Ministry of Higher Education and Scientific Research of the Republic of Tunisia

TEK-UP Private Higher School of Technology and Engineering

RAPPORT OF SECURITY PROJECT

Computer Engineering Program of Study

Under the theme :

Secure Portable Router Project with Honeypot, DNS Filtering, and VPN Integration

Presented by :
Saii Nassim

Academic year 2025-2026

Table des matières

Table des figures

General Introduction

In recent years, the rapid evolution of technology has transformed the way humans interact with the world around them. Today, almost every aspect of our daily lives relies on networked systems, from smart homes equipped with interconnected devices to smart cities managing critical infrastructure and public services. These developments offer unprecedented convenience, efficiency, and connectivity, allowing for automation, remote monitoring, and real-time data processing across multiple domains.

However, this increasing dependence on networked technologies also introduces a growing set of vulnerabilities. As systems become more interconnected, the attack surface expands, creating new opportunities for malicious actors. The democratization of attack tools has made cyber threats more accessible ; even individuals with minimal technical expertise, often referred to as script kiddies, can exploit poorly secured networks. In parallel, advanced persistent threats from organized groups continue to evolve, making the landscape of cyberattacks increasingly complex and diverse.

In this context, network security is no longer an optional consideration ; it has become a fundamental requirement for both private and public networks. Public spaces, such as airports, cafes, and transportation systems, are particularly vulnerable due to the large number of transient users and heterogeneous devices connected to these networks. The potential consequences of security breaches range from personal data theft and privacy violations to critical infrastructure disruptions with societal impact.

This reality underscores the necessity of proactive security measures that not only defend against traditional attacks but also adapt to emerging threats. The challenge lies in designing systems that are resilient, scalable, and capable of monitoring, detecting, and mitigating malicious activities effectively. Strengthening security in modern networks requires a combination of technical solutions, best practices, and continuous vigilance, ensuring that as technology evolves, so too does the ability to protect it.

Chapitre 1

Project Scope

Table des matières

Introduction

The scope of this project is to design and implement a secure portable network solution capable of addressing modern threats in both personal and public environments. With the proliferation of network-dependent technologies, the need for resilient and adaptive security mechanisms has become critical. The objective is to create a system that not only provides connectivity but also incorporates mechanisms for monitoring, controlling, and protecting network traffic.

The project focuses on several key aspects :

1.1 Enhancing Network Security

In an era where attacks can originate from both opportunistic individuals and organized groups, the system must detect, log, and mitigate unauthorized activities. This is essential to prevent breaches that could compromise sensitive data or disrupt operations.

1.2 Traffic Control and Filtering

Efficient management of network traffic ensures that only legitimate and secure communication is allowed. By implementing traffic control mechanisms, the system can protect users from accessing harmful or malicious content while maintaining overall network performance.

1.3 Secure Internet Access

As privacy concerns increase, secure connections for outbound traffic are necessary to prevent eavesdropping, data interception, or manipulation. Providing encrypted channels ensures that sensitive information remains confidential and integrity is maintained.

1.4 Monitoring and Logging

Collecting detailed information about network activity is crucial for both real-time response and post-event analysis. By monitoring traffic patterns and user interactions, administrators can identify potential threats early, understand attack methods, and improve security policies over time.

1.5 Portability and Flexibility

The system is designed to be compact, mobile, and easily deployable, allowing it to function in various scenarios, from temporary public installations to educational or experimental setups. Portability ensures that security measures can be applied wherever they are needed without requiring extensive infrastructure.

1.6 Resilience and Scalability

The project aims to develop a robust solution capable of handling multiple devices simultaneously while maintaining high availability. The system should be adaptable to different network sizes and structures, making it suitable for diverse deployment environments.

Conclusion

Overall, the project is conceived to provide a practical demonstration of modern network security principles. It emphasizes the importance of proactive protection, visibility into network activities, and the implementation of effective security mechanisms to safeguard both end-users and infrastructure. This scope reflects the growing necessity to anticipate and mitigate threats in a landscape where technological advancement and cyber risks evolve simultaneously.

Chapitre 2

State of the Art

Table des matières

Introduction

The rapid development of networking technologies and the expansion of the Internet of Things (IoT) have significantly transformed the landscape of information systems. From small-scale smart homes to city-wide infrastructure, almost every digital service now relies on continuous network connectivity. While this connectivity enables automation, convenience, and efficiency, it also introduces significant security challenges. Understanding the current state of the art in network security is essential for designing effective protective solutions.

2.1 Evolving Threat Landscape

Modern networks face a wide spectrum of threats, ranging from opportunistic attacks by individuals with limited technical skills to sophisticated campaigns orchestrated by organized cybercriminals or state-sponsored actors. The increasing availability of pre-built attack tools has lowered the barrier for conducting cyberattacks, enabling even non-professional actors to exploit vulnerabilities in networked systems.

Public networks, such as those in airports, hotels, and universities, are particularly vulnerable due to the diversity and volume of devices connecting simultaneously. In addition, the widespread use of IoT devices often introduces poorly secured endpoints, expanding the potential attack surface. These developments have highlighted the urgent need for proactive monitoring, threat detection, and preventive security measures.

2.2 Intrusion Detection and Monitoring

Intrusion detection systems (IDS) have become an essential component of modern network security. These systems monitor network traffic and identify suspicious or malicious activities, providing actionable insights to administrators. High-interaction monitoring, such as honeypots or decoy services, allows security teams to capture attack techniques in a controlled environment, offering valuable intelligence on attacker behavior. This approach not only helps prevent breaches but also contributes to the understanding of emerging threats and the development of countermeasures.

2.3 Traffic Filtering and Network Control

As networks grow in complexity, controlling and filtering traffic has become a central focus in network security research. Systems that can intercept, analyze, and selectively block malicious or unwanted traffic protect users from malware, phishing, and other attacks. Advanced DNS filtering and content control mechanisms are widely deployed in both enterprise and public networks to enhance resilience against evolving threats while maintaining acceptable performance and usability.

2.4 Secure Communication Channels

Privacy and confidentiality are increasingly critical in networked environments. Encrypted communication channels, such as those provided by Virtual Private Networks (VPNs) or secure tunneling protocols, are essential for preventing eavesdropping and data manipulation. As remote work, mobile devices, and cloud services become pervasive, secure connectivity ensures that sensitive information remains protected, even over untrusted networks.

2.5 Integration Challenges

While various security solutions exist, integrating them into a cohesive, portable, and scalable system remains a challenge. Balancing security, usability, and performance requires careful design and configuration. Modern approaches emphasize modularity, central monitoring, and adaptability, enabling administrators to deploy security solutions effectively across different environments and adjust them according to emerging threats.

Conclusion

In summary, the state of the art demonstrates that network security is a dynamic and multifaceted field, driven by technological innovation and the evolving nature of cyber threats. Effective protection requires a combination of monitoring, traffic control, secure communication, and adaptive design, providing both preventive measures and real-time insights into network activity. These principles form the foundation for the design of modern secure network systems and guided the development of the solution presented in this project.

Chapitre 3

Requirements specification and theoretical study

Table des matières

Introduction

Designing a secure portable network system requires a clear understanding of both the functional and non-functional requirements that the solution must satisfy, as well as the theoretical principles underlying its operation. This chapter outlines the specifications and provides a study of the concepts that support the project's architecture and security objectives.

3.1 Functional Requirements

3.1.1 Network Connectivity

The system must provide reliable network connectivity for multiple devices within a defined local area network (LAN), enabling seamless access to both local and internet resources.

3.1.2 Intrusion Detection and Monitoring

The solution should be capable of detecting and logging unauthorized access attempts, providing detailed information about attacker behavior and methods. This functionality is essential for proactive defense and forensic analysis.

3.1.3 Traffic Filtering and Control

The system must implement mechanisms to manage, filter, and restrict network traffic, preventing access to malicious or harmful content while ensuring legitimate traffic flows without disruption.

3.1.4 Secure Internet Access

Outbound traffic must be secured through encrypted channels, ensuring confidentiality, integrity, and protection against eavesdropping or interception.

3.1.5 Portability and Ease of Deployment

The system should be compact, lightweight, and easily deployable in diverse environments, from home networks to public spaces or temporary installations.

3.1.6 Logging and Reporting

Network activity, security events, and potential threats must be logged and stored systematically. Logs should support both local review and optional remote forwarding to central monitoring systems for advanced analysis.

3.2 Non-Functional Requirements

3.2.1 Performance and Scalability

The system must handle multiple concurrent devices without significant performance degradation. It should be scalable to accommodate increasing numbers of connected devices or traffic volume.

3.2.2 Reliability and Availability

Security services and network connectivity must remain operational under normal and adverse conditions, ensuring minimal downtime.

3.2.3 Security and Resilience

The system must withstand common network attacks, provide segmentation between different network zones, and maintain the integrity of traffic flows.

3.2.4 Maintainability

The architecture should allow for easy updates, configuration changes, and integration of additional security measures as threats evolve.

3.3 Theoretical Study

The operation of a secure portable network system relies on several fundamental networking and security principles :

3.3.1 Intrusion Detection Principles

Monitoring network activity enables the identification of suspicious behaviors. High-interaction decoys or honeypots emulate vulnerable services, attracting attackers and capturing their methods for analysis. This approach provides actionable intelligence while minimizing the risk to actual network resources.

3.3.2 DNS Filtering and Traffic Control

Intercepting DNS queries and managing traffic flows allow for selective blocking of harmful or undesired content. By analyzing requests and applying filtering rules, the system can prevent exposure to malware, phishing, and other threats while preserving normal user experience.

3.3.3 Secure Communication via Encryption

Encryption protocols such as VPN tunnels protect the confidentiality and integrity of data traversing public or untrusted networks. Secure communication ensures that sensitive information cannot be intercepted or modified by attackers.

3.3.4 Network Segmentation and Firewalling

Dividing the network into zones, such as LAN, WAN, and secure tunnels, allows granular control over traffic and access permissions. Firewalls enforce security policies, preventing unauthorized interactions and isolating critical components from potential threats.

3.3.5 Centralized Monitoring and Logging

Systematic collection and analysis of logs provide both real-time alerts and historical data for forensic investigation. Centralized logging enhances visibility into network activity and improves response times to potential incidents.

Conclusion

The requirements specification and theoretical study highlight the complex interplay between functionality, security, and usability. A secure portable network system must not only provide reliable connectivity and efficient traffic management but also incorporate proactive monitoring, threat detection, and encrypted communication. These principles form the foundation for the architecture and implementation described in the following chapter, ensuring a solution that is both practical and robust in addressing contemporary network security challenges.

Chapitre 4

Architecture Implementation

Table des matières

Introduction

Designing a secure portable network solution requires a modular and layered architecture that integrates connectivity, monitoring, and security functionalities. This chapter describes the system architecture, its components, and the implementation approach, highlighting how different modules interact to provide a cohesive and secure network environment.

4.1 Work environment

The working environment of the project includes both hardware and software components, chosen to ensure performance, portability, and flexibility :

4.1.1 Hardware Environment

Raspberry Pi 4 (4 GB RAM, 32 GB SD Card) : Serves as the main processing unit and router platform. Its compact form factor and GPIO capabilities allow flexible deployment in portable setups.

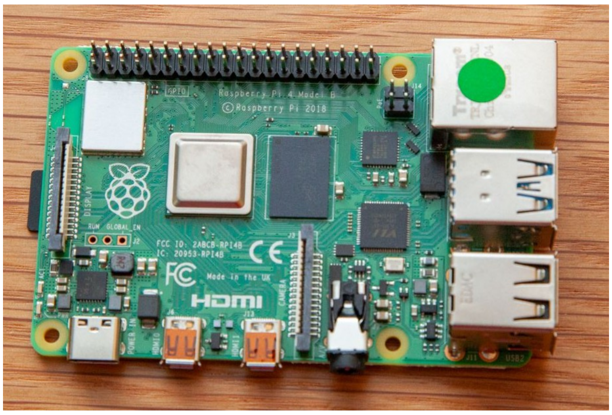


FIGURE 4.1 – Raspberry Pi 4

Network Interfaces :

Built-in Ethernet port for LAN connectivity.

Optional USB Wi-Fi adapters for additional wireless interfaces for WAN connectivity.

FIGURE 4.2 – USB Wi-Fi Adapter

4.1.2 Software Environmen

Operating System

The system is based on OpenWRT, providing a lightweight and flexible platform capable of running on portable hardware such as a Raspberry Pi.

FIGURE 4.3 – OpenWRT Logo

The OpenWrt Project is a Linux operating system targeting embedded devices. Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management. This gives freedom from the application selection and configuration provided by the vendor and allows us to customize the device through the use of packages to suit any application. For developers, OpenWrt is the framework to build an application without having to build a complete firmware around it ; for users this means the ability for full customization, to use the device in ways never envisioned.

Monitoring and Security

The intrusion detection and traffic control modules are deployed to monitor network activity and enforce security policies. Logs are generated systematically for analysis and auditing purposes, for that we choose Snort is a free, open-source network intrusion detection system (IDS) and intrusion prevention system (IPS) that analyzes network traffic for malicious activity.

FIGURE 4.4 – Snort Logo

Secure Connectivity

Encrypted tunnels are established to protect outgoing traffic, ensuring secure access to the internet. This approach safeguards user data even when the system operates in public or untrusted networks,that what provided by OpenVPN, secure remote access for businesses. Our self-hosted and cloud-managed solutions and offer zero trust network access.

FIGURE 4.5 – OpenVPN Logo

4.2 Implementation Overview

4.2.1 Conceptual Architecture Diagram

Below is a high-level conceptual representation of the system architecture :

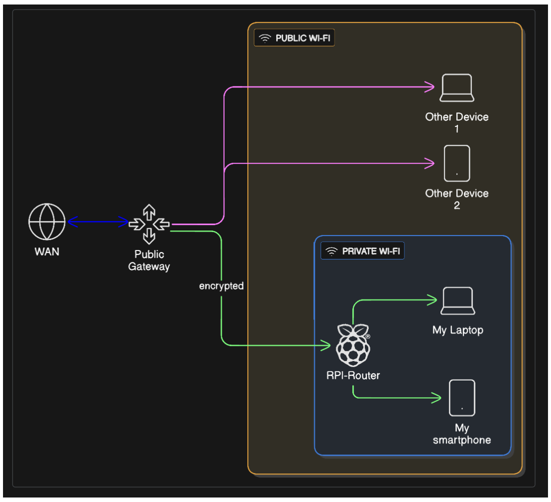


FIGURE 4.6 – Architecture overview

This diagram illustrates the flow of traffic from internal devices to the internet, passing through the security and monitoring layers, while ensuring secure communication and logging at each stage.

4.2.2 Network Segmentation and Routing

The architecture leverages segmentation to separate LAN, WAN, and secure connections. Firewalls and routing rules control the flow of traffic, minimizing the attack surface and isolating critical components from potential threats.

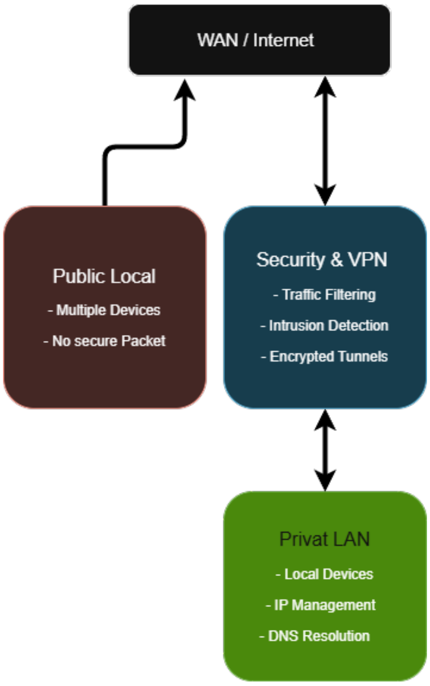


FIGURE 4.7 – Overview Diagram

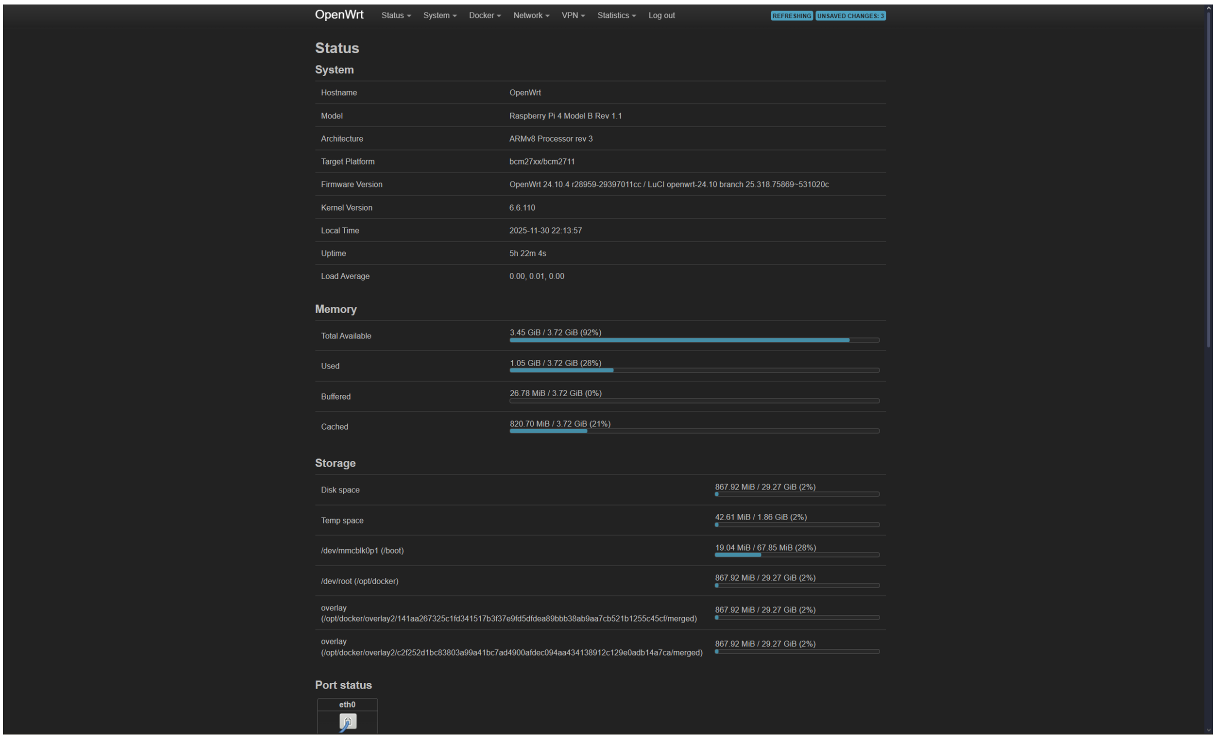
4.2.3 OpenWRT Deployment and Configuration

OpenWRT serves as the core operating system of the portable router. Its lightweight architecture and flexible configuration options make it ideal for embedded devices such as Raspberry Pi.

Implementation Steps :

- Flash the Raspberry Pi with the latest OpenWRT image and expand the root filesystem.
- Configure the LAN and WAN interfaces, including IP addressing, subnet masks, and routing policies.
- Set up firewall zones to separate internal, external, and secure traffic channels.
- Install and configure package management tools for additional software deployment.
- Validate connectivity between LAN devices and the internet, ensuring routing and DNS resolution are functional.

OpenWRT provides the foundation for integrating security modules, traffic control, and monitoring tools.



Status

System

Hostname	OpenWrt
Model	Raspberry Pi 4 Model B Rev 1.1
Architecture	ARMv8 Processor rev 3
Target Platform	bcm27xx/bcm2711
Firmware Version	OpenWrt 24.10.4 r28959-29397011cc / LuCI openwrt-24.10 branch 25.318.75869~531020c
Kernel Version	6.6.110
Local Time	2025-11-30 22:13:57
Uptime	5h 22m 4s
Load Average	0.00, 0.01, 0.00

Memory

Total Available	3.45 GiB / 3.72 GiB (92%)
Used	1.05 GiB / 3.72 GiB (28%)
Buffered	26.78 MiB / 3.72 GiB (0%)
Cached	820.70 MiB / 3.72 GiB (21%)

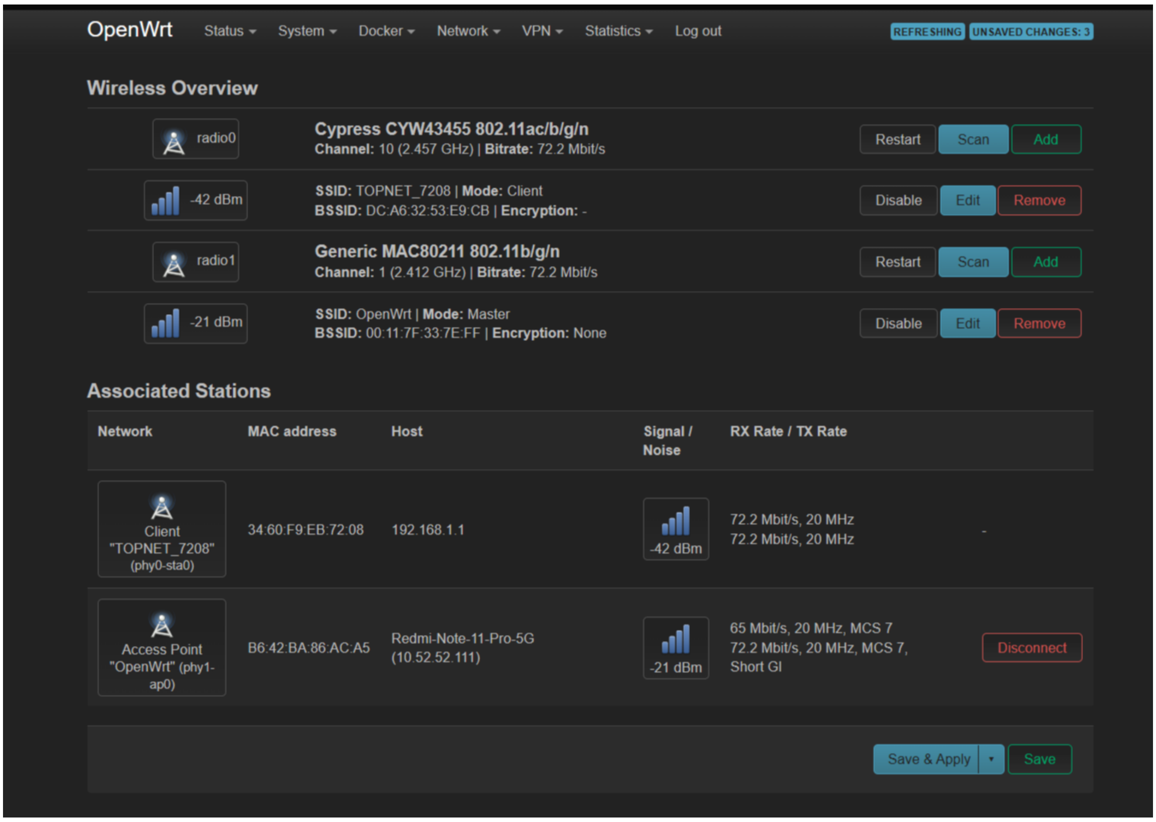
Storage

Disk space	867.92 MiB / 29.27 GiB (2%)
Temp space	42.61 MiB / 1.86 GiB (2%)
/dev/mmcblk0p1 (/boot)	19.04 MiB / 67.85 MiB (28%)
/dev/root (/opt/docker)	867.92 MiB / 29.27 GiB (2%)
overlay (/opt/docker/overlay2/141aa267325c1fd341517b3f37e9fd5dfdea89bbb38ab9aa7cb521b1255c45cf/merged)	867.92 MiB / 29.27 GiB (2%)
overlay (/opt/docker/overlay2/c2f252d1bc83803a99a41bc7ad4900afdec094aa434138912c129e0adb14a7ca/merged)	867.92 MiB / 29.27 GiB (2%)

Port status

eth0

Figure 4.8 – OpenWRT dashboard



Wireless Overview

radio0 — **Cypress CYW43455 802.11ac/b/g/n**
Channel: 10 (2.457 GHz) | **Bitrate:** 72.2 Mbit/s

-42 dBm — **SSID:** TOPNET_7208 | **Mode:** Client
BSSID: DC:A6:32:53:E9:CB | **Encryption:** -

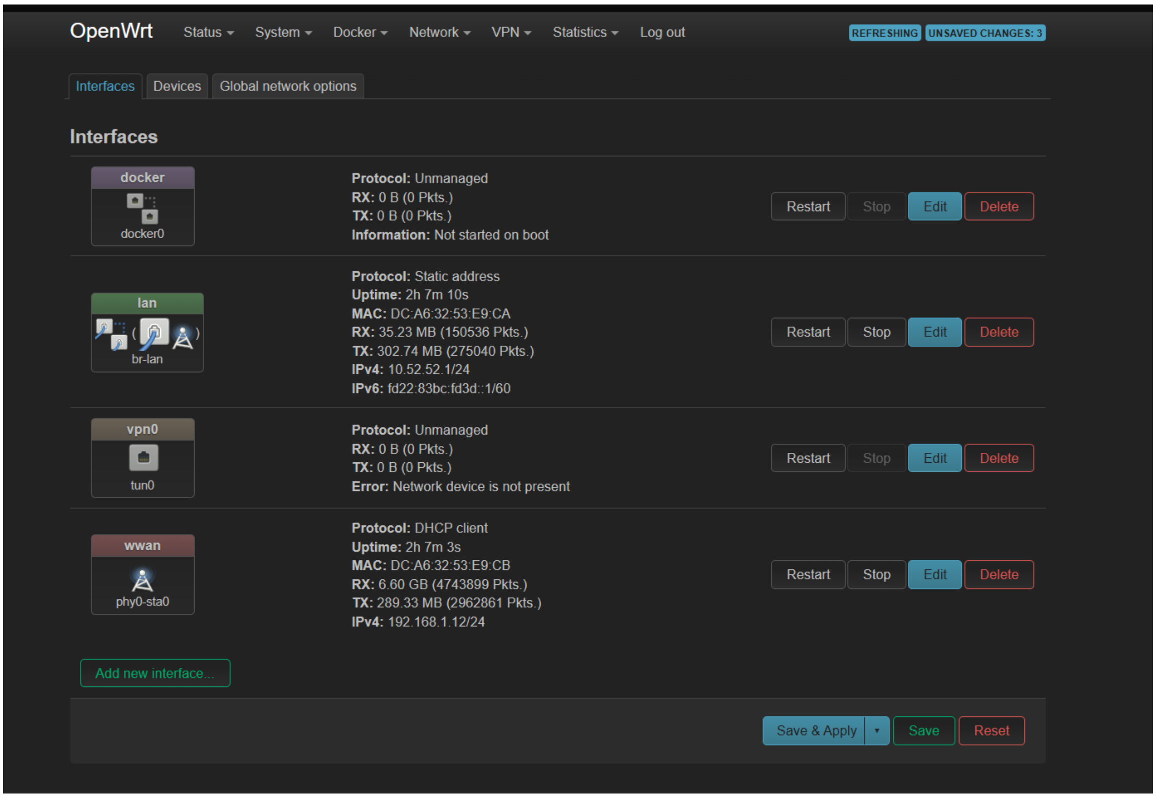
radio1 — **Generic MAC80211 802.11b/g/n**
Channel: 1 (2.412 GHz) | **Bitrate:** 72.2 Mbit/s

-21 dBm — **SSID:** OpenWrt | **Mode:** Master
BSSID: 00:11:7F:33:7E:FF | **Encryption:** None

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate	
Client "TOPNET_7208" (phy0-sta0)	34:60:F9:EB:72:08	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:BA:86:AC:A5	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	Disconnect

FIGURE 4.9 – Wireless Interfaces OpenWRT



Interfaces

docker (docker0)
Protocol: Unmanaged
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Information: Not started on boot

lan (br-lan)
Protocol: Static address
Uptime: 2h 7m 10s
MAC: DC:A6:32:53:E9:CA
RX: 35.23 MB (150536 Pkts.)
TX: 302.74 MB (275040 Pkts.)
IPv4: 10.52.52.1/24
IPv6: fd22:83bc:fd3d::1/60

vpn0 (tun0)
Protocol: Unmanaged
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Network device is not present

wwan (phy0-sta0)
Protocol: DHCP client
Uptime: 2h 7m 3s
MAC: DC:A6:32:53:E9:CB
RX: 6.60 GB (4743899 Pkts.)
TX: 289.33 MB (2962861 Pkts.)
IPv4: 192.168.1.12/24

FIGURE 4.10 – Physical Interfaces OpenWRT

4.2.4 Snort Intrusion Detection System

Snort is a lightweight network intrusion detection and prevention system (IDS/IPS) capable of monitoring network traffic for malicious activity.

Implementation Steps :

- Install Snort on the OpenWRT platform or on an attached monitoring server.
- Configure network interfaces to capture LAN traffic.
- Load appropriate rule sets for detecting common attack patterns, such as port scans, malware signatures, or suspicious payloads.
- Enable logging and alerting, storing detected events locally or forwarding them to a centralized monitoring system.

Snort provides real-time threat detection and complements other monitoring mechanisms within the system.

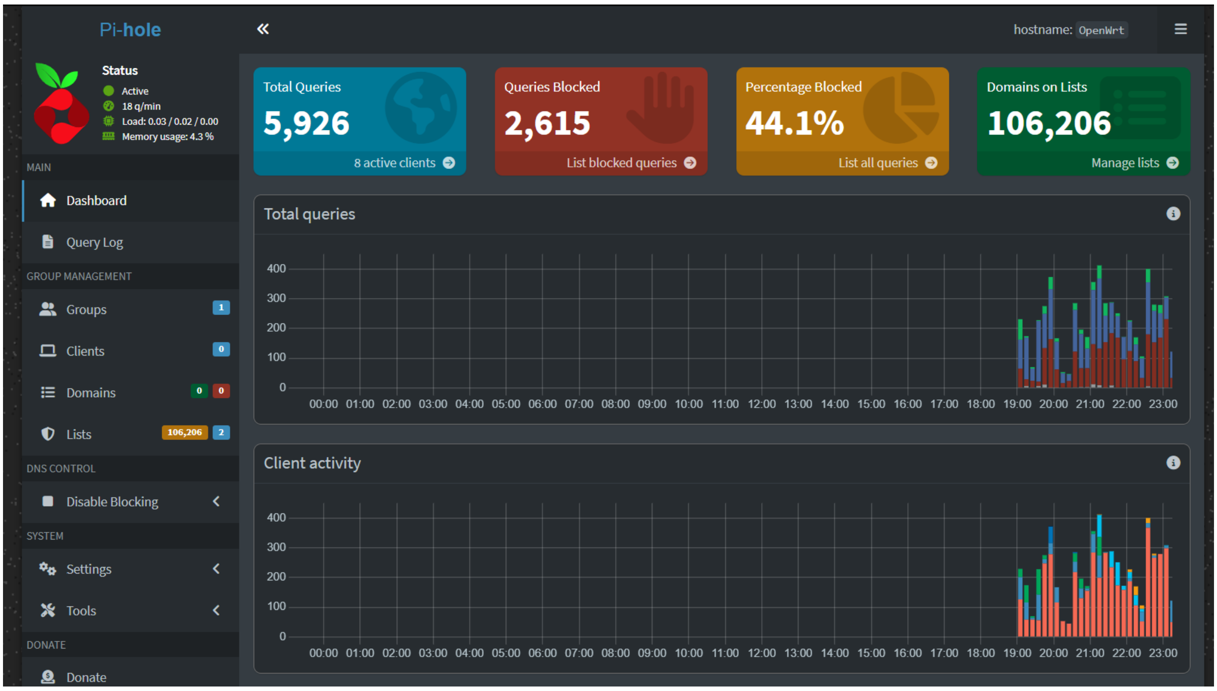
4.2.5 Pi-hole DNS Filtering

Pi-hole acts as a network-wide DNS filter, blocking ads, malicious domains, and unwanted content for all connected devices.

Implementation Steps :

- Deploy Pi-hole on the Raspberry Pi in a containerized environment.
- Configure Pi-hole as the primary DNS server for the LAN network.
- Define whitelists and blacklists to control domain filtering policies.
- Integrate Pi-hole with OpenWRT firewall rules to ensure all DNS queries pass through the Pi-hole service.
- Test DNS resolution for different scenarios, verifying that malicious or unwanted domains are correctly blocked.

Pi-hole enhances security by preventing exposure to malware and harmful content across the entire network.



Status
Active
18 q/min
Load: 0.03 / 0.02 / 0.00
Memory usage: 4.3 %

hostname: OpenWrt

Total Queries 5,926 — 8 active clients
Queries Blocked 2,615 — List blocked queries
Percentage Blocked 44.1% — List all queries
Domains on Lists 106,206 — Manage lists

Figure 4.11 – PiHole Dashboard

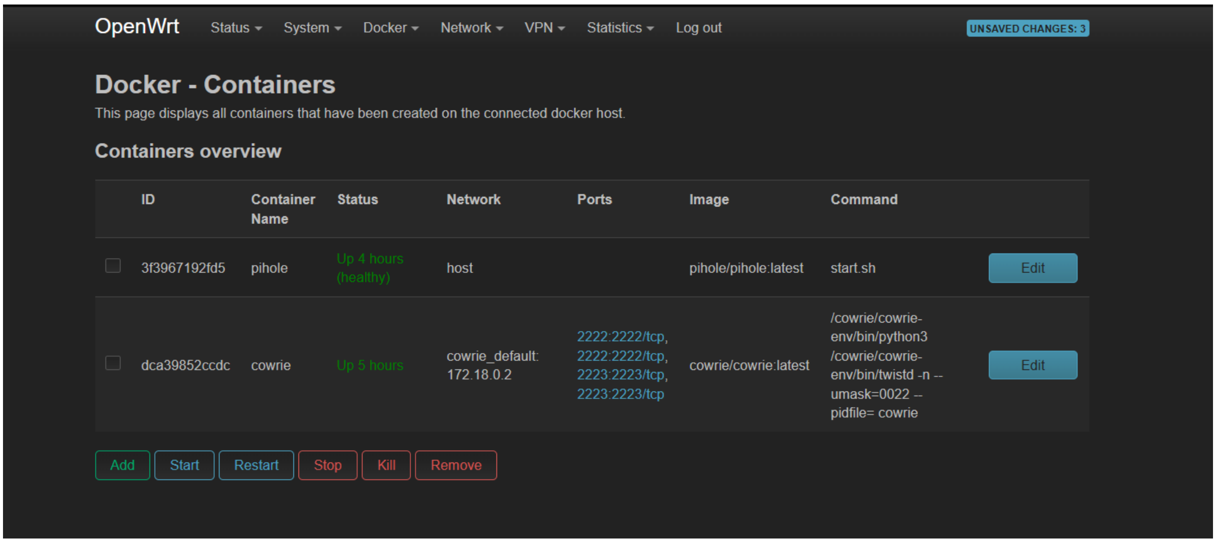
4.2.6 Cowrie Honeypot

Cowrie is a high-interaction SSH and Telnet honeypot used to capture attacker activity and analyze malicious behavior.

Implementation Steps :

— Install Cowrie on the Raspberry Pi or in a Docker container.
— Configure Cowrie to emulate SSH and Telnet services on chosen ports.
— Enable logging of all interactions, including attempted commands, connection details, and malware uploads.
— Optionally forward logs to a centralized monitoring server for analysis.
— Test the honeypot by simulating login attempts to ensure proper logging and activity capture.

Cowrie provides valuable intelligence on attack methods, assisting in proactive security measures and forensic analysis.



Docker - Containers

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

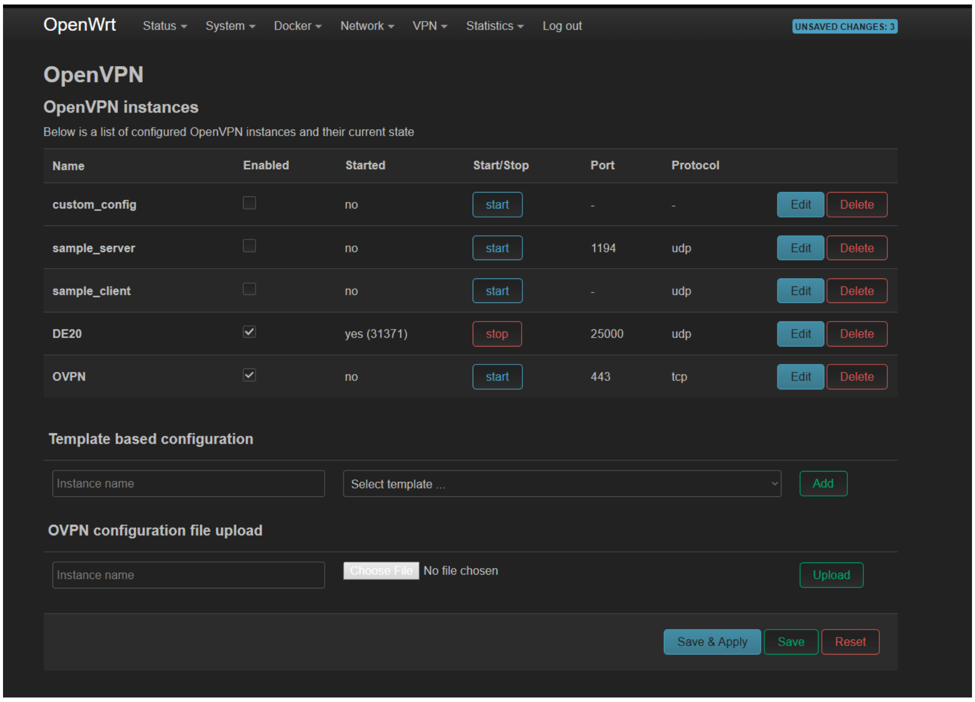
Containers overview

	ID	Container Name	Status	Network	Ports	Image	Command	
□	3f3967192fd5	pihole	Up 4 hours (healthy)	host		pihole/pihole:latest	start.sh	Edit
□	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	Edit

Figure 4.12 – Dashboard Of Containers

4.2.7 OpenVPN Implementation

OpenVPN is used in this project to secure outgoing traffic from the portable router and ensure encrypted communication over untrusted networks. By routing LAN clients' traffic through a VPN tunnel, the system protects user privacy and mitigates risks associated with public Wi-Fi environments.



OpenVPN

OpenVPN instances

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

Name	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	□	no	start	-	-	Edit Delete
sample_server	□	no	start	1194	udp	Edit Delete
sample_client	□	no	start	-	udp	Edit Delete
DE20	☑	yes (31371)	stop	25000	udp	Edit Delete
OVPN	☑	no	start	443	tcp	Edit Delete

Template based configuration

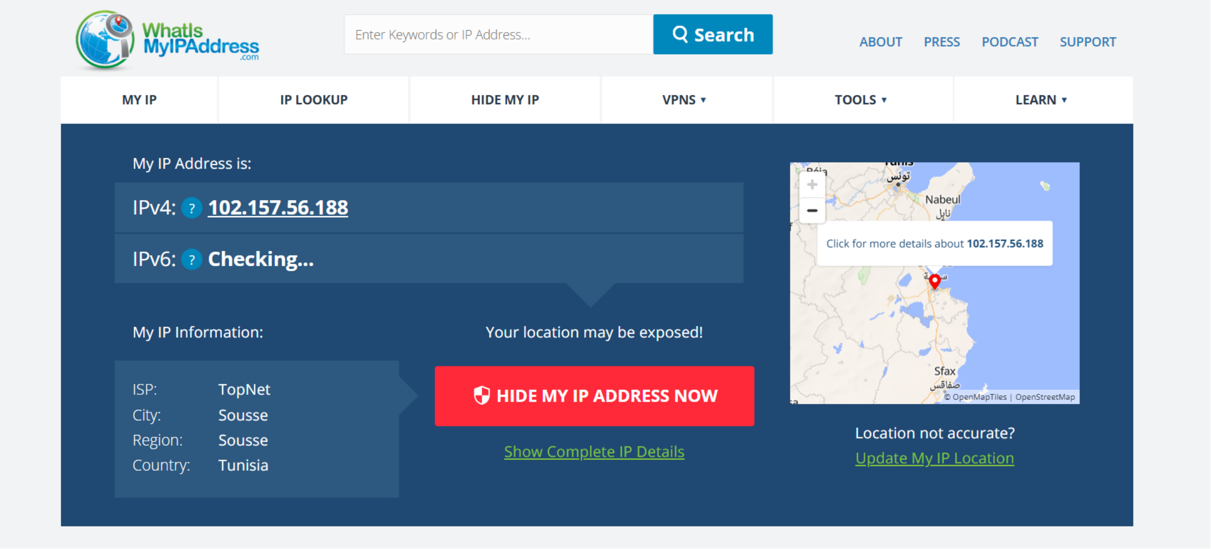
Instance name | Select template ... | Add

OVPN configuration file upload

Instance name | Choose File No file chosen | Upload

Figure 4.13 – OpenVPN Client

OpenVPN strengthens the security posture of the portable router by ensuring confidentiality, anonymity, and protection against traffic interception, especially in public or untrusted environments.



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

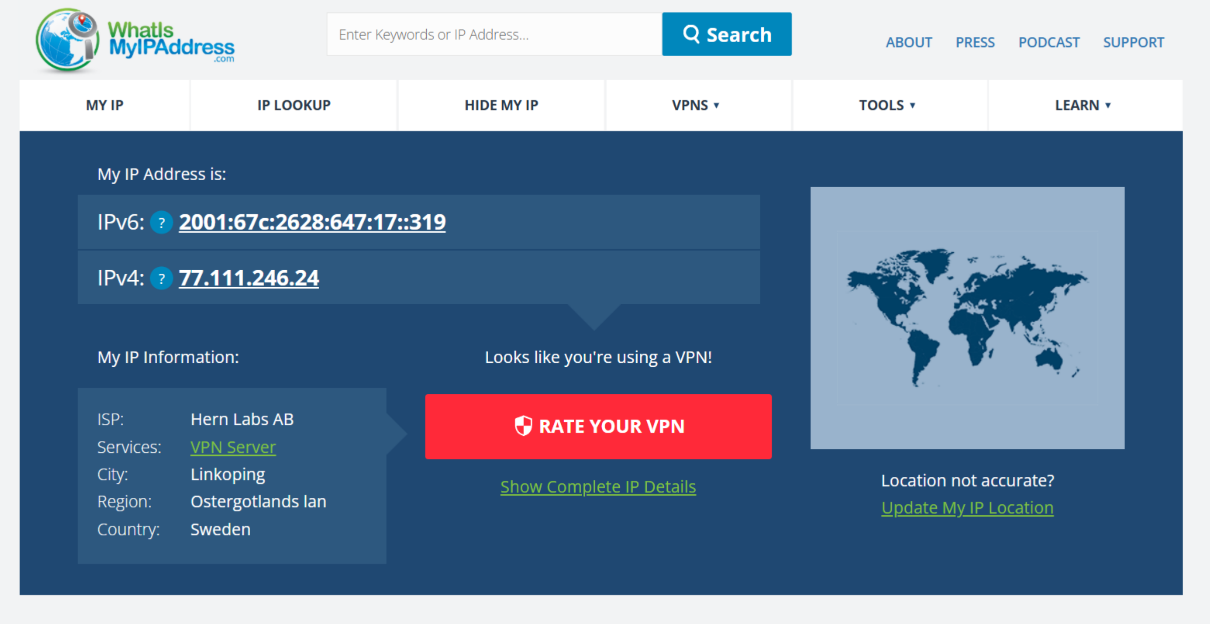
Show Complete IP Details

Click for more details about 102.157.56.188

Location not accurate?

Update My IP Location

Figure 4.14 – Before activating OpenVPN



My IP Address is:

IPv6: ? 2001:67c:2628:647:17::319

IPv4: ? 77.111.246.24

My IP Information:

Looks like you're using a VPN!

ISP: Hern Labs AB
Services: VPN Server
City: Linkoping
Region: Ostergotlands lan
Country: Sweden

Location not accurate?

Figure 4.15 – After activating OpenVPN

Conclusion

The architecture and implementation demonstrate a modular and resilient approach to network security. By combining segmentation, monitoring, traffic filtering, and secure connectivity, the system provides a comprehensive solution for protecting portable networks. The design emphasizes both security and usability, ensuring that the system can operate effectively in diverse scenarios, from home networks to public installations, while maintaining high standards of reliability and performance.

General Conclusion

The evolution of technology has transformed modern networks into the backbone of daily life, enabling smart homes, connected devices, and city-wide infrastructures. This widespread reliance on networked systems, however, comes with increased exposure to cyber threats. The proliferation of attacks, including those launched by non-professional actors and opportunistic individuals, has highlighted the urgent need for robust, adaptive, and portable security solutions.

This project has presented the design and implementation of a secure portable network system, addressing the key challenges of connectivity, monitoring, and protection. By adopting a modular architecture, the system successfully integrates network segmentation, traffic control, intrusion detection, secure communication, and centralized logging, providing a comprehensive framework for defending against modern threats.

The solution demonstrates that portable and flexible security systems can be both effective and practical. It emphasizes proactive monitoring, data confidentiality, and resilient network design, ensuring that the system remains functional and secure even in diverse and potentially hostile environments. Furthermore, the project highlights the importance of combining theoretical knowledge with practical implementation to create security solutions that are adaptable, scalable, and capable of addressing evolving risks.

In conclusion, the project reinforces the critical role of network security in contemporary technology environments. It provides a foundation for further enhancements, including advanced threat detection, automated alerting, and integration with centralized monitoring platforms. This work illustrates that with careful design, even compact and portable systems can deliver high levels of security, contributing to safer networks for both personal and public applications.

—
—
—
—