WLAN Security Applications Using pfSense.

A. Serdar ŞAHİN
Department of Software Engineering
Ankara Bilim University
Ankara, Turkey
s210204008@ankarabilim.edu.tr

***Abstract*—I had more than a decade old equipment sitting in my room, collecting dust and being an eyesore. I wanted to sell them, but they practically had no resell value. Before throwing them away, I decided to give them a last chance. So I spent several of my weekends trying to set up an environment for myself to practice network security applications, using the open-source pfSense Community Edition to implement a Suricata service, an OpenVPN instance, and IP and DNS blocking using pfblockerNG while making use of existing hardware.**

***Index Terms*—pfsense, legacy equipment, home lab**

I. Related Works

Project with a similar idea but on a bigger scale have been done in this example [1]. The study mentioned above mainly focuses on the creation of a laboratory intended for cyber security education. In addition to creating an environment for practicing security applications, my intention is to build on my project to make it a home lab setup that can also be used for daily activities.

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 intention. 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

A. Preparing the Hardware:

Starting the project, biggest driving factor for me was to make use of old equipment. The only piece of new equipment was a discounted Ethernet adapter, everything else was recycled except the wattmeter that I borrowed. I used the following 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.

I initially considered installing OpenWrt on the TP-Link router, but the device was a custom model for an ISP without OpenWrt support. Then my 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 for my new LAN as shown in Fig. 1.

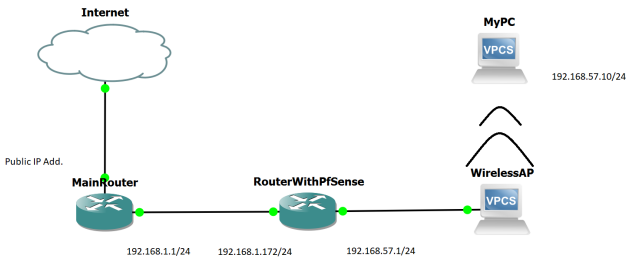


Fig. 1. General network representation

B. Installing pfSense:

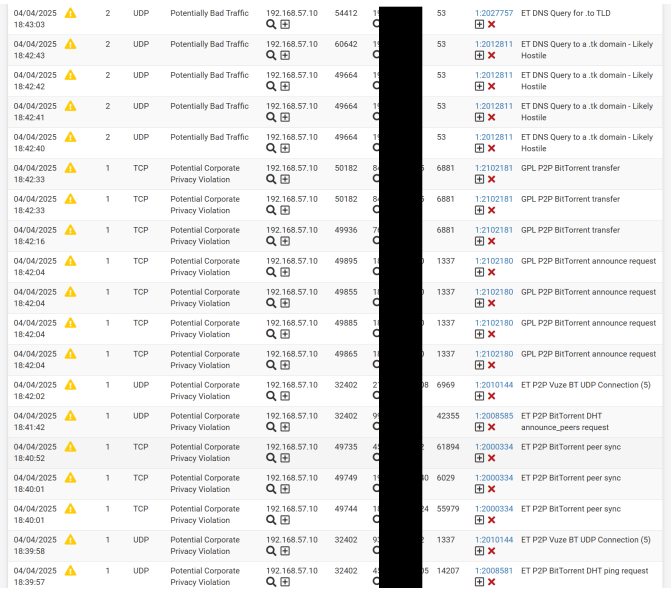
Installation is rather straightforward and well explained on the pfSense documentation webpage [4], and this tutorial [5] But in my case it had some extra steps since I was using legacy equipment.

The motherboard on the designated computer was running legacy BIOS, which made it impossible for me to perform the installation using a USB stick. The computer had a DVD-RW installed on it, so I burned the pfSense image to a disc. Then I tried to use the DVD-RW, but it was not reading the disc. Upon inspection, the drive looked bent. I bent it back into shape, but that did not fix it. So, I decided to remove the hard drive and install the image using another computer. Following this, I reinstalled the hard drive and completed the pfSense setup by following the configuration wizard.

C. Customization:

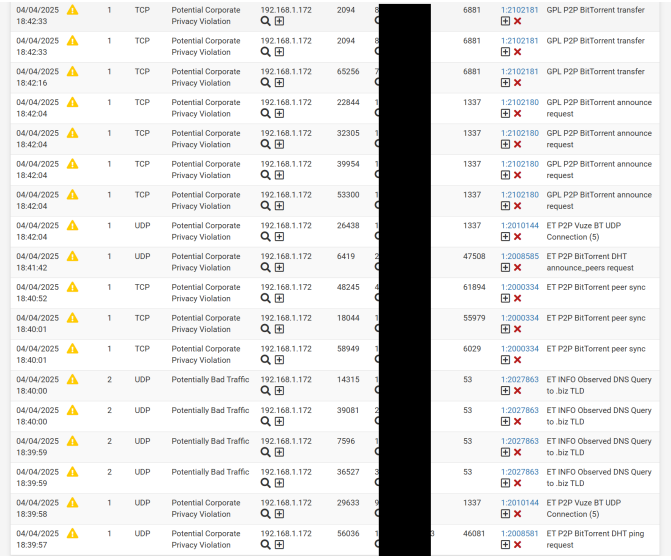
During installation of following services, I have benefited from these videos: For Suricata [6], for pfBlockerNG [7], and for OpenVPN [8]. I experienced small complications during the customization process, but with several reinstallations I figured out my mistakes along the way.

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



04/04/2025 18:43:03	2	UDP	Potentially Bad Traffic	192.168.57.10	54412	[redacted]	53	1:2027757	ET DNS Query for .to TLD
04/04/2025 18:42:43	2	UDP	Potentially Bad Traffic	192.168.57.10	60642	[redacted]	53	1:2012811	ET DNS Query to a .tk domain - Likely Hostile
04/04/2025 18:42:42	2	UDP	Potentially Bad Traffic	192.168.57.10	49664	[redacted]	53	1:2012811	ET DNS Query to a .tk domain - Likely Hostile
04/04/2025 18:42:41	2	UDP	Potentially Bad Traffic	192.168.57.10	49664	[redacted]	53	1:2012811	ET DNS Query to a .tk domain - Likely Hostile
04/04/2025 18:42:40	2	UDP	Potentially Bad Traffic	192.168.57.10	49664	[redacted]	53	1:2012811	ET DNS Query to a .tk domain - Likely Hostile
04/04/2025 18:42:33	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	50182	[redacted]	6881	1:2102181	GPL P2P BitTorrent transfer
04/04/2025 18:42:33	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	50182	[redacted]	6881	1:2102181	GPL P2P BitTorrent transfer
04/04/2025 18:42:16	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49936	[redacted]	6881	1:2102181	GPL P2P BitTorrent transfer
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49895	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49855	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49885	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49865	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:02	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402	[redacted]	6969	1:2010144	ET P2P Vuze BT UDP Connection (5)
04/04/2025 18:41:42	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402	[redacted]	42355	1:2008585	ET P2P BitTorrent DHT announce_peers request
04/04/2025 18:40:52	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49735	[redacted]	61894	1:2000334	ET P2P BitTorrent peer sync
04/04/2025 18:40:01	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49749	[redacted]	6029	1:2000334	ET P2P BitTorrent peer sync
04/04/2025 18:40:01	1	TCP	Potential Corporate Privacy Violation	192.168.57.10	49744	[redacted]	55979	1:2000334	ET P2P BitTorrent peer sync
04/04/2025 18:39:58	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402	[redacted]	1337	1:2010144	ET P2P Vuze BT UDP Connection (5)
04/04/2025 18:39:57	1	UDP	Potential Corporate Privacy Violation	192.168.57.10	32402	[redacted]	14207	1:2008581	ET P2P BitTorrent DHT ping request

Fig. 2. Suricata Alerts LAN interface



04/04/2025 18:42:33	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	2094	[redacted]	6881	1:2102181	GPL P2P BitTorrent transfer
04/04/2025 18:42:33	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	2094	[redacted]	6881	1:2102181	GPL P2P BitTorrent transfer
04/04/2025 18:42:16	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	65256	[redacted]	6881	1:2102181	GPL P2P BitTorrent transfer
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	22844	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	32305	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	39954	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	53300	[redacted]	1337	1:2102180	GPL P2P BitTorrent announce request
04/04/2025 18:42:04	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	26438	[redacted]	1337	1:2010144	ET P2P Vuze BT UDP Connection (5)
04/04/2025 18:41:42	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	6419	[redacted]	47508	1:2008585	ET P2P BitTorrent DHT announce_peers request
04/04/2025 18:40:52	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	48245	[redacted]	61894	1:2000334	ET P2P BitTorrent peer sync
04/04/2025 18:40:01	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	18044	[redacted]	55979	1:2000334	ET P2P BitTorrent peer sync
04/04/2025 18:40:01	1	TCP	Potential Corporate Privacy Violation	192.168.1.172	58949	[redacted]	6029	1:2000334	ET P2P BitTorrent peer sync
04/04/2025 18:40:00	2	UDP	Potentially Bad Traffic	192.168.1.172	14315	[redacted]	53	1:2027863	ET INFO Observed DNS Query to .biz TLD
04/04/2025 18:40:00	2	UDP	Potentially Bad Traffic	192.168.1.172	39081	[redacted]	53	1:2027863	ET INFO Observed DNS Query to .biz TLD
04/04/2025 18:39:59	2	UDP	Potentially Bad Traffic	192.168.1.172	7596	[redacted]	53	1:2027863	ET INFO Observed DNS Query to .biz TLD
04/04/2025 18:39:59	2	UDP	Potentially Bad Traffic	192.168.1.172	36527	[redacted]	53	1:2027863	ET INFO Observed DNS Query to .biz TLD
04/04/2025 18:39:58	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	29633	[redacted]	1337	1:2010144	ET P2P Vuze BT UDP Connection (5)
04/04/2025 18:39:57	1	UDP	Potential Corporate Privacy Violation	192.168.1.172	56036	[redacted]	46081	1:2008581	ET P2P BitTorrent DHT ping request

Fig. 3. Suricata Alerts WAN interface

2) pfBlockerNG: For pfBlockerNG, I set GeoIP blocking with a MaxMind license key and downloaded a recommended IP block list from the Feeds section. I also created a custom DNS black list (DNSBL) group with Steven Black's ADs list, EasyList's Turkish list, and 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.

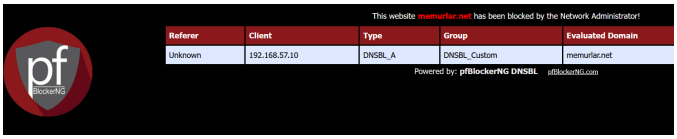
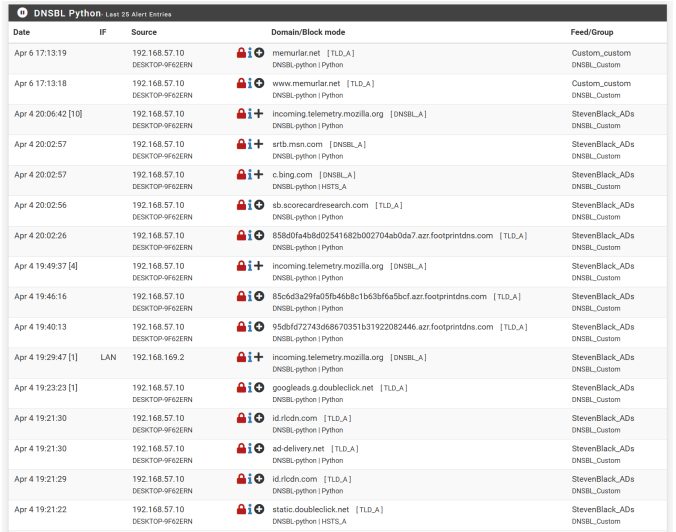


Fig. 4. Example blocked website



DNSBL Python - Last 25 Alert Entries

Date	IF	Source	Domain/Block mode	Feed/Group
Apr 6 17:13:19		192.168.57.10 DESKTOP-9F62ERN	memurlar.net [TLD_A] DNSBL-python | Python	Custom_custom DNSBL_Custom
Apr 6 17:13:18		192.168.57.10 DESKTOP-9F62ERN	www.memurlar.net [TLD_A] DNSBL-python | Python	Custom_custom DNSBL_Custom
Apr 4 20:06:42 [10]		192.168.57.10 DESKTOP-9F62ERN	incoming.telemetry.mozilla.org [DNSBL_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 20:02:57		192.168.57.10 DESKTOP-9F62ERN	srtb.msn.com [DNSBL_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 20:02:57		192.168.57.10 DESKTOP-9F62ERN	c.bing.com [DNSBL_A] DNSBL-python | HSTS_A	StevenBlack_ADs DNSBL_Custom
Apr 4 20:02:56		192.168.57.10 DESKTOP-9F62ERN	sb.scorecardresearch.com [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 20:02:26		192.168.57.10 DESKTOP-9F62ERN	858d0fa4b8d02541682b002704ab0da7.azr.footprintdns.com [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:49:37 [4]		192.168.57.10 DESKTOP-9F62ERN	incoming.telemetry.mozilla.org [DNSBL_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:46:16		192.168.57.10 DESKTOP-9F62ERN	85c6d3a29fa05fb46b8c1b63bf6a5bcf.azr.footprintdns.com [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:40:13		192.168.57.10 DESKTOP-9F62ERN	95dbfd72743d68670351b31922082446.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-9F62ERN	googleads.g.doubleclick.net [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:21:30		192.168.57.10 DESKTOP-9F62ERN	id.rlcdn.com [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:21:30		192.168.57.10 DESKTOP-9F62ERN	ad-delivery.net [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:21:29		192.168.57.10 DESKTOP-9F62ERN	id.rlcdn.com [TLD_A] DNSBL-python | Python	StevenBlack_ADs DNSBL_Custom
Apr 4 19:21:22		192.168.57.10 DESKTOP-9F62ERN	static.doubleclick.net [TLD_A] DNSBL-python | HSTS_A	StevenBlack_ADs DNSBL_Custom

Fig. 5. PfBlockerNG alerts

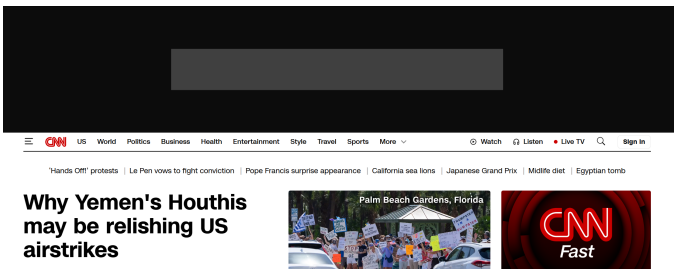


Fig. 6. Example ad-blocked website

Fig. 7. Example ad-blocked website

3) OpenVPN: For OpenVPN, I set up a port forwarding rule on the web interface of my main router. Then I connected the WAN side of the router with pfSense to the LAN side of the original router. I specified an address range for the tunnel network and the address of the DNS server for the clients. With the openvpn-client-export packet, 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 users 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 has sufficient functionality 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 low-cost 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 *ICERI2016 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, 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.