International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I8P108

Volume 72 Issue 8, 62-72, August 2024
© 2024 Seventh Sense Research Group®

Original Article

Design of a pfSense-based Wireless Network to Transition from the Use of Proprietary Software in the Campus of the University of Sciences and Humanities, Lima, Peru

Jacqueline Coquis-Flames[1], Hugo Flor-Cunza[1], Alicia Alva-Mantari[2]

[1]*Faculty of Sciences and Engineering, University of Sciences and Humanities, Lima, Perú.*
[2]*Image Processing Research Laboratory (INTI-Lab), University of Sciences and Humanities, Lima, Perú.*

[2]*Corresponding Author : aalva@uch.edu.pe*

Received: 15 February 2024 Revised: 17 June 2024 Accepted: 06 July 2024 Published: 28 August 2024

Abstract *- The present work is the proposed design for the wireless network of the University of Sciences and Humanities to transition from the current design that uses the proprietary software of Ruckus Networks to a free and open-source option with pfSense to lower the costs and maintain a high level of security. In the present time, it is very important to keep the information secured, technological development has also given hackers new ways to attack networks and obtain private information, and universities and educational institutions are also at risk of intrusion from attackers. In this sense, universities need to ensure that the network on the campus has all of the proper measures in place to prevent the loss of information. For the design of the proposed network for the University of Sciences and Humanities, the configuration of pfSense was done on VirtualBox, and four VLANs were created with firewall rules to ensure higher security. Finally, the proposed network design and the firewall rules were tested with a simulation in which pfSense was installed on a laptop to act as a server. The Results show that the firewall rules and the proposed design operate appropriately for the needs of the university campus.*

Keywords *- pfSense, Ruckus networks, Network security, Virtual machine, VirtualBox.*

1. Introduction

In the present time, cybersecurity is a challenge for all the different organizations and institutions since it is vital to make sure that the internal system does not allow access to attackers who want to access the information for personal benefit. There are many cases in which the methods applied for system protection and prevention of attacks have not been enough, and attackers have stolen valuable data. In 2016, the University of Calgary was impacted by a ransomware attack, and the University had to pay the attackers an amount of 20,000 dollars to prevent the disclosure of private information [1]. In 2020, Dundee and Angus College suffered a ransomware incident in which the entire network stopped working, and it was not possible to communicate through the system since file servers had been encrypted, the database for the Virtual Learning Environment and the student database were not affected. Despite the disturbance caused, Dundee and Angus College was able to recover in a matter of weeks [2]. When a network does not have the proper security systems in place, this can lead to loss of information and a waste of time and money to repair the structures. The University of Sciences and Humanities is located in Lima, Peru, with a total of 3507 students; it has an internal wireless network security system based on equipment from the company named Ruckus Networks and its proprietary software[24]. Ruckus Networks is an American company acquired by CommScope that manufactures equipment for wired and wireless networks. At the University of Sciences and Humanities, the main devices being used for the functioning of the wireless network are three models of access points (Ruckus R500, Ruckus R310 y, Ruckus T300), and a Zone Director ensures that the access points are synchronized, adjusts their frequencies and transmission power.

Nevertheless, Ruckus Networks also has a history of vulnerabilities; in the 36th Chaos Communication Congress carried out in Leipzig, Germany, in 2019, the speaker Gal Zror showed a series of vulnerabilities that were found on Ruckus devices [3]. The Cybersecurity & Infrastructure Security Agency also added these vulnerabilities to their Catalog of Known Exploited Vulnerabilities, and in 2023, more weaknesses were found and given identification numbers in the catalogue [4][5]. These vulnerabilities put Ruckus Networks's clients at risk of an attack on their networks.

It is vital in a university to ensure that the information in the system is well protected; this is the reason why it is important to execute a transition to pfSense, a free and open-source firewall with threat management. This software dcan enhance the security of the system and also allow for the use of a wider variety of equipment for the deployment of the network. The objective of this study is to design and plan a transition from the current proprietary software in use at the University of Sciences and Humanities to the free and open-source option pfSense.

2. Literature Review

In [6], the authors indicate that in recent years, the number of cyberattacks and security threats has been increasing in frequency, and the refinement of the methods used by attackers to access information and breach system rules has become more modern. In this sense, they mention that firewalls have become an essential part of the cybersecurity architecture in any business. Therefore, they present the development of a hybrid intrusion detection system based on Suricata with pfSense with the objective of helping businesses stay protected against threats and cyberattacks through a reduction of DDoS attacks on IPv6 networks. They use the Suricata packet on pfSense as an intrusion detection system to identify the destination of Distributed Denial of Service attacks so that the pfSense firewall can block the packets sent by an attacker. The results showed a decrease in CPU utilization by 81.23%, from 78.3% to 14.7%, there was an increase of 57.32% in the average number of packets sent, the jitter value decreased by 88.78% and an increase of 1.08% in throughput value, which shows more efficiency in data transmission. The authors concluded that the combination of pfSense and Suricata proved to be a successful way of protecting the network against DDoS attacks, including the ones using IPv6.

In [7], the author indicates that cyber-attacks, with the development of technology, have also been becoming more sophisticated and keep on representing a major threat to all kinds of organizations. Therefore, the author proposes the adoption of an Intrusion Detection System (IDS) in academic institutions for early detection of network attacks and allow the prevention of intrusion. The objective is to adapt an IDS for academic institutions, Snort is chosen as an IDS and is downloaded as a package on the pfSense software. The results showed that the Snort IDS allows the effective detection of intrusions to the system and suspicious behaviour by sending alerts and performing inspection of traffic. The author concludes that the study performed was able to identify the necessary process and configure the system to accommodate user requirements and recommends adding the appropriate number of rules to the IDS and performing regular updates. In [8] the authors indicate that with the development of technology and the advancement of the internet, the number of threats to web applications has been growing and affects the availability of the service and risks the confidentiality of the information. In this sense, the authors have used the pfSense firewall and Apache Mod-Security for protection to a server and their main objective is to focus on the current vulnerabilities in web application technologies. The authors did their work in four stages: during the first stage, they implemented a fully functioning network; in the second stage, they detected vulnerabilities in the network; in the third stage, they deployed Mod-Security for Apache alongside Snort; and in the fourth stage, they enhanced the performance. The results showed that most of the exploitation attempts were successfully blocked, but some vulnerabilities were not blocked by their implementation, and 10-20% of the performance was lost due to the tools that were used, which is why they concluded that web application evolvement is key to accomplishing a more secure application.

In [9] the authors mention that ensuring network server security is vital for good availability of service in the systems. In this context, the authors propose the implementation of a security system for networks using Honeypot in combination with the Snort package on the pfSense software at Muhammadiyah University of East Kalimantan. Their objective is to implement honeypots to keep attackers from getting to their intended target. The methodology shows that they have implemented the pfSense firewall with Snort IDS and have created the Honeypot using PentBox. They opened port 80 to make attackers believe it is a weak point in the network, but instead, it is going to record the suspicious activities providing the information needed on the techniques they have used and use it to protect the network further. To test the system, they used the Slowloris attack with the Denial of Service (DoS) method, GoldenEye with the Distributed Denial of Service (DDoS) attack and LOIC (Low Orbit Ion Cannon) testing also with the DDoS attack method. The results showed that the combination of both software increased the network's overall security. Honeypot detected the Slowloris attack in 2 seconds and by Snort in 180 seconds; for the GoldenEye attack, the Honeypot was able to detect it in 2 seconds and by Snort in 120 seconds. Finally, for the LOIC attack, Snort was able to detect it in 180 seconds. The authors concluded that Honeypot was able to detect Slowloris and GoldenEye attacks successfully, and pfSense was able to provide information on the attacks. They recommend understanding the strengths and weaknesses of both software to be able to combine the tools effectively and provide good network security.

In [10], the authors mention that the security in today's private networks is being threatened by the new methods of intrusion that are developed with the advancement of technology; since digital education has taken even more importance in present times, it is vital to ensure a good security system for the campus. In this sense, the authors carry out an analysis of campus network security. They have as their main objective the introduction of important concepts like "campus network" and its characteristics and analysis of the problems of a campus network in terms of its security. The authors do a systematic analysis of the literature referencing campus network security in China and abroad and finally, they present a number of measures to improve on traditional security solutions. The authors concluded that it is important that in addition to technical measures, it is also necessary to apply the laws and regulations applicable to the network, and these should be improved by implementing the appropriate software and hardware.

In [11], the authors indicate that one of the main challenges in computer networks is ensuring proper security measures. One of the systems used to protect computer networks is a firewall. However, it is also important to implement good anomaly detection for firewall policy anomalies in order to enhance the level of security. The authors focus on packet-filtering firewalls; with this kind of firewall, a hacker could provide fake IP addresses to the network through the spoofing method. Since this is an imminent risk for the network, it is vital to have an anomaly detection system in place to prevent attacks. The main objective is to create an anomaly detection framework for detecting intra-firewall policy anomaly rules. The authors developed a policy anomaly detection model and implemented it as part of a Java Web Application platform for the detection of firewall policy anomalies. The developed tool uses two modules, one for the detection of four main anomalies, these ones being shadowing, redundancy, generalization and correlation named FPAD, and the second one used for packet simulation named PS. In their results, they show that the use of the FPAD module was effective in detecting firewall policy anomalies for a large number of rules. In conclusion, the authors mention that the use of logic programming allows for more scalability when an anomaly detection engine is implemented to maintain a good performance.

In [12], the authors mention that the multiple devices in network architectures are at risk of passive and active attacks in case of vulnerabilities, which is the reason why network security is so important. Therefore, they propose the use of a Next-Generation Firewall (NGFW) to protect an enterprise network against a series of threats like DoS, DDoS, Aurora attacks, Malware attacks, IP spoofing, etc. Their main objective is to enhance security through the use of the firewall by applying different policies and tasks. They focus on strengthening aspects like the VPN and Port Forwarding to enhance security through the execution of rules and policies; in their methodology, they also analyse concepts like IP Spoofing, Insider Intrusion and Denial of Service (DDoS). They also analyse the current network architecture, and they propose a model to improve the existing model by providing Strong Authentication, High Data Security, Multilevel Protection, Network traffic encryption, No Insider Intrusion, Strong Masquerades, IP security, Port forwarding, Internet traffic filtering and Different web access policies for users. The authors show in their results that the bandwidth improved with the use of the proposed model while also being cost-effective in comparison with Adaptative Security Appliances since it uses a Fortinet firewall. The authors conclude by saying that the proposed network model provides a better solution for preventing the attacks and that it showed that it can protect the network from different kinds of threats, but there is not guarantee that it will detect all new attacks.

In [13], the authors mention that Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks have become one of the main threats to network security at university campuses because of all the services that are provided online. Therefore, the authors have the objective of presenting in their paper how Defense-In-Depth (DID) is not capable of defending from these attacks, and they propose a new model using Defense-through-deception that applies deception techniques to expose the limitation of DID models.

In their methodology, the researchers conducted a survey in the selected state universities and colleges in the Philippines, showing that only 53% of institutions installed an Intrusion Detection System and only 53% used a network antivirus to protect against DOS and DDOS attacks. The proposed system is meant to prevent a hacker who has already entered the network from damaging the actual system. It disorients the attacker by placing fake servers, and Honeypot was also used in the model as a deception tool. In the results, the authors showed how many minutes an attacker wasted attacking the wrong system. They use DOS tools available online, simulating three DOS attacks; the results show that in the first attack done through the DOS Attack-Online method, the time consumed by the attacker was 21.88 minutes; in the DOS Attack-LAN, which was the second method they used, the result was of 92.33 minutes consumed by the attacker, and finally, in the DOS Attack-HOIC Online the time consumed by the attacker was 26.47 minutes in this third method. When concluding, the authors indicate that it is impossible to secure a network 100%, especially in DOS and DDOS attacks, so this proposed model in which the attacker is delayed to gain time to organize defensive measures is what the authors recommend prioritizing cybersecurity mitigation.

3. Methodology

The methodology is based on the use of a virtual environment on VirtualBox to do the necessary configuration for the proposed network architecture. The pfSense firewall will be installed as a virtual machine on VirtualBox, and a Windows 10 virtual machine will be used to do the necessary configuration on the web platform of the firewall. The current Wide Area Network architecture at the University of Sciences and Humanities is as shown in Figure 1, where the Internet service for the campus is received through a company named "Win Empresas" there are two branches, Line 1 and Line 2. Line 1 is the main line in use, and Line 2 is kept to use in case of contingency; both lines have a Media Converter and a Router, and the two of them are connected to an Ethernet

Router protected with ATM-Fortinet to which the Local Area Network connects. Line 1 has a capacity of 300 MB, and Line 2 of 80 MB. The network will be divided into four VLANs (Administration, Faculty, Students and Visitors) to be able to configure different rules on the firewall depending on the VLAN; pfSense's dashboard will also allow for centralized management of the network security as it is shown in Figure 2.

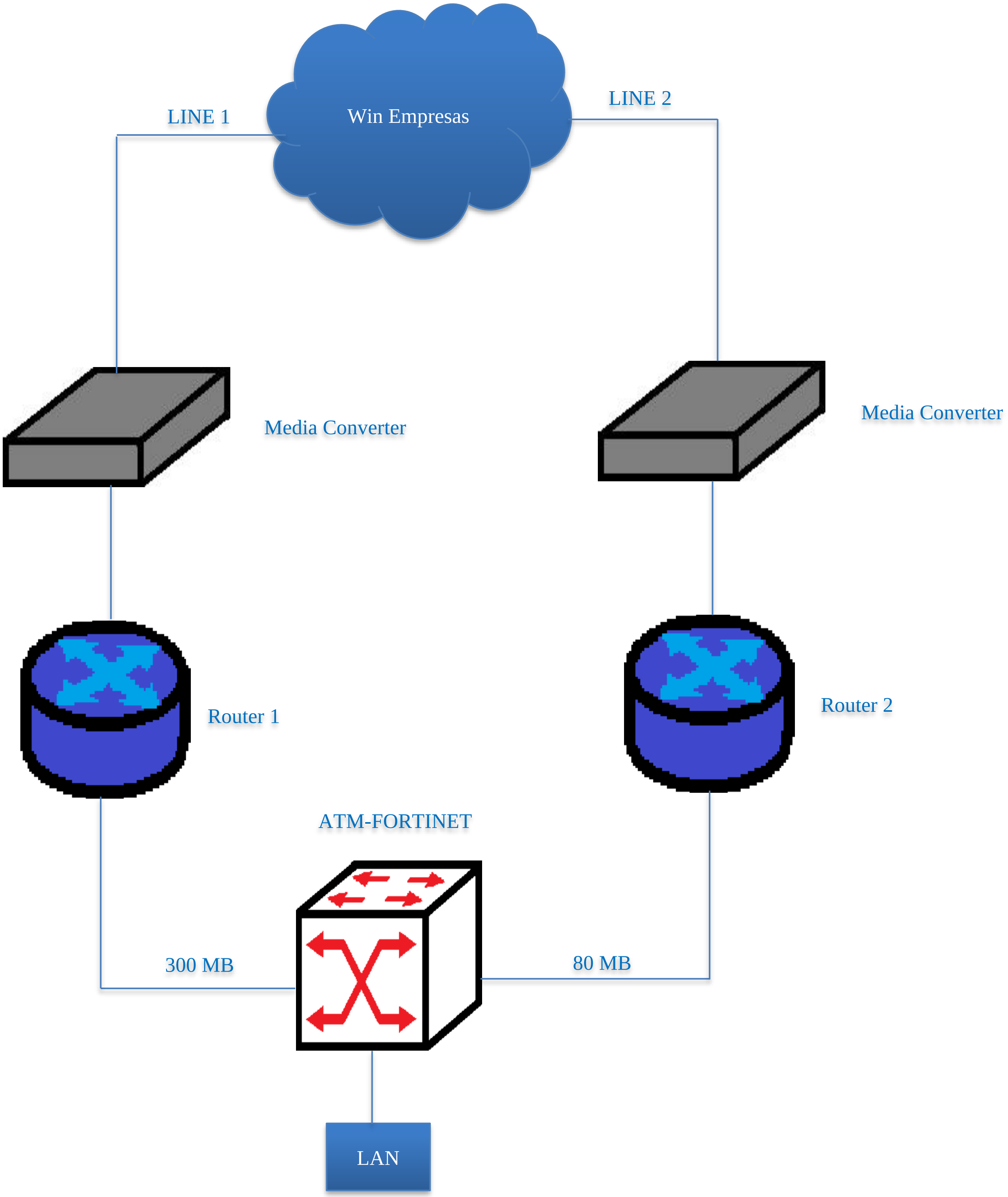


Fig. 1 Current wide area network architecture at the University of Sciences and Humanities

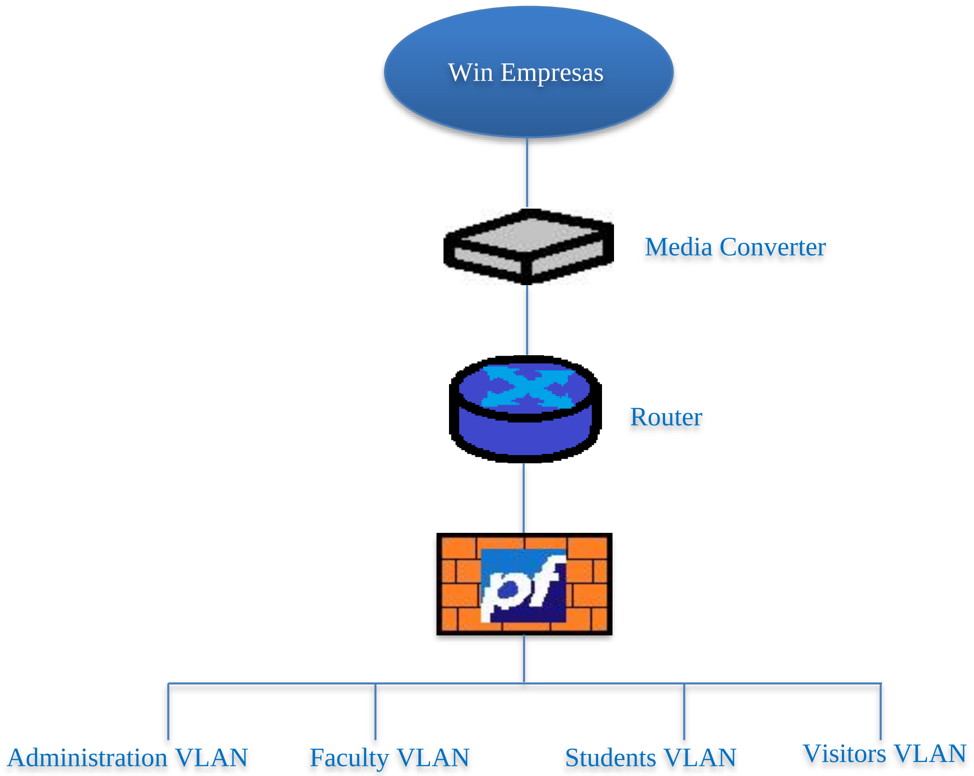


Fig. 2 Proposed network architecture

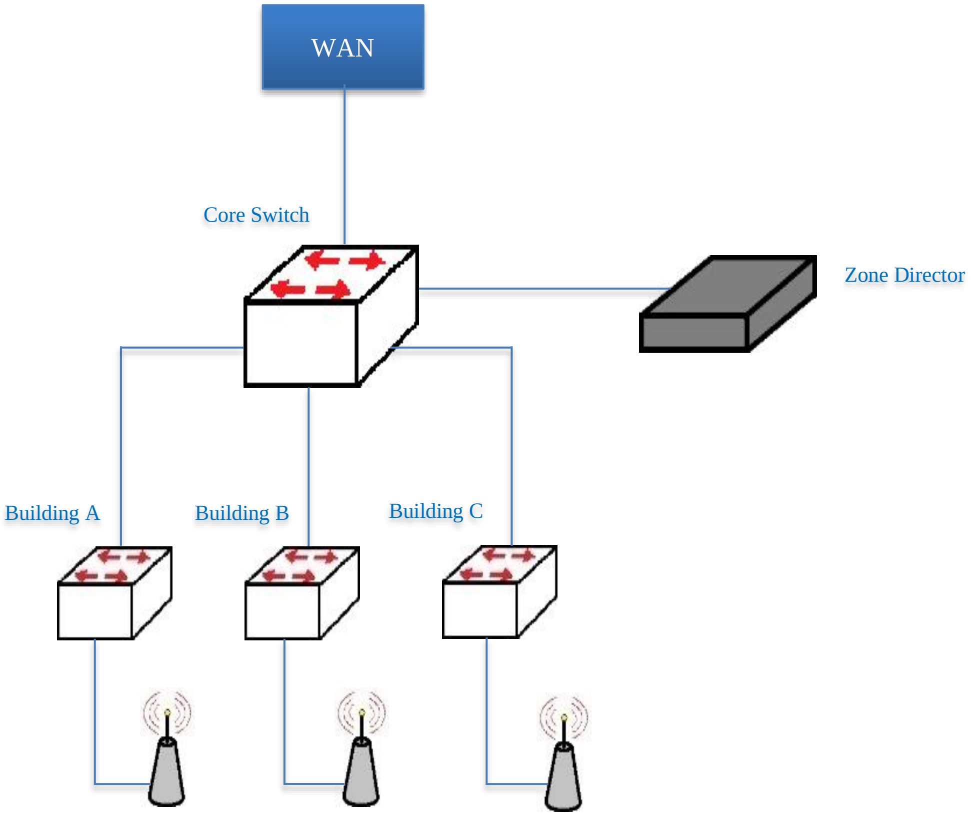


Fig. 3 Current local area network at the university of sciences and humanities

The proposed architecture of the network in Figure 2 shows that the optical fibre internet service would be received from the company Win Empresas; the use of a Media Converter is required to be able to do the connection to a main router and, from there, connect to the pfSense server in which the configurations will be made to divide the network into four Virtual Local Area Networks, each with different firewall rules. The University of Sciences and Humanities currently uses Ruckus Network's Zone Director as the centre of their internal network. The use of Ruckus Networks products and software requires the purchase of a license with a one-time payment. From there, each year, payment must be made for the updates in the software; these payments are important because, without the updates, the network would be at risk for attacks. The price for the license is $30.00 per Access Point, and the support for the updates is $450 per year. [CommScope, 2022b]

The transition to the use of the pfSense Software would help in lowering the costs since it is a free and open-source alternative that is highly secure and allows for the use of a wider variety of devices of different brands that can help give more scalability to the network and can adapt better to the specific structure of the network. Figure 3 shows how the current Local Area Network has a Core Switch to which the Zone Director is connected; from the main switch, the connections to the other switches in each building of the university campus are made, and the Access Points are distributed from each switch so that all wireless devices can access the network through the Wi-Fi. A server would replace Ruckus Networks's Zone Director with pfSense to have centralized control of the network. The design for the proposed network architecture will be done on VirtualBox, which is a platform in which virtual machines can be created to simulate networks on a host computer, being able to make modifications and the necessary configurations before installing pfSense as an operating system on a computer to work as the main server. On VirtualBox, the virtual machines that will be used for the configuration are a pfSense virtual machine and a Windows 10 virtual machine. Once installed, both of them need to be placed in the same internal network.

VirtualBox allows for the possibility to create internal networks; being in the same network, both virtual machines are able to communicate with each other, then the pfSense Virtual Machine can be started to make the initial configurations through the terminal, and from there, the IP addresses for the WAN and LAN networks can be configured, and the DHCP servers. Once the initial configuration is completed, the Windows 10 virtual machine can be started to access pfSense's online platform through the browser. The online platform has the main Dashboard, and on the upper part of the screen there are several options for configuration. The basic configuration can be done through pfSense's Wizard; once completed, several other things can be configured like a VPN, Port forwarding, Dynamic DNS, a Captive Portal, and several packages can be downloaded like a Service Watchdog, Suricata and Snort to strengthen the security of the network.

On the Interfaces tab, there is the option to create the VLANs for the network. To create a new VLAN, it is necessary to choose a Parent Interface; in this case, the Parent Interface is the LAN network; a VLAN Tag also needs to be added as a description; the VLANs Tag chosen for each VLAN was 20 for Administration, 30 for Faculty, 40 for Students and 50 for Visitors. Setting a VLAN Tag is important because when configuring the switch for the simulation of the network, that same VLAN Tag also needs to be set in the switch so that it can follow the rules configured in the pfSense firewall for each VLAN. A DHCP pool was created for each VLAN. Once the VLANs are created, new rules can be configured in the Firewall Rules tab according to the requirements of the university's network. When creating a new rule, traffic from one VLAN to another can be blocked or it can be allowed to pass; this is done so that there can be a separation for the VLANs in the network.

3.1. Firewall Rules for each VLAN

- Administration VLAN: The Administration VLAN was permitted to comunicate with all of the other VLANs, but the traffic was blocked from the other VLANs to the Administration VLAN.
- Faculty VLAN: The Faculty VLAN was permitted to communicate only with the Students VLAN; traffic from the Faculty VLAN to the other VLANs was blocked.
- Students VLAN: The Students VLAN was permitted to communicate only with the Faculty VLAN; traffic from the Students VLAN to the other VLANs was blocked. For this VLAN, a rule was also created to block access to three websites: Facebook, Twitter and Instagram.
- Visitors VLAN: The Visitors VLAN was not permitted to communicate with any of the other VLANs, and traffic from the Visitors VLAN to the other VLANs was blocked.

3.2. Simulation

For the simulation of the proposed network, pfSense will be installed as an Operating System on a laptop that will act as a server. From this laptop all of the other connections will be made. The devices used for the simulation are shown in Figure 4. The main device is the laptop in which pfSense will be installed since it has all of the configurations done previously on VirtualBox; this main laptop needs to have two ethernet ports, one of the ports must be connected to the modem with the internet service from the ISP, the other port must be connected to a switch, and from the switch an Access Point is connected to provide wireless internet service through pfSense to all of the devices in the network. To verify the correct functioning of the rules configured in the firewall, another laptop must be connected wirelessly to the Access Point. Once connected, the rules will be verified on the command prompt.The switch will also be configured with the corresponding VLAN Tags to match the ones on pfSense.

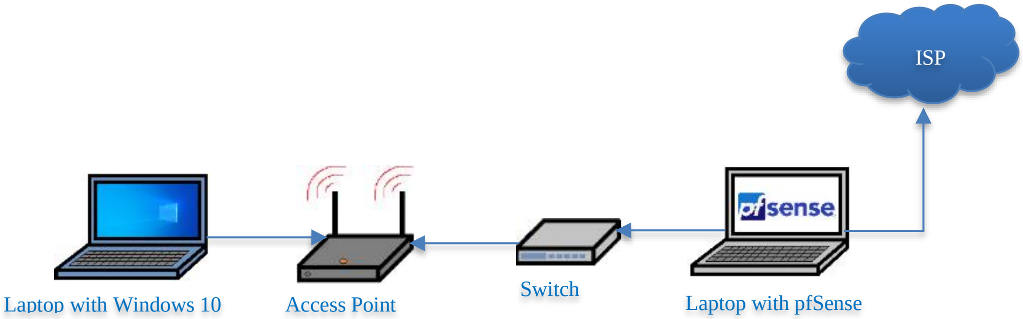


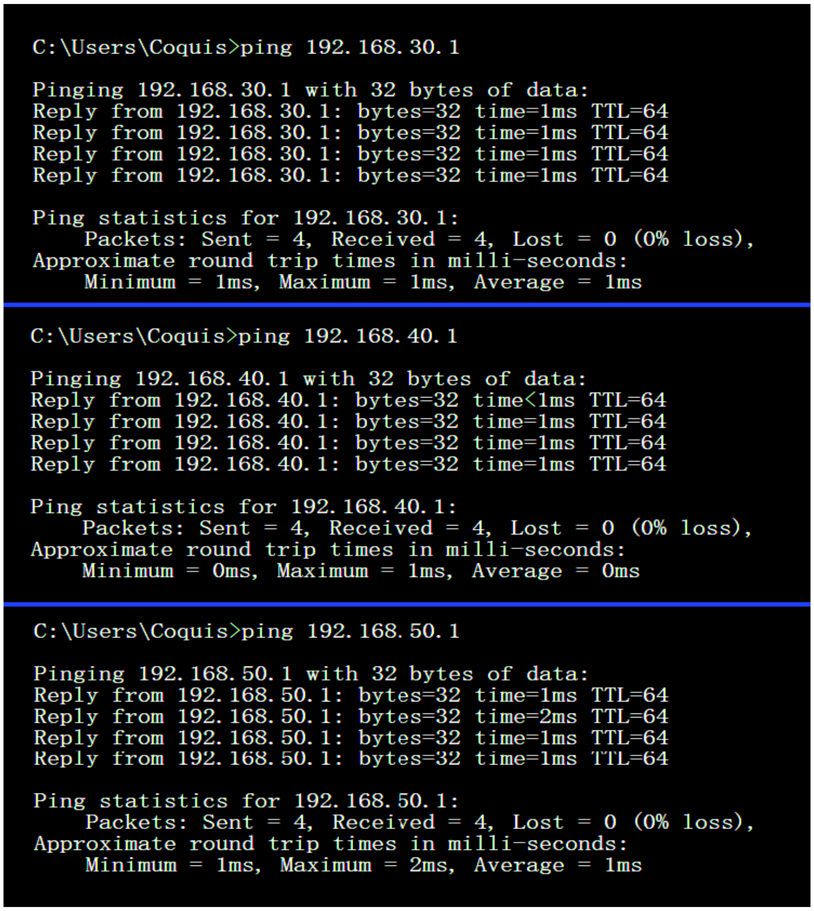
Fig. 4 Devices used for the simulation

4. Results

4.1. Verification of the pfSense Firewall Rules

When verifying in the Command Prompt of the Windows 10 Laptop, the response obtained was in accordance with the firewall rules configured in the pfSense Firewall for all VLANs.

- Administration VLAN: Through ping testing the connection with all the other three VLANs without the loss of any packages was verified, as it is shown in Figure 5.
- Faculty VLAN: Through ping testing, the connection with the Student VLAN was verified, as well as the inability to communicate with any of the other VLANs as shown in Figure 6.
- Students VLAN: Through ping testing the connection with the Faculty VLAN was verified, as well as the inability to communicate with any of the other VLANs as it is shown in Figure 7. It was also verified that the Students VLAN doesn't have access to the websites blocked on the firewall rules (Facebook, Twitter and Instagram) as shown in Figure 8.
- Visitors VLAN: Through ping testing, the inability to communicate with any of the other VLANs was verified, as shown in Figure 9.

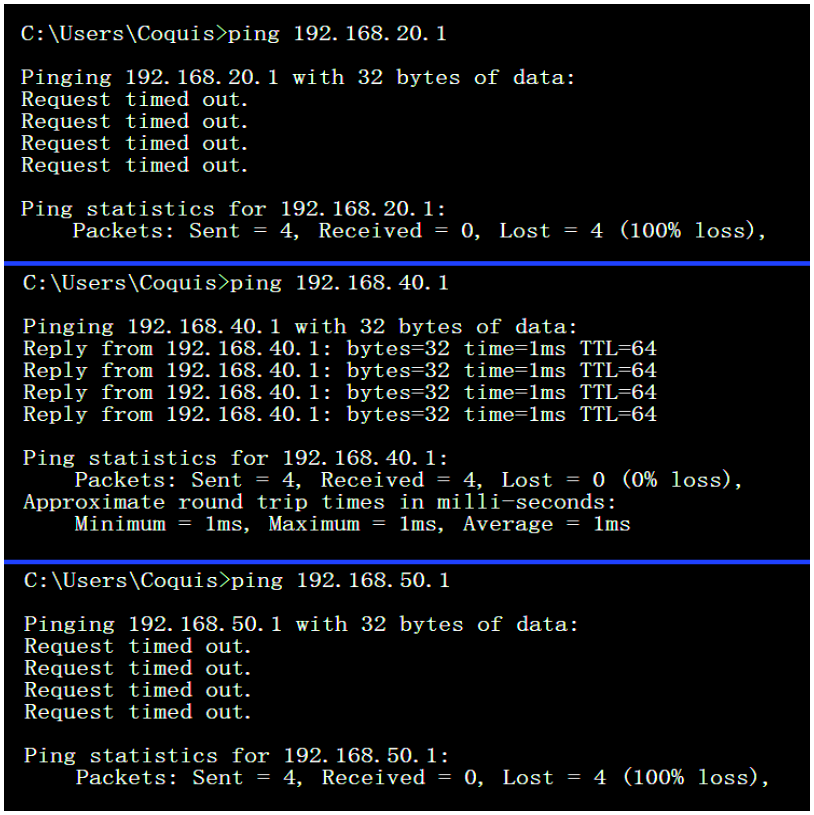


```
C:\Users\Coquis>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\Coquis>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:
Reply from 192.168.40.1: bytes=32 time<1ms TTL=64
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\Users\Coquis>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time=1ms TTL=64
Reply from 192.168.50.1: bytes=32 time=2ms TTL=64
Reply from 192.168.50.1: bytes=32 time=1ms TTL=64
Reply from 192.168.50.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Fig. 5 Ping tests to verify firewall rules in Administration VLAN

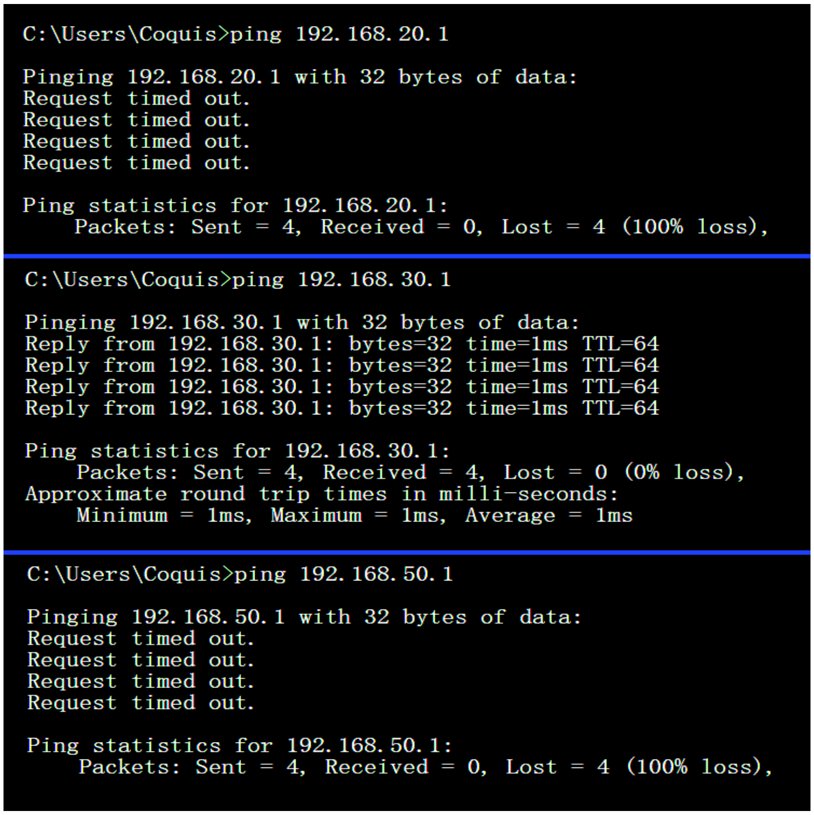


```
C:\Users\Coquis>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Coquis>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64
Reply from 192.168.40.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\Coquis>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 6 Ping tests to verify firewall rules in Faculty VLAN

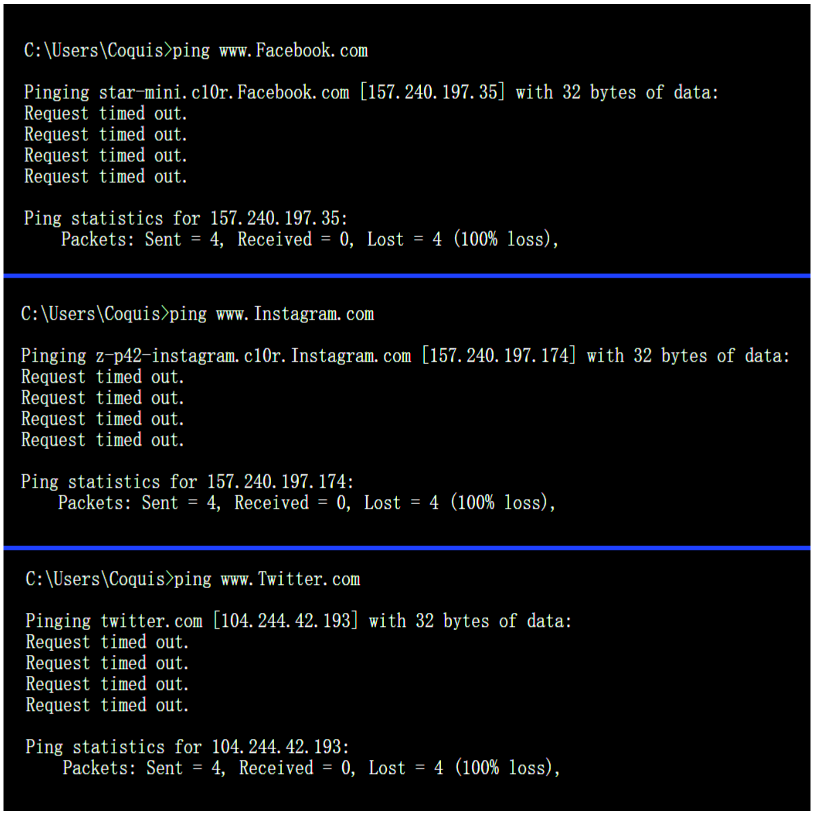


```
C:\Users\Coquis>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Coquis>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64
Reply from 192.168.30.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\Coquis>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 7 Ping tests to verify firewall rules in Students VLAN.

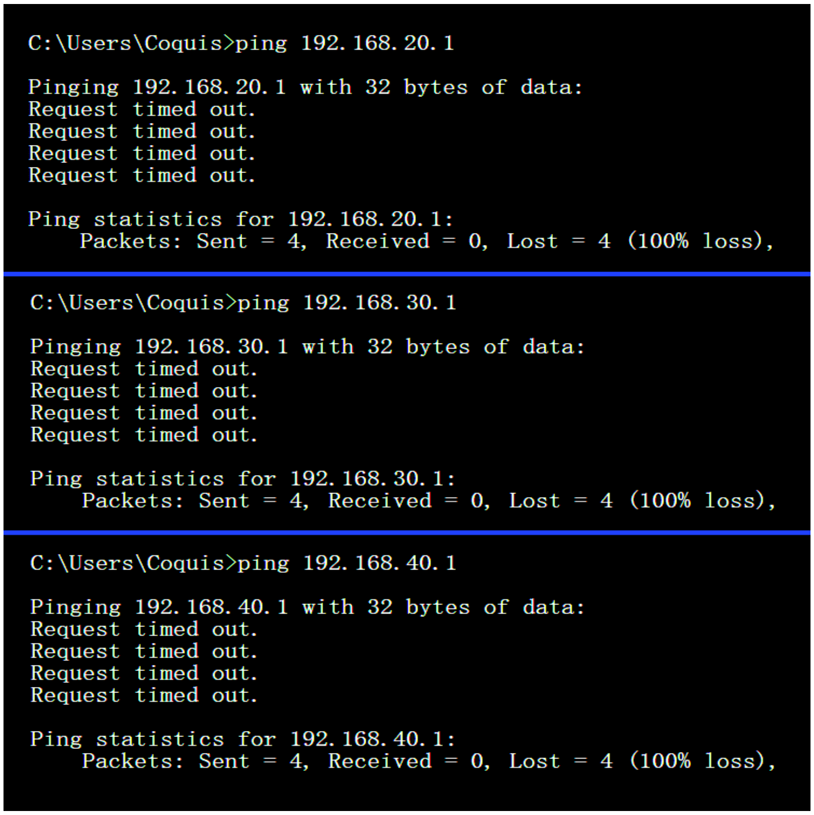


```
C:\Users\Coquis>ping www.Facebook.com

Pinging star-mini.c10r.Facebook.com [157.240.197.35] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 157.240.197.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Coquis>ping www.Instagram.com

Pinging z-p42-instagram.c10r.Instagram.com [157.240.197.174] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 157.240.197.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Coquis>ping www.Twitter.com

Pinging twitter.com [104.244.42.193] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 104.244.42.193:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 8 Ping tests to verify websites block rule in Students VLAN



```
C:\Users\Coquis>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Coquis>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Coquis>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 9 Ping tests to verify firewall rules in Visitors' VLAN

5. Discussion

The objective of the presented work was to design and plan a transition from the current proprietary software of Ruckus Networks to the free and open-source option of pfSense in the network of the University of Sciences and Humanities to lower the costs and provide more security through the division of the LAN network into four VLANs. It has already been shown that in a private network, it is important to apply appropriate laws and regulations in addition to suitable hardware and software applicable to the network architecture. Chu, Lan, Xu and Sun [10] did the analysis of campus network security and they mentioned that it is vital for the student service and the administration. This analysis was done through the introduction of important concepts and it examines various sources that can cause security issues in the campus's network. In the main results of the research, they mention the importance of the use of a firewall in combination with an Intrusion Detection System. This study can be compared with the present study because both focus on network campus security, and in both, firewall technology has been found as a good solution to protect the internal network from external attacks in combination with an IDS to provide an extra level of security. In the work of Chu, Lan, Xu and Sun, the study was more analytical, but in the present study, there was also a simulation performed to test the effectiveness of the firewall rules created so that the University of Sciences and Humanities can have an alternative to the current system that is in use. Additionally, we have shown in this work that it is beneficial to divide the LAN into VLANs so that the rules applied can be customized according to each group of users and set the restrictions that are necessary for the specific network architecture in use.

The proposed solution with pfSense is a solution that can be applied to different architectures, and different packages can be installed depending on the security needs, as Oluseye-Paul shows [7] in his implementation of an intrusion detection system on MTU network; the author also used pfSense in combination with the Snort package as the IDS. The main results showed that, once installed, the Snort package keeps a list of alert log entries from blocked hosts, and it is able to adequately display suspicious activity in the network. This study can be compared with the present study because both use pfSense firewalls, focus on networks of academic institutions, and both emphasize that pfSense and Snort are open-source software and also free, which is cost-effective since academic institutions sometimes have limited resources for network security. However, the results are not comparable since the present work focuses on the separation of the network on different VLANs to further the security of the network and the results were based on verifying the effectiveness of the firewall rules created through a simulation. In our contribution, we also did the installation of the Snort package and the Service Watchdog for the VPN of the LAN network; however, in our results, we focused more on showing the correct functioning of the rules configured for the firewall on each VLAN as it is shown in [12] that different web access policies for users and packet filtering helps prevent attacks and protects the network from different threats. Arefin, Uddin, Evan and Alam [12] defined attacks and threats on a computer network and mentioned different techniques used to fight these attacks and protect the system finally implementing a security-enhanced model for an enterprise network, the design was done on GNS3, and they used three cisco routers and two Fortinet firewalls and some non-manageable switch. In their implementation they also used a VPN and did Port Forwarding.

The main results show that, after doing a performance analysis, the bandwidth utilization in the proposed system is better. This study can be compared with the present work because, in both, a firewall was implemented to enhance network security. However, Arefin, Uddin, Evan and Alam used FortiGate as the chosen firewall, did not divide the network into different VLANs and did not implement an Intrusion Detection System.

6. Conclusion

The importance of good network security is evident in the present times since technology has been evolving rapidly and new ways of intruding private networks have been developed. There is a benefit to doing a transition from Ruckus Networks, the current software in use at the University of Sciences and Humanities, to the open-source alternative pfSense, since it will help in decreasing the costs since it is free and it also allows for the separation of the network in different VLANs which will also increase the security. It is also possible to install a number of packages like Intrusion Prevention Systems and Intrusion Detection Systems like Suricata and Snort to protect the network further. It was possible to design an appropriate network architecture for the campus of the University of Sciences and Humanities, and it was possible to simulate the proposed network to verify its correct functioning.

References

[1] University of Calgary Paid $20K in Ransomware Attack, Canadian Broadcasting Corporation, 2016. [Online]. Available: https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979

[2] John Chapman, and David Maguire, "The Impact of Cyber Security Attacks on Colleges and Universities: Who, How, and Why?," *Campus Crime: Legal, Social,* pp. 1- 386, 2022. [Google Scholar] [Publisher Link]

[3] Commscope, *Security Bulletins*, 2019. [Online]. Available: https://support.ruckuswireless.com/security_bulletins/299

[4] Cybersecurity & Infrastructure Security Agency, Vulnerability Summary for the Week of January 20, 2020. [Online]. Available: https://www.cisa.gov/news-events/bulletins/sb20-027

[5] Cybersecurity & Infrastructure Security Agency, CISA Adds Seven Known Exploited Vulnerabilities to Catalog, 2023. https://www.cisa.gov/news-events/alerts/2023/05/12/cisa-adds-seven-known-exploited-vulnerabilities-catalog

[6] Supriyanto Praptodiyono et al., "Development of Hybrid Intrusion Detection System Based on Suricatawith pfSense Method for High Reduction of DDOS Attacks on IPV6 Networks," *Eastern-European Journal of Enterprise Technologies*, vol. 125, no. 9, pp. 75-84, 2023. [Google Scholar] [Publisher Link]

[7] I. Oluseye-Paul, Implementation of an Intrusion Detection System on MTU Network, Mountain Top University, 2022. [Online]. Available: http://ir.mtu.edu.ng/xmlui/handle/123456789/1011

[8] Thaer Monther Alhanafi, Salah Ahmed, Mohammad A. Mikki, "Web Vulnerabilities Detection and Protection," pp. 1-7, 2022. [Google Scholar] [Publisher Link]

[9] Faldi Faldi, Dinamita Romadoni, and Muhammad T. Sumadi, "The Implementation of Network Server Security System Using Honeypot," *Journal of Informatics and Computers*, vol. 6, no. 2, pp. 122-130, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Han Chu et al., "Analysis of Campus Network Security," *Journal of New Media*, vol. 4, no. 4, pp. 219-229, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Cengiz Togay et al., "A Firewall Policy Anomaly Detection Framework for Reliable Network Security," *IEEE Transactions on Reliability*, vol. 71, no. 1, pp. 339-347, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Md. Taslim Arefin et al., "Enterprise Network: Security Enhancement and Policy Management Using Next-Generation Firewall," *Computer Networks*, *Big Data and IoT*, pp. 753-769, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] M.A. Naagas et al., "Defense-Through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593-600, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] José Luis Alcántara Castro, "*Design and Implementation of A Multiplatform Mobile Application with Encryption and Data Privacy Functions Aimed at Student Security at the University of Sciences and Humanities, District-Los Olivos 2014,*" Bachelor's thesis, University of Sciences and Humanities, pp. 1-247, 2017. [Google Scholar] [Publisher Link]

[15] Naga Srinivasarao Chilamkurthy et al., "Low-Power Wide-Area Networks: A Broad Overview of Its Different Aspects," *IEEE Access*, vol. 10, pp. 81926-81959, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Murat Kuzlu, Corinne Fair, and Ozgur Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity," *Discover Internet of Things*, vol. 1, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ping-Jing Lu, Ming-Che Lai, and Jun-Sheng Chang, "A Survey of High-Performance Interconnection Networks in High-Performance Computer Systems," *Electronics*, vol. 11, no. 9, pp. 1-23, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] S. Muntaka et al., "An Integrated System Using Open source Nethserver OS; A Case Study of Kessben University College Local Area Network," *International Journal of Progressive Sciences and Technologies*, vol. 30, no. 1, pp. 427-439, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Shamneesh Sharma et al., "Secure and Efficient Bandwidth Management for Local and Personal Area Networks Using Customized Open Source Application on a Commodity Hardware: RadSense—An Integration of pfSense Over Radius and MySQL," *Innovations in Information and Communication Technologies*, pp. 379-386, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Gaurav Somani et al., "DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions," *Computer Communications*, vol. 107, pp. 30-48, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ahmad F. Subahi et al., "Packet Drop Battling Mechanism for Energy Aware Detection in Wireless Networks," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 2077-2086, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Andrei-Daniel Tudosi et al., "Research on Security Weakness Using Penetration Testing in a Distributed Firewall," *Sensors*, vol. 23, no. 5, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Hendro Wijayanto, and Iwan Ady Prabowo, "Cybersecurity Vulnerability Behavior Scalein College During the Covid-19 Pandemic," *Sisfokom Journal (Information Systems and Computers)*, vol. 9, no. 3, pp. 395-399, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Shalom Adonai Huaraz Morales et al., "Augmented Reality: Prototype for the Teaching-Learning Process in Peru," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, pp. 806-815, 2022. [CrossRef] [Google Scholar] [Publisher Link]