

# Using Tailscale and PfSense for Security and Anonymity of IoT Environments

Daniel-Florin Hrițcan, Doru Balan  
 Dept. of Computers, Automation and Electronics  
 University "Ștefan cel Mare" Suceava  
 Suceava, Romania  
 daniel.hritcan@usm.ro,  
 dorub@usm.ro

**Abstract**—The mission of researching security solutions that can help IoT infrastructures grow has become an especially important topic these days. Around the world many people are trying day by day to find the next best solutions or improve and optimize the existing ones, thus giving an edge to companies and even governments that invest in the field of IoT. Unfortunately, like those people who are trying to develop protection solutions, there are always the same amount or more people who are finding and developing exploits to break or even bypass the protection. In this paper, the approach to security is a little bit different and includes the part that is not so commonly debated, that being the anonymity of a network over the internet. This concept might sound strange, but it makes sense because for a potential attacker becomes a challenge to start breaking after he or she knows about a particular network.

**Keywords**—IoT; Tailscale; pfSense; VPN; Wireguard; encryption;

## I. INTRODUCTION

A large portion of the data gathered by IoT devices within smart environments is typically stored on web-accessible platforms such as the "Cloud." Numerous IoT devices and systems reliant on cloud infrastructure are recognized to possess security weaknesses, rendering them susceptible to hacking and cyber threats. Furthermore, data transmissions, including video data from cameras, may occur without encryption when transmitted over the Internet [1].

Newly developed technologies are being leveraged to combat security risks within the realm of IoT, including blockchain, fog computing, and machine learning. These innovations bolster security by incorporating decentralized data storage, localized data processing, control over access, and the detection of potential threats. Furthermore, it underscores the multitude of hurdles in IoT security, ranging from authentication and authorization issues to access control dilemmas and concerns regarding privacy. In conclusion, it stresses the critical nature of tackling these obstacles to ensure the ongoing advancement of IoT security [2].

For now, in IoT environments, the security solutions that are usually used nowadays by many people revolve around some form of encryption of the data acquired by the sensor networks

in the field. Also, after encrypting the data, it could be sent by using either VPN protocols or some other protocols that can use SSL/TLS certificates for encryption. As mentioned in [3], security concerns endure when accessing data via public networks, where data might lack adequate encryption and be vulnerable to unauthorized access. As a solution, a preliminary design for a Virtual Private Network (VPN) is suggested, utilizing for its many advantages a Raspberry Pi device to create a VPN gateway link connecting home networks with Internet Service Provider (ISP) networks. This setup guarantees both security and expandability for household systems. The document emphasizes the importance of VPNs in guaranteeing protected communications, especially in the context of IoT devices.

According to [4], the significance of ensuring secure communication in IoT is emphasized, drawing attention to the dangers linked with transmitting data without encryption, such as potential "man in the middle" attacks. As a precautionary measure, an architecture utilizing SSL/TLS v1.2 certificates for secure communication over port 8883 the secured option of Message Queuing Telemetry Transport (MQTT) protocol is suggested. Additionally, firewalls are configured to guarantee security.

## II. TECHNOLOGIES USED

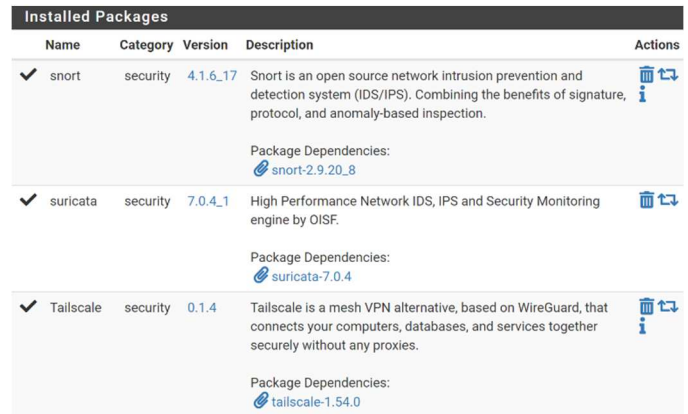
### A. PfSense

Primarily pfSense is utilized as either an external or internal firewall and router for small to medium-sized enterprises. Positioned as an external firewall, pfSense typically resides at the network's perimeter, shielding the internal network from external threats, a capability further enhanced by its Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). When employed as an internal firewall, it safeguards internal resources and segments the network. Moreover, pfSense is widely esteemed for its role in facilitating VPN connectivity, implementing traffic shaping, and providing access to other advanced networking functionalities. Countless enterprises, educational establishments, governmental entities, and non-governmental organizations spanning all seven continents have placed their trust in pfSense software to meet their secure networking requirements over the years [5].

Some capabilities of pfSense according to [6] can include the following:

- LAN/WAN router, linking local and wide area networks. A LAN comprises interconnected devices sharing a communication line, typically within a confined space like an office.
- Wi-Fi hotspot or captive portal, offering superior functionality compared to standard small office/home office (SOHO) security devices. Notably, it can host guest Wi-Fi networks beyond the primary firewall and even employ a distinct public IP for NAT purposes.
- A VPN router enhances security and privacy for both private and public networks like Wi-Fi hotspots and the internet, commonly employed by businesses to protect confidential information. Virtual Private Network appliance, provides VPN features seamlessly alongside existing firewall setups, supporting multiple VPN protocols.
- pfSense software is primarily utilized as a perimeter firewall, commonly supporting networks with various internet connections, local area networks (LANs), and demilitarized zone (DMZ) networks.
- DHCP / DNS Server that enables centralized control over device network configurations, automating IP address allocation even during device relocation. It works seamlessly with both IPv4 and IPv6. Utilizing DHCP and domain name resolution directly on the firewall streamlines network traffic configuration to precise requirements.
- Multi-WAN Router or Load Balancer, capable of distributing and managing traffic from a LAN across multiple internet connections. It employs load balancing to evenly distribute traffic across available WANs and automatically switches to backup connections if one fails, minimizing user latency.
- Port Forwarding and NAT (Network Address Translation), which enables a firewall to assign public addresses to computers within a private network. Acting as gateways between internal and external networks, NAT devices enhance security by preventing direct access to internal network systems from external sources.

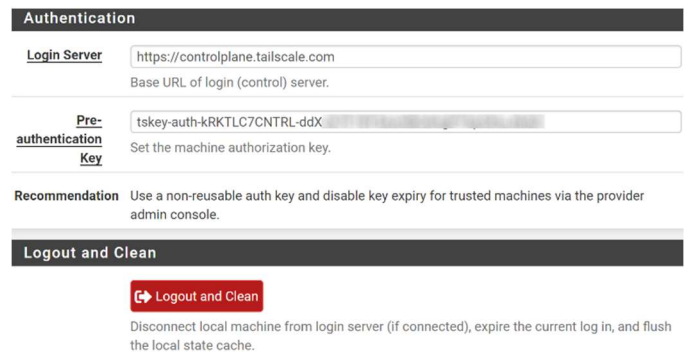
In this paper, the pfSense software was installed on a machine with an x86 architecture processor, 4 gigabytes of RAM, and 404 gigabytes of storage space. These specifications are enough for lab testing and even a small business. The version of the installed software is the latest community one, in other words free of charge.



Installed Packages				
Name	Category	Version	Description	Actions
✓ snort	security	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.  Package Dependencies: snort-2.9.20_8	🗑️ ↺ ⓘ
✓ suricata	security	7.0.4_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF.  Package Dependencies: suricata-7.0.4	🗑️ ↺ ⓘ
✓ Tailscale	security	0.1.4	Tailscale is a mesh VPN alternative, based on WireGuard, that connects your computers, databases, and services together securely without any proxies.  Package Dependencies: tailscale-1.54.0	🗑️ ↺ ⓘ

Fig. 1. Pfsense package manager panel.

The first figure shows the package manager available by accessing the tab “System” in the main menu. PfSense allows the installation of different plugins that can add even more capabilities to it, like intrusion detection and intrusion prevention systems. The plugin that is used in this paper, which stands as the base for this solution is called Tailscale. Right now the compatible version that is installed and used is 0.1.4, but in the future, if there are updates, the package manager will warn us to install the latest one. Making this operation much easier for any user even whether they have a technical background or not.



**Authentication**

**Login Server**   
Base URL of login (control) server.

**Pre-authentication Key**   
Set the machine authorization key.

**Recommendation** Use a non-reusable auth key and disable key expiry for trusted machines via the provider admin console.

**Logout and Clean**

Disconnect local machine from login server (if connected), expire the current log in, and flush the local state cache.

Fig. 2. Tailscale authentication panel.

The second figure presents the authentication page of Tailscale which can be accessed from the “VPN” tab in the main menu. As it can be seen the first field contains the address of the Tailscale network control panel and the second field represents the access key necessary to gain access to the network. For security reasons, a part of the key was blurred out. To get this key, it is necessary to generate one from the control panel associated with the account created on the official platform.

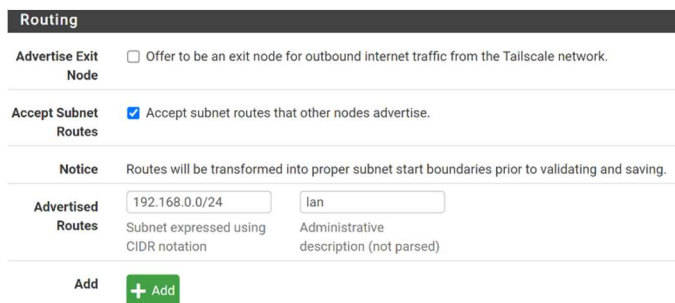


Fig. 3. Tailscale subnet exposure.

After a successful connection from the pfSense side to the Tailscale main network a route needs to be given in the image from above showing how to add a subnet that inside the firewall is most likely associated with an interface that provides internet connection to everything that is connected to it. In the case of implementing this for IoT environments, this could be an isolated interface that could not compromise the entire network managed by the firewall. This is an additional good practice for enhancing security inside a network.

**B. Tailscale**

Originally designed for developers collaborating across various networks, Tailscale is a highly effective application that ensures security on public Wi-Fi networks, offers convenient device connectivity, and prevents file access obstacles between work and home locations.

Despite being open-source software, which typically lacks user-friendly installers and comprehensive documentation, Tailscale defies expectations with its user-friendly interface. Setting up is straightforward for Tailscale, just sign up for an account and install the client on all your devices, including laptops, desktops, smartphones, and tablets. Once logged in, Tailscale establishes a private network connecting all your devices regardless of their physical location [7]. A few of the main features that are provided by this platform are:

- Peer-to-peer connections

Tailscale employs the WireGuard VPN protocol to establish fast, direct connections between peers, ensuring minimal latency.

- Split tunneling

Split tunneling optimizes latency by directing only internal network traffic through the VPN while allowing other traffic to bypass it.

- Short DNS hostnames

MagicDNS automatically registers DNS names to make them more easily readable by humans, enhancing discoverability.

- IP space collision resolution

To facilitate routing traffic between overlapping IPv4 subnets without requiring renumbering, 4via6 subnet routers are employed. This is achieved by assigning distinct IPv6 addresses to each subnet, allowing seamless communication while maintaining individual subnet integrity.

- End-to-end encryption

Tailscale employs the WireGuard VPN protocol to ensure robust end-to-end encryption, safeguarding data transmission across networks with high-security standards.

- Exit node

Direct all network traffic through a specified egress point, akin to the functionality of a privacy-focused VPN service [8].

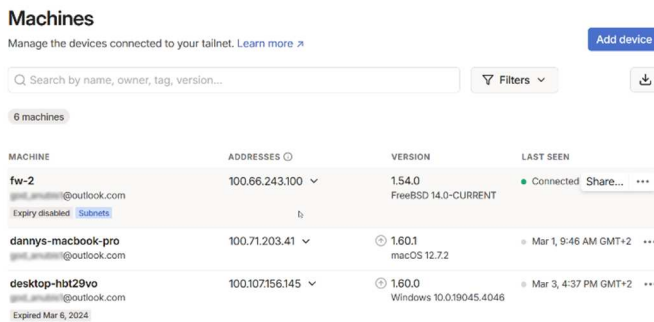


Fig. 4. Tailscale dashboard with connected devices.

Figure 4 represents the main dashboard that contains all the devices enrolled in the private network. Each device comes with a set of information that represents the IP address associated with the network, the version of the client installed on that specific device, and the connection status.

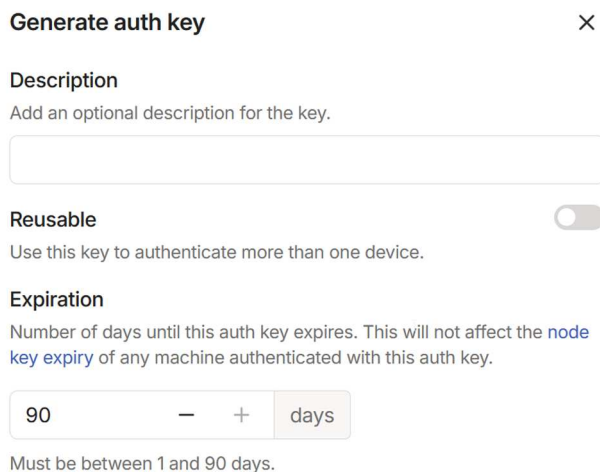


Fig. 5. Tailscale authentication key generation.

As mentioned earlier in the paper, to authenticate the client installed on the pfSense side it is necessary to generate a key from the Tailscale dashboard. In the image above it is presented how to generate such with and what particularities it needs to have in the end. Two of the most important particularities are the expiration period which can be between 1 to 90 days and if the key could be used just with one device or more. Another option that could be selected while generating the key that is not so often used is addressing the device settings which is called ephemeral. When this is used all the devices that were enrolled with this key, will be automatically removed from the main dashboard if the devices are compromised, lose connection or power, and go offline.

### C. Raspberry Pi

When it comes to implementing an IoT network with different devices and sensors in the field, mainly in remote locations where there is no power grid or stable internet connection the best solution is to use devices that consume a small amount of power and have GSM capabilities. That's why a single board computer like a Raspberry Pi would be a good compromise because it has a good amount of computing power and is compatible with Tailscale client, while it could be powered from a 5V power bank.

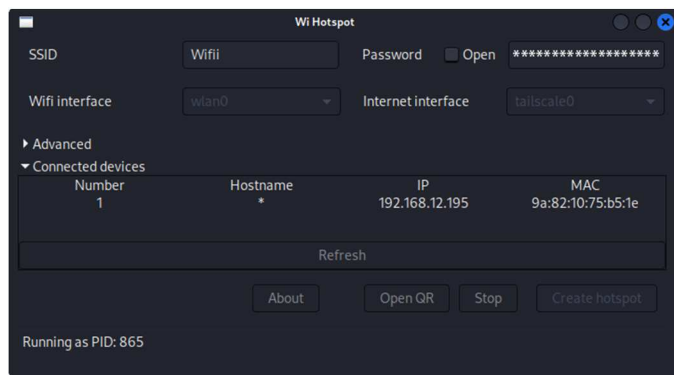


Fig. 6. Wi-fi hotspot gateway on Raspberry Pi.

Figure 6 shows the Wi-Fi hotspot app installed on the Raspberry Pi transforming it into a gateway that is connected to the Tailscale private network, thus giving access to all devices and sensors that could connect to this hotspot.

### III. TESTING RESULTS

In the testing phase, the preferred operating system was Kali Linux, because of its stability being based on Debian. Besides the stability, the other advantages of this operating system are the tools destined for penetration testing and network analysis.

One of the most used tools to analyze networks is called Nmap and for testing the solution proposed in this paper was employed.

TABLE I. TESTING WITH NMAP

Nr.	Scanned ports with classic VPN		
	Ports	Open	Closed
1.	1194	√	
2.	51820	√	

In the table above the scan was made on the public IP address and the ports of the classic VPN protocols like OpenVPN and Wireguard were discovered. Normally this must be happening because otherwise the connection between client and server won't happen and there is no use. Many people would say that there must be no problem because the protocols used by VPNs are encrypted and the data must be decrypted to be usable. This presumption is valid because decrypting data needs a lot of computing power and very advanced algorithms that are not at the disposal of any random attacker. The most common way to

compromise entire servers is usually distributed denial of service (DDOS) attacks by making use of thousands sometimes even millions of compromised computers around the world that are part of what is called a Botnet.

When using the solution proposed in this paper based on the Tailscale private network, scanning with Nmap will find no port open. If there is no port open usually an attacker would not know the public IP address because it has no use anywhere.

### IV. CONCLUSIONS

A first conclusion would be that IoT technologies are now expanding at an accelerated rate and security plays a critical role in ensuring this growth. Simple solutions are now beginning to get overwhelmed and that's why researching for better new ones should be the main focus.

Based on the Nmap tests in this paper it is clear that attackers will always try to exploit anything they can to achieve their final goal. Opening ports and exposing public IP addresses could be fatal in some cases especially when a potential attacker has some form of zero-day exploit that is not known or patched.

It could be a good practice to implement solutions that will anonymize the traffic and even the network by itself, especially now that there are technologies like Tailscale that allow such implementation.

### ACKNOWLEDGMENT

This work was supported by the project Integrated Center for Research, Development, and Innovation in Advanced Materials, Nanotechnologies, and Distributed Systems for Fabrication and Control (MANSiD).

### REFERENCES

- [1] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kemande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in *IEEE Access*, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
- [2] Singh, G. Singh and S. Negi, "Evaluating Security Principals and Technologies to Overcome Security Threats in IoT World," 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2023, pp. 1405-1410, doi: 10.1109/ICAAIC56838.2023.10141083.
- [3] J. R. Raj and S. Srinivasulu, "Design of IoT Based VPN Gateway for Home Network," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 561-564, doi: 10.1109/ICEARS53579.2022.9751838.
- [4] N. Nikolov and O. Nakov, "Research of Secure Communication of Esp32 IoT Embedded System to.NET Core Cloud Structure using MQTTS SSL/TLS," 2019 IEEE XXVIII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 2019, pp. 1-4, doi: 10.1109/ET.2019.8878636.
- [5] "What is pfSense best for?," Itandgeneral, 2022. [Online]. Available: <https://www.itandgeneral.com/about-pfsense/>. [Accessed: 08-March-2024].
- [6] "What Are The Popular Uses for pfSense® software?," Zenarmor, 2020. [Online]. Available: <https://www.zenarmor.com/docs/network-security-tutorials/pfsense/>. [Accessed: 10- March- 2024].
- [7] Matt Haughey, "How to reach any of your devices from anywhere with Tailscale", Zapier, 2023. [Online]. Available: <https://zapier.com/blog/what-is-tailscale>. [Accessed: 12- March- 2024].
- [8] "Features", Tailscale, 2019. [Online]. Available: <https://tailscale.com/features>. [Accessed: 12- March- 2024].