Enhancing Network Security with a Firewall

Introduction

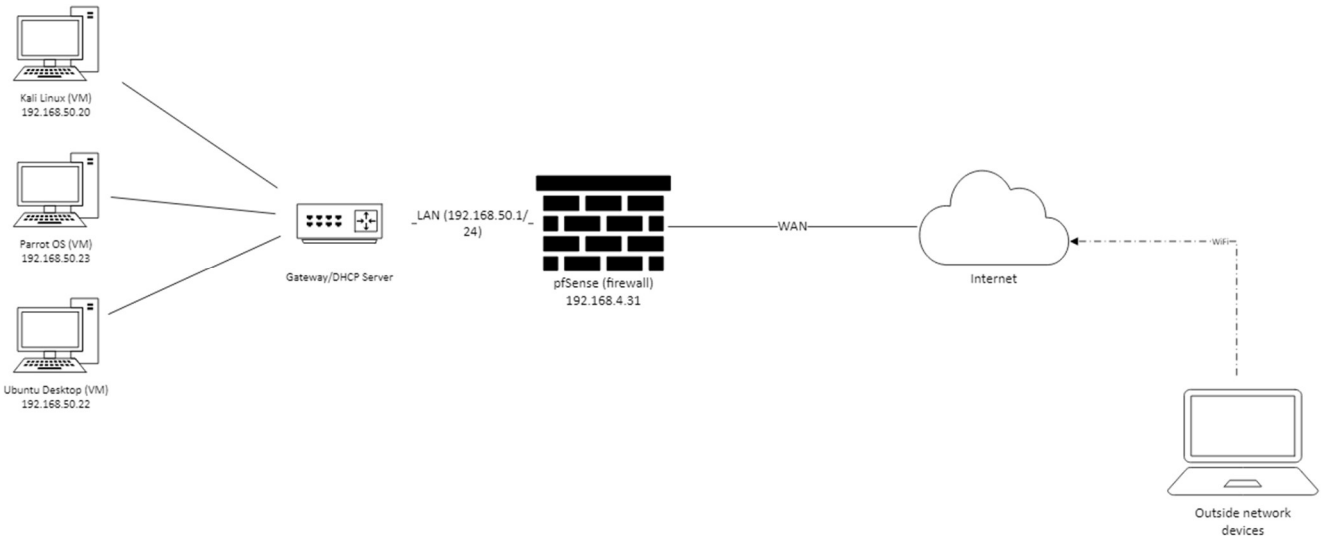
Network security is a growing concern in the information technology (IT) industry. Organizations and individuals are looking for ways to enhance network security in their environment to counter the rise of cyber-attacks. To provide insight into how much of a threat having low network security is in a network environment, “cloud environment intrusions increased by 75% over the past year. Malware-free activity made up 75% of detected identity attacks in 2023” [1]. In addition to, devices like gateways were the most common way for attackers to first penetrate a network [1]. To help reduce the number of cyber-attacks, individuals and organizations implement firewalls.

The firewall’s purpose is to “provide protection against outside cyber attackers by shielding computers or networks from malicious or unnecessary network traffic” [2]. Firewalls can provide features like blocking unnecessary ports, blocking incoming or outgoing traffic to specific locations through IP addresses, and blocking applications from running on the network. Firewalls can come in two forms, hardware, and software. The hardware-type firewall is a physical system installed between the router and the systems on the network. The other type, software, is where an operating system comes with a pre-installed firewall application. The application allows you to modify the network traffic that enters the system. Both forms of firewalls offer positives and negatives.

The purpose of this research is to analyze how important and effective a firewall can be in a small office or home network environment as well as build a better understanding of network protocols like user diagram protocol (UDP), transmission control protocol (TCP), and hypertext transfer protocol secure (HTTPS). For experimentation, the free open-source software firewall, pfSense, was used. There is other free open-source firewall software; however, during initial research, pfSense is known to have features of industry-leading firewall software. For example, Check Point, Cisco PIX, Cisco ASA, and Juniper are common industry-leading firewalls. Another benefit to using pfSense is the software being open source. Open-source software is “computer software whose source code is developed in an open and collaborative way and made available with a copyright license that complies with the Open-Source Initiative's Open-Source Definition (OSD)” [3]. Individuals or companies can develop or install third-party packages that can enhance the software features or introduce new ones. As stated before, since cyber-attacks are on the rise, it is best to understand how one person or a company can implement more effective network security in an environment. The analysis will cover the firewall architecture and design, the implementation process, an analysis of results, roadblocks and solutions, and future improvements.

Firewall Architecture and Design

The network architecture and environment are shown in Figure 1. The environment simulates a small office or home network environment running on a virtual machine software called Oracle VirtualBox. The virtual environment is composed of three internally connected computer systems running different operating systems (OS). One system is running Kali Linux, Parrot OS, and Ubuntu Desktop OS. The pfSense firewall software is running on a standalone virtual machine with network adapters configured to simulate a gateway, a local-area network (LAN), and a wide-area network (WAN). Finally, one device outside the virtual environment was used to conduct network traffic and detection experiments.



(Figure 1)

Timeline

Phase	Tasks	Start Date	End Date	Duration
Planning and Research	Research firewall software options, define objectives, brainstorm experiments	08/29/2024	09/05/2024	7 Days
Design	Draft architecture, configure virtual environment and systems	09/05/2024	09/08/2024	3 Days
Experiment	Monitor network traffic, analyze network communication from outside devices, understand port forwarding and blocking	09/08/2024	9/14/2024	6 Days
Documentation	Document findings and virtual environment configuration, develop an analysis of the findings	09/14/2024	09/15/2024	1 Day

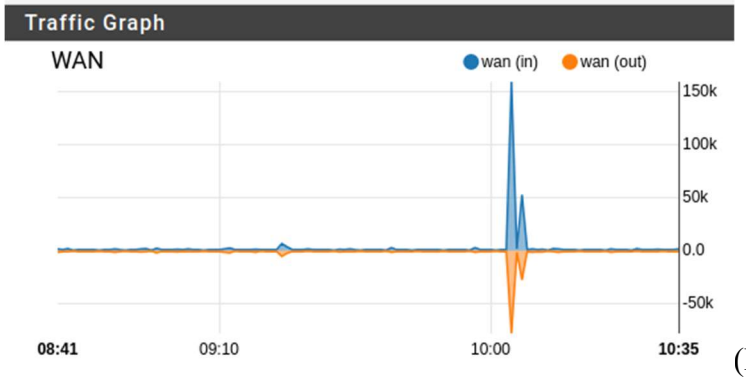
Review	Develop final reports	9/15/2024	09/25/2024	10 Days

Implementation Process

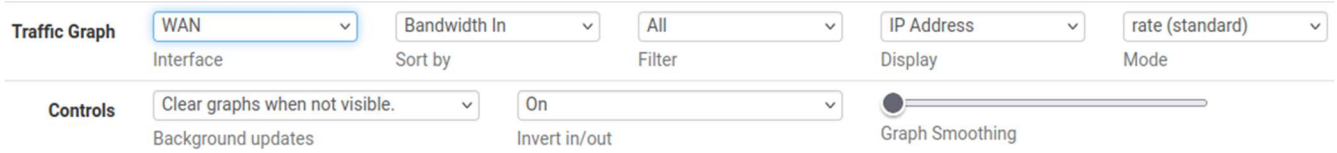
To properly configure the network environment in Figure 1, the pfSense firewall virtual machine required two network adapters. Adapter One was configured to bridge the connection between the computer and the router, which represents the WAN connection. Adapter Two was configured as an internal network, meaning, the virtual systems will have their own subnet. Adapter Two will act as the LAN and the DHCP server. When configuring the virtual systems to be hosted in the virtual environment, it was important to modify their network adapters to be connected to the LAN by having the network adapters for each system set to the internal network.

After installing pfSense and completing the installation process, modification in the pfSense interface was necessary. For the LAN, a rule was needed to allow IPv4 and IPv6 connections to go through the firewall. This allows each virtual system to connect to the internet. A firewall rule is telling the LAN connection how to work with the incoming and outgoing network traffic. Each rule can be configured to allow or reject network traffic.

The pfSense software comes with a traffic graph feature. The traffic graph provides a visual display of the network traffic coming in and out of the firewall. The feature also provides an option to change what the graph displays; however, the graph is not detailed and provides insufficient information when it comes to enhancing network security and monitoring traffic. Figure 2 is an example of the traffic monitor graph. Figure 3 shows the graph settings provided.



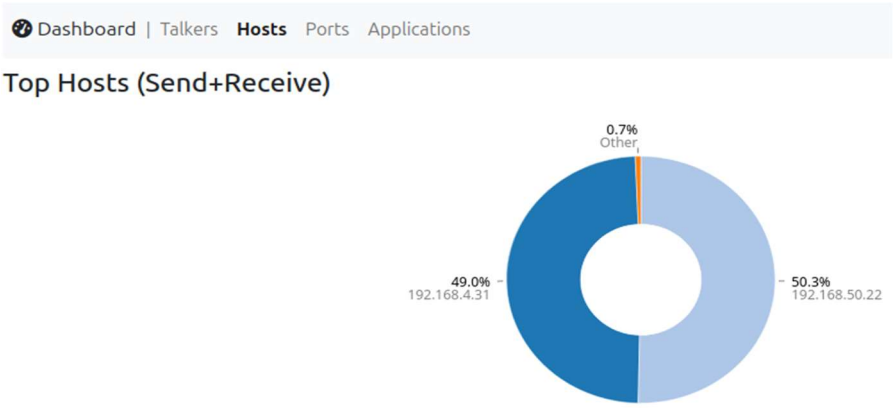
(Figure 2)



(Figure 3)

One suggestion to counter the insufficient graph is installing the package ntopng. Ntopng is a traffic monitoring application that is web-based, allowing users to view and control network traffic through a support web browser inside the pfSense firewall software [5]. Figure 4 is one example of a graph ntopng provided in pfSense. The package places network traffic data in pie chart form with

percentage usage between every device in the network. Overall, ntopng allows for more sufficient data retrieval when monitoring network traffic.

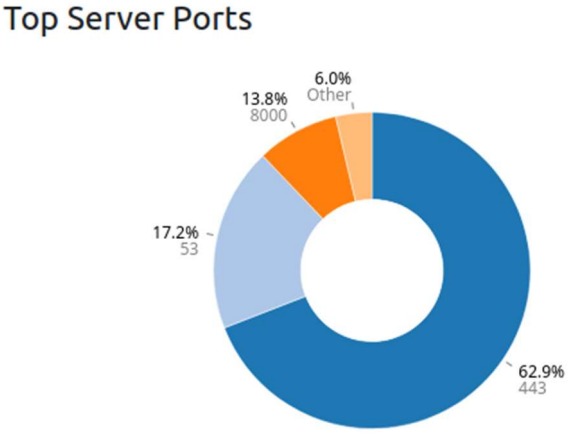


(Figure 4)

Analysis of Results

The first experiment was composed of reading network traffic coming in and out of the firewall. To simulate network traffic, a Python web server was created on a laptop system that is not connected to the security system. The virtual systems connect to the Python web server through a web browser by typing in the IP address followed by the port. In this experiment, the web server IP address was 192.168.4.24 running on port 8000. In Figure 5, port 8000 appears under the WAN firewall server ports.

The report shows that 13.8% of the network traffic is connected to port 8000 through the WAN connection. In terms of network security, network administrators can gather the data and determine the reason end-users are connecting to a system through port 8000. After analyzing the reason for using port 8000, individuals can create a WAN firewall rule to block outgoing traffic to port 8000, enhancing the security of the network.

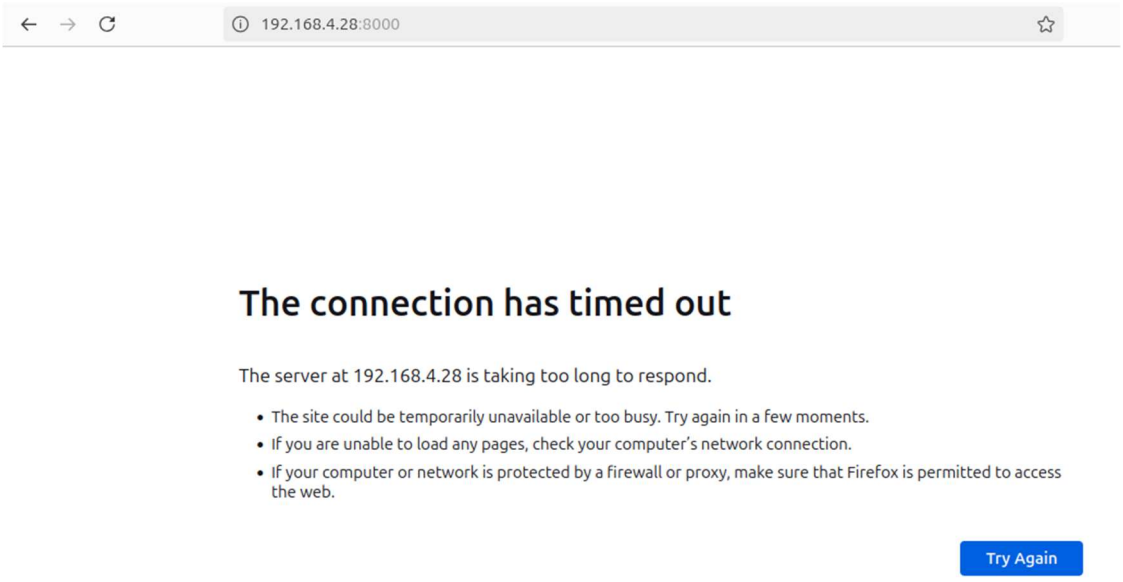


(Figure 5)

To further understand the first experiment, individuals can create rules to block any unnecessary network ports that can potentially be used to cause harm. There are three different types of ports, system ports, registered ports, and private ports [6]. System ports are common TCP, UDP, and SCTP ports. For example, HTTPS runs on both port 80 and 443 [6]. HTTP communicates using port 80, like HTTPS; however, the network traffic is unencrypted. Registered ports run between 1024 and 49,151 [6]. These ports operate for different services like OpenVPN, VNC, and HTTP. Finally, private ports operate between 49,152 and 65,535 [6]. Private ports can be used for custom applications; however, they may conflict with any existing processes. Overall, knowing what applications and processes run on the network ports can elevate network security in the environment.

The second experiment is to analyze firewall rules and understand how blocking network communication can increase network security. Restricting systems to connect to outside systems or websites can lessen the possibility of individuals installing malware on a system. For instance, if a system connects to an unencrypted network, like HTTP, criminals have the opportunity to track the system's data and inject malicious code [7].

The firewall rule was created for the LAN communication. The action for the rule is configured to block network packets. The block configuration will drop the network packet silently, without telling the end-user. To increase security, the setting regarding log packets that try to handle the rule was enabled. This feature provides data regarding what systems in the environment are trying to access port 8000. Figure 7 is an example of what end-users receive when trying to access a website that uses the blocked port.



(Figure 7)

Figure 8 shows the log data generated when a system tries to connect when using a blocked port.

(Figure 8)

To summarize, blocking unnecessary ports and unencrypted network communication can mitigate attacks for open vulnerabilities. By having an unnecessary port open, “attackers can easily exploit weakness in the applications listening on a port” [8]. With that, hackers take advantage of unpatched security vulnerabilities in older systems and applications [8]. The writer, Alessandra Descalso, provides an example of how a port is abused. Alessandra states that Microsoft’s remote desktop protocol (RDP) is used to access systems remotely [8]. “Some of them are unpatched systems with known vulnerabilities where they can bypass all authentication and get right into whatever is hosting RDP right away” [8]. Overall, understanding what network ports are unnecessary eliminates the possibility for cyber criminals to access an individual's network.

Roadblocks and Solutions

One significant roadblock encountered was during the configuration of the virtual environment. This challenge arose because the configuration of pfSense in a virtual environment is different compared to configuring pfSense on a standalone system that is connected directly to a home router. To address the issue, I reviewed documentation regarding how the networking functions in the Oracle VirtualBox software [9]. The documentation provides insight into how the different network settings

perform in the software. This approach not only resolves the issue but also improves my understanding of the Oracle VirtualBox software.

Another roadblock that occurred was the virtual systems not able to connect to the internet. In the beginning, this roadblock created limitations for the experiments because the data would be limited and what information could be tested. To fix this, I addressed the issue by asking ChatGPT for advice on how to overcome the networking issue [10]. ChatGPT suggested connecting pfSense to open domain name services (DNS) servers [10]. For example, using Google's DNS 8.8.8.8 and Cloudflare's DNS 1.1.1.1 [10]. The other suggestion is to verify the setting DNS Server Override is enabled [10]. By following the suggestion, the virtual systems were able to connect to the internet and access websites hosted outside the firewall.

Future Improvements

After analyzing how experiments were performed and how the virtual environment was configured, one future improvement is to duplicate the virtual machines. Oracle VirtualBox allows users to duplicate a virtual machine [11]. By duplicating the virtual machines, it can help with roadblocks related to misconfigurations in pfSense. If one rule is misconfigured, it can cause issues with accessing the pfSense firewall software through the web browser.

Conclusion

The objective of the project was to implement a firewall to understand how individuals can enhance their network security in their environment. The project used an open-source software called pfSense as the firewall. Not only was the project's objective to understand network security, but it was also to build a better understanding in managing virtual environments, understanding network ports, and how to configure a firewall.

The project proved ways individuals can enhance network security in their homes by monitoring network traffic and by declaring network port rules. Monitoring network traffic allows individuals to see what systems are connecting to what applications outside the network. Finding and blocking malicious or unsafe websites lowers the possibility of malware or cyber criminals connecting to an individual's home network. Examples of unsafe websites could be websites using unencrypted communication like HTTP. Malicious websites typically prompt the user to download an application that contains malware. Not only does blocking the websites in the firewall rules help, but individuals can also block unnecessary network ports. By blocking these ports, it limits the access a cybercriminal has when it comes to attacking your home network.

Despite the roadblocks encountered, particularly the virtual environment configuration provided an opportunity to broaden my understanding of virtual environments. Understanding how to configure a network environment enhances my job search in the cybersecurity field. Virtual environments not only are a good skill, but they also provide the opportunity to create cyber security labs in a standalone environment. This way, the experiments do not affect personal systems on the home network. The other roadblock regarding the virtual machines not being able to receive internet connectivity, provided the opportunity to understand why DNS is important and how firewalls should be configured. Having strict firewalls and not having proper DNS settings configured could have restricted the experiments performed in the project. In conclusion, the roadblocks provided an opportunity to enhance my cybersecurity skills.

In the future, firewalls could be enhanced with artificial intelligence (AI). By combining machine learning algorithms, firewalls could have AI configured to automatically detect security threats in real-time and develop a report automatically for individuals to review. This can limit the analysis process an individual must perform. For example, checking the website a system accessed outside the firewall, what ports are being used, how long the system has been connected, and more. With AI being integrated into other computer systems, it will not be long until AI is configured in firewall software and hardware.

The project highlighted the critical role a firewall plays in network security. When deploying a configured firewall, individuals can monitor network traffic and lessen the possibility of a cyber-attack in their home network, since cyber-attacks are on the rise and are increasing every year [1]. Firewalls provide a foundational layer of security in a home network. Routers can direct traffic; however, they are limited to what security functionalities are installed. For example, routers focus on routing network connectivity between devices and the internet whereas a firewall provides the opportunity to monitor network traffic and investigate any security incidents [12].

References

[1] tprestianni, "101 Cybersecurity Statistics and Trends for 2024 | NU," *National University*, Feb. 15, 2024. https://www.nu.edu/blog/cybersecurity-statistics/
[2] CISA, "Understanding Firewalls for Home and Small Office Use | CISA," *Cybersecurity and Infrastructure Security Agency CISA*, Feb. 23, 2023. https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use
[3] "Open Source Software Overview," *www.cms.gov*. https://www.cms.gov/tra/Application_Development/AD_0210_Open_Source_Overview.htm
[4] "Wireless LAN Security: What Hackers Know That You Don't." Available: https://s26142.pcdn.co/wp-content/uploads/2014/04/What-Hackers-Know_id42.pdf
[5] "What is ntopng — ntopng 5.7 documentation," *www.ntop.org*. https://www.ntop.org/guides/ntopng/what_is_ntopng.html
[6] N. House, "List of Common Ports Cheat Sheet," *Station X*, Jul. 07, 2020. https://www.stationx.net/common-ports-cheat-sheet/
[7] "Unencrypted communications," *portswigger.net*. https://portswigger.net/kb/issues/01000200_unencrypted-communications
[8] A. Descalso, "Open Ports: What They Are and Why You Need to Secure Them," *www.itsasap.com*, Jul. 27, 2021. https://www.itsasap.com/blog/why-secure-open-ports
[9] "Chapter6.Virtual Networking," *Virtualbox.org*, 2000. https://www.virtualbox.org/manual/ch06.html
[10] OpenAI, "ChatGPT ," *ChatGPT*, 2024. https://chatgpt.com/
[11] "Virtual Storage," *Oracle Help Center*, 2022. https://docs.oracle.com/en/virtualization/virtualbox/7.0/user/storage.html#cloningvdis (accessed Sep. 16, 2024).
[12] M. Pramatarov, "Router vs firewall, can you guess which is better?," *ClouDNS Blog*, Jul. 13, 2023. https://www.cloudns.net/blog/router-vs-firewall-hardware-software/