Practical Project

Aloysius Egbo Ike

College of Arts & Sciences, Niagara University

CSO 540: Network Security

Dr. Glenn Papp

April 14, 2024

INTRODUCTION

On this Practical Project, Niagara Manufacturing is transitioning from a brick-and-mortar retail setup to a digital marketplace. As a newly hired Network Security Engineer for the company, my primary objective is to design and implement an in-house infrastructure that supports both internal (intranet) and external (internet) connectivity. This is to align with the company's Strategic Innovation Plan, which aims to enhance its digital presence and facilitate online operations. The project entails creating a network topology that encompasses various departments within the organization and ensures secure and efficient communication between them.

My tasks includes designing a network layout that accommodates the specific needs of different departments, such as the call center/storefront, shipping department, administration offices, and a designated web server network acting as a pseudo-DMZ.

Each department has unique requirements regarding workstations, VoIP phones, printers, internet access, and restrictions on network communication with other internal segments. The Call Centre and the Shipping Department should only communicate with each other and no other internal network, the Admin could access the other internal networks while the DMZ should not be able to contact any internal network directly.

I started by drawing out the Network Topology which is an arrangement or layout showing how the devices and links interconnect and communicate in a network. The topology indicated the structure of the whole Network, typically showing how the different devices on the networks were placed and interconnected and also showing the data flow. This was drawn out based on the information provided for the project. Using the network topology, I proceeded with implementation; I advanced to the technical set up stage, incorporated the network layout by

setting up 2 Virtual Machines by installing pfsense and Kali Linux on Hyper V, through a process known as virtualization, which is typically spinning off a virtual machine VM (or VMs) within another one. 5 virtual switches were comfigured on Hyper V, using the virtual switch manager, with one connected to the internet (external network) while the other 4 were internal networks (LAN), and then imported the VMs. Kali Linux was configured to have one network interface which I could switch between, while pfsense was configured to have all 5 network interfaces.

The interfaces and firewall rules were set in line with the requirements and the necessary ports blocking requirement.

Armed with the pfsense documentation and those of Microsoft and Kali Linux, I was able to carry out the necessary installations and configurations including other functionalities on pfsense such as traffic shaper limiter for improved Quality of service, Open VPN to enable remote access for admin staff on transit and Squid Antivirus for maximum protection of the network.

Additional Functionalities such as Services Status, Gateway and Open VPN were enabled on the Home page for a quick and global view of the general status of the network.

Additionally, the project involves setting up virtual machines using Hyper-V technology, installing and configuring pfSense and Kali Linux VMs, and establishing virtual switches to manage network interfaces effectively.

At the end of this project, I should create a robust network infrastructure that meets Niagara Manufacturing's digital demands and enhances overall operational efficiency and security.

TASKS 1:

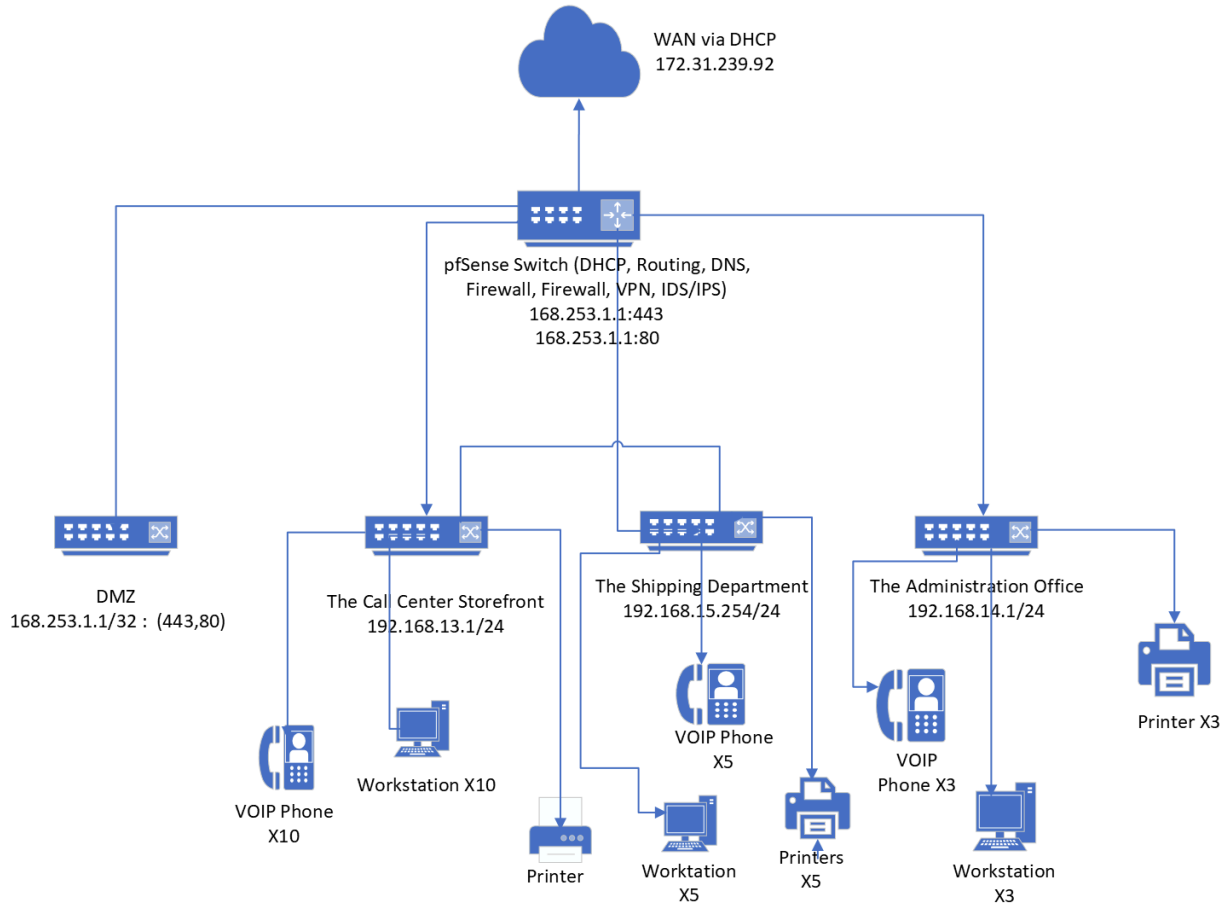

Fig 1: Network Topology for Niagara Manufacturing

Network Topology

Network topology refers to the arrangement of devices and connections in a network. It defines how devices are interconnected and the structure of communication paths within the network. It can be physical, representing the actual layout of devices and cables, or logical, focusing on the flow of data in the network.

(Kaviani & Sohn, 2020) explores the impact of network structure on the performance of artificial neural networks (ANNs). It discusses how the fully-connected complex structure of ANNs can

lead to high computational time, energy consumption, and space requirements, prompting research into altering the network topology for improved efficiency.

Mapping out network topology is crucial according to (Kaviani & Sohn, 2020) because it allows researchers and practitioners to explore the influence of different network structures on the performance of networks. By understanding and analyzing the topology of Networks, such as fully-connected, random, small-world, and scale-free networks, researchers can identify more efficient and less complex structures that can lead to improved performance in terms of computational efficiency, energy consumption, and space utilization.

Niagara Manufacturing's network topology in Fig 1 above has an external network with connection from the internet, Wide Area Network WAN and 4 Local Area Network LAN with its server connected externally to the Internet, Wide Area Network, WAN via Dynamic Host Configuration Protocol DHCP through which NM receives connection and internally to 4 Internal Private Networks. This means that it has no control over the external IP address as it is dynamically assigned a public IP address by the ISP. Internally, IP addresses was assigned with unique subnets for the 4 LAN networks. They were set up to have unique subnets

The four Private Networks are as follows;

- Call Centre: The department was assigned IP with the subnet 172.16.1.1/24. The available 254 IP Addresses range is more than enough to accommodate the requirements of the department with 1 Printer, 10 PCs and 10 VoIP and even cater for possible expansion in the future. The dotted line between the Call Centre and the Shipping Department indicates that they can communicate internally between them.
- Shipping Department: The department was assigned IP with the subnet 172.16.10.1/24 which is unique to the Call Centre. Again the range will be sufficient for the 5 Printers,

5PCs and 5 VoIP. Just as above, the dotted lines indicate communication with Call Centre.

- Admin Department: The department was assigned IP with the subnet 172.16.15.1/24 which again is unique to the previous 2 departments. The range is also more than sufficient for the number of staff in the department and at present will cater for 3 Printers, 3 PCs and 3 VoIP.
- DMZ Network: This was already assigned 168.253.1.1/32 and would not communicate with any internal network.

TASK 2

Technical Setup

Would require that Hyper V, Kali and Pfsense are all set up and working correctly as a requirement for the project to be successful.

-Installing the 2 Virtual Machines VMs.

To install the 2 Virtual machines(VM), I used Hyper-V. Hyper-V is a Microsoft hardware virtualization product that enables one to create and run the software version of multiple computers called VMs. This is done by the process known as Virtualization. By Virtualization, a software version of computer is able to run its Operating System and Programs on another machine.

-Enabling Hyper V on my Machine

To enable Hyper-V on my system, I navigated to the start Menu, clicked on the “Turn Windows Features on and Off” and was able to see my machine name, meaning it was enabled on Hyper V. Otherwise, I would have required “nested virtualization” feature again to my VM to enable it on my machine. I ensured that the 2 features were ticked as highlighted above in fig 2 below.

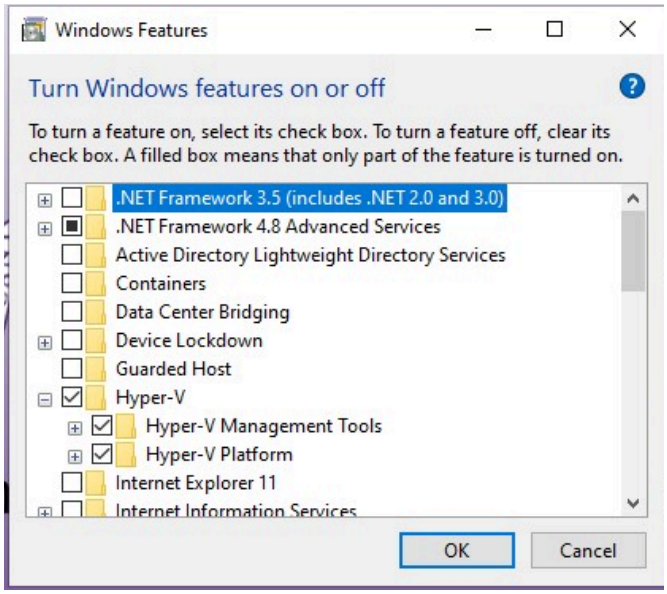

Fig 2: Screenshot of Hyper-V enabled

- Creating virtual switches using Hyper-V Virtual Switch Manager

After enabling the Hyper V on my Machine, I proceeded to configure the virtual switches for the external and 4 private networks using the Virtual Switch Manager in line with the network topology I had earlier designed. I ran configurations using the Hyper V switch managers and configured the external and internal networks.

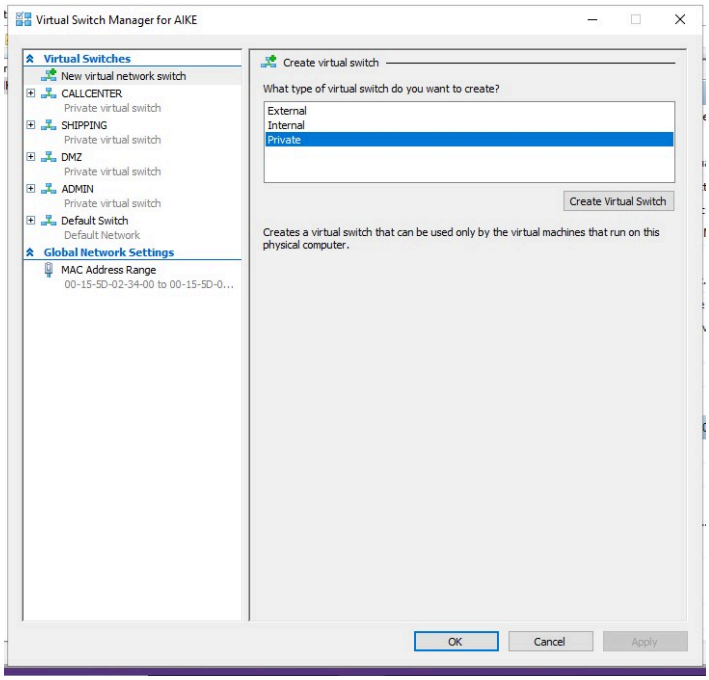

Fig 3: Screenshot of my Virtual Switch Manager

- Creating/Virtualizing the VMs with Hyper V

Virtualization is creating or spinning off a computer within another computer, i.e creating another computer off one's computer as though they were physically available. Yang et al., (2014) describe it as a technology that can divide one system into several logical systems or combine multiple systems into one system. They added that virtualization assigns hardware resources to VMs and is able to function through them. According to Batalla et al., (2016), which explores the realm of virtualization, a technique that enables the operation of multiple operating systems and applications on virtual machines hosted on a single physical platform. By isolating guest operating systems and applications from each other, virtualization creates the illusion of distinct physical environments. Batalla et al., focuses on the performance implications of virtualization, especially in the context of I-IoT, where resource control and isolation are crucial. It compares two prominent hypervisors, XEN and KVM, emphasizing the importance of throughput and latency in I-IoT applications. Their analysis highlights the significance of

choosing the right virtualization platform to optimize performance and efficiency in industrial IoT settings just as I am also doing in this project with Niagara Manufacturing.

After creating the switches, I proceeded to create the VMs, starting with Kali. Following the pfsense documentation, I navigated to Action under Hyper V and clicked on New, then on the Virtual Machine wizard, I specified the name Pfsense, selected Generation 2, set the memory size to 4096MB, Checked the box “Use dynamic memory for this virtual machine”. Set the size of the dynamically expanding Hard disk to 30 GB, downloaded the ISO files of pfsense and clicked on Finish.

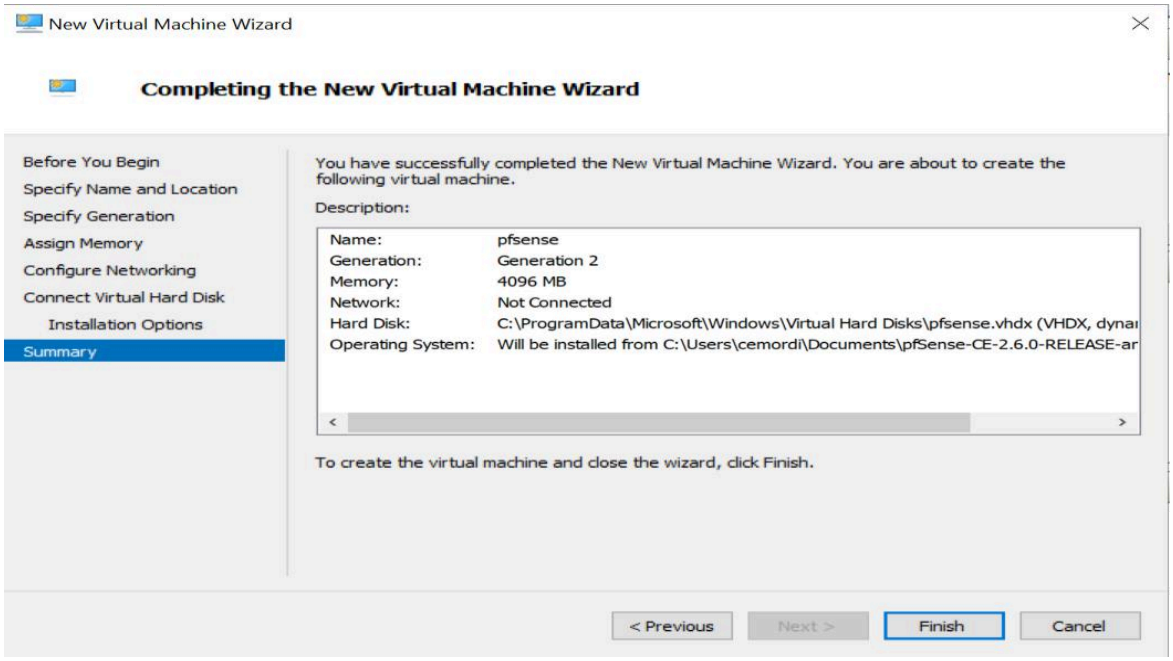

Fig 4: Screenshot of my Successful creation of VM

- Installation and Configuration of Kali Linux – Virtualizing with Hyper V

To install and set up Kali, I first need to have virtualization capability enabled and then followed the steps as provided to instal Kali, with the virtual disk size which set at 40G because of the amount of activity expected on it and the selected interface which was set to “Call Centre”.

I changed the name to have CSO in it, I change the memory from 2GB to 4GB of RAM, upped the virtual processor from 1 to 4 that should help in terms of loading time and setting the default Network Adapter to Call Centre, which can be switched between the other interfaces unlike pfsense where additional 4 network adapters will be configured for the 4 internal networks, with the Default switch being the WAN.

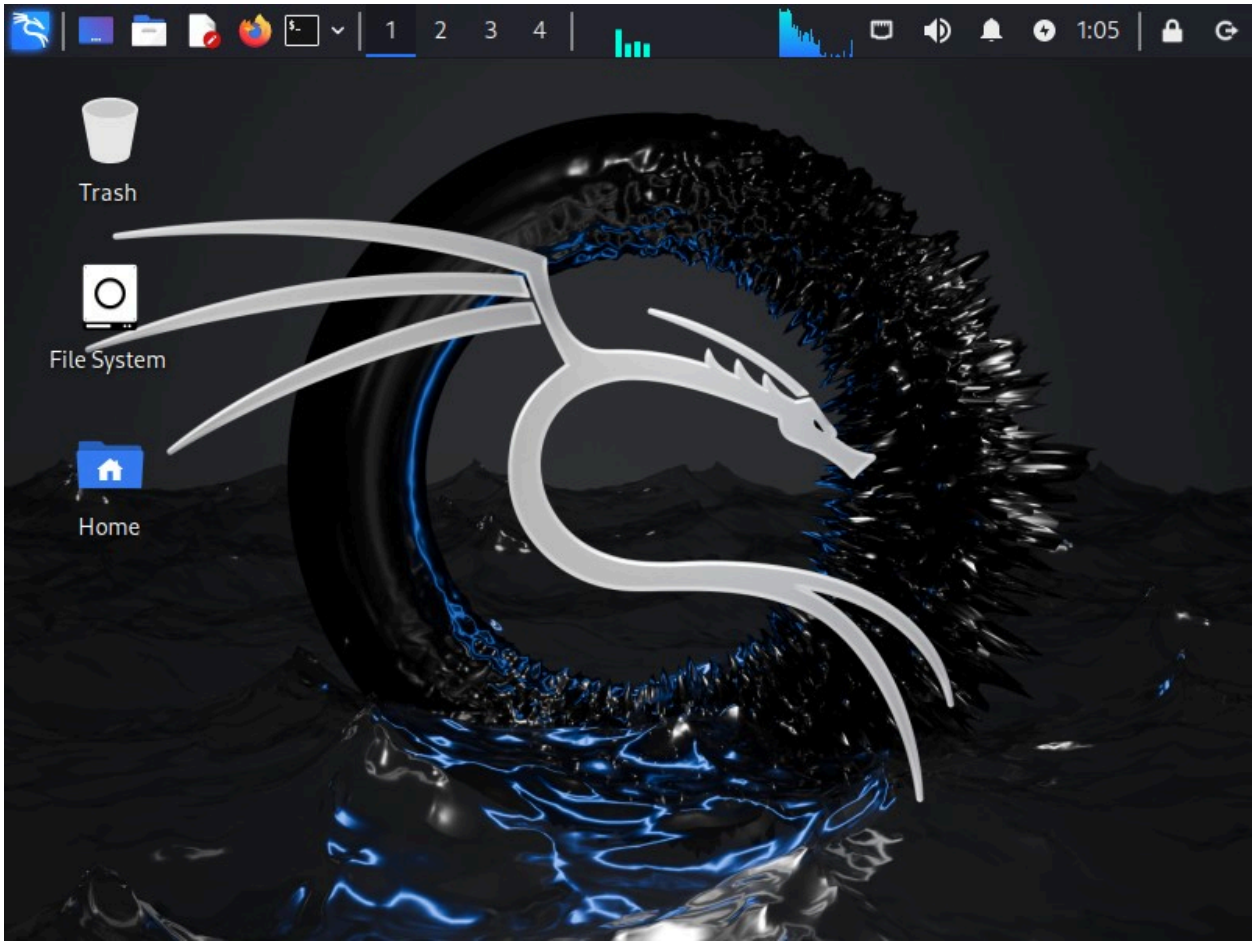

Fig 5: Screenshot of Kali Linux successfully installed

-Installation and Configuration of pfsense

Typically, same process as Kali other than increasing the virtual Processor to 2 for pfsense as against 4 for Kali and setting the additional 4 network adapters to be configured for the 4 internal networks, with the Default switch being the WAN. I disabled the secure Boot and increased the

Processors from the default setting of 1 to 2 to be able to effectively power the processes and activities of pfsense. I also configured additional network adapters, increasing it from 1 (default) network adapter to 5 network adapters and mapped the added 4 adapters to the 4 private networks of Call, Shopping, Admin and DMZ, while the first one which was the default switch, was the WAN and left all of them in one box so that pfsense will be able to control them. The checkpoints were also disabled in order not to break the VM. This was because I discovered that Checkpoint is a file that captures the status and data of the Virtual Machine when in operation. Nicolae & Cappello, (2013) refer to it as periodically saving the state of an application to persistent storage thereby allowing the possibility to resume the application from such intermediate states especially when it goes off. This makes it difficult to restart the VM when there's a problem as a result of the persistent storage. hence it is advisable not to be enabled.

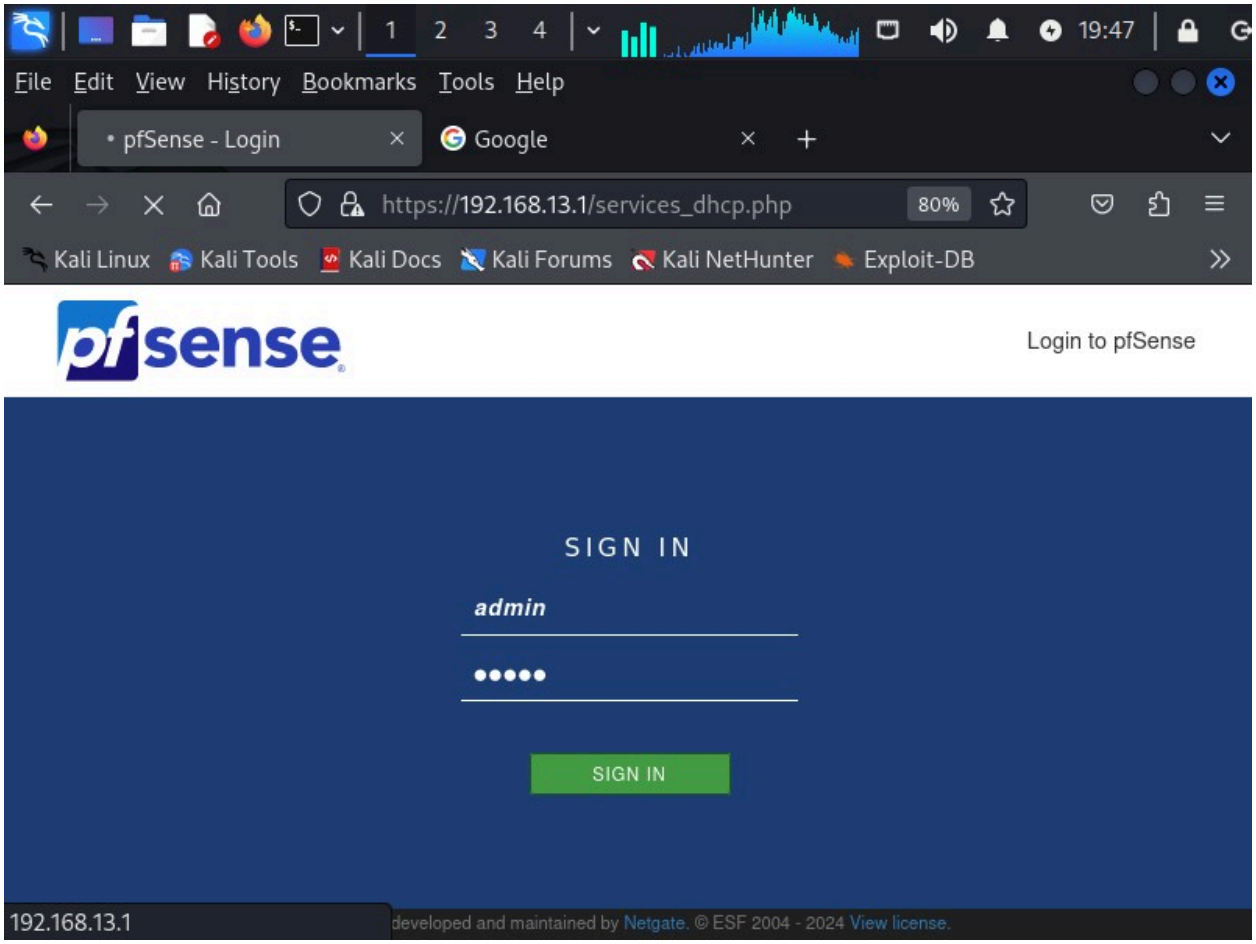

Fig 6: Screenshot of pfSense successfully installed

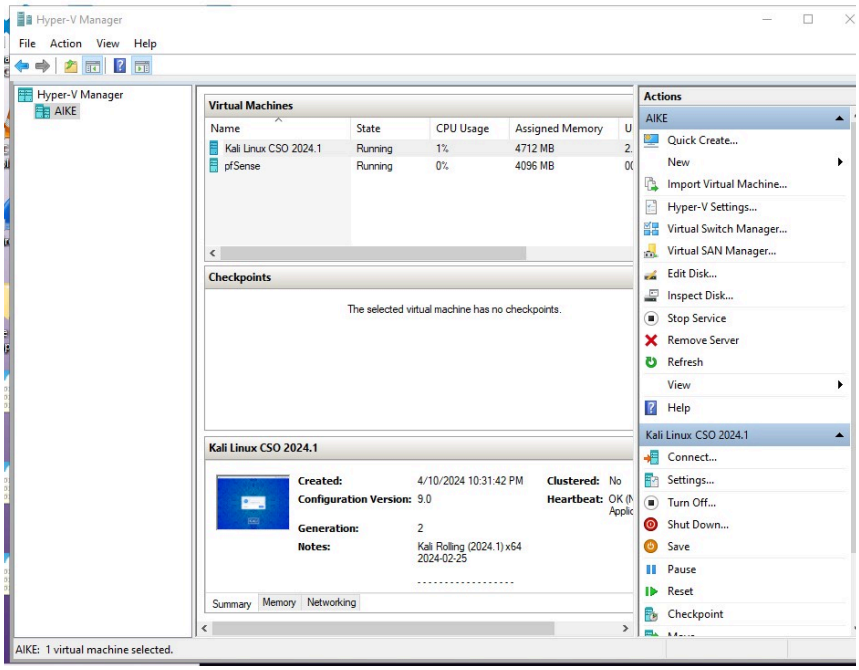

Fig 7: Kali Linux & pfsense successfully virtualized with Hyper V

- Assigning the Interfaces

To get my interfaces to work just as it is in the network topology in fig 1, after setting up the VMs and connecting to the Virtual Switch for connection, I navigated to the interface tab and assignmtn from the drop down to assign the LAN Network to Call Centre and configuring it accordingly with the Call Centre details as depicted in fig 8 below;

Fig 8: Screenshot of my interfaces in pfSense

I followed up with manually adding the other interfaces using the “available Network Port” to create additional LAN networks which I set up for Shipping, Admin and DMZ respectively configuring with the right IP Address, CIDR Range, Subnet Mask as requested.

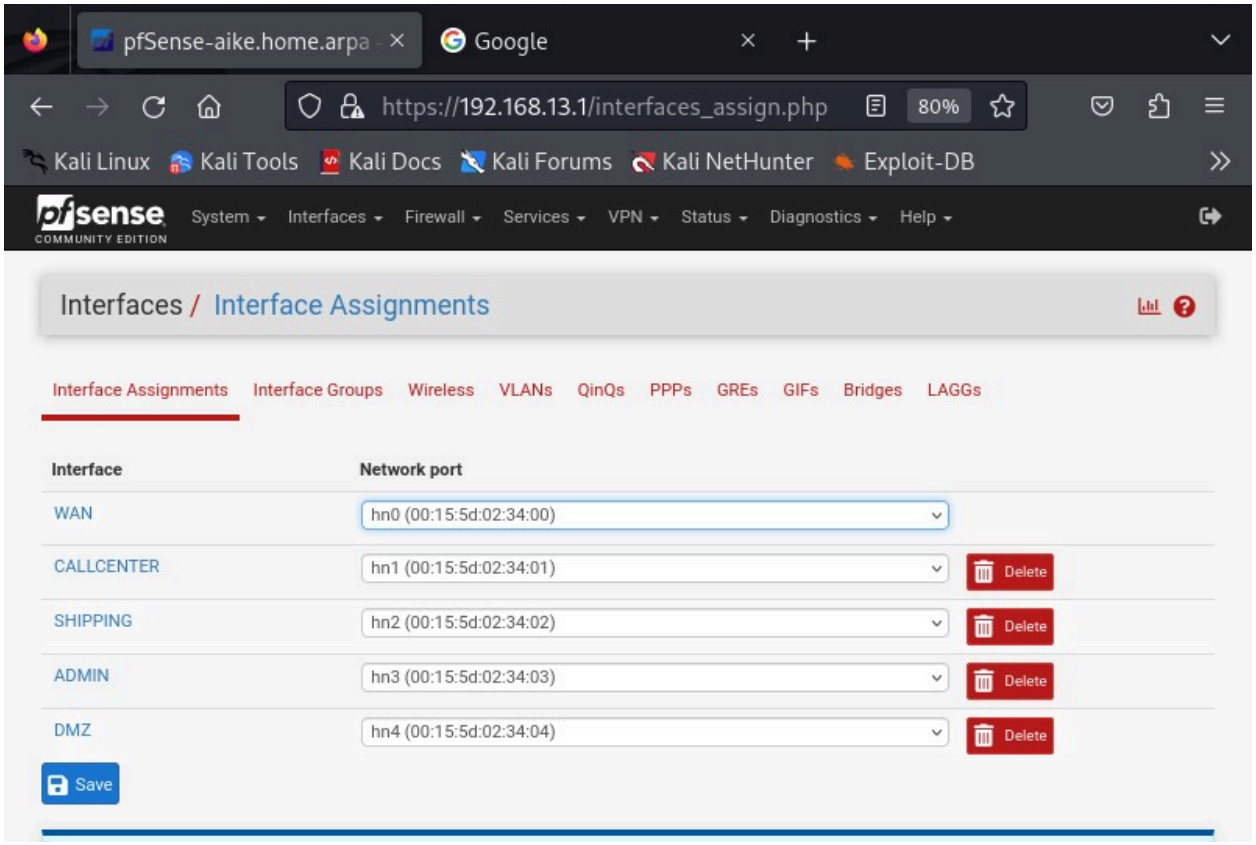

Fig 9: Screenshot of my interfaces in pfSense

-Enabling DHCP Server on my Interfaces and assigning the IP Address Range

I enabled the DHCP server to dynamically assign IP addresses within the subnet. Showing the number of IP Addresses available to each User, I ensured a range that could accommodate the requirements of each departments. For the Call Center, I used 192.168.13.1/24

Call Centre

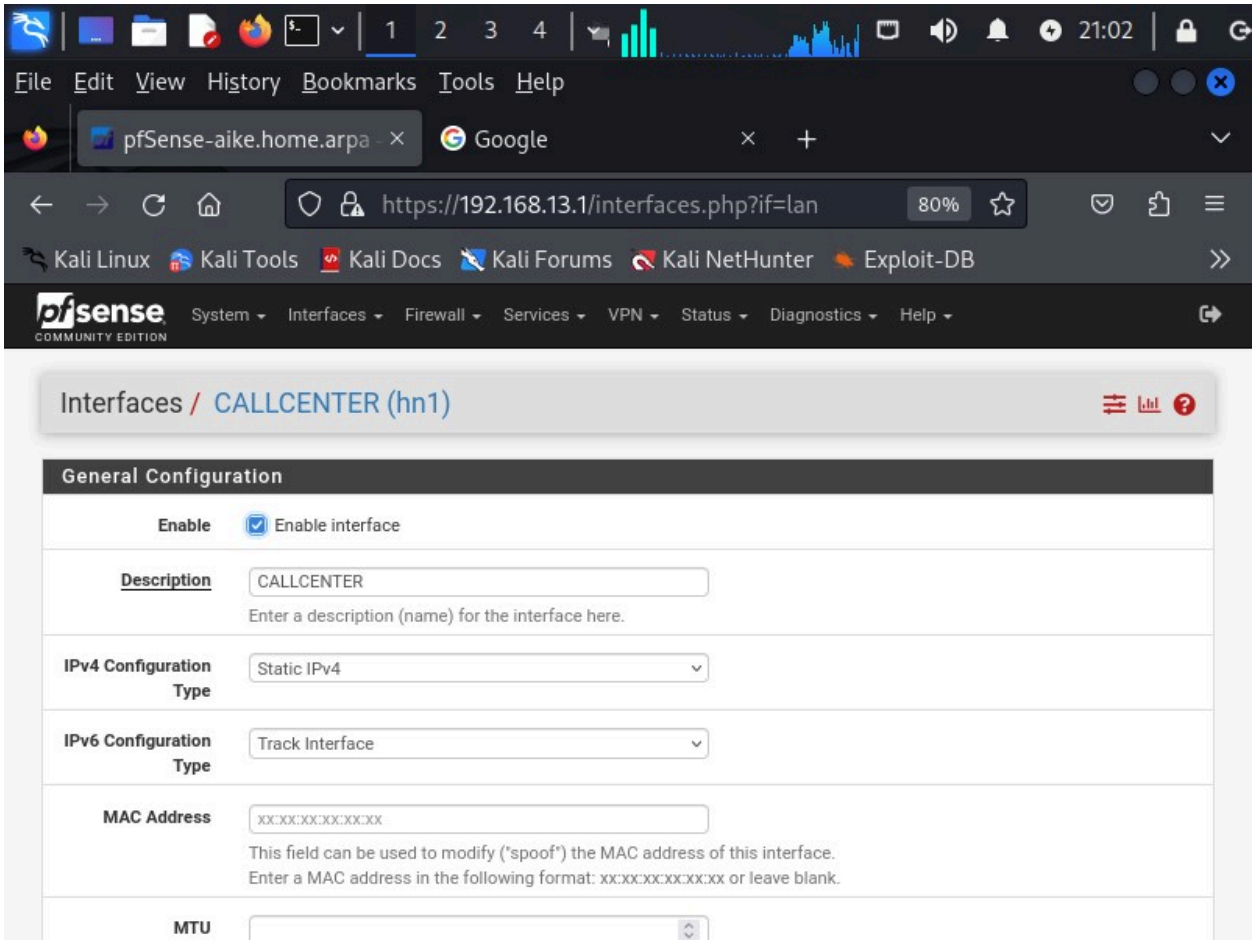

Fig 10: Call Centre DHCP Server Set Up

I did same for all the other interfaces which is for Admin, Shipping and DMZ.

-Configuring FireWall Rules

At Niagara Manufacturing, the Firewall Rules set were for the Call Centre and Shipping to be able to communicate internally and not to assess other departments, Admin was to be able to communicate to them and DMZ not communicate to any network.

I implemented these firewall rules by navigating the firewall section on pfsense, located “Rule” and configured as follows;

I started with setting the Call Centre Firewall rule for DMZ

On the CallCentre interface, I set the Action to “Reject” all traffic going to DMZ. Then set the interface to Call Centre, Protocol to “Any” and Destination to DMZ. This was for the firewall to reject all traffic going to DMZ from Call Centre in line with the network topology and plan. Secondly, I proceeded to configure the Call Centre rule for Admin, this time, the Acton was set at “Pass”, Destination was Admin with the “Invert Match” checked, Interface remained Call Centre and Protocol “Any”. This meant that the firewall should allow all traffic except to Admin. This was because, Call Centre could only communicate with Shipping which was the only remaining department, having already rejected traffic going to DMZ. See the rule below for Callcenter;

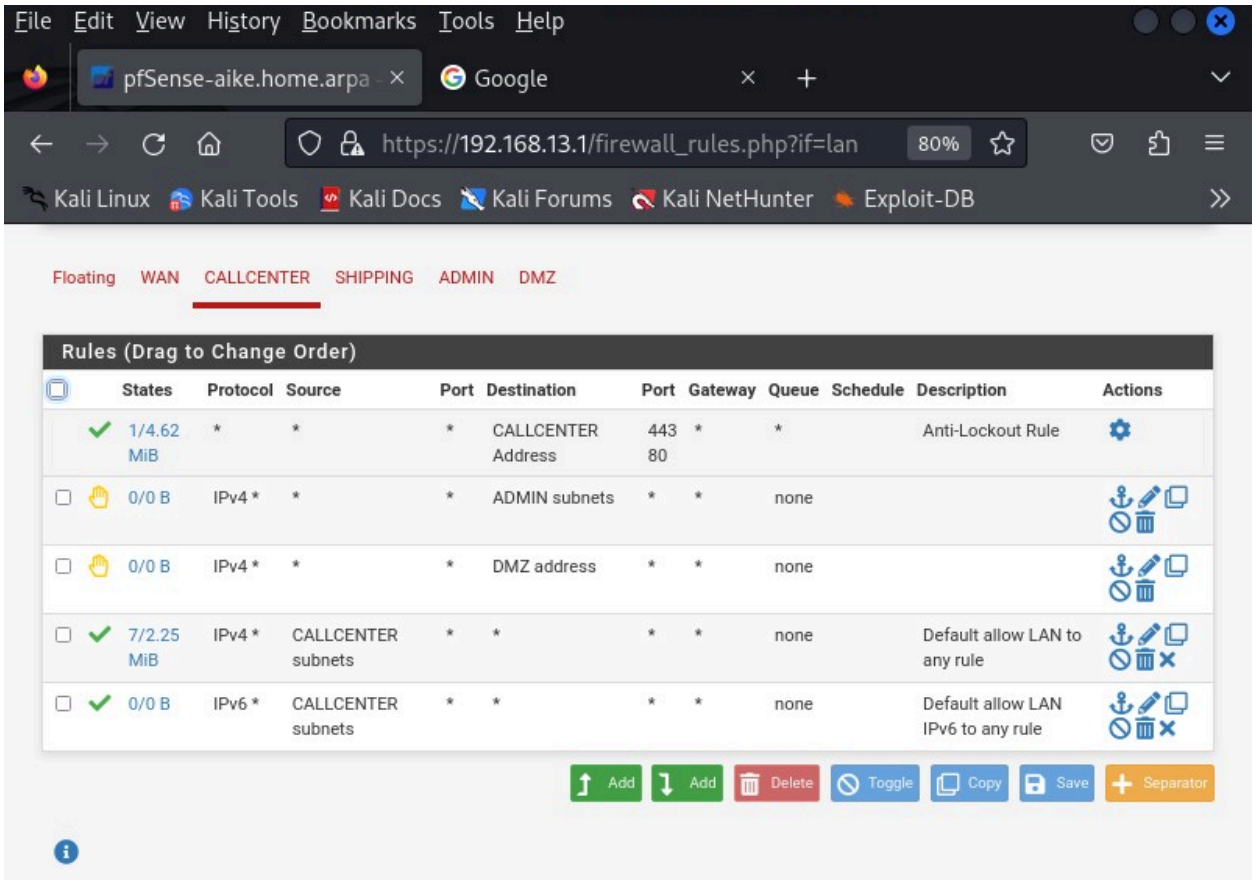

Fig 11: Firewall rule for Call Center

I repeated the procedure for Shipping setting the interfaces to Shipping to reflect same.

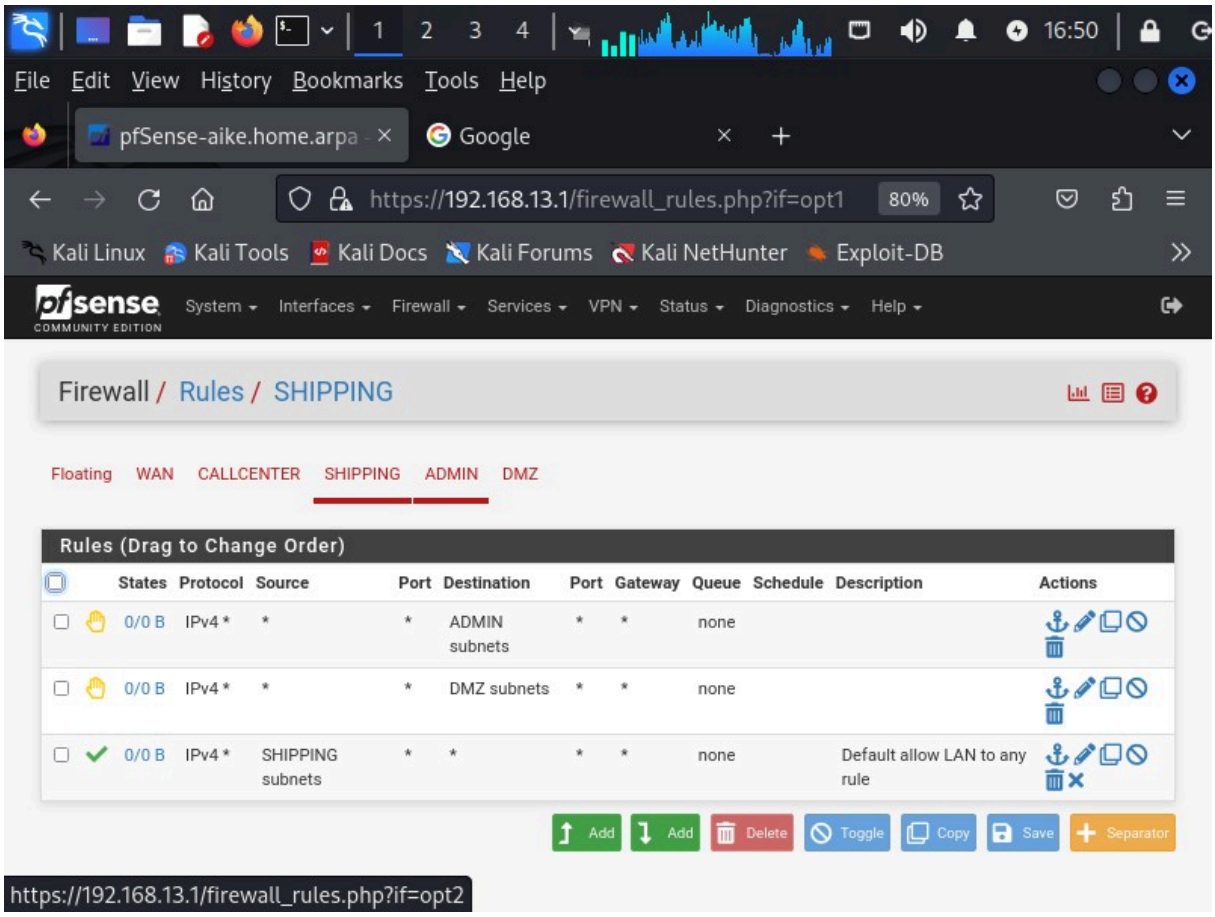

Fig 12: Firewall Rule for Shipping, rejecting Traffic to DMZ, Allow all traffic, but Admin

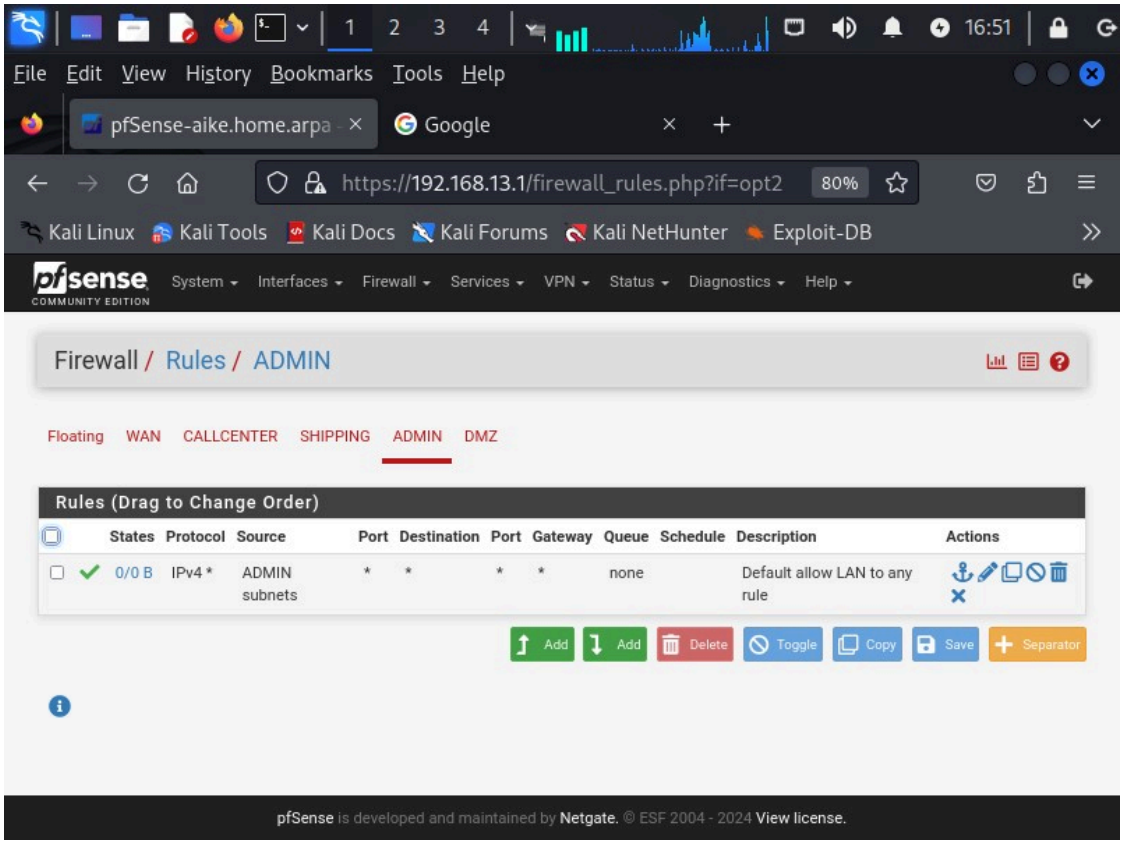

Fig 13: Firewall Rule for Admin

To set the firewall rule for DMZ, I opened the wizard on the firewall, located Rule and clicked on DMZ, then set the Action to “Reject”. Selected DMZ as Interface and “IPv4” as address family and set protocol to “Any” Proceeded to Destination and selected Call Centre net in order to reject assess to call centre network. Then clicked on “save” to apply the firewall rule. Then I copied the rule and modified Call Centre with Shipping.

Did the same for Shipping by selecting Shipping net in order to reject assess to shipping network. Lastly, for Admin, I set Action to “Allow”, Selected DMZ as interface, then set “IPv4” as address family and set protocol to “Any”. This time at Destination, I clicked invert Match and selected “Admin Net” This rule allows for passage of all networks except for Admin.

Then saved.

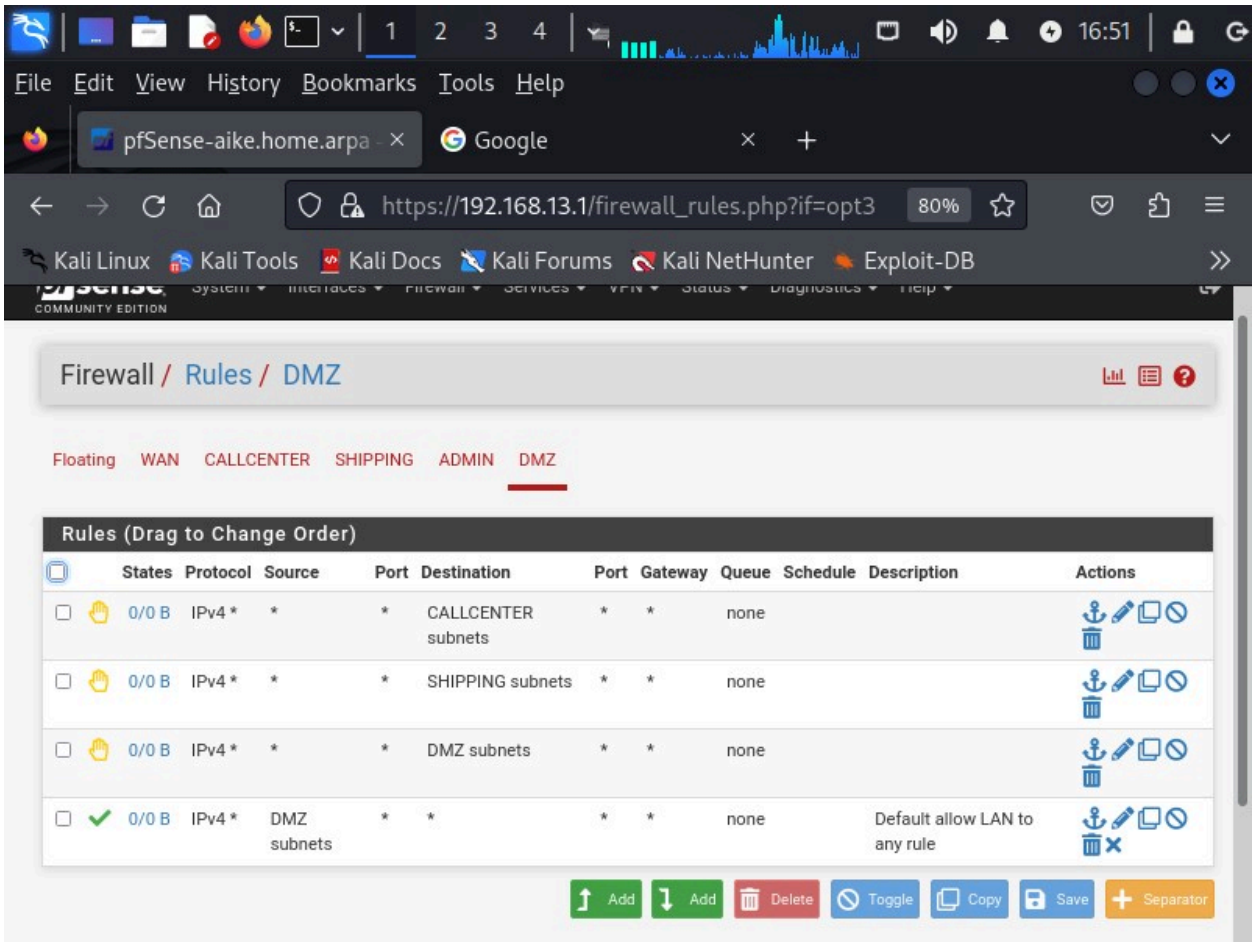

Fig 14: Firewall Rules for DMZ, rejecting traffic to Call Centre and Shipping, and allow all traffic but Admin.

Kim et al., (2013) emphasized the critical role of firewalls in network security due to increasing cyber threats. Firewalls are highlighted as core elements in network security, responsible for allowing or denying network packets by filtering out unwanted network traffic based on predefined security policy requirements. The complexity of managing firewall policies is acknowledged as a potential limitation to the effectiveness of firewall security.

Furthermore, Kim et al., (2013) discusses how a firewall policy may contain anomalies, where a packet could match with multiple filtering rules. Managing these anomalies requires careful

attention to rule relations and interactions to ensure the correct ordering of rules and maintain the security policy semantics. As the number of filtering rules increases, the difficulty of writing new rules or modifying existing ones also escalates, especially in large-scale enterprise networks with hundreds of rules written by different administrators over time.

Kim et al., (2013) highlights the importance of providing effective policy management techniques and tools to enable network administrators to analyze, purify, and verify the correctness of firewall rules. By addressing these challenges, organizations can enhance the security of their protected networks and mitigate potential risks posed by anomalies in firewall policies.

-Testing the Firewall Rules

From Call Centre, I was able to ping Shipping but not Admin and DMZ as seen in Fig 15 Below

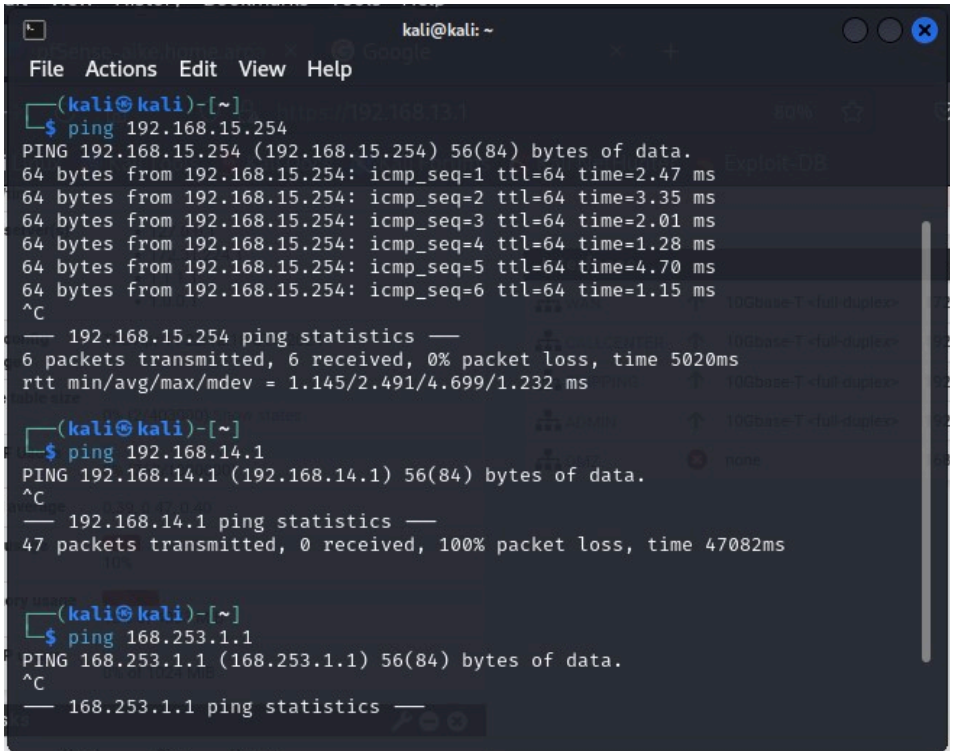

Fig 15: Screenshot of Call Center pinging Shipping, Admin and DMZ

From Shipping, I was able to ping Call Centre but not Admin and DMZ as seen in Fig 17 Below.

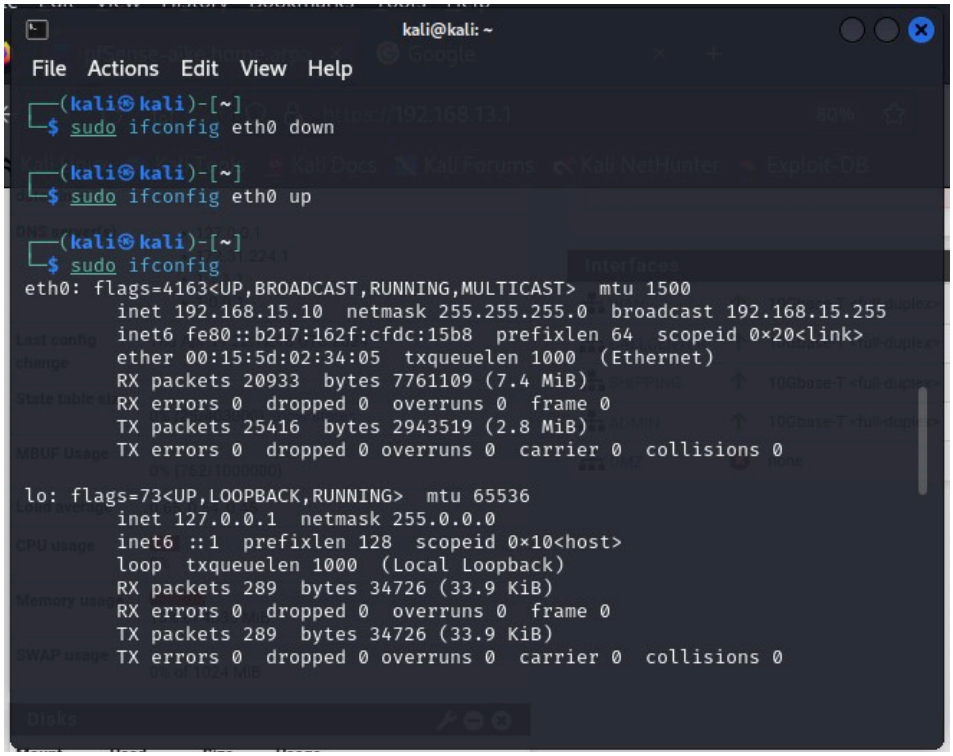

Fig 16: Screenshot showing disabling and enabling of the interface to Shipping

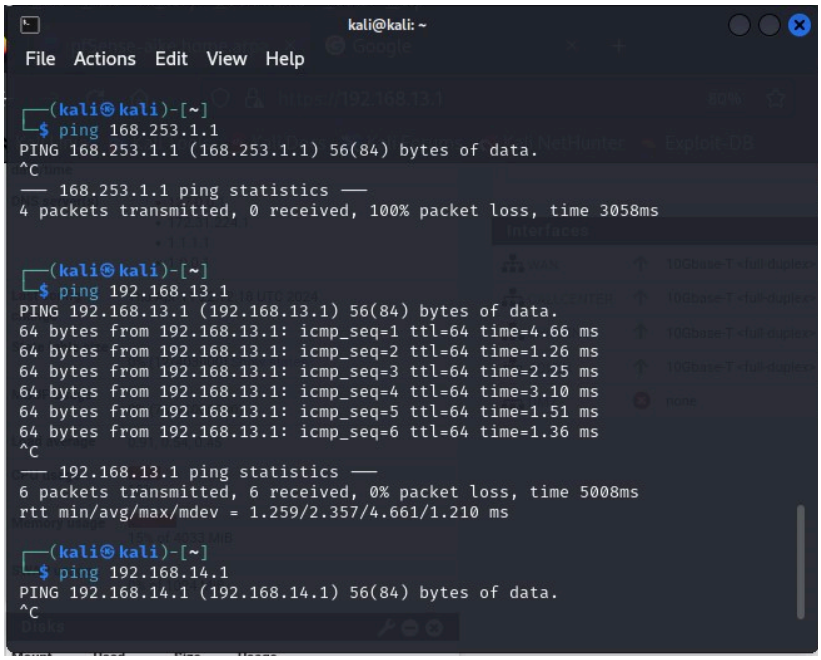

Fig 17: Screenshot of Shipping pinging Call Center, Admin and DMZ

Admin able to ping and talk to Shipping & Call Centre

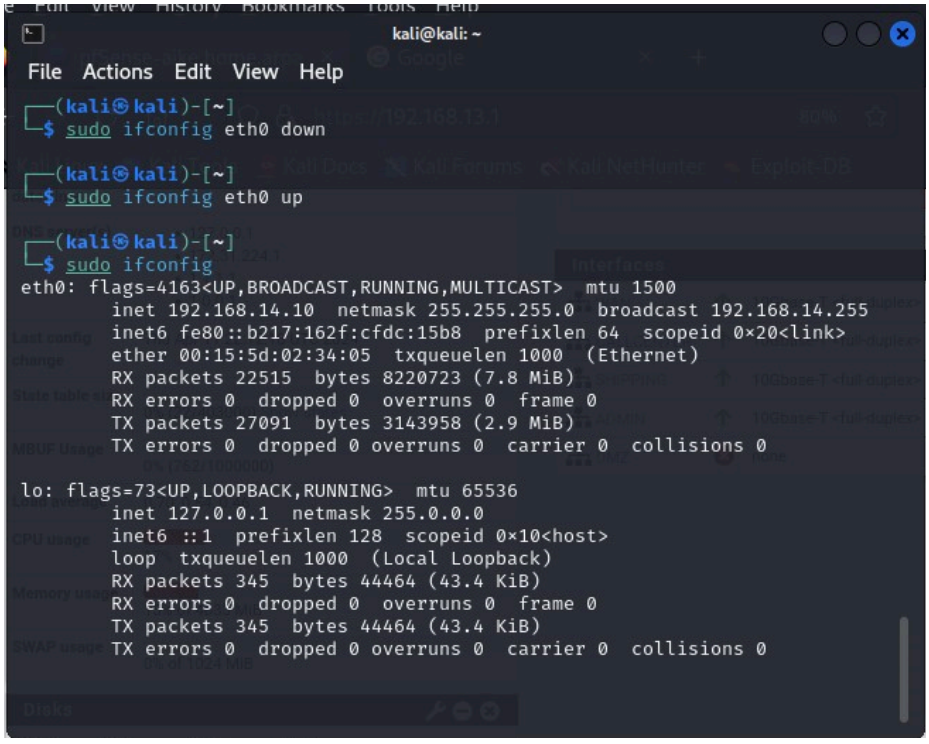

Fig 18: Screenshot showing disabling and enabling of the interface to Admin

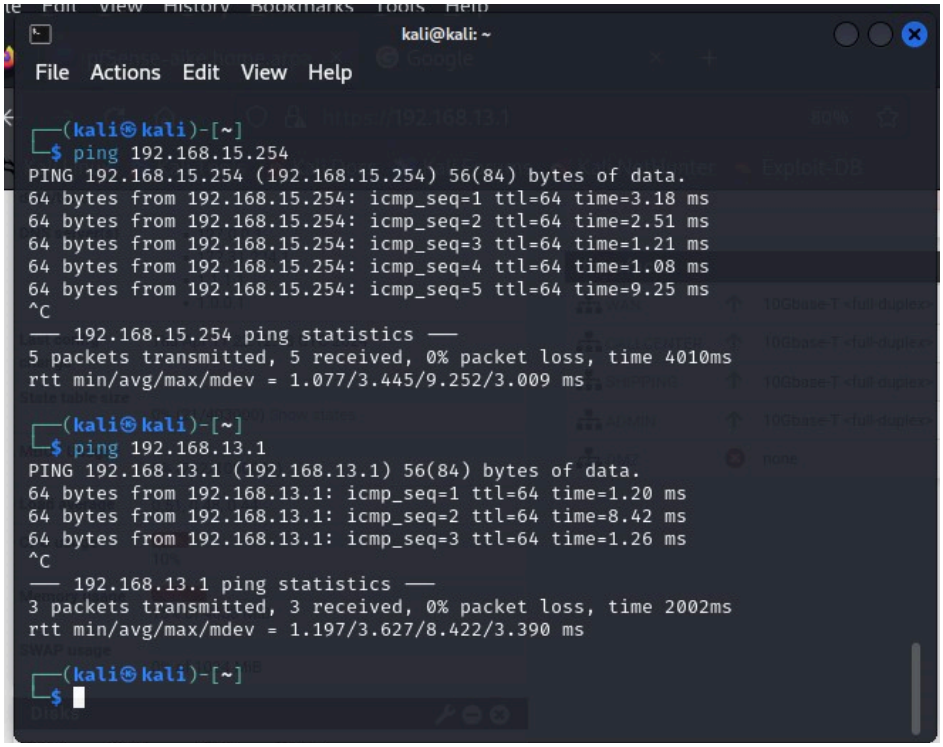

Fig 19: Screenshot of Admin pinging Call Center and Shipping.

TASK 3

-Implementing Additional Features

Niagara Manufacturing cannot afford fiber-optic-based internet connection and would rather rely on a cable-based connection and because of that, they are worried about the attendant issues with their VoIP phones such as apparent call dropping, and therefore will require lower and more consistent Latency. This required implementing a traffic shaping limiter that uses CoDel Active Queue Management to improve the reliability of latency on the networks. For starters, it is necessary to start by testing the network for latency using the buffer bloat Internet Speed test. This will enable me to know the up and down speed of the internet.

Latency is the time it takes for a data packet to move from one point to the end across a network. In other words, it is simply the delay or lag in communication, such that a longer delay will be known as High Latency while a faster transmission time will be low Latency. Therefore, the lower the Latency, the better the network.

Kuhn et al., (2017) described buffer bloat as a phenomenon in computer networking where excessive buffering of data packets occurs within network devices such as routers and switches. This excessive buffering can lead to significant latency and jitter, degrading the performance of real-time applications such as VoIP calls. When a network device experiences congestion, such as during periods of high traffic or when data rates exceed the capacity of the network link, packets can be queued in buffers awaiting transmission. If these buffers are too large, they can hold onto packets for longer periods than necessary, increasing latency and causing delays. This delay can be particularly problematic for real-time applications that require low latency to function effectively like the company's VIOP Phones. This is where we require traffic shaping to ensure flow for the priority packets.

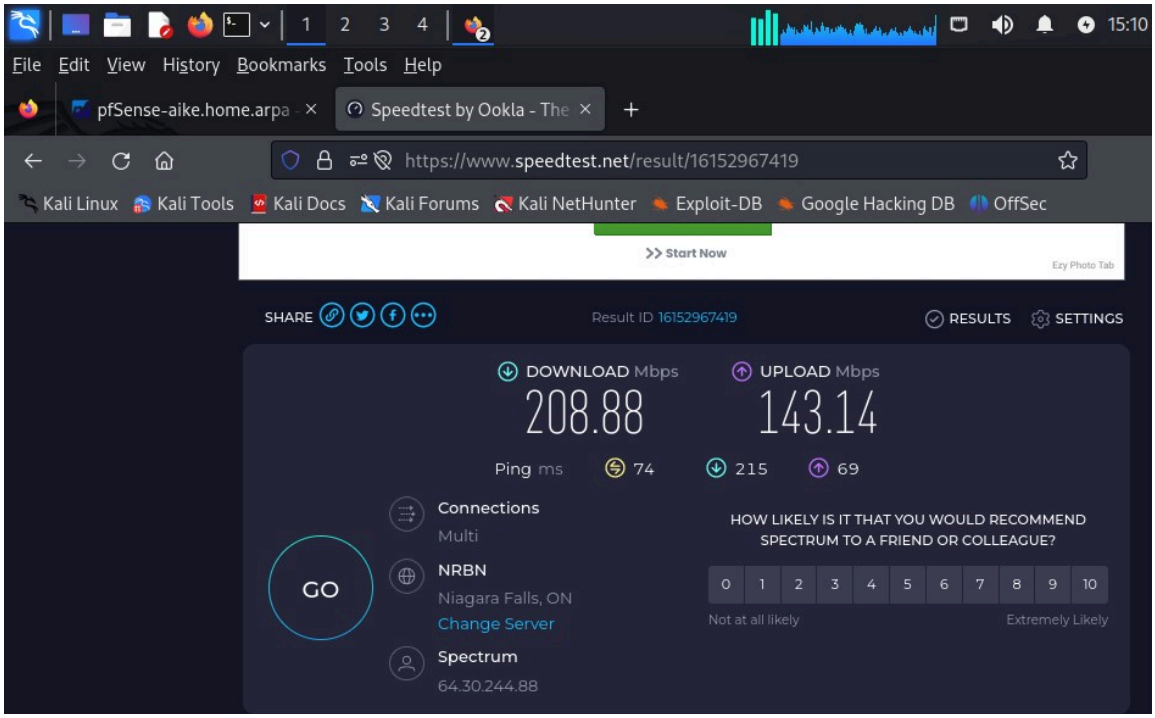

Fig 20: Screenshot of my bufferbloat test showing my up and down bandwidth.

Kim, (2014) explores the practice of traffic shaping by Internet service providers (ISPs) and its impact on user experience in broadband shared access networks. It disucsses the importance of shaping subscribers' traffic to regulate the flow of data and ensure quality of service for different types of traffic. The study emphasizes the need to base the design and optimization of access networks on user behaviors and actual performance perceived by end-users. By using traffic models based on user behaviors and application/session-layer metrics, the research aims to quantify user-perceived performance for various types of traffic, including HTTP, FTP, and streaming video.

According to Kim, (2014), Traffic shaping was designed for connection based networks to regulate a network flow at a user network interface even as Internet Service Providers now use it to regulate combined flows from a subscriber in different mode of connectionless IP networks. Traffic shaping is aided by the limiter to prevent occasional traffic peaks in the network. It

reduces traffic into the network and can be used to block or rate limit certain applications and improve the quality of service utilizing an Active Queue Management AQM algorithm to boost the reliability of the network and ensure needed packets are processed as required and not just on first come first served basis. The AQM available for use in the project was CoDel. CoDel, an abbreviation for Controlled Delay is an Active Queue Management AQM algorithm for countering buffer bloat.

Kim, (2014) also discusses the challenges and issues associated with current ISP traffic shaping practices, such as the lack of formal definitions for traffic conformance and the difficulty in providing different levels of Quality of Service (QoS) to diverse traffic flows from the same subscriber. It points out the conflicting requirements of guaranteeing QoS to subscribers while efficiently sharing unused capacity among them. It suggests that the proper sizing of the token bucket, which determines the average and peak rates of a service, is crucial for effective traffic shaping by ISPs. Overall, the research provides insights into the complexities of traffic shaping in shared access networks and its implications for user-perceived performance.

Kuhn et al., (2017) also states that the authors of CoDel claim it controls delay while being insensitive to Round Trip delays, link rates and traffic loads.

However, the traffic shaping here is for a different purpose. The cable connection is apparently epileptic with latency, therefore requiring active queue management to delay the packets in the network in order to perform optimally. Hence, the first thing I did was to test the network for buffer bloat. Basically, to check the reliability of the network. So on Kali VM, I launched the Firefox web browser, typed speedtest.com and clicked on the Go button, which ran the test. Result yielded; 208.88mbps Download and 143.14mbps Upload, implying that my connection was ok and at optimal performance level as shown in Fig 20 above.

-Configuring the Traffic Shaper Limiter

To configure the Traffic Shaper Limiter, I proceeded to Firewalls Tab, under traffic shaper, opened the “limiters” tab, and clicked new limiter. I configured the limiter and then the Queue, following the guideline on the pfsense documentation. I highlighted “Enable limiter”, Set the name to “WANDown” Set the Bandwidth to the value in Mbit/s that I got during the Buffer Bloat test which is 200, Queue Management Algorithm was set to “Tail Drop” (This basically ensures it is turned off when it should be off). Selected “FQ_CODEL” for the scheduler and Set queue length to “1000”, then clicked on Save and add New Queue, following the guide.

Then clicked on Add New Limiter and repeated the same process for the WANUp. These eventually turned out as below, with the Limiter appearing as a folder and the queue as a sub directory.

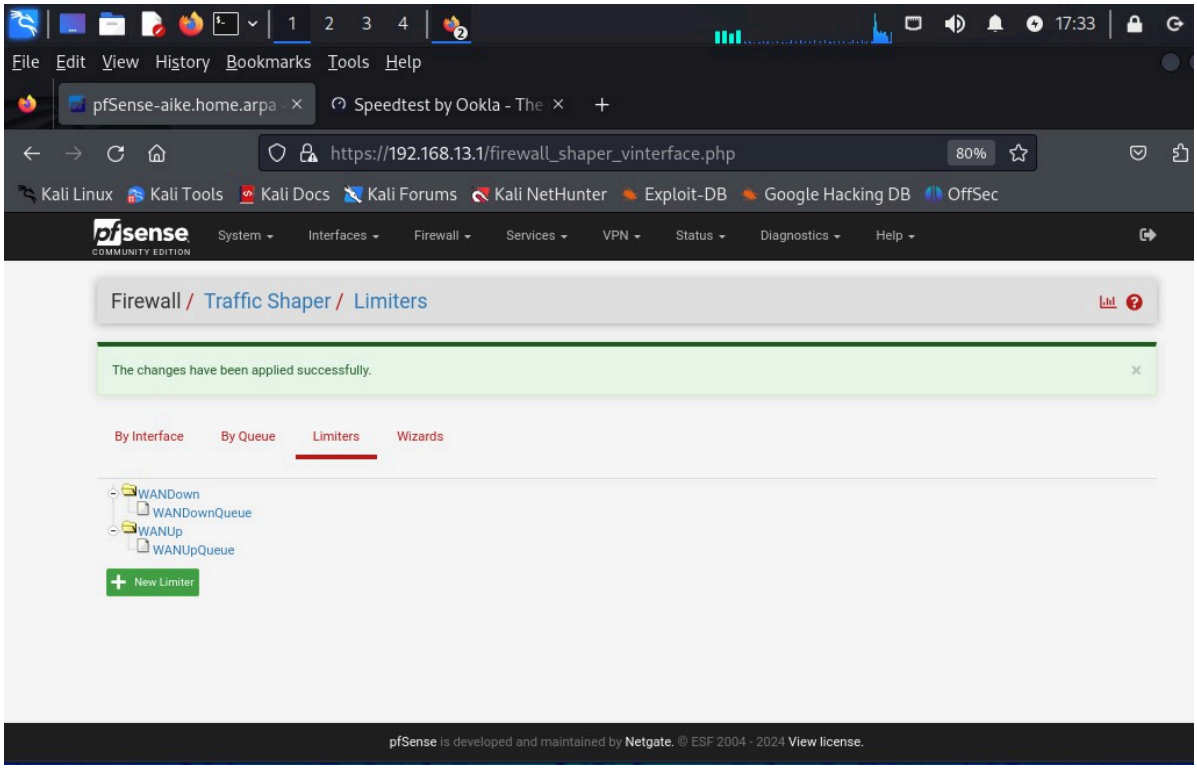

Fig 21: Traffic Shaper Limiter

I then applied the limiters to the firewall to operate effectively.

-Setting the Floating Rule

Configuring and saving the Traffic Shaper tool, does not mean it is in effect, as they are currently working but are not receiving or dealing with any network traffic. They are only set up and ready to go. I have to create a floating firewall rule.

To create the Floating firewall rule, I proceeded to set the firewall rule on the floating tab. The floating tab enables the rule to float across the interfaces i.e apply to the interfaces. Using the pfsense guide I configured the firewall rule on the floating tab using the WanUpQueues and WanDownQueues from the limiters earlier set up. This was set up on the WAN interface using the WAN DHCP address. Then saved and applied the changes. I then checked the buffer bloat again after manually reducing the download speed to 1 for both WANDown and WANUp and discovered that the test result was not much different from the first. The Buffer Bloat Grade remained A. However, the pfdocumentation notes that if a score does not improve, there might be a configuration issue, citing examples of how the bandwith values being higher than what the circuit can deliver, the queue sizes may need increased or the coDel parameters need change.

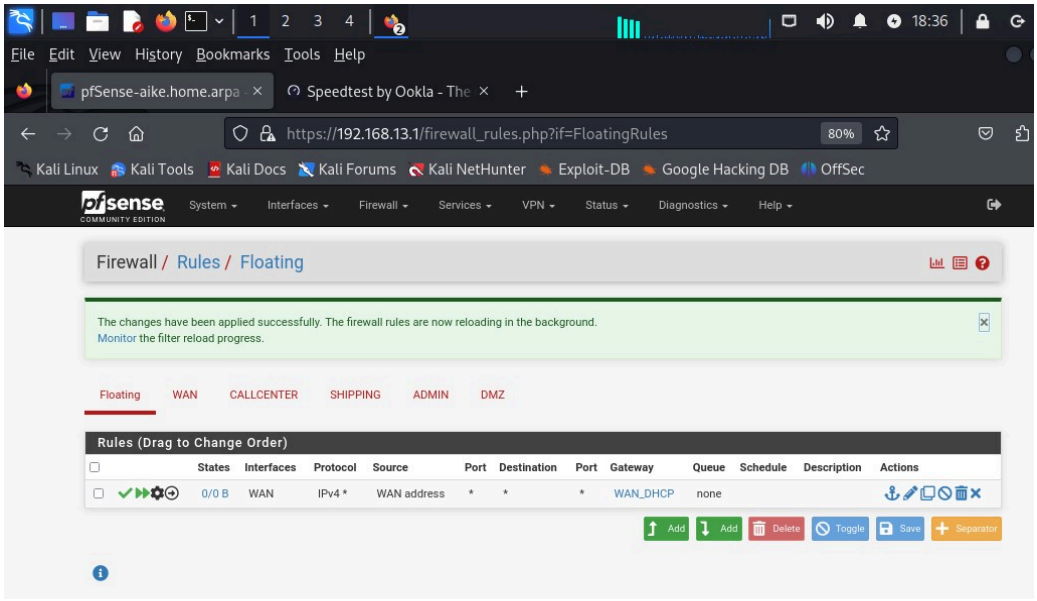

Fig 22:

Screenshot of Traffic Shaper limiter

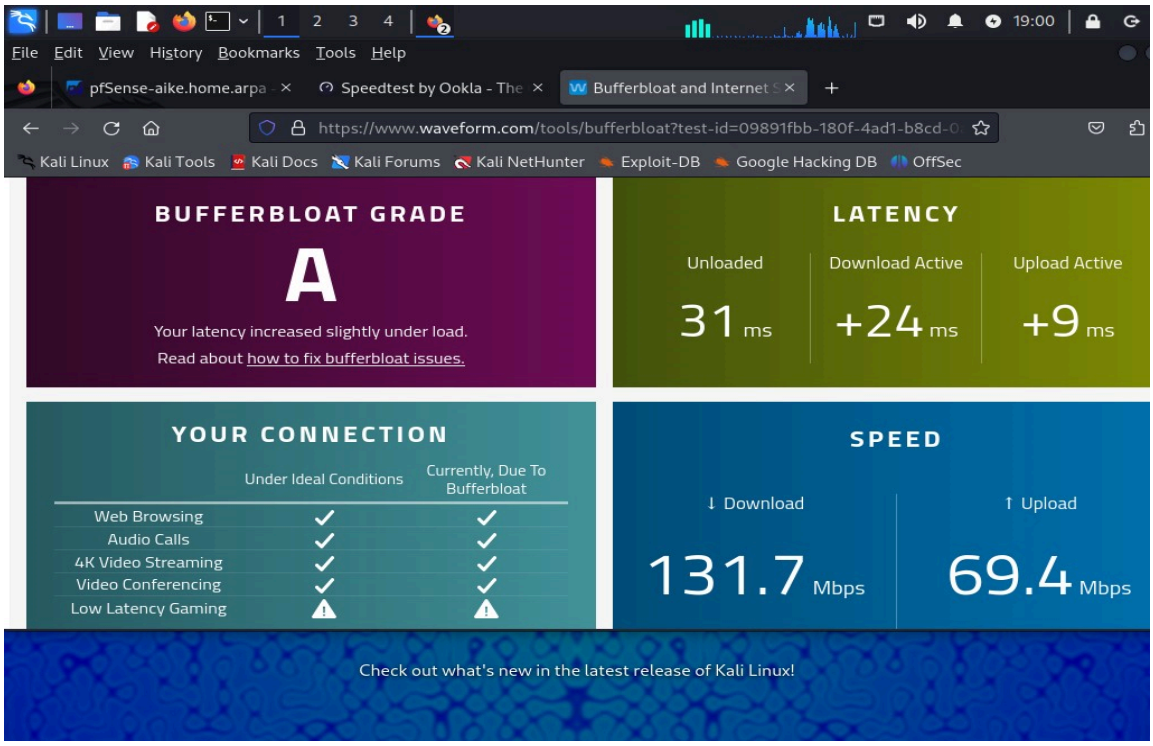

Fig 23: Screenshot of Buffer Bloat Test

-Port Blocking

As a network engineer for Niagara Manufacturing, I was faced with the problem of selecting the right ports to open or block in the course of this project, this is because of the implication of opening or blocking a wrong port. According to (Hussain et al., 2012) opening the wrong ports could expose the clients to dire consequences while blocking the wrong ones can restrict users from accessing desirable services including web browsing, FTP services, mails services etc. Therefore, due caution must be taken to select the ports in order to avoid issues for the clients. The situation is made worse by the sheer number of available Ports. The Author indicated that a maximum of 1,024 ports has to be opened out of a maximum of 65,536 ports. This was corroborated by Cheng & Tang, (2013) who further identified that Port exploitation based

network intrusion, mainly exploit common ports, and attacks hosts through known system bugs as well as, planting of Trojan horses to victim hosts through backdoors opened by other network vulnerabilities. It is worth noting that port numbers used by various malicious software (e.g., Trojan programs) are widely distributed and don't only use registered ports. Several articles have been written with some sharing their thoughts on the vulnerability of some Ports, such as Baykara, (2022), in an article published by the PCIDSS, who reinstated the SANS institute's recommendation of at least blocking outbound traffic using some protocols including the (SNMP) UDP Port 161. The Simple Network Management Protocol is used by Network Administrators to monitor devices such as the computer, router, switches etc. However, it has limitations which can be exploited by criminals. This is because it is often used without any encryption which makes it a security risk. Although, there is a Version 3 of the protocol which has enhanced security features, however it is also still somewhat vulnerable and does not exactly pose commensurate benefit to the client. Schrader, (2022) Identified that Port 21 (FTP) is File Transfer Protocol ports that allow users to send and receive files from servers. He further noted that FTP is known for being outdated and insecure and therefore often attacked by brute-forcing passwords, cross site scripting. It also allows for anonymous authentication, which allows logs into the port with "anonymous" as username and password. The Author also identified that Port 23 Telnet is a TCP protocol that connects users to remote computers but has been superseded by Port 22 SSH (secure Shell) and as such it's outdated and insecure and therefore vulnerable to numerous attacks. It also sends messages in plain text, zero encryption. Consequently, these were the 3 Ports I decided to block for Niagara Manufacturing to protect the Organization from these known vulnerabilities. Some other Ports were also suggested for blocking by these authors, however, the consideration that this is a business that may be adversely affected by such

restrictions outweighed the concerns generated. Also, the implemented Router, the firewalls in place coupled with the disciplined practice in the organization more than compensates for that.

To configure the ports blocking, I went to Firewall tabs and clicked on Rules from the dropdown, clicked on CallCenter tab and copied the first rule, set the destination, admin and protocols to block the protocols/ports' traffic on the respective interfaces.

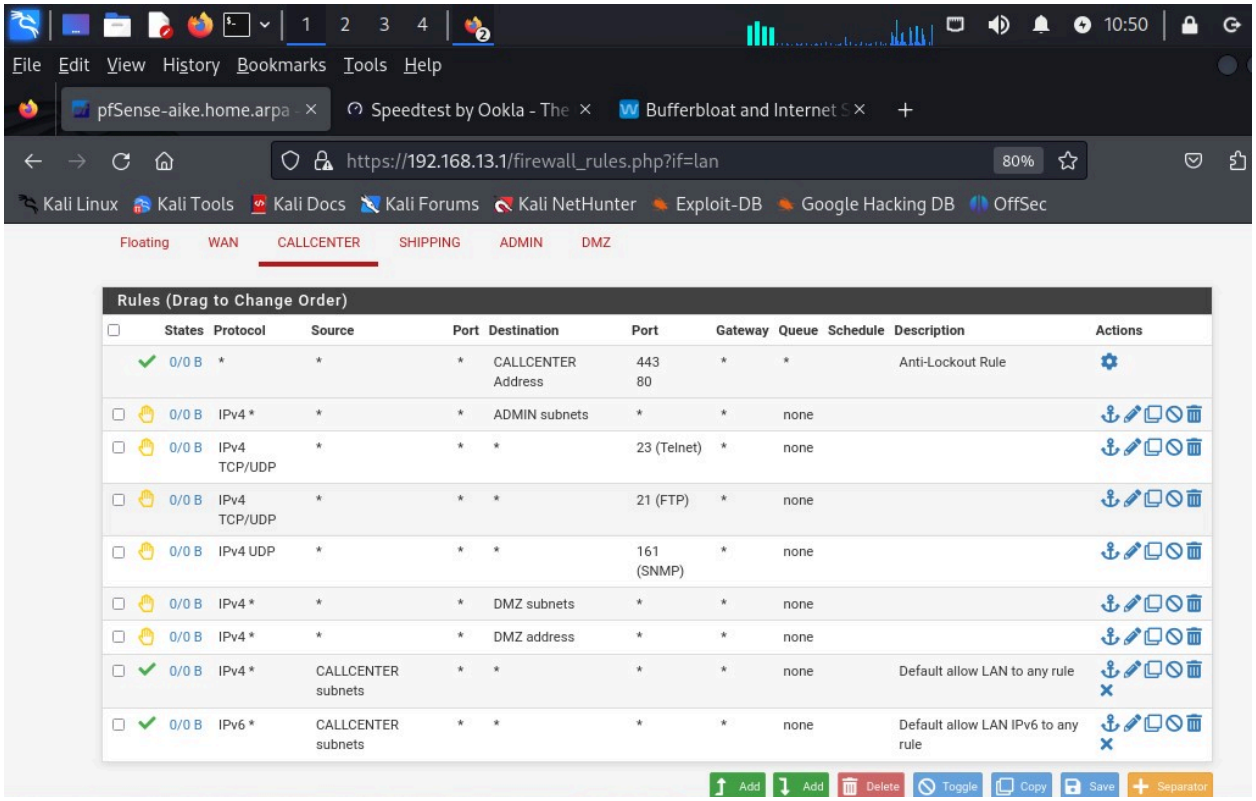

Fig 24: Port Blocking on my Call Centre Interface

Port 443 80 remains open in order to occasionally be able to talk to pfsense to make changes.

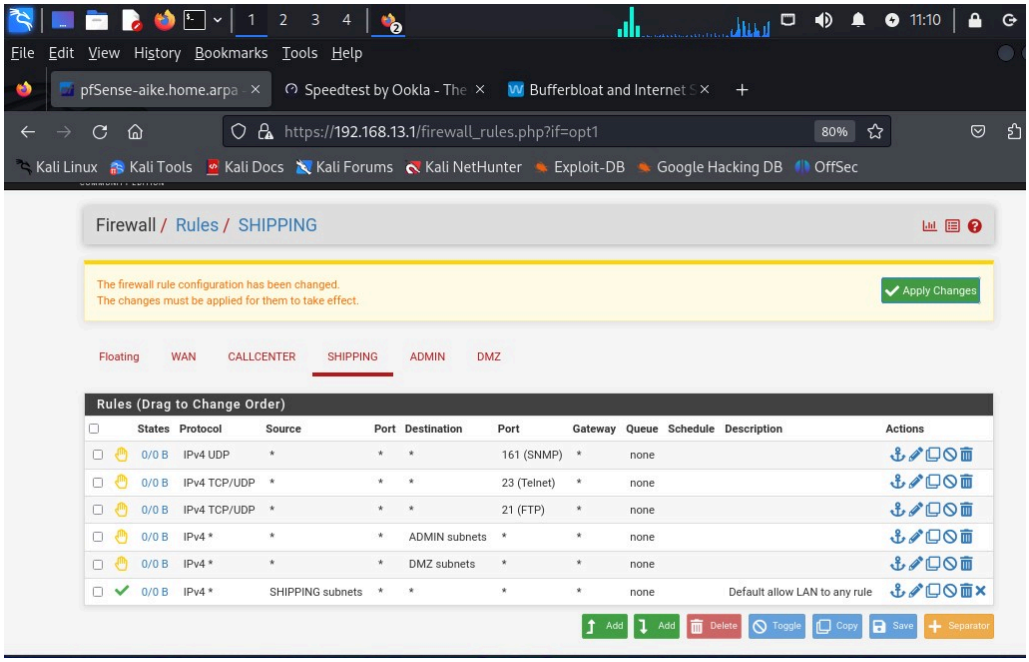

Fig 25: Firewall Rule on Shipping Interface.

-Universal Plug and Play and NAT-PMP

Universal Plug & Play UPnP is used to conveniently connect devices on the same network without configuration. As the name suggest, it is convenient and easily compatible with devices on the same network. This is why it is commonly used for Internet of Things IoT devices, Gaming Consoles and video streaming. However, it is vulnerable.

Chen et al., (2008) explores the integration of services with a UPnP agent for smart home environments, emphasizing the significance of consumer electronics and intelligent appliances in modern homes. It discusses the development of a smart campus network using enhanced UPnP technologies to provide individualized information to users at the right time and place. Chen et al., (2008) aims to simplify user interactions with technology and enhance the overall living experience. It showcases how UPnP facilitates seamless connectivity between devices and networks, enabling automatic configuration and communication with devices on the Local network. While this simplifies the network setup and enhances user experience by automating

connectivity processes such as device discovery and service integration espcially in a home setting, it is rather worrisome to be used in a corporate network such as Niagara Manufacturing. Although, there are capabilities in some routers that can offer some protection provided they are regularly updated, the security risk it poses far outweight the convenience this provides to Niagara Manufacturing. It is more commonly used and needed in a home environment than a corporate setting, with terrabytes of customer's information kept in trust, a breach could potentially ruin the firm, hence my decision not to enable it on their interfaces.

Snort

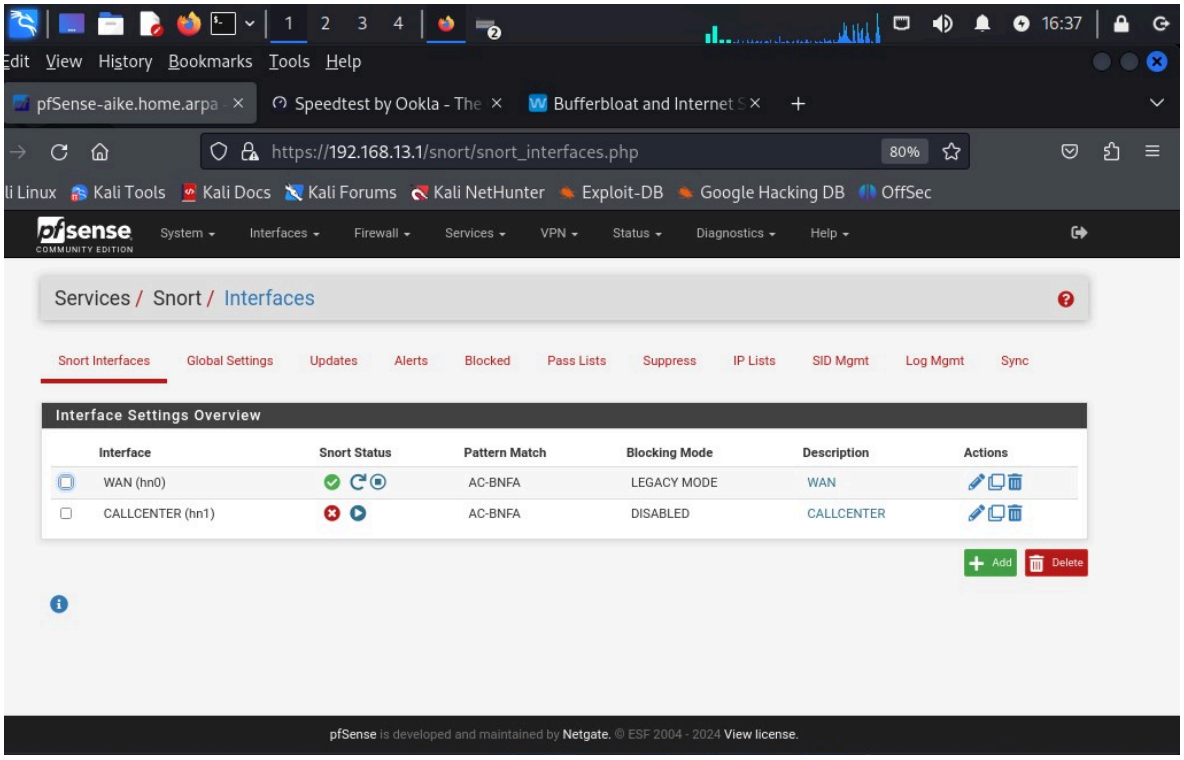

Fig 26: Screenshot of Snort package installed.

As a company that is transitioning to a digital marketplace with an in-house infrastructure that supports both intranet and internet connectivity, choosing Snort over pfBlocker-NG basically aligns with the need for robust intrusion detection and prevention capabilities. This is because the company will be venturing into a space where online threats are prevalent, hence having a

dedicated intrusion detection and prevention system like Snort will enhance the security posture of their infrastructure, safeguarding sensitive data, customer information, and business-critical assets from potential cyber threats.

While pfBlocker-NG offers DNS-based blocking and filtering capabilities, which can be useful for controlling access to specific websites and filtering malicious domains, it may not provide the comprehensive intrusion detection and prevention features required for protecting NM's digital infrastructure. Therefore, opting for Snort would better align with the company's security needs and strategic objectives in transitioning to the digital marketplace.

Waleed et al., (2022) offers a detailed examination of using Snort as a potential solution for implementing a basic intrusion detection/prevention system (IDS/IPS) in a digital marketplace such as Niagara Manufacturing. Snort, known for its widespread use as a signature-based IDPS tool supporting both IDS and IPS modes, is highlighted for its relatively ease of configuration and ability to monitor network traffic. Waleed et al., (2022) emphasizes Snort's capability to compare received packets against signatures and preset rules, log attacks, and provide attack statistics, making it a valuable tool for detecting and preventing intrusions in a digital marketplace setting. However, the evaluation also points out limitations in Snort's performance under high traffic rates, particularly in the multi-threaded version, due to inefficiencies in the implementation of the multi-threaded architecture.

Furthermore, Waleed et al., (2022) underscores the importance of considering Snort's default packet capturing module, Libpcap, and the subsequent stages in the detection process, such as decoding packets, normalization, and rule application. While Snort excels in misuse detection and alert generation in IDS mode, it falls short in supporting anomaly-based detection by default. In IPS mode, Snort can block malicious packets, enhancing its capabilities for intrusion

prevention in a digital marketplace environment. The evaluation provides valuable insights into Snort's functionality and performance characteristics, enabling organizations to make informed decisions when selecting an IDS/IPS solution for network security in a digital marketplace. Lastly, the study's findings suggest that while Snort offers essential features for implementing an IDS/IPS in a digital marketplace, it may face challenges in handling high traffic volumes efficiently, especially in the multi-threaded version. Organizations considering Snort for their network security needs in a digital marketplace should weigh its strengths in signature-based detection and alerting against potential performance limitations under demanding conditions.

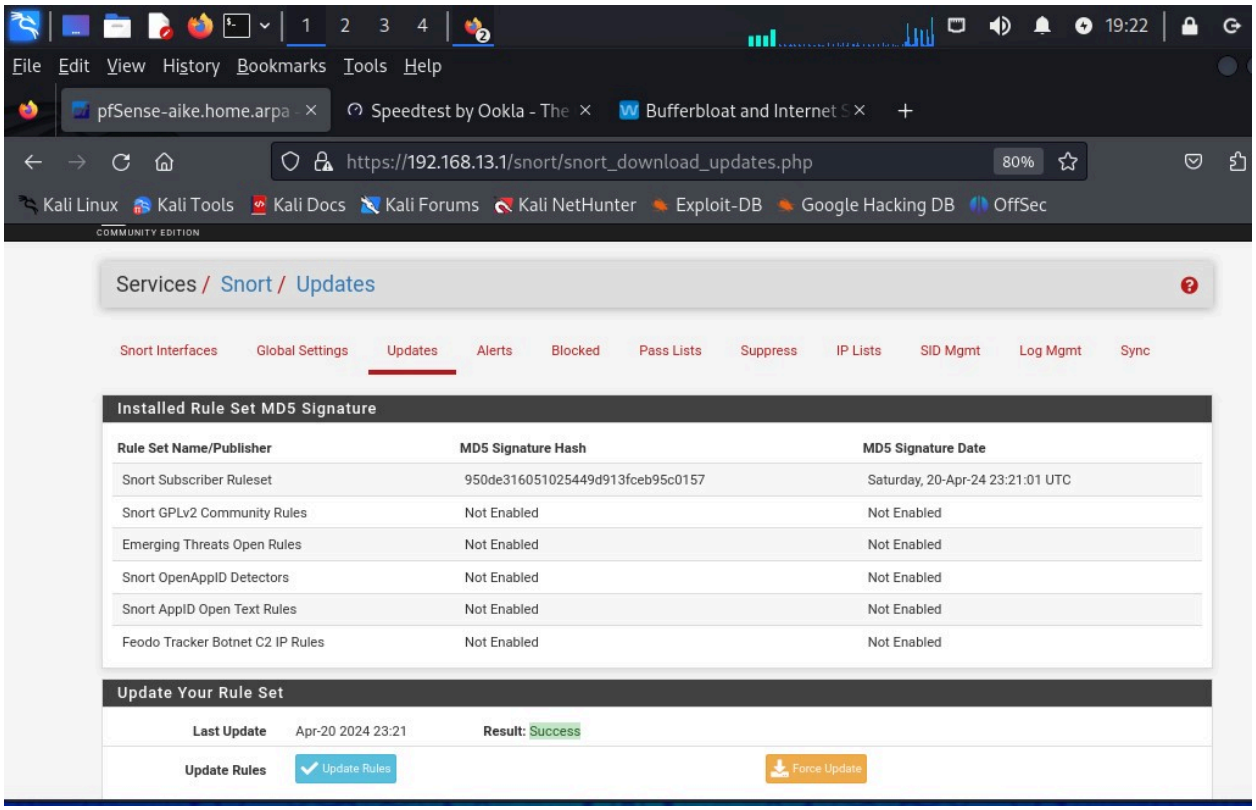

Fig 27: Screenshot of Snort VRT and Emerging Threats Open rule packages successfully downloaded.

-Zero Trust Framework

Tang et al., (2023) present a privacy-preserving authentication scheme based on zero trust architecture, emphasizing the importance of identity authentication in ensuring data security in digital communications and networks. Zero trust architecture challenges the traditional network security model by eliminating the concept of trusted and untrusted entities, emphasizing continuous verification and access control. By utilizing a Traceable Universal Designated Verifier Signature (TUDVS), the proposed scheme aims to protect user privacy by preventing server administrators from disclosing client access behavior to third parties. This approach aligns with the principles of zero trust, where every access request is treated as potentially malicious, and strict authentication measures are implemented to mitigate risks.

Transitioning from brick-and-mortar retail to the digital marketplace requires a robust network infrastructure that can support both internal and external connectivity while maintaining security and privacy. Implementing measures based on zero trust principles becomes crucial in this scenario to safeguard sensitive data and prevent unauthorized access. By adopting a privacy-preserving authentication scheme like the one proposed by Tang et al., (2023), businesses can enhance their cybersecurity posture and ensure secure communication channels for both intranet and internet connectivity.

Huang et al., (2023) also presents a comprehensive approach to enhancing security in power IoT environments by integrating zero trust access control and attribute-based encryption. This scheme addresses the growing threat of compromised devices, which can lead to sensitive data leakage and economic losses. By implementing a dynamic trust evaluation system and secure channel establishment, ZT-Access ensures that only trusted entities can access resources, thereby mitigating the risks associated with vulnerable smart devices. The use of attribute-based

encryption allows for fine-grained access control based on specific attributes, enhancing data privacy and security in power IoT settings.

Again, the principles of zero trust architecture are also highlighted, as the ZT-Access scheme is crucial for establishing a secure network infrastructure. When setting up a network to support both intranet and internet connectivity, priorities must be on security measures such as continuous monitoring, access control, and identity management. Adopting a zero trust principle ensures that Niagara Manufacturing can ensure its outside network (WAN) and inside network (LAN) and all devices and users are verified and authenticated before accessing resources, regardless of their location or network connection. This approach not only safeguards sensitive data but also protects the organization's digital assets, strengthens the overall security posture of the network, and making it resilient against potential threats in the digital marketplace environment. Consequently, segmenting things and securing LAN as much as WAN during setup is necessary as seen in Fig 26 above. Therefore, this is my guiding principle in this project, as I also enabled “Block Offenders” option in the WAN settings. This will automatically block hosts that generate snort alerts within the network and from outside the network.

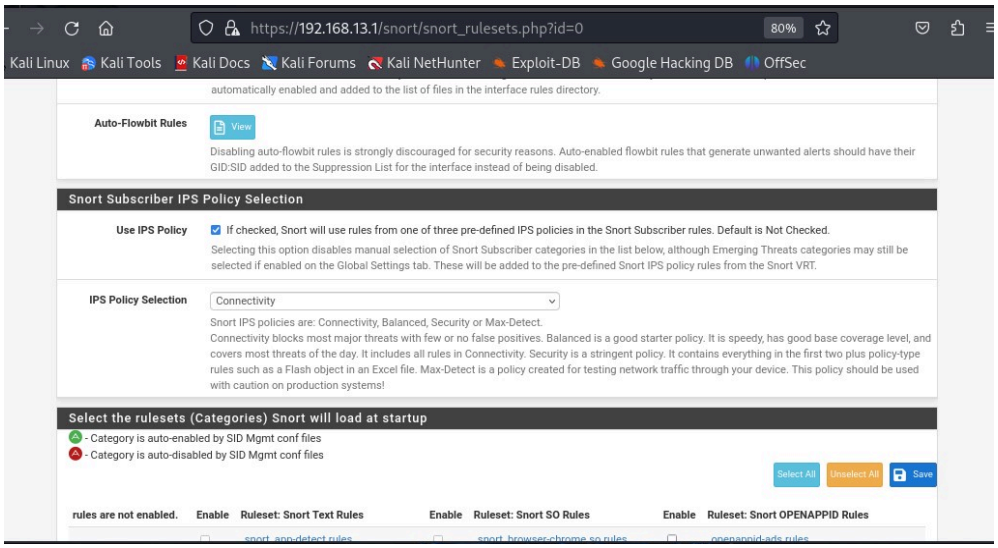

Fig 28: Screenshot of IPS Rules set to Connectivity.

Snort Rules (and only those rules, not the Emerging Threats rules nor any other available rules) have added metadata tags in them that are put there by the rule its authors and the Snort VRT (Vulnerability Research Team). These tags associate certain rules with an IPS Policy. There are four defined policies, and out of the four, one of them is for testing only. The four policies are "Connectivity", "Balanced", "Security", and "Max Detect". The fourth one, which is "Max Detect", is for testing only and it is advised to never be enabled on a production system as it will generate lots of likely false-positive alerts.

The policy names in Snort, indicate the philosophy of the rules selected by the policy. "Connectivity" which I selected means only rules that detect severe threats are enabled for blocking, while rules for other less severe threats are either not loaded, or are set to alert only. "Balanced" means more rules are selected to be enforced, but there is a rising possibility of false-positive alerts and blocks depending on what constitutes "normal traffic" in a given network. "Security" goes farther by enabling more rules, and having them block traffic. But there is also a much higher potential for false positives with this policy. This policy is never recommend to be piked by users unless they want to watch the IDS/IPS 24-hours a day to clear false positive blocks.

As a beginner who only installed Snort for the first time, it is advisable to run it for at least a month with no blocking enabled to get a feel for what kinds of alerts are going to be generated in the network. Then one can evaluate to determine if they are false positives. For those, one would likely have to suppress those alerts or disable those specific rule SIDs. By checking ips policy and choosing one of the 4 profiles, it basically automatically applies the snort rules from the list and saves users from having to go through said list and check each one

-Configuration of Virtual Private Network

Virtual Private Network is simply a service for used for securing private networks communications over the public network. Shunmuganathan et al., (2020) discusses the critical aspect of safeguarding VPN networks from both insider and outsider threats to maintain the security and efficiency of data transfer within globally dispersed corporate offices. By proposing protection mechanisms such as a probability-based rate limiting model for insider attacks and an Access Token Embedded Encapsulating Security Payload (ATE-ESP) for outsider attacks, the article emphasizes the importance of proactive defense strategies at the edge routers of VPN sites. These mechanisms not only prevent bandwidth flooding attacks but also ensure the effective utilization of reserved bandwidth, ultimately safeguarding the VPN service and the ISP from potential disruptions. By utilizing a secure VPN with robust protection mechanisms, such as those discussed in Shunmuganathan et al., (2020), network administrators can securely connect to the administration network from anywhere, enabling them to maintain operational oversight even when outside the office and carry out other administrative/clerical functions. This not only enhances operational efficiency but also ensures that sensitive business information remains protected from potential insider and outsider threats, aligning with the needs of a dynamic and mobile workforce in a digital marketplace.

Seraj et al., (2023) state that VPNs were first designed for employees to virtually connect to their office network from outside the office environment, however, they are used more for security reasons. These reasons are actually why the VPN was configured for Niagara Manufacturing, to enable staff on transit to connect remotely and securely to the network. VPN requires 3 features to effectively offer a complete and satisfactory service to a security conscious customer who is concerned about his communications on a private network over a public infrastructure.

These are as listed below;

1. Authentication: Not VPN that anybody can log into

2. Encryption: Don’t want transmission in plain text.

3. Encapsulation: Process of being in a tunnel. Ensuring all the traffic and data goes through the tunnel.

There is really no fool proof VPN, hence the Testing for DNS leaks while connected to the VPN. Because sometimes, one is connected to a VPN and something still gets out. To ensure the admin staff are able to securely and remotely connect to the network from wherever they are. In order to do that, the VPN requires some kind of authentication source. I went to System, User Manager and created a new User as part of the Admin.

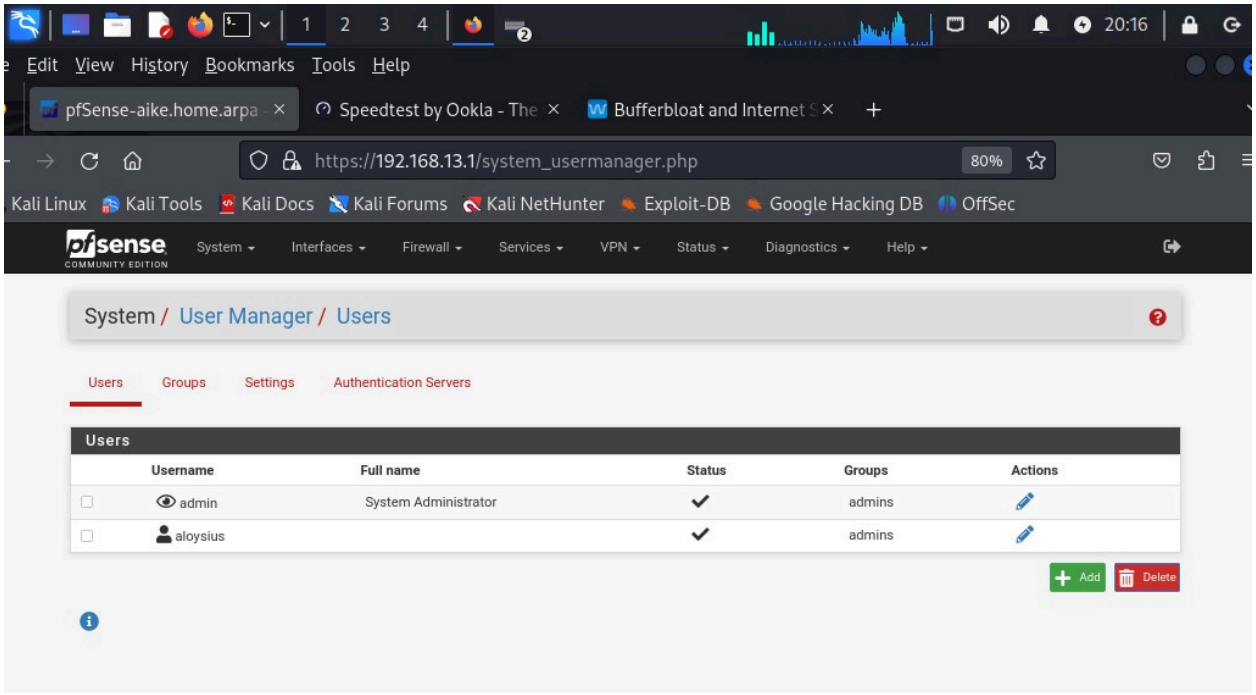

Fig 29: Screenshot of creation of a new User in Admin

I logged out as Admin and logged in as the new user I just created, Aloysius, with same privilege, I was able to see everything as the main admin. This is because I needed a non admin

user for the VPN set up to work and there are not too many people working for Niagara Manufacturing as at now. However, when things change, the organization would provide the active directory credentials to us, so I can just forward the authentication request to that.

To configure the VPN, I navigated to VPN, clicked on OpenVPN from the dropdown and opened the wizard. Following, the pfsense guide on the configuration, I created the Certificate Authority (aikeCert). After which, I created it on the WAN Interface where it will listen for connections from outside. I enabled “UDP on IPv4” on the protocol because it is faster and because of its reliability over TCP for its support for more activities as I imagined that the Admins may want to also share files, videos, etc. UDP is believed to be a straightforward protocol and is used when speed is a concern, such as for DNS queries, streaming of data and Voice Over IP (VOIP) as data simply flows between 2 systems with no verification of the data packets.

I selected the default Port 1194 as the port that will be listening on the WAN interface for incoming connections and selected all default encryption algorithm supported that was available, such that if one computer does not support one, it will bounce between them. Hence the probability of protection in different environments is higher. I enabled the CBC- Fall Back Data Encryption Algorithm, which is usually the hardest encryption to break, then “Checked” the Firewall and Open VPN rule which permits connections from clients anywhere on the internet and allows all traffic from connected clients to pass through the tunnel respectively.

I then proceeded to Certificate Authority, Server certificate, and Open VPN server instance, before creating a tunnel for this VPN on a unique and uncommon subnet. 172.16.10.0/24 The VPN Clients will get a similar IP address as the Tunnel (172.16.10.X). where X can be anything between 1 and 254. With proper routing, the VPN clients will be able to communicate to the network.

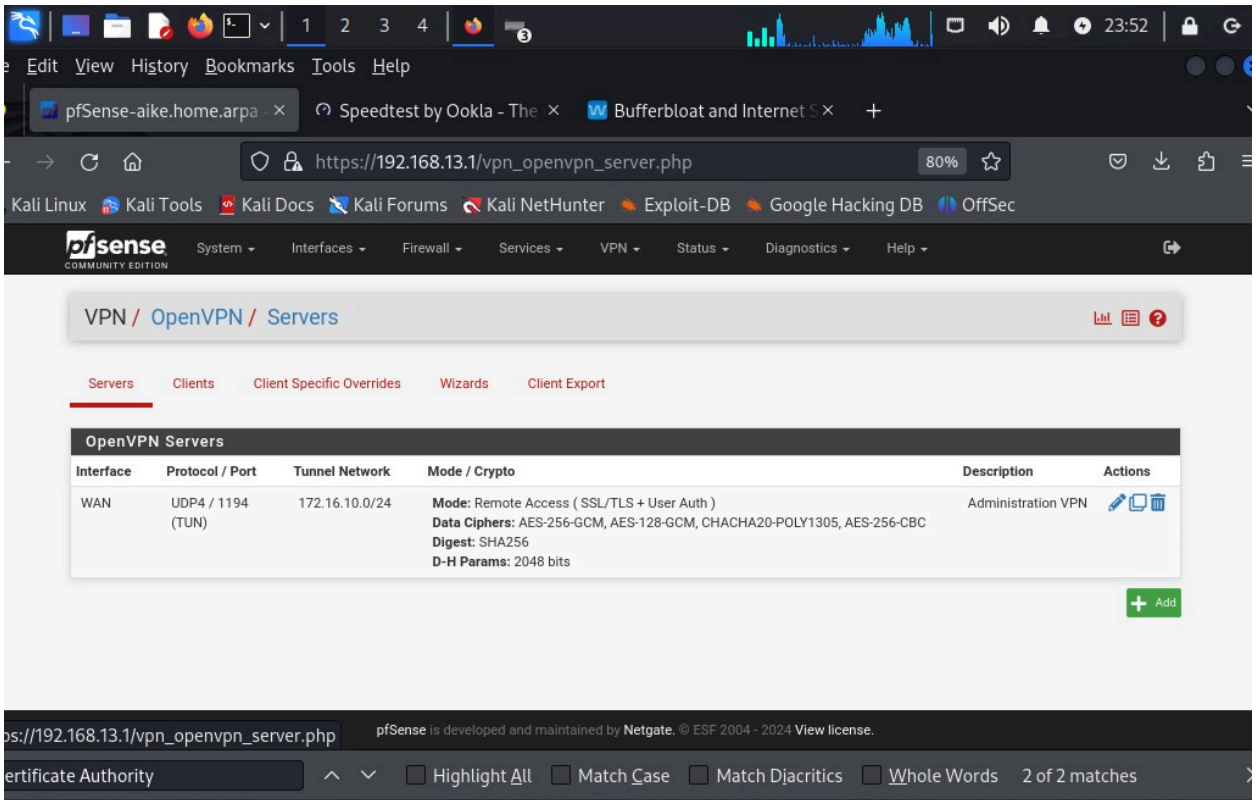

Fig 30: Screenshot of setting up the VPN Server

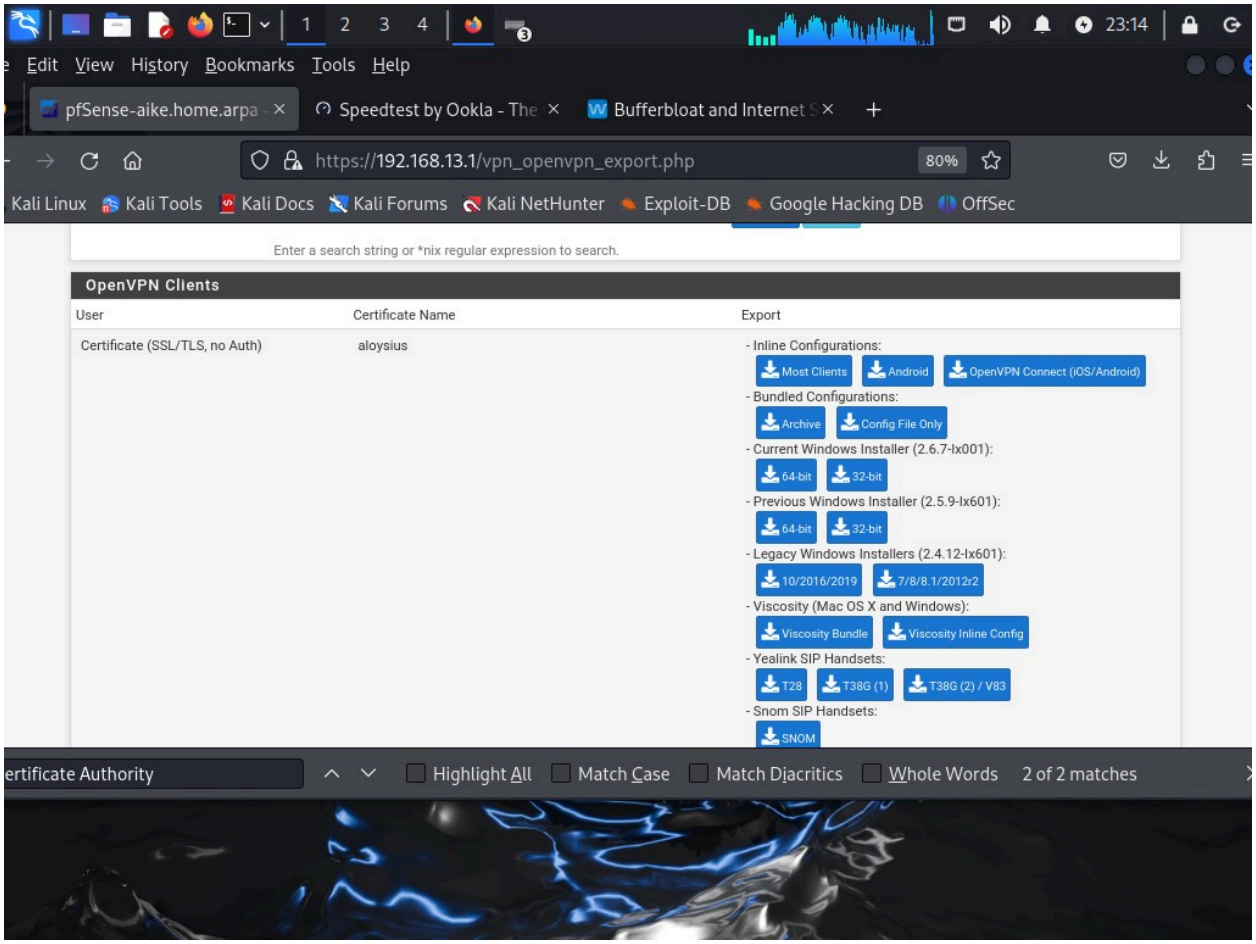

Fig 31: screenshot of the VPN certificate for the user ‘Aloysius’

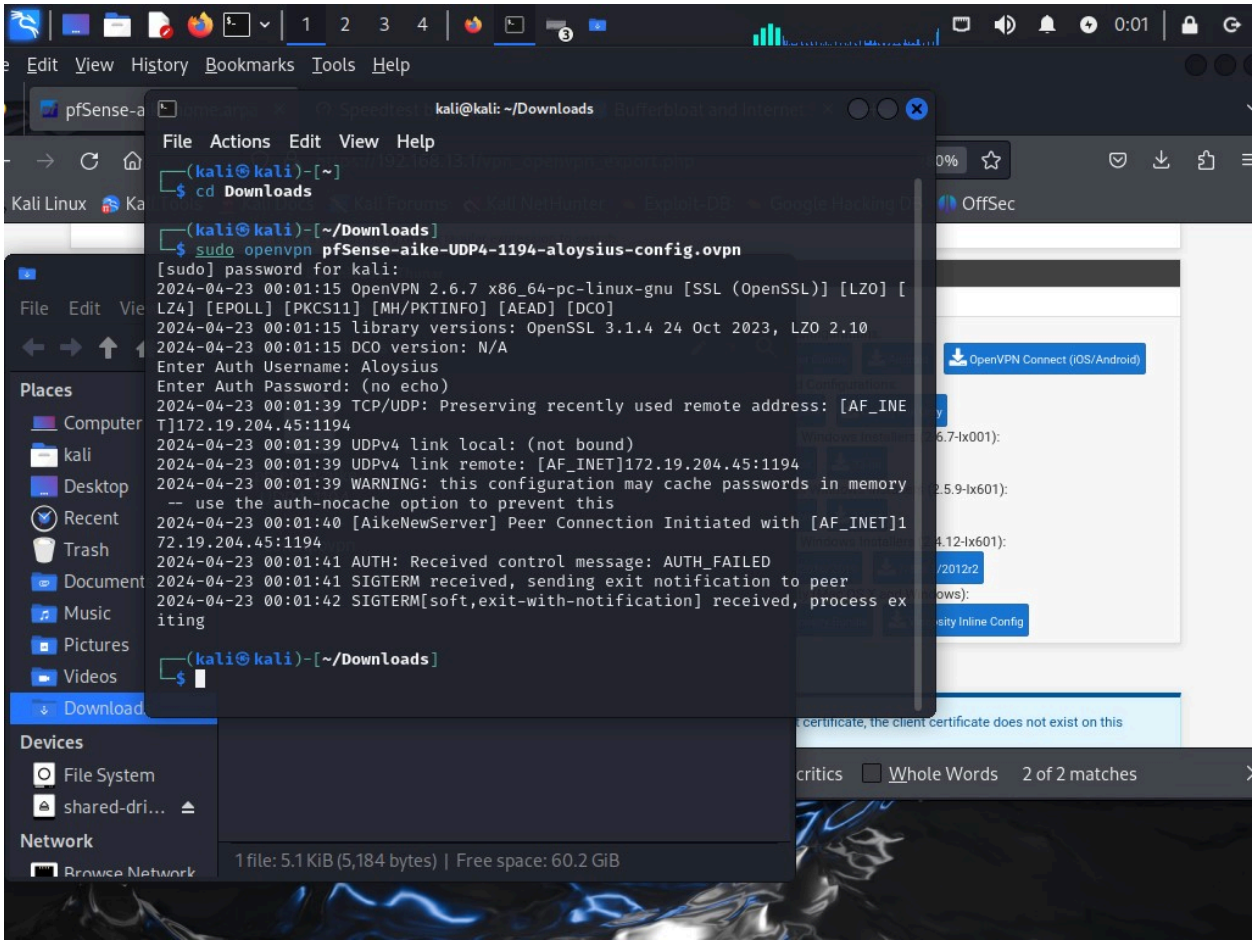

Fig 32: Screenshot of testing Kali OpenVPN Client

I first exported the OenVPN client by going to Client Export tab in OpenVPN and clicked to download the Most Clients. I then opened Shell window, ran the command “Sudo openvpn [filename]”, then keyed in Kali password and Openvpn user authentication details which provided the result as seen in Fig 32 above.

Lastly, I generated and downloaded the pfSense backup XML file through the pfSense web interface configuration as XML file as requested by going to Diagnostics, then to Backup & Restore, left everything as default and choosed Download configuration as XML under Backup Configuration.

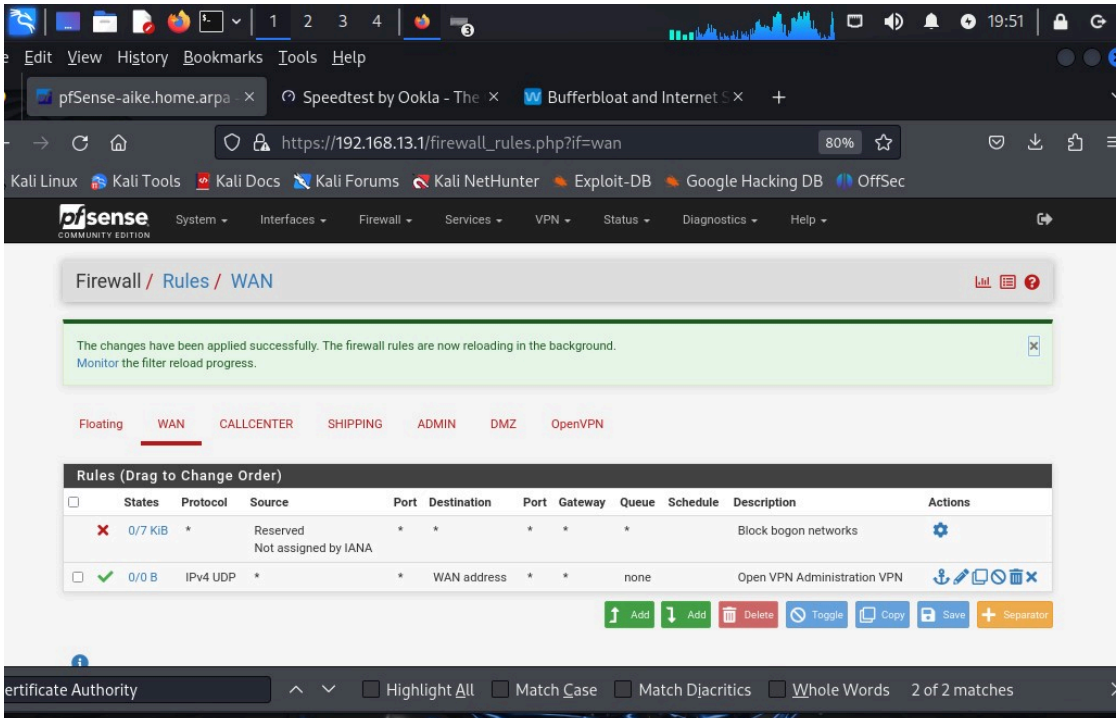
Edit View History Bookmarks Tools Help
pfSense-aike.home.arpa
Speedtest by Ookla - The
Bufferbloat and Internet
https://192.168.13.1/firewall_rules.php?if=wan
80%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Firewall / Rules / WAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating WAN CALLCENTER SHIPPING ADMIN DMZ OpenVPN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
0/7 KiB * Reserved Not assigned by IANA * * * * * Block bogon networks
0/0 B IPv4 UDP * * WAN address * * none Open VPN Administration VPN
Add Add Delete Toggle Copy Save Separator
ertificate Authority
Highlight All
Match Case
Match Diacritics
Whole Words
2 of 2 matches

Fig 32:

LIMITATIONS/DIFFICULTIES

The practical project is indeed a wonderful experience with several limitations and difficulties with the seemingly complexities of integrating and configuring various network security tools and technologies such as PfSense, Kali and Hyper-V.

Starting out, it looked challenging but the guides and documentation provided made the entire process easy. I also find the screenshots very helpful as it made following the guides and documentation relatively easy.

I also had a bit of a challenge with configuring OpenVPN but the Lawrence Systems youtube channel shared by Dr. Papp was helpful. Another challenging part of this practical project was the research aspect, where I needed to review articles that guided my decision-making; I also found this process exciting as it made me appreciate the science of Network Security.

Lastly, I think that ensuring seamless communication and data transfer between different departments with unique requirements, such as the call center, shipping department, and administration offices, while maintaining strict network segmentation and access controls, presented itself to be difficult.

CONCLUSION

The Practical Project for Niagara Manufacturing has been successfully executed, showcasing an understanding of network infrastructure, designed to support the company's transition to the digital marketplace. All of the knowledge I gained from Network Security is compiled into this practical project. It gave me the chance to apply the majority of the theoretical knowledge I had learned to real-world and virtual experiences. The design of the network topology and the implementation of the in-house infrastructure that supports both internal and external connectivity, provided me with hands-on experience of real life network administration and virtualisation. The integrating of nested VMs running pfSense and Kali Linux, along with configuring network interfaces and security measures, highlights the comprehensive approach required for network security and management.

Furthermore, the project's focus on enhancing network functionalities through features like traffic shaping limiters with CoDel active queue management, protocol/port blocking, and the implementation of additional services like Snort highlights the importance of these tools to optimizing network performance and security. Also, the exploration of integrating and configuring tools like PfSense, Kali, and Hyper-V also highlights the complexity and challenges involved in implementing robust security measures. My ability to navigate these challenges with the help of guides, documentation, and external resources like the peer reviewed articles reflects the importance of taking a proactive and resourceful approach to problem-solving in network security.

The summation of all the knowledge I have gathered, was implemented in setting up the networks and configuring all the firewall rules requested for, by Niagara Manufacturing. I was also able to confirm OpenVPN set up and tested the rules by carrying out a test on Kali to

confirm the efficacy and effectiveness of the rules, while coming to terms with the reality of the extensive work done. By addressing the unique requirements of different departments within the organization, such as the call center/storefront and the shipping department, the network design effectively balances the need for internet access with the imperative to restrict communication between internal networks. The deployment of VPN servers for remote access and the documentation of configurations and active services in the PDF report reflect a thorough and meticulous approach to network design and management.

Lastly, it was a good learning hands-on learning experience successfully completing the Practical Project as it not only fulfills the objectives set forth by Niagara Manufacturing but also lays a solid foundation for my network administrative skills.

REFERENCES

Chen, W., Kuo, S.-Y., & Chao, H.-C. (2008). Service integration with UPnP agent for an ubiquitous home environment. Information Systems Frontiers, 11(5), 483–490. https://doi.org/10.1007/s10796-008-9122-3

Baykara, S. (2022, March 20). Firewall rule configuration best practices. PCI DSS GUIDE. Retrieved May 5, 2023, from https://www.pcidssguide.com/firewall-rule-configuration-best-practices/

Cheng, G., & Tang, Y. (2013). PortView: Identifying port roles based on port fuzzy macroscopic behavior. Journal of Internet Services and Applications, 4(1), 9. https://doi.org/10.1186/1869-0238-4-9

Hussain, S., Olayemi, A., & Yeo, S.-S. (2012). Genetic algorithm for effective open port selection for a web filter. Personal and Ubiquitous Computing, 17(8), 1693–1698. https://doi.org/10.1007/s00779-012-0602-6

Kaviani, S., & Sohn, I. (2020). Influence of random topology in artificial neural networks: A survey. ICT Express, 6(2), 145–150. https://doi.org/10.1016/j.icte.2020.01.002

Kim, K. S. (2014). The effect of ISP traffic shaping on user-perceived performance in broadband shared Access Networks. Computer Networks, 70, 192–209. https://doi.org/10.1016/j.comnet.2014.06.001

Kuhn, N., Ros, D., Bagayoko, A. B., Kulatunga, C., Fairhurst, G., & Khademi, N. (2017). Operating ranges, tunability and performance of Codel and pie. Computer Communications, 103, 74–82. https://doi.org/10.1016/j.comcom.2016.07.013

Schrader, D. (2022). Open port vulnerabilities list. Common. Retrieved May 5, 2023, from https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/

Seraj, S., Khodambashi, S., Pavlidis, M., & Polatidis, N. (2023). MVDroid: An Android malicious VPN detector using neural networks. Neural Computing and Applications. https://doi.org/10.1007/s00521-023-08512-1

Shunmuganathan, S., Saravanan, R. D., & Palanichamy, Y. (2020). Securing VPN from insider and outsider bandwidth flooding attack. Microprocessors and Microsystems, 79, 103279. https://doi.org/10.1016/j.micpro.2020.103279

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source ids? Snort, suricata or Zeek. Computer Networks, 213, 109116. https://doi.org/10.1016/j.comnet.2022.109116