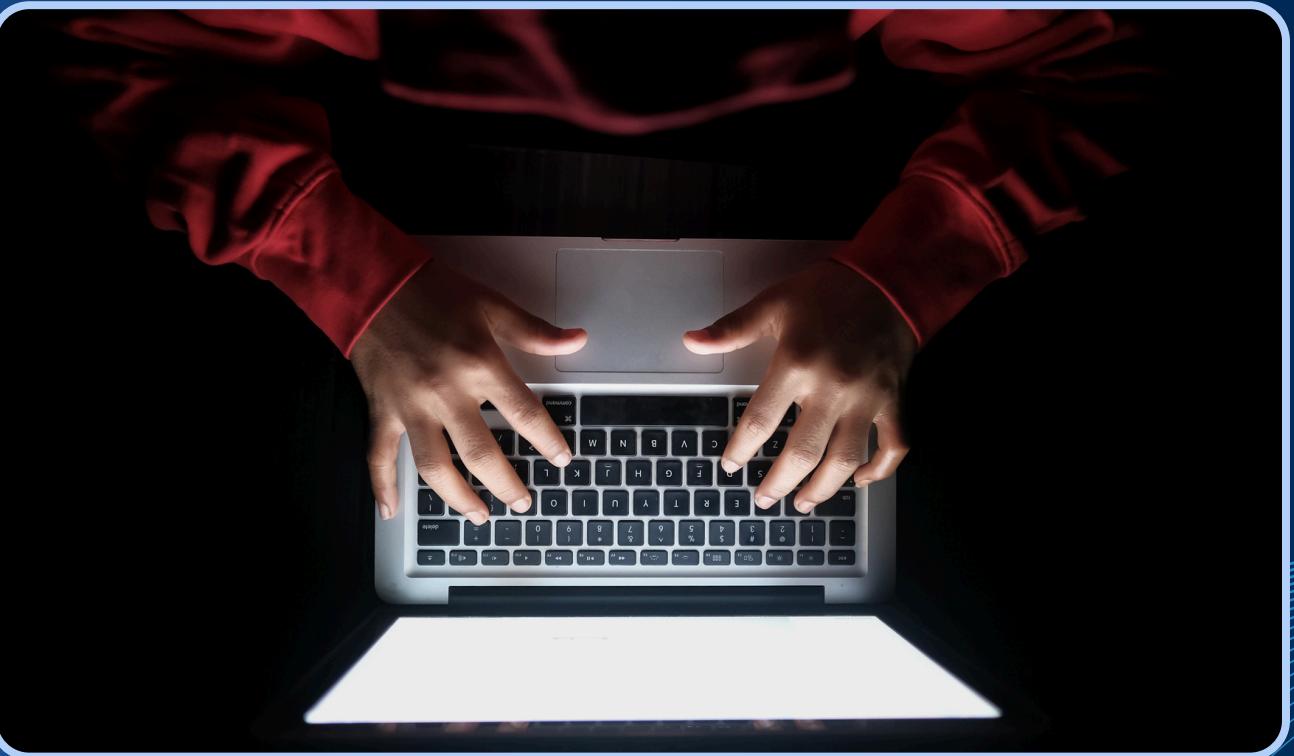
eth0	1 GbE
▲ 6.2 GiB	
▼ 286.9 MiB	

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