WLAN Security Applications Using pfSense.

A. Serdar ŞAHİN
Department of Software Engineering
Ankara Science 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 get rid of them, but they had practically 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 practise network security applications, using open-source pfSense community edition and with minimal spending while making use of existent 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]. However my project is tailored explicitly regarding my needs, since I am the only user.

Study mentioned above mainly focuses on creation of a laboratory intended for cyber security education. Whereas my intent is to make this project into a home lab setup, which I plan to use for my daily activities as well. Aside from creating a safe network for me to play around; I implemented a Suricata service, an OpenVPN instance and a content filter using pfblockerNG.

Following study [2] describes the process of creating a home lab for cyber security purposes. 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. Just like the previous case, this study is limited to cyber security education. While I have more of a holistic approach to my home lab project.

In this study [3] they talk about an open virtual cloud lab solution for network and security education purposes. This study is related to my project in a sense that, I might have not done a home lab implementation if I had access to a virtual one through my university. I wanted to mention it to show my motivation with a contrast.

This paper [4] is rather old, but they describe the home server concept clearly. Their proposal includes a digital TV service, a remote multimedia service, and an instant message service etc. I wanted to consider it for future steps for my project. Even though my implementation might differ from what is proposed, the paper conveys the general idea.

II. System Model

A. Preparing the Hardware:

Starting the project, biggest driving factor for me was to make use of old equipment. Only piece of new equipment was a discounted Ethernet adapter, everything else was recycled. I used the following for the project: TP-Link Archer C5v AC1200 router, computer with i3-550 processor and 4GBs of RAM, Samsung monitor, power cables, Ethernet cables, VGA cable, DVI to VGA adapter, USB Ethernet adapter with AX88179.

My plan was to set up pfSense on the computer with the monitor connected. Then connect it to my original network, and using the Ethernet adapter turn the specified router to a wireless access point for my new LAN.

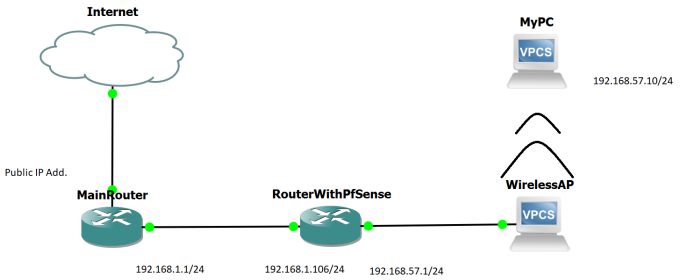

Image 1 = General network representation.

B. Installing pfSense:

Installation is rather straightforward and well explained on pfSense documentation webpage [6], and this tutorial [7] But in my case it had some extra steps since I was using legacy equipment.

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. After I tried to use the DVD-RW, but it was not

functioning properly. So, I took it out of the computer for inspection and it looked bent. I bent it back into place, but it did not work. So, I decided to take out the hard drive and installed the image using another computer. After that I followed the wizard, getting the pfSense up and running.

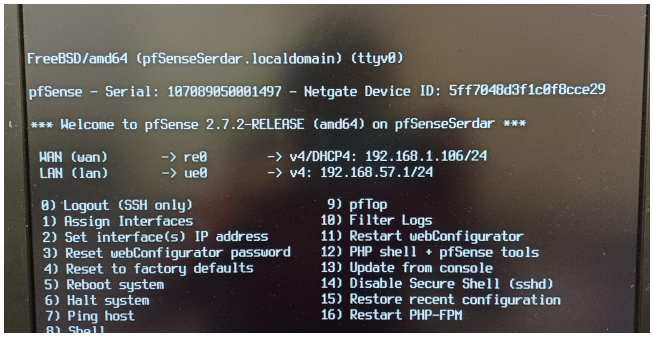

Image 2 = PfSense console.

C. Customization:

During installation of following services, I profited massively from these videos: For Suricata [10], for pfBlockerNG [8], and for OpenVPN [9]. I experienced small complications during the customization process, but figured out my mistakes along the way resulting in several re-installations.

1) Suricata: Installed Suricata with ETOpen Emerging Threats rules and Snort GPLv2 Community rules. I left it with default settings, without any blocking it acts as an IDS.

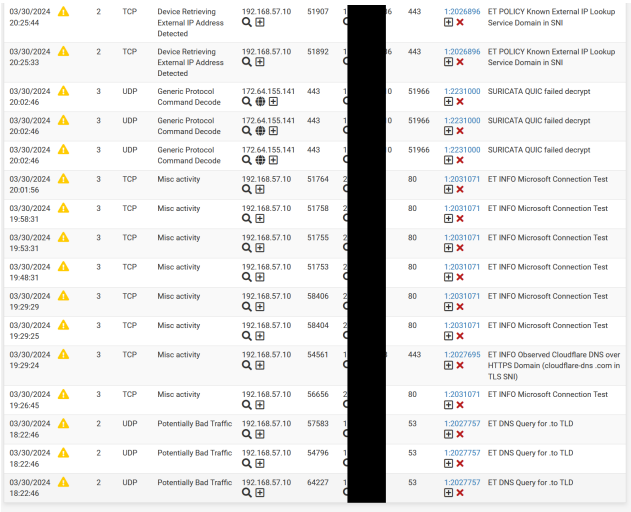

Image 3 = Suricata Alerts.

2) pfBlockerNG: For pfBlockerNG, I set up GeoIP blocking and got a recommended IP block list from the Feeds section. Created a custom group for DNSBL, and verified that my DNS sinkhole was working properly. With that pfBlockerNG also acts as a network wide ad blocker.

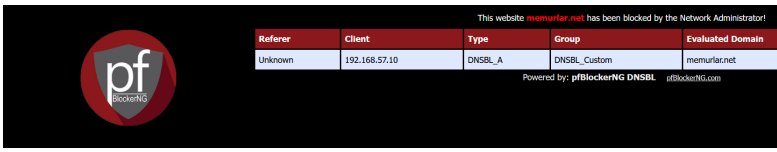

Image 4 = Example blocked website.

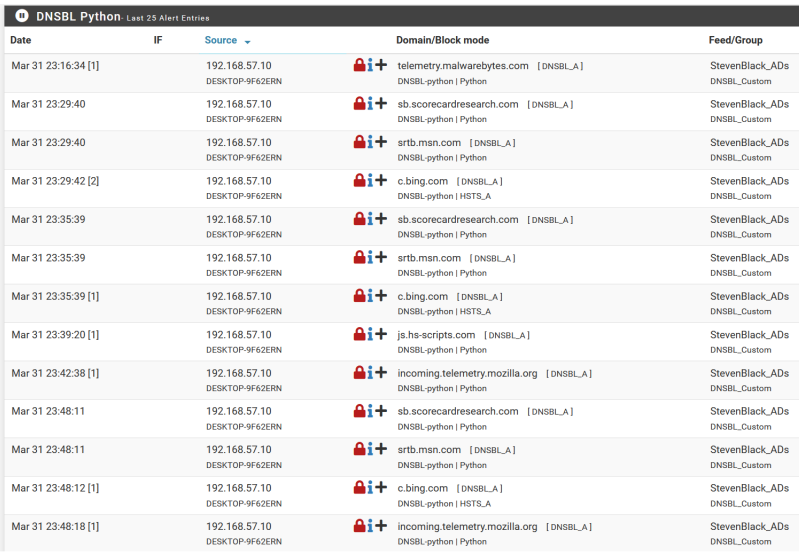

Image 5 = PfBlockerNG Alerts.

Image 6 = Example ad blocked website.

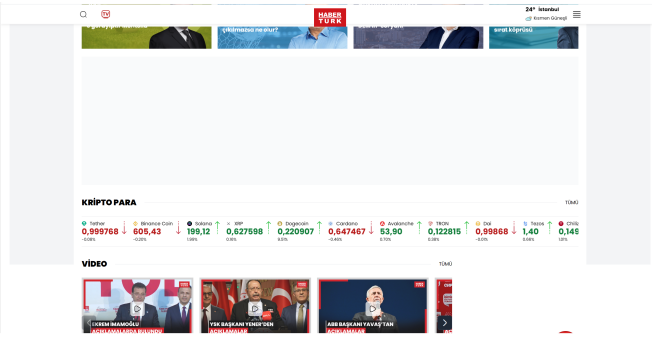

Image 7 = Example ad blocked website.

3) OpenVPN: I was not able to get permission to change my original modem to bridge mode, therefore WAN side of pfSense just connects to LAN side of the original modem. Without a public IP address best came to my mind was to set up a connection from the original LAN to LAN side of pfSense. So I did it, this was rather to see how it works, and gain experience.

```
2024-03-30 21:43:48 OpenVPN 2.6.7 [git:v2.6.7/53c9033317b3b8fd] Windows [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11]
2024-03-30 21:43:48 Windows version 10.0 (Windows 10 or greater), amd64 executable
2024-03-30 21:43:48 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-03-30 21:43:48 DCO version: 1.0.0
2024-03-30 21:43:51 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.106:1194
2024-03-30 21:43:51 UDPv4 link local: (not bound)
2024-03-30 21:43:51 UDPv4 link remote: [AF_INET]192.168.1.106:1194
2024-03-30 21:43:51 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option
2024-03-30 21:43:51 [LANTestServerCA] Peer Connection Initiated with [AF_INET]192.168.1.106:1194
2024-03-30 21:43:52 open_tun
2024-03-30 21:43:52 tap-windows6 device [OpenVPN TAP-Windows6] opened
2024-03-30 21:43:52 Set TAP-Windows TUN subnet mode network/local/netmask = 192.168.169.0/192.168.169.2/255.
2024-03-30 21:43:52 Notified TAP-Windows driver to set a DHCP IP/netmask of 192.168.169.2/255.255.255.0 on i
2024-03-30 21:43:52 Successful ARP Flush on interface [57] {C9CB7D7B-74EC-4494-8A90-BE7B282AF3F1}
2024-03-30 21:43:52 IPv4 MTU set to 1500 on interface 57 using service
2024-03-30 21:43:57 Initialization Sequence Completed
2024-03-30 22:43:27 [LANTestServerCA] Inactivity timeout (--ping-restart), restarting
```

Image 8 = Logs from the OpenVPN app.

III. Results

I made use of otherwise obsolete pieces of equipment, temporarily reducing electronic waste. Created myself a separate network, allowing me to test and play around without disturbing the network in use. Gained practical experience regarding network traffic analysis and home networking.

If we were to compare my current setup to buying a Netgate product for a similar scale e.g. Netgate 1100 pfSense+ Security Gateway, other than pfSense+ (Which is in itself not an absolute positive since I as an individual can profit from open-source community edition version.) it boils down to cost. As of April 2024, said Netgate product is listed for 189 USD and consumes around 0.015 USD worth of electricity per day. Whereas my new setup only has the initial cost of 10 USD from the Ethernet adapter and consumes upto 0.75 USD worth of electricity per day. One net negative of my new setup is that it is mildly loud, ugly and it takes up some space.

IV. Conclusions And Future Works

Both on small and larger scales, making use of legacy equipment for non commercial use is possible. Creating low cost alternatives for either a cyber security lab or a beginners home setup. But especially in larger scale, cost of running the hardware and hardware compatibility topics should be thought about.

Regarding pfSense I would like to make it compliant to CIS pfSense Firewall Benchmark v1.1.0, but I simply ran out of time. Although I am not the intended audience, I would like to go through this study [5] to implement CIS Critical Security Controls on my network.

As mentioned in related works section, I would like have a home server [4]. It is a fact that cloud solutions are efficient, but I do not want to pay monthly fees to have an ”access” and not own anything. As of today it seems more logical to make some time and hardware investments to own what I use. In the near future, I aim to transform this to a proper home laboratory. From website hosting to having my own media server to stream movies.

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] Y. Maleh *et al.*, “Building open virtual cloud lab for advanced education in networks and security,” in *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1–6, Nov 2017.

[4] 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.

[5] B. Shamma, “Implementing CIS Critical Security Controls for Organizations on a Low-Budget,” Ph.D. dissertation, University of Houston, 2018.

[6] Netgate, “Installing and Upgrading,” Available online: https://docs.netgate.com/pfsense/en/latest/install/index.html, Accessed: 01.04.2024.

[7] Lawrence Systems, “2020 Getting started with pfSense 2.4 Tutorial: Network Setup, VLANs, Features & Packages,” Available online: https://www.youtube.com/watch?v=fsdm5uc_LsU, Accessed: 01.04.2024.

[8] Lawrence Systems, “Setup Guide / Tutorial for pfBlockerNG 2.2.5 on pfSense with DNSBL & GeoIP Blocking,” Available online: https://www.youtube.com/watch?v=OJ8HHwpGxHw, Accessed: 01.04.2024.

[9] Lawrence Systems, “From Ciphers to Certificates: Your Comprehensive Guide to Configuring OpenVPN on pfSense,” Available online: https://www.youtube.com/watch?v=I61t7aoGC2Q, Accessed: 01.04.2024.

[10] Lawrence Systems, “Suricata Network IDS/IPS Installation, Setup, and How To Tune The Rules & Alerts on pfSense 2020,” Available online: https://www.youtube.com/watch?v=S0-vsjhPDN0, Accessed: 01.04.2024.