

# Repurposing Legacy Equipment: A Home Lab for Network Security with pfSense

A. Serdar ŞAHİN

Department of Software Engineering

Ankara Bilim University

Ankara, Turkey

s210204008@ankarabilim.edu.tr

**Abstract**—This project investigates the viability of transforming legacy computing equipment into a personal network security lab using open-source tools. The key components implemented are Suricata, OpenVPN, and pfBlockerNG within a pfSense setup. The resulting environment supports secure access, intrusion detection, and domain/IP filtering, offering a cost-effective alternative for security education and experimentation.

**Index Terms**—pfsense, legacy equipment, home lab, network security, open-source tools

## I. RELATED WORKS

This study [1] focuses on the development of a cyber security laboratory using legacy equipment to support the education of undergraduate students. Although legacy equipment is similarly repurposed to create a secure environment for practicing security applications, my intention is to build a personal home lab that can be expanded to support other networking applications.

The following study [2] describes the process of creating a home laboratory to practice security applications. They used pfSense to create an isolated network and have remote access with openVPN. Aside from pfSense, they had a software platform called "Splunk" for log management, monitoring, and data analysis; and "Security Onion" for network security monitoring, security information and event management, and intrusion detection.

This paper [3] is rather old, but it describes the concept of home server from a holistic perspective that aligns with my vision. Their proposal includes multimedia services, information appliance control services, and information management services. Although my implementation will differ from what is proposed, the paper conveys the general idea that I have for the future steps of my project.

## II. SYSTEM MODEL AND SETUP PROCESS

### A. Preparing the Hardware:

Starting the project, the main driving factor was making use of old equipment. The only piece of new equipment used was a discounted Ethernet adapter; everything else was reused

or repurposed. The following were used for the project: a TP-Link Archer C5v AC1200 router, a computer with an i3-550 processor and 4GB of RAM, a Samsung monitor, a keyboard, a wattmeter, power cables, Ethernet cables, a VGA cable, a DVI to VGA adapter, and a USB Ethernet adapter with an AX88179 chipset.

The installation of OpenWrt on the TP-Link router was initially considered, but the device was a custom model without OpenWrt support. Afterwards, the plan was to set up pfSense on a spare computer and use an Ethernet adapter to connect the TP-Link router, turning it into a wireless access point, as shown in Fig. 1.

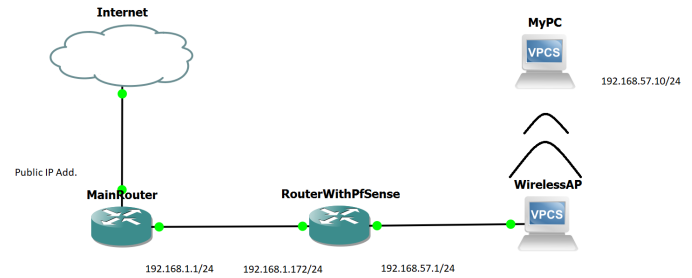


Fig. 1. General network representation

### B. Installing pfSense:

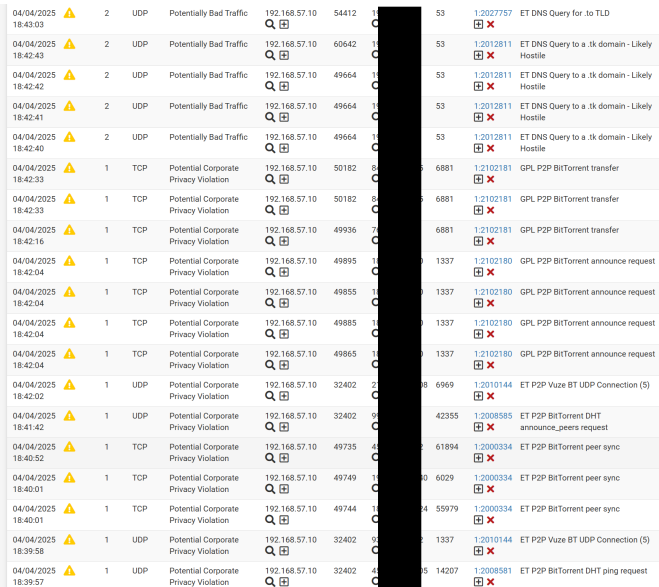
Installation is rather straightforward and well explained on the pfSense documentation webpage [4], and in this tutorial [5]. However, due to the usage of legacy equipment, my installation had some extra steps.

The motherboard on the designated computer was running legacy BIOS, which makes installation using a USB stick impossible. The computer had a DVD-RW installed on it, so the pfSense image was burned to a disc. An installation attempt was made using the disc, but it could not be read. Upon inspection, the drive looked bent and bending it back into shape did not fix the problem. Finally, the image was installed by removing the hard drive and using another computer.

### C. Customization:

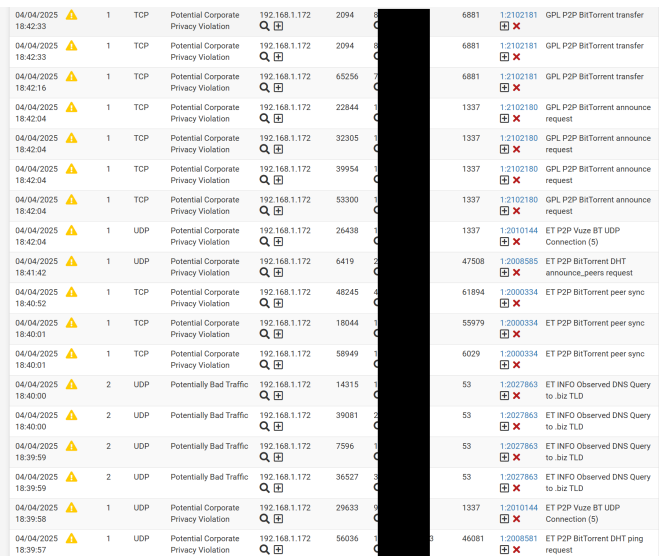
During my customization of pfSense, I experienced many small complications. In this process, I have benefited from the following videos: For Suricata [6], for pfBlockerNG [7], and for OpenVPN [8].

1) *Suricata*: Suricata was installed with the ETOpen Emerging Threats rules and the Snort GPLv2 Community rules. With default settings, it acts as an intrusion detection system (IDS) without blocking any threats. Figs. 3–4 below are from the Alerts section of Suricata, showing example alert entries.



Time	Icon	Rule ID	Rule Name	Action	Source	Destination
04/04/2025 18:43:03	Warning	2	UDP	Potentially Bad Traffic	192.168.57.10	54412
04/04/2025 18:42:43	Warning	2	UDP	Potentially Bad Traffic	192.168.57.10	60542
04/04/2025 18:42:42	Warning	2	UDP	Potentially Bad Traffic	192.168.57.10	49664
04/04/2025 18:42:41	Warning	2	UDP	Potentially Bad Traffic	192.168.57.10	49664
04/04/2025 18:42:40	Warning	2	UDP	Potentially Bad Traffic	192.168.57.10	49664
04/04/2025 18:42:33	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	50182
04/04/2025 18:42:33	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	50182
04/04/2025 18:42:16	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49936
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49895
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49885
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49885
04/04/2025 18:42:02	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402
04/04/2025 18:41:42	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402
04/04/2025 18:42:52	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49735
04/04/2025 18:42:01	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49749
04/04/2025 18:42:01	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49744
04/04/2025 18:39:58	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402
04/04/2025 18:39:57	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402

Fig. 2. Suricata Alerts LAN interface



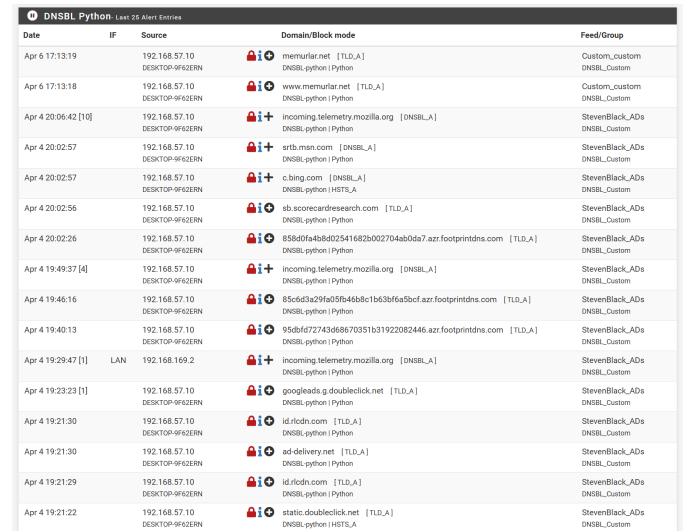
Time	Icon	Rule ID	Rule Name	Action	Source	Destination
04/04/2025 18:42:33	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	2094
04/04/2025 18:42:33	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	2094
04/04/2025 18:42:16	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	45256
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	22844
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	32305
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	39954
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	53300
04/04/2025 18:42:04	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	26438
04/04/2025 18:41:42	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	6419
04/04/2025 18:40:52	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	48245
04/04/2025 18:40:01	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	18044
04/04/2025 18:40:01	Warning	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	58949
04/04/2025 18:40:00	Warning	2	UDP	Potentially Bad Traffic	192.168.1.172	14315
04/04/2025 18:40:00	Warning	2	UDP	Potentially Bad Traffic	192.168.1.172	39081
04/04/2025 18:39:55	Warning	2	UDP	Potentially Bad Traffic	192.168.1.172	7596
04/04/2025 18:39:55	Warning	2	UDP	Potentially Bad Traffic	192.168.1.172	36527
04/04/2025 18:39:58	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	29633
04/04/2025 18:39:57	Warning	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	56036

Fig. 3. Suricata Alerts WAN interface

2) *pfBlockerNG*: GeoIP blocking was set with a MaxMind license key, and a recommended IP block list from the Feeds section was downloaded and used. I created a custom DNS blacklist (DNSBL) group with Steven Black's ADs list, EasyList's Turkish list, and the domain names of websites I wanted to block. Domain names that are in the block list are not resolved by the Unbound DNS resolver. With the custom DNSBL, pfBlockerNG also acts as a network wide ad-blocker. Figs. 5–8 below show examples of a blocked website, pfBlockerNG DNSBL alerts, and ad-blocked websites.



Fig. 4. Example blocked website



Date	IP	Source	Domain/Block mode	Feed/Group
Apr 6 17:13:19	192.168.57.10	DESKTOP-9F6ZERIN	memurfar.net [TLD,A] DNSBL_python [Python]	Custom_custom DNSBL_Custom
Apr 6 17:13:18	192.168.57.10	DESKTOP-9F6ZERIN	www.memurfar.net [TLD,A] DNSBL_python [Python]	Custom_custom DNSBL_Custom
Apr 4 20:06:42 [10]	192.168.57.10	DESKTOP-9F6ZERIN	incoming telemetry.mozilla.org [DNSBL,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 20:02:57	192.168.57.10	DESKTOP-9F6ZERIN	adblock.msn.com [DNSBL,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 20:02:57	192.168.57.10	DESKTOP-9F6ZERIN	c.bing.com [DNSBL,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 20:02:56	192.168.57.10	DESKTOP-9F6ZERIN	sb.scorecardresearch.com [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 20:02:26	192.168.57.10	DESKTOP-9F6ZERIN	858d0fa4b8d52541682b002704ab0da7.azr.footprintdns.com [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:49:37 [4]	192.168.57.10	DESKTOP-9F6ZERIN	incoming telemetry.mozilla.org [DNSBL,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:46:16	192.168.57.10	DESKTOP-9F6ZERIN	55cd32a29fad5b464b1b63f0fa30cf.azr.footprintdns.com [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:40:13	192.168.57.10	DESKTOP-9F6ZERIN	95dbf47274366670351b1922082446.azr.footprintdns.com [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:29:47 [1]	LAN	192.168.169.2	incoming telemetry.mozilla.org [DNSBL,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:23:23 [1]	192.168.57.10	DESKTOP-9F6ZERIN	googleads.g.doubleclick.net [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:21:30	192.168.57.10	DESKTOP-9F6ZERIN	id.ricdn.com [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:21:30	192.168.57.10	DESKTOP-9F6ZERIN	ad-delivery.net [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:21:29	192.168.57.10	DESKTOP-9F6ZERIN	id.ricdn.com [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom
Apr 4 19:21:22	192.168.57.10	DESKTOP-9F6ZERIN	static.doubleclick.net [TLD,A] DNSBL_python [Python]	StevenBlack_Ads DNSBL_Custom

Fig. 5. PfBlockerNG alerts

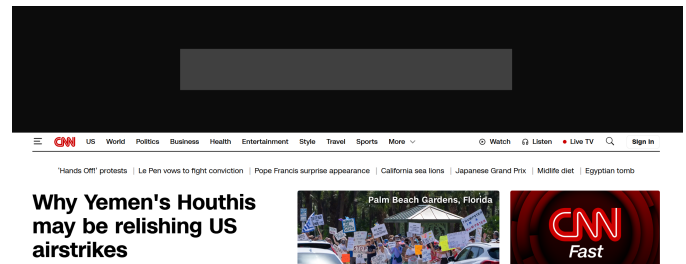


Fig. 6. Example ad-blocked website



Fig. 7. Example ad-blocked website

3) *OpenVPN*: For OpenVPN, a port forwarding rule had to be set on the web interface of the main router. With the port forwarding rule in place, we can use the main router's public address for the VPN connection by connecting the WAN side of the pfSense router to the LAN side of the main router. For the configurations, an address range for the tunnel network and the address of the DNS server for the clients were entered. With the `openvpn-client-export` utility, client configurations or installers can be exported with or without user certificates depending on the server mode configuration. I created a test user in pfSense, downloaded, and ran the installer for Windows. After installation, I entered the test user's credentials into the OpenVPN GUI, successfully connecting to my LAN from the internet. Fig. 9 shows that the IPv4 address of the device is in the tunnel network address range, and Fig. 10 shows that the device is sending its DNS queries to the pfSense router.

```
Unknown adapter OpenVPN TAP-Windows6:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::83ff:1a62
IPv4 Address. . . . . : 192.168.169.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Fig. 8. Ipconfig command on cmd

```
C:\Users\User2>nslookup google.com
Server:  pfSenseSerdar.localdomain
Address:  192.168.57.1

Non-authoritative answer:
Name:     google.com
Addresses: 2a00:1450:4017:811::200e
          172.217.17.142
```

Fig. 9. Nslookup command on cmd

### III. RESULTS

I made use of otherwise obsolete pieces of equipment, temporarily reducing electronic waste. I created a separate network, which allows me to test and experiment without impacting the primary network. And I gained practical experience regarding network traffic analysis and home networking.

Comparing my current setup to a Netgate product of a similar scale such as the Netgate 1100 pfSense+ Security Gateway, while the Netgate product comes with online support and extra functionalities open-sourced Community Edition is sufficient for my needs. Furthermore, Netgate's decision to discontinue the free Home+Lab version of pfSense Plus suggests a shift towards monetizing their user base more aggressively. Consequently, I am hesitant to commit to a Netgate product and would like to keep my options open for an alternative solution such as OPNsense. For costs, as of April 2025, the said Netgate product is listed for 189 USD and consumes less than 5W. In contrast, my setup only had the initial cost of 10 USD from the Ethernet adapter and consumes around 120W. Although the difference in energy consumption is substantial, this is a temporary setup that I plan to upgrade. In addition to the energy consumption difference, my setup is louder and takes up more physical space.

### IV. CONCLUSIONS AND FUTURE WORKS

In conclusion, both on small and large scales making use of legacy equipment can be a cost-effective alternative for non-commercial use, such as a cyber security lab or a home server for beginners. However, especially on a larger scale, the cost of running the hardware and hardware compatibility topics should be thought about.

Moving forward, it is clear that cloud solutions are efficient, but I prefer to avoid paying monthly fees for access to resources that I do not own. It seems more logical to make the time and hardware investments to own what I use. In the near future, my aim is to build on top of this setup to have a home server that is capable of hosting websites and streaming media locally.

### V. ACKNOWLEDGMENT

I would like to thank my instructor Dr. Alican TOPÇU for their guidance and support throughout the project.

### REFERENCES

- [1] M. Ellabidy, C. H. Yu, and M. Yun, "Building a Cybersecurity Lab with Legacy Equipment," in *ICER12016 Proceedings*, pp. 4407–4411, 2016, IATED.
- [2] C. Dadiyala *et al.*, "Designing and Implementing an Effective Cybersecurity Home Lab for Detection and Monitoring," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–8, July 2023.

- [3] C. Bae *et al.*, "Home server for home digital service environments," in *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1129–1135, Nov 2003.
- [4] Netgate, "Installing and Upgrading," Available: <https://docs.netgate.com/pfsense/en/latest/install/index.html>, Accessed: Apr. 1, 2025.
- [5] Lawrence Systems, "2020 Getting started with pfSense 2.4 Tutorial: Network Setup, VLANs, Features & Packages," Available: [https://www.youtube.com/watch?v=fsdm5uc\\_LsU](https://www.youtube.com/watch?v=fsdm5uc_LsU), Accessed: Apr. 1, 2025.
- [6] Lawrence Systems, "Suricata Network IDS/IPS Installation, Setup, and How To Tune The Rules & Alerts on pfSense 2020," Available: <https://www.youtube.com/watch?v=S0-vsJhPDN0>, Accessed: Apr. 1, 2025.
- [7] Lawrence Systems, "Tutorial: pfsense and pfBlockerNG Version 3," Available: <https://www.youtube.com/watch?v=xizAeAqYde4>, Accessed: Apr. 1, 2025.
- [8] Lawrence Systems, "From Ciphers to Certificates: Your Comprehensive Guide to Configuring OpenVPN on pfSense," Available: <https://www.youtube.com/watch?v=I61t7aoGC2Q>, Accessed: Apr. 1, 2025.