Secure VM Network

Abstract

The goal for the client was a small, private and somewhat isolated and/or highly secured network that was cheap and simple. The purpose of this network was to train IT staff, so the initial concerns were mostly security and ease of use. The process was a wide variety of free and open-source security software with leftover parts of older machines being reset and repurposed for this specific project. The client was limited in budget as well as space, having only a small office to contain their network environment. By using well-known materials and plentiful research, the network that was developed met the specifications set by the client in all aspects such as development time, budget restraints and ideal usage outcomes. The result is a network consisting of lightweight hardware and software that is simple for the client to use but at the same time providing a breadth of avenues for beginner and intermediate IT staff to begin conducting training in network technology.

Table Of Contents

1. Virtual Computing
   1. Introduction
   2. Virtual Machine Technology
   3. Virtual Machine Solutions
   4. Cost
2. ConstructZilla
   1. Introduction
   2. Staff
   3. Budget & Equipment
   4. Security
3. Implementation
   1. Initial Setup
   2. Initial Security Concerns
   3. Physical and Virtual Structure
   4. Security Implementation
      1. *Snort*
      2. *SSH*
   5. Testing
      1. *Ntopng*
      2. *Snort*
      3. *SSH*
   6. Administration
   7. Documentation & Training
4. Ethical Issues
5. Business v Budget
6. Closing Thoughts

# Virtual Computing

## Introduction

In the past, many companies would install their operating systems on a physical machine. As the network grew it became very expensive to deploy and maintain equipment. The rise of the virtual machine introduces a new method of system structure in which a piece of software called a hypervisor separates the hardware of a host operating system into a pool of resources which can then be utilized by isolated guest operating systems [1]. The virtual machine is essentially a *guest* operating system run on top of an existing operating system that has access to the same hardware as the *host* operating system. The two operating systems, for example, a Windows host OS and an Ubuntu guest OS, can run on the same hardware while being completely isolated from each other [2]. Instead of dual installing an OS and going through more in-depth or time-consuming processes to establish different operating systems on a single set of hardware, VM technology makes it extremely quick and easy to test different software or work inside of different systems with a single machine. With virtualization, a company now has the ability to buy one powerful server and deploy many machines on top of that one server virtually [3]. This provides great benefits to organizations that want to cut costs on maintenance and deployments. An organization can go out and download Hyper-V virtualization software for free to deploy on one of their servers[4]. In this respect, virtualization provides greater flexibility. You can dynamically increase or decrease resources to your virtual machines, dynamically or manually[5]. If a virtual server crashes then one can easily replicate the server using a clone[6], eliminating the need to rebuild anything from scratch. This archives the type of robust fault tolerance ConstructZilla is looking for. Virtualization allows us to save snapshots [7] at any point for things like penetration testing[8], or maintenance. Virtualization can also provide some security, as the theory behind VM isolation makes it difficult to access a host from a guest or vice versa[9].

## Virtual Machine Technology

In the world of virtualization one will come across different types of virtualization architecture. The main ones typically used are type 1 and type 2 hypervisors [10]. As stated prior, a hypervisor isolates the guest operating system from the host, but also schedules processes [11] to be run inside of the host OS that the guest is requesting to run. A type 1 hypervisor will act as the OS of the hardware it is running on. Type 1 hypervisors are directly installed on bare metal hardware. Type 2 hypervisors run on top of an Operating System[12]. The operating system is installed on bare metal hardware, and then hypervisors are installed on top of that. There are benefits to both. Most enterprises will like to install a type 1 hypervisor as this allows for more control. For example, type 1 hypervisors will always be more scalable since they do not rely on an underlying operating system[13]. Type 1 hypervisors are always faster due to no reliance on an underlying OS. An organization can not ignore these benefits as well as the added security that a type 1 hypervisor provides. Type 1 hypervisors will always be more secure when compared to type 2 hypervisors[14]. Type 2 hypervisors have a weakness that needs to be kept in mind and that is any problem in the base operating system affects the entire system including the protected hypervisor[15]. Type 2 hypervisors have their own use cases as well. They are simple and easy to set up. It is great for experimenting and testing[16]. If resources are an issue then type 2 hypervisors are the way to go since it does not directly access the host hardware resources. Popular type 1 hypervisors are VMware ESXI[17], Microsoft Hyper-V[18], and Citrix XenServer[19]. Popular type 2 hypervisors are VMware Workstation Player[20], Microsoft Virtual PC[21], and Virtual Box[22]. As we saw earlier there are many different types of Virtualization software. Type 2 hypervisors are convenient for testing new software and research projects. It allows the user to use one physical machine to run multiple instances with different operating systems to test how an application behaves in each environment or to create a specific environment. We chose VMware Workstation because it is free and full of advanced features such as cloning[23], NAT[24], host-only[25] and bridged network technologies[26].

## Virtual Machine Solutions

With virtual machines, we have an entirely new method of implementing solutions to problems. The platform itself can be used by individuals and can be scaled all the way up to large organizations[28]. The concept of virtualization can be applied big or small. In the case of small businesses that don’t have the capital to purchase large physical infrastructure and expensive hardware, virtualization becomes a key part of expansion. Virtual machines contribute to over 90% [28] of companies today in the form of server virtualization. For smaller deployments, with something like VMWare Player, an individual can install a different guest OS on their machine [29] to test it out instead of committing to a full install on their hardware [20].

## Cost

Physical implementation will always be more costly. The reason for this is if an organization is quickly growing then they need more capital upfront to deploy the machines. One must also account for the additional costs of hiring more employees to deploy and maintain all that hardware. Further, if the organization were to implement a virtual solution, then they can cut costs [31] in many areas such as equipment, staff, and licensing. When you factor in electricity then the savings are even more significant since servers require power. The more servers you add the more power you need. Virtualization is the solution to all of this.

# 2. Constructzilla

## Introduction

The objective of this project was to provide our client organization, ConstructZilla, with a secure virtual network that will be used for testing purposes. ConstructZilla is a manufacturing company and wants to better understand networking and security architecture to train their internal IT staff, so that future deployments are as secure as possible when put in a production environment. To get this secure virtual network setup for our client we needed a desktop. The desktop that we chose for our testing environment has 8 GB of RAM, a wireless NIC to connect to the physical network, a 512GB spinning disk drive and an intel i5 CPU. ConstructZilla does not need something with high performance since this is a testing environment that will run very lightweight systems. The company sells construction materials such as bars, stay cables, and now wants to move into the infrastructure intelligence sector. In order to take their company to the next level they need to provide a new image of their company and create awareness among their clients with the new offerings. They need technology to be able to reach out to their clients and build trust that they are indeed a secure organization. Too many times this company implemented systems into production that ended up having vulnerabilities. To mitigate this we advise that before anything gets shown to customers it must be implemented in a test environment. This is why the client has asked us to create a virtual environment.

1. *Staff*

The company has an IT staff that needs to get up to speed with security. The current staff is running legacy systems and has outdated knowledge on network security. The staff they currently have that will be working in this virtual environment is an IT manager and 2 interns. The client has asked us to leave an admin account with full privileges, an IT manager account with most privileges but not all, and 2 intern accounts that are heavily restricted to viewing configurations so that they can learn but are not able to make any edits to the configuration. There will be no other staff that needs access to this system so no other accounts have been made since this network is intended to be used strictly by IT staff only. The staff has limited knowledge on networking and security so they can use this environment to make all the configuration mistakes that can possibly be made and then learn from that before deploying a firewall for a company in a live network.

## Budget & Equipment

This company is a global manufacturing company with locations in over 50 countries worldwide. The office that we will deploy the desktop that's running the VMs is located in Bolingbrook Illinois. We will need to go onsite to get this virtual network installed in their on-premises data closet. The client has said that if this virtual environment is beneficial to their staff then they will ask us to implement similar environments for their staff across the company. We have provided the client with peace of mind that implementing this globally for the organization would not be difficult since we are running Vmware and we can replicate these environments across the WAN with ease. The company currently has a small data closet at their Bolingbrook Location. The data closet consists of 3 42U racks, a wireless access point, 2 switches, a firewall and 2 internet connections coming into the building for redundancy. This is an extremely budget friendly build. Constructzilla had a used desktop laying around the office so that is free. The software running in our virtual environment is also completely free of cost.

## Security

Perhaps a few security concerns to keep in mind would be that we have remote access enabled using public key only. We have told the staff not to share their private keys with anyone as this can allow the unauthorized user access to the virtual environment. Another security concern is that we have asked the company to implement a biometric security lock on the data closet door so there’s no way an unauthorized user can simply walk into the data closet and plug in a USB with malware into one of the servers. With all of this information in mind, we opted for a small virtual network setup on the aforementioned hardware that could be altered as needed, maintained by the users, and scaled in respect to the follow on actions of the company.

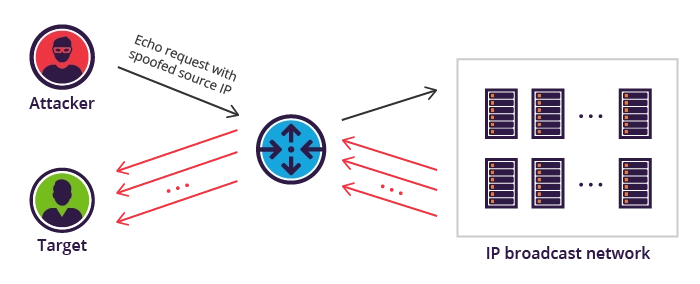
# 3. Implementation

## Initial Setup

To begin the setup for this project, we started with an internet line coming into the facility and then connecting to the WAN interface of the ISP-supplied router. We recommended going with Comcast and our client already had an account set up with that ISP for their office use. Once that was done, we started building our secured virtual LAN.

## Initial Security Concerns

For the firewall, we chose Pfsense [32] since it is well suited for small to medium scale enterprises due to its wide variety of features and low to no cost. It provides security features such as anti-spoofing [33], Sandboxing and content filtering [34]. Anti-spoofing is an important security feature in this project. “Spoofing” in regards to a firewall is essentially the act of a malicious agent attempting to send traffic with a fake or “spoofed” IP address. IP address spoofing is one method network attacks can use to carry out DoS/DDoS [35] attacks or attain access to a network [36]. The attack will generally begin with the attacker sending data, even something simple like a ping request, to a server and falsifying the incoming IP address as the target machine [37]. The IP broadcast network, generally servers that have the capacity for high volumes of data flow, will then see the spoofed IP and send all of the data requested by the attacker back to the target machine. When done correctly, the target machine will then be overwhelmed with the response and this can easily crash an unprepared network.

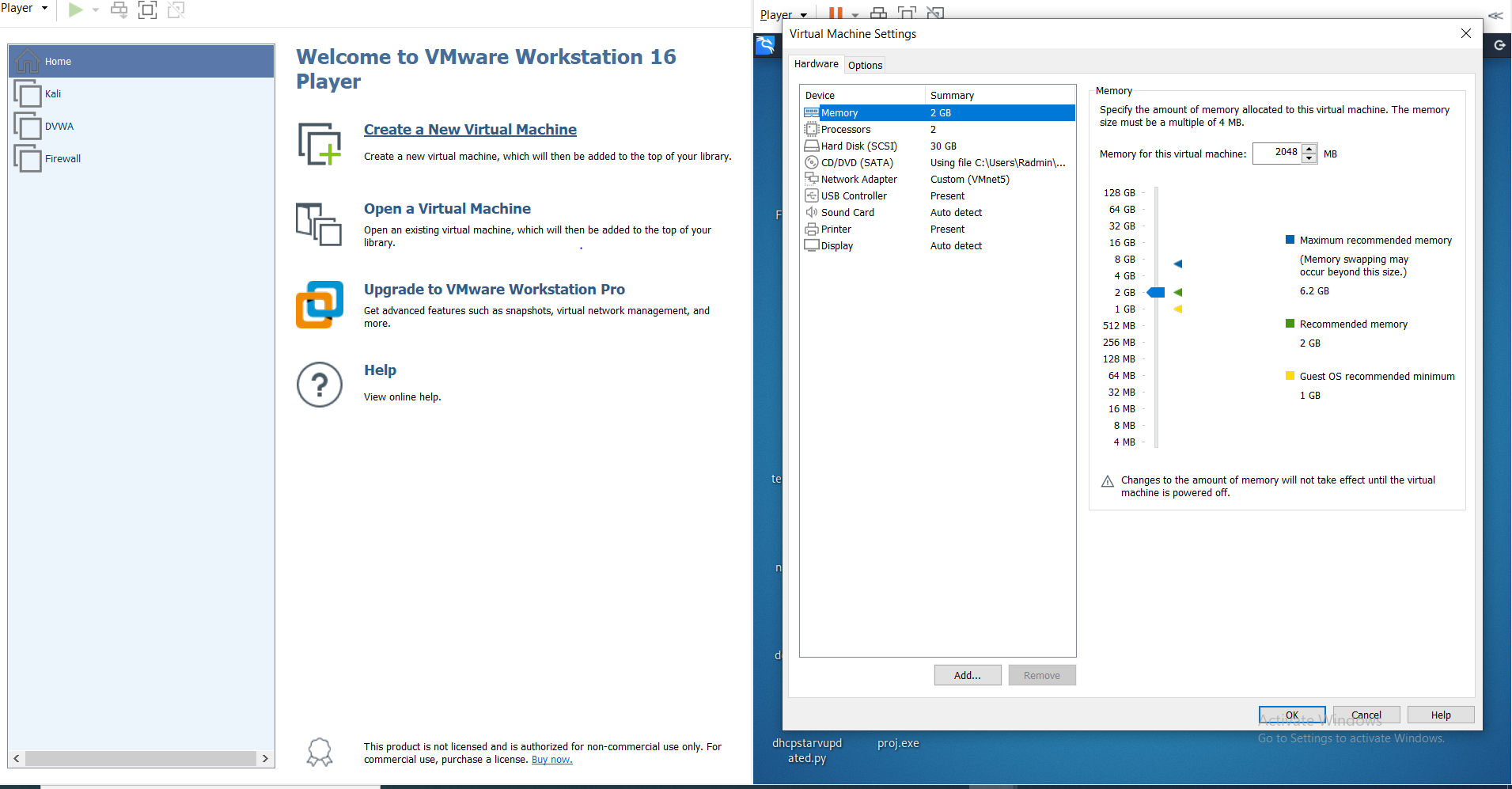


|  |
| --- |
| Fig 1: How spoofing attacks work |

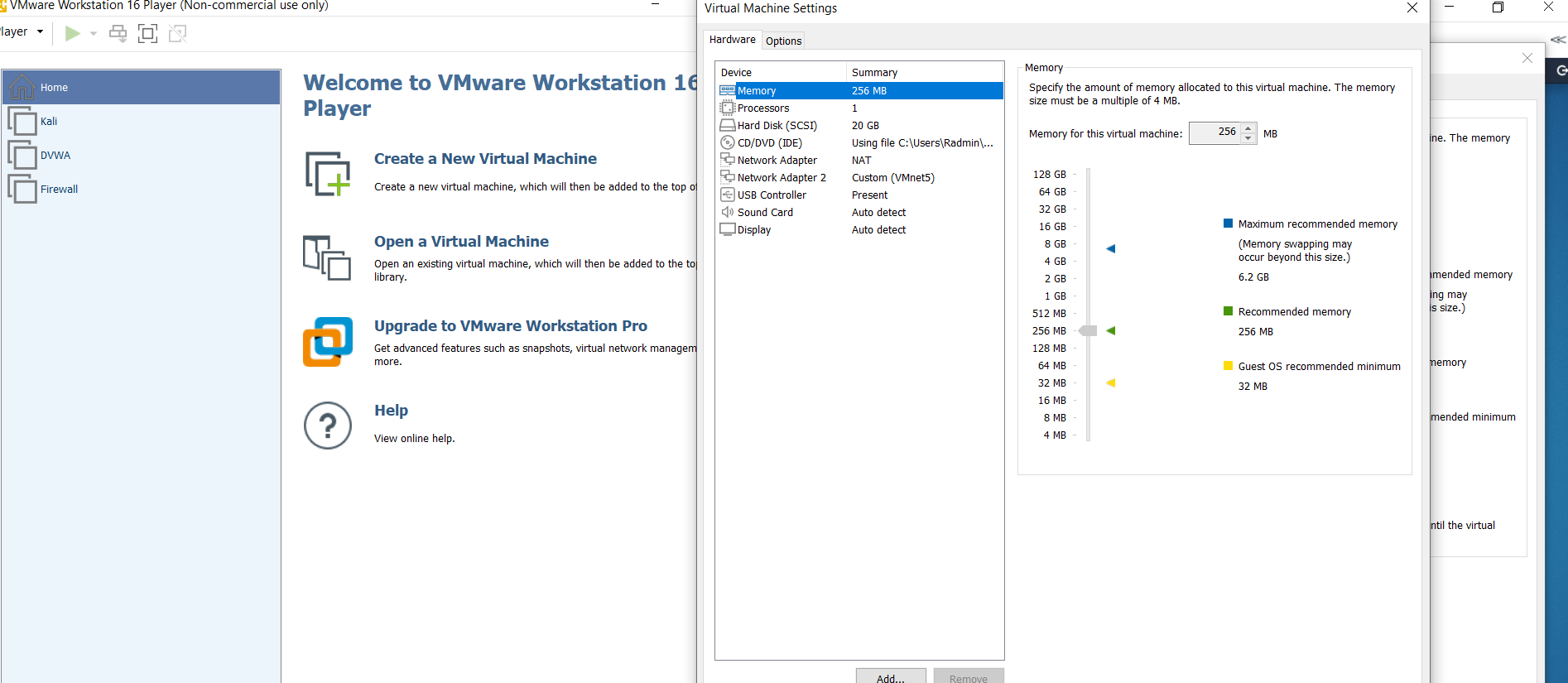
Sandboxing will allow our organization to regulate and control the code they test and allow to run, adding further protection for staff learning more about cybersecurity. Content filtering is another good security tool used for blocking certain specified network traffic (specific web pages for example) from being accessed. It is also easy to manage with the web GUI Console which was important since at the start this network was being used for training and managed by a single admin.

1. *Physical & Virtual Structure*

The physical machine the VMs are deployed on will get its IP address from the ISP supplied router [38]. For the physical topology, we have a desktop with 8GB RAM and a core i5 CPU. From the desktop we have 2GB of RAM assigned to our kali Linux machine and 2GB of RAM being assigned to our Pfsense machine. On our pfsense machine we have 2 NICS installed.

**

|  |
| --- |
| Fig 2: Kali Machine Setup in VM |

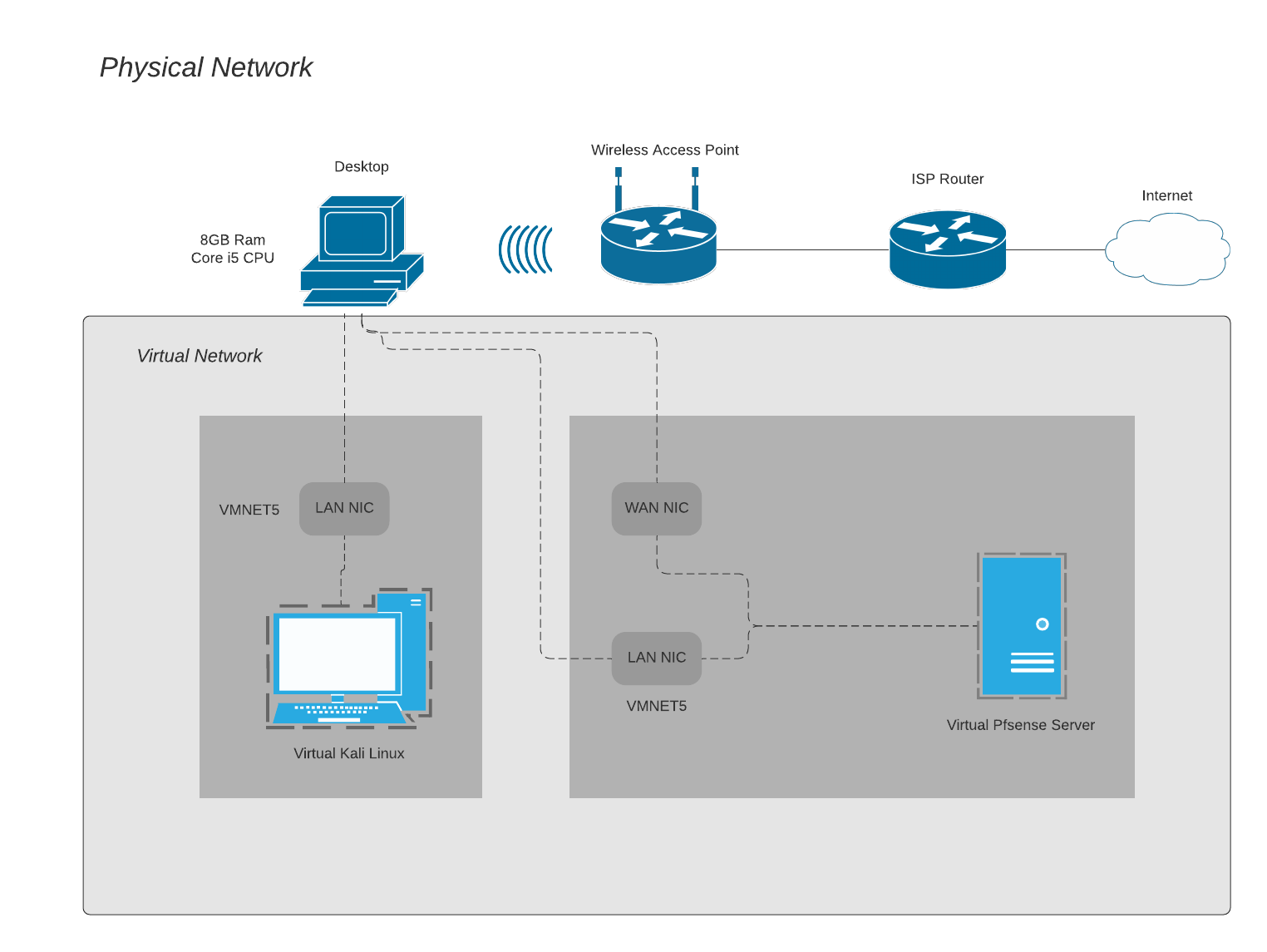


|  |
| --- |
| Fig 3: Pfsense Firewall Setup in VM |

Our WAN side is on 192.168.74.128. While designing our network we needed to come up with an address scheme that follows network standards. The two most crucial ways to design your IP structure is with an IPv4 network setup or an IPv6 network setup, or you can run a dual stack which is when a network supports both IPv4 and IPv6. Starting on a higher level, an IP (Internet Protocol)address is a numerical label assigned to each device connected to a computer network that uses the IP protocol for communication [39]. An IP address acts as an identifier for a specific device on a particular network. The IP address is also called an IP number, or Internet address. IP address specifies the technical format of the addressing and packets scheme [40]. Most networks combine IP with a TCP [41] (Transmission Control Protocol). The internet protocol version 4 (IPV4) is a protocol for use on packet-switched Link Layer networkssuch as ethernet [42]. IPv4 provides an addressing capability of approximately 4.3 billion addresses [43]. IPv4 was designed during the early days of the internet and was not designed for the massive growth we see today. Despite being older, many networks today still operate on IPv4 and will continue to for the foreseeable future. IPV6 has the capability to provide a virtually unlimited [44] number of addresses and is replacing IPv4 due to the growing number of networks being used today, reducing the number of available IP addresses. Taking into consideration IPv6 can have a wider attack surface when compared with IPv4, because of IPv6 having wide support for address autoconfiguration, this means that your endpoints may be accepting IPv6 traffic without administrators even knowing it. Link-Local addresses are configured on any endpoint that has IPv6 enabled. Meaning IPv6 can be present on the network even if you are not aware. Another difference between IPv4 and IPv6 is the appearance of the IP addresses because of the larger range. IPv4 uses four single byte decimal numbers, separated by a dot (e.g. 192.168.1.1), while IPv6 uses hexadecimal numbers that are separated by colons (e.g. fe80**::**d48a**:**6435**:**d2d8**:**d9f3b11). Under consideration that the client is using the network we are building for testing it would be a waste of time and resources to set up an IPv6 network for something that will never take full advantage of IPv6 capabilities. For example, at most the number of machines on the virtual network as it is currently intended would be ten. Since IPv4 can handle 4.3 billion addresses, IPv6 would be overkill for a network of this size and purpose. The current staff at ConstructZilla has IPv4 setup across all their sites. They still need an ample amount of training in IPv6 before they can roll out this type of configuration company wide.

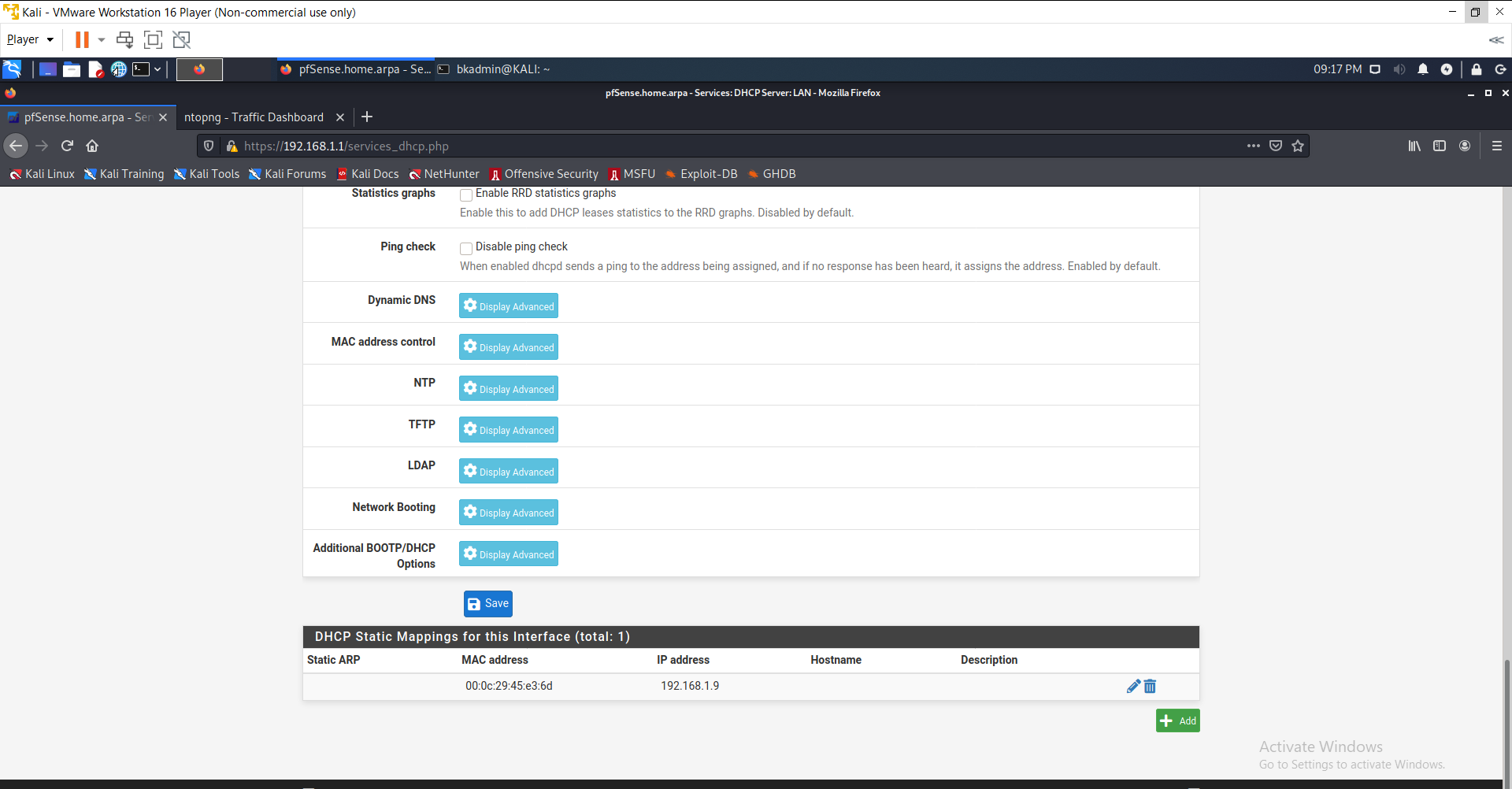
The WAN NIC is running on NAT mode, which means that your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. Dynamic Host Configuration Protocol, or DHCP [46], is a network protocol where a DHCP server assigns IP addresses to each host on a network. This enables communication between endpoints of the network. DHCP also assigns the subnet mask [47], default gateway and Domain Name Server (DNS) address. DHCP is a crucial aspect to simplify the IP address assignment for networks. Manual allocation of IP addresses can lead to messy issues, such as IP conflicts in which 2 hosts have the same IP address. Even on small scale networks manually assigning IP addresses can be confusing, time consuming and lead to errors. DHCP client-to-server communication operates on DORA [48]. DORA stands for Discover, Offer, Request, Acknowledgement. Starting with Discover the host will send a broadcast Discover message in the network to find a DHCP server. Broadcast packets are in the form 255.255.255.255. Broadcast packets are sent to ALL devices on the network. The next packet is the offer packet which is sent as unicast. When the server receives the discovery request then it responds with the DHCP offer request to the client which contains information related to IP address and the lease duration that a host can use. Then comes the DHCP request packet. It is sent as a broadcast. The host receives the offer packet then it replies back with a request message that tells the server that it's ready to accept the IP address that the server offered. Lastly, the DHCP acknowledged packet is sent as a unicast. The server gets the request from the host. This message is a reply to the request message to the host. It will send the DHCP acknowledge request to the host along with information such as the IP address and the subnet mask that the server allowed for the host.

The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination. With NAT, the virtual machine can use many standard TCP/IP [50] protocols to connect to other machines on the external network. For example, you can use HTTP [51] to browse Web sites, FTP [52] to transfer files and Telnet [53] to log on to other computers. Our LAN side of the second NIC is on 192.168.1.1. This NIC is set to be on VMNET5. Our Kali Client that is connected to PFsense is also on VMNET 5 which will allow us to communicate with our pfsense gateway [54].



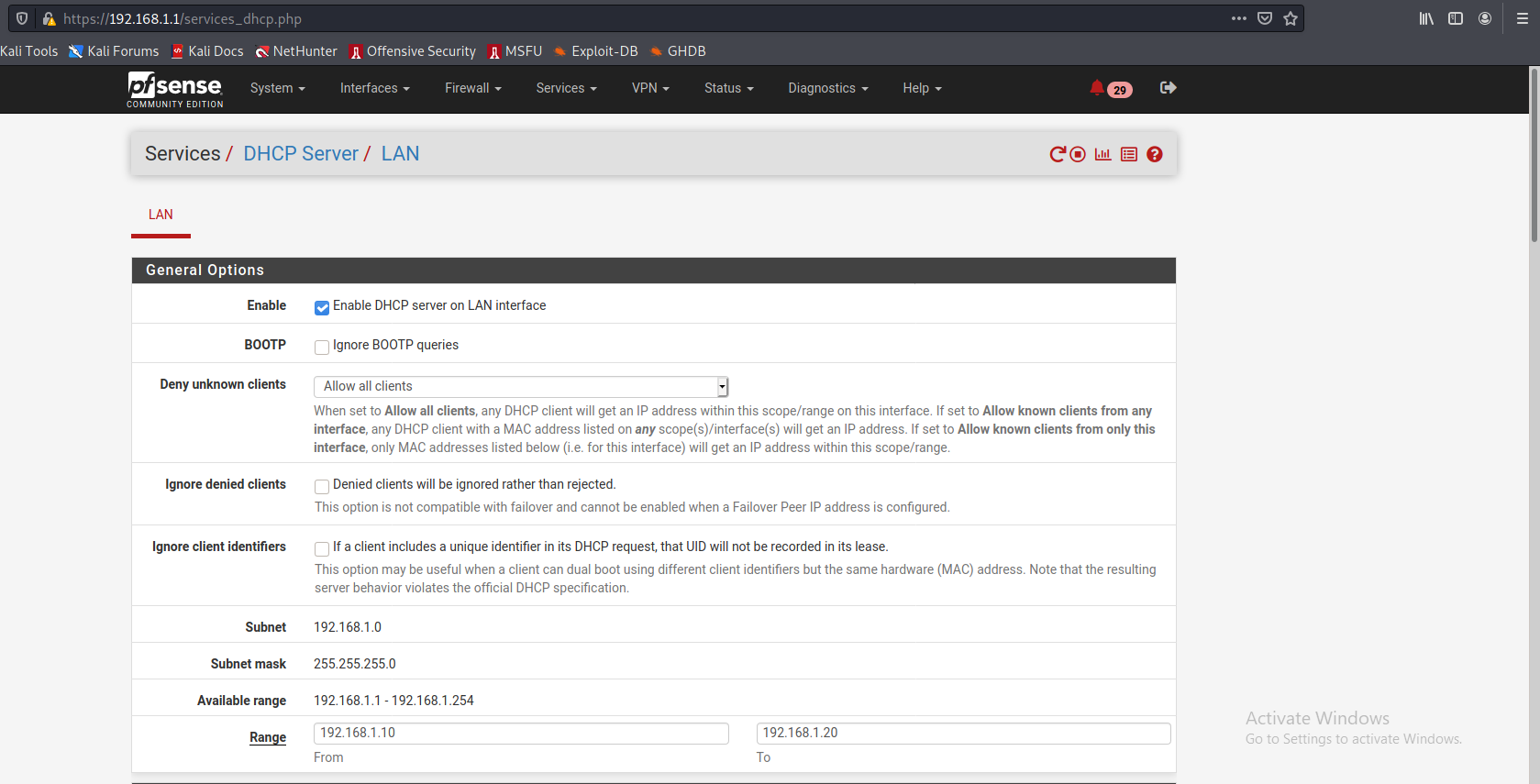
|  |
| --- |
| Fig 4: Diagram depicting the virtual machines utilizing the virtual network |

A MAC address table [55] was implemented, which also allows for expedited data transfer. A MAC address is essentially an identification number unique to a device that generally remains unchanged and in the case of certain devices cannot be altered. When devices attempt to communicate across networks, data is sent from one machine to a switch to a network with an address to a receiver device. But without knowledge of where that device physically is and what routes to take to get there, the switch doesn’t have a way of getting that data to the receiver device.



|  |
| --- |
| Fig 5: MAC Address table for the client network |

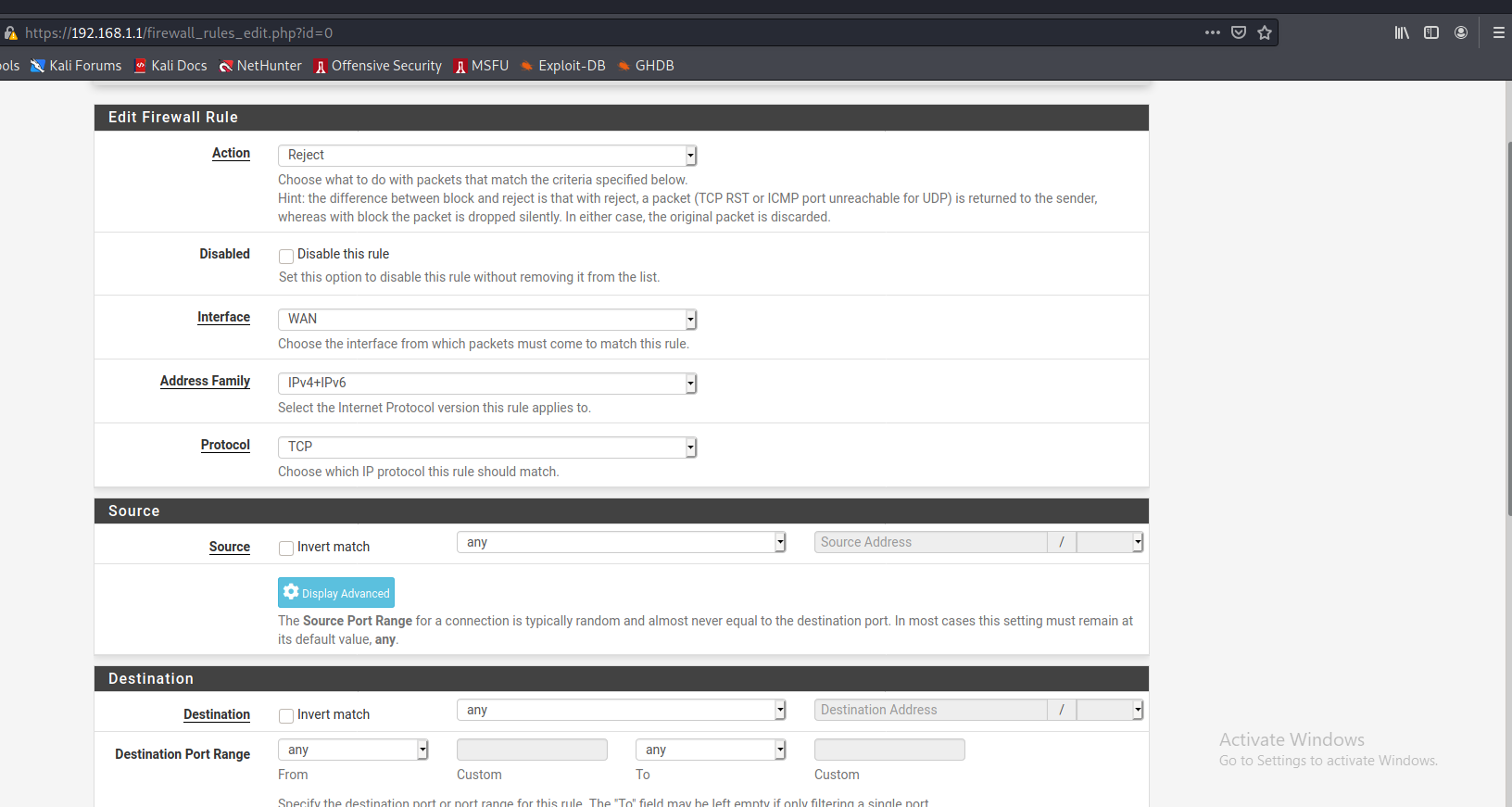
To find out where that machine is, the switch must send out a broadcast in a method known as ARP [56]. This essentially pings all machines on the network and attempts to establish where that MAC address is and how to get there. Once this is complete, that MAC address is recorded in its MAC address table and as long as the switch maintains that table, there is no need for this added broadcast to find the machine. At this point in the project during a review meeting, the client expressed that they would like to add on to the setup by adding manual IP to MAC address mapping. To accomplish this we set up static DHCP mapping. When we create the IP to MAC mapping it creates a static IP for our client machine in order to prevent a break-in availability in the case of a network attack or an issue with the DHCP. outside of the current DHCP pool. Now, whatever clients we have on our network its IP and mac addresses will be bound together. We told the client that we would limit the scope for added security [57], as the range it was at at the time was (192.168.1.1 - 192.168.1.254), which was unnecessary. Our client expressed that despite us limiting the scope they would still like to keep some addresses in the DHCP pool so that way the network can scale well as the network grows and machines are added. To do this we limited our DHCP range from (192.168.1.10 - 192.168.1.210) to (192.168.1.10 - 192.168.1.20). We assigned the client machine a static IP of 192.168.1.9 (outside the DHCP range).



|  |
| --- |
| Fig 6: DHCP Scope after limiting range |

## Security Implementation

It was understood early on that this network ought to have a lot of security measures. Ntopng [58] was one such security measure, thought of less importance than some of the others. Ntopng is essentially a network monitor [59] that gives feedback data about network traffic. Ntopng allows for full visibility as to what’s going on in the network. This way, we can monitor clients and be sure to provide proactive security when the system is handed off to the client. We also added a rule to reject all incoming connections and are logging this rule for additional security. The difference between block/drop and reject is that with reject, a packet (TCP, RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently [60]. In either case, the original packet is discarded.

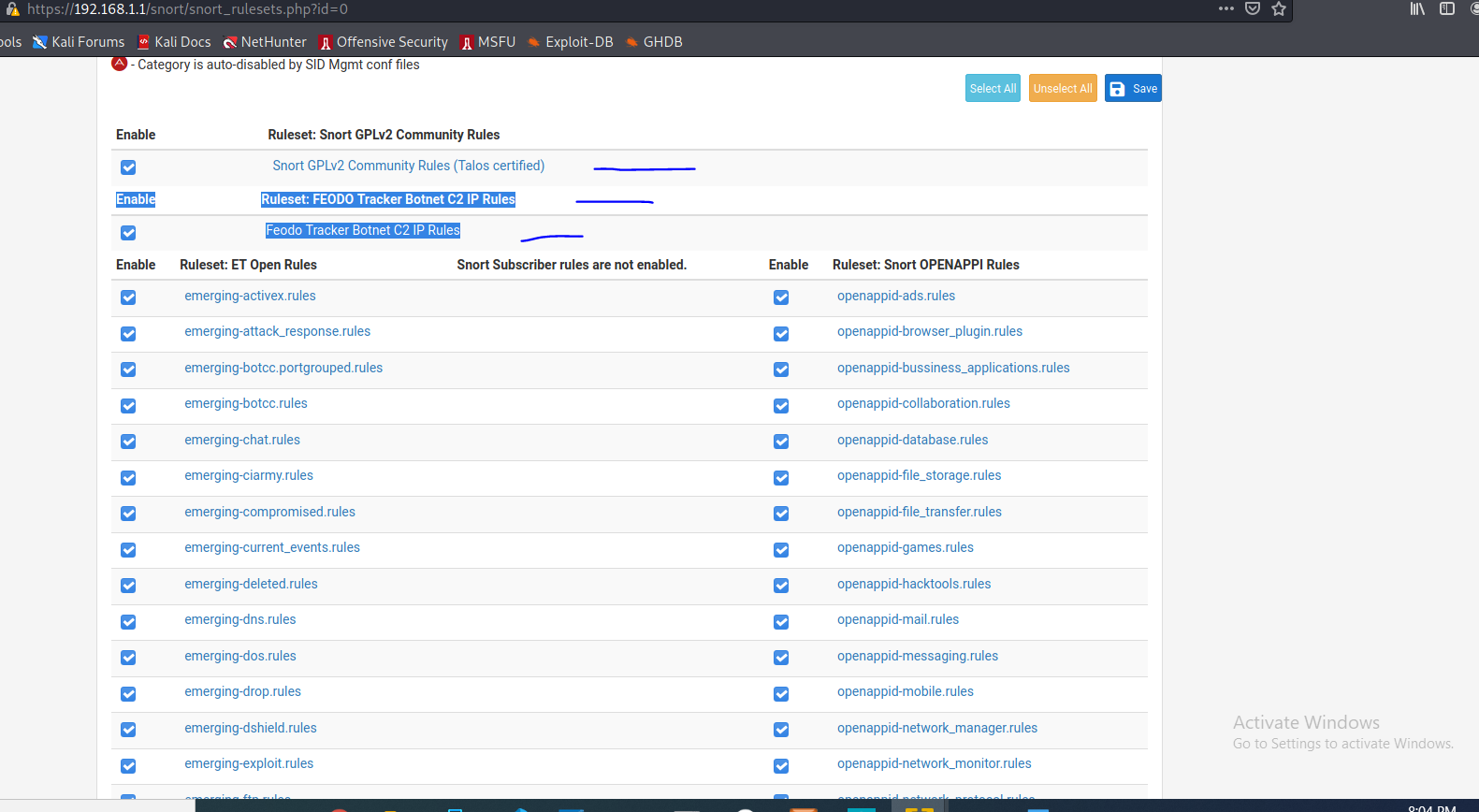


|  |
| --- |
| Fig 7: PFSense ruleset |

To achieve additional security, we decided to install the open source IDS known as Snort [61]. Open source [62] is beneficial for a variety of different reasons. The reason why we chose open source solutions for our client is that it is cost-effective which meets the budget requirements of our client. Open source is also a great solution since the code is freely available and is maintained by an active community that is constantly making improvements to the open source platform. Snort is free, yet has all the advanced features [63] of any high end IDS on the market. It will allow us to detect any intrusions [64] happening on our network. From there the client's network administrators can manually take action once the IDS picks up malicious traffic. It can be configured to simply log and detect network events to both log and block them. Thanks to OpenAppID [65] rectros and rules, Snort package enables application detection and filtering as well. This will be good for the client since it will allow for additional visibility into the network. An account is required for the client to use the Snort rulesets, so an account was created for this purpose. The pre-configured rules that come with Snort were deployed, as well as the Emerging Threats Open Rule set. Emerging Threats Open Rules has the added benefit of being available for free with no registration which saves money for our client, but yet still meets the security standards of our client.

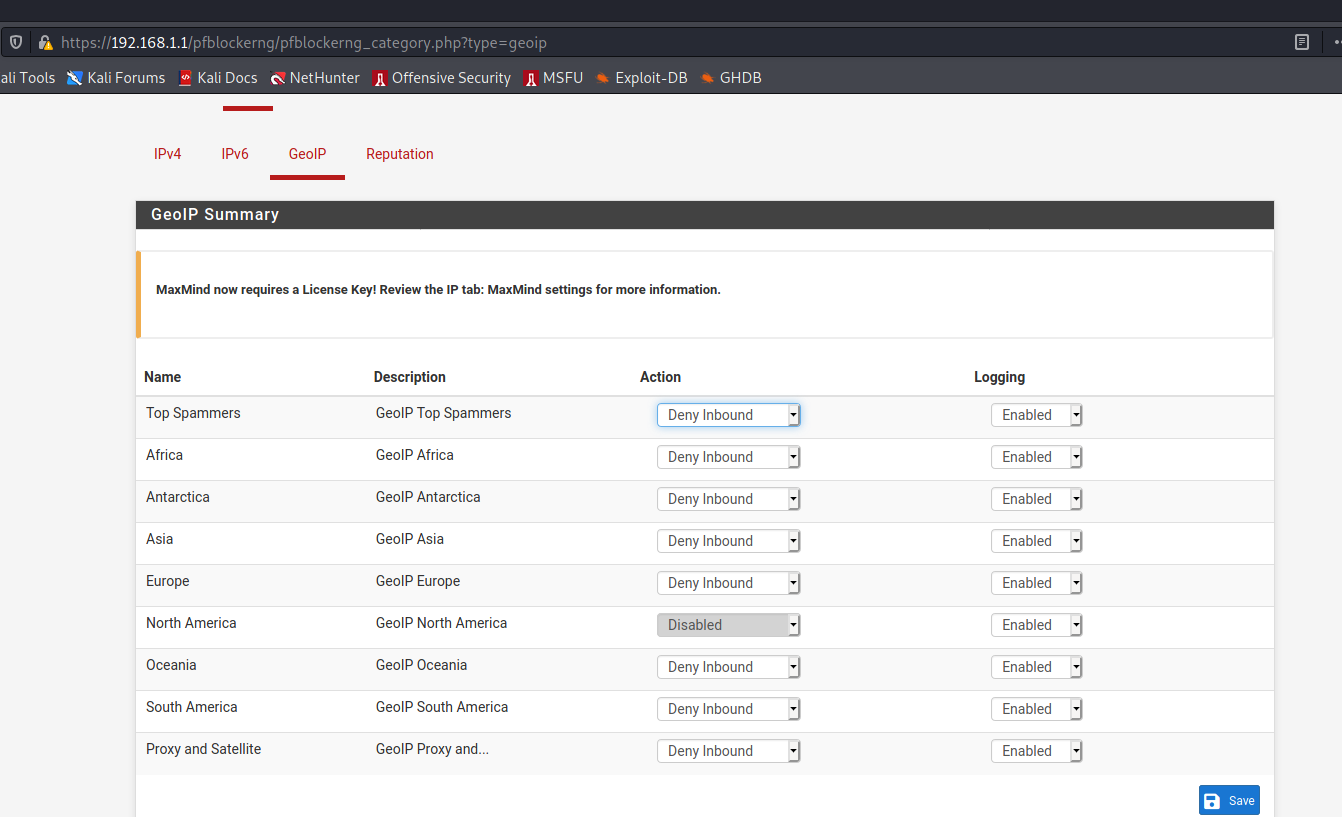


|  |
| --- |
| Fig 8: Snort configuration that allows download of Snort rulesets |



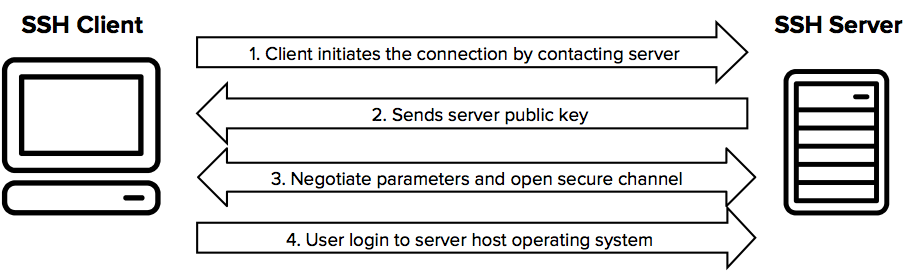
|  |
| --- |
| Fig 9: Enabling emerging threat rules in Snort interface |

This is the best rule one could use on a budget. According to nestgates official website [65] they strongly suggest obtaining a paid subscription from Snort or using the Emerging Threats in order to download the most current rules. They highly recommend the paid subscription for commercial applications, but since this is a test network this emerging threats rule meets our standards and is more than enough to catch any bad actor. When setting the Snort package up for the first time, there were a wide variety of rules that can be implemented. The Snort Global settings were the first. The network has automatic download enabled for Snort GPLv2 Community rules. The Snort Community Ruleset is a GPLv2 Talos certified [66] ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is also updated daily and is a subset of the subscriber rule set. Within the Snort Global settings, the next ruleset enabled is the download of emerging threats open rules. ETOpen is an open-source set of Snort Rules whose coverage is more limited than ETPro. We enabled OpenAppID. The OpenAppID detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules. AppID open text rules were also downloaded, which is maintained and hosted by the pfsense team. The next option enabled within just the system's Global setting is the download of FEODO Tracker BotNet C2 IP rules. The Feodo tracker tracks certain families that are related to or that evolved from Feodo. Originally, Feodo was an online banking Trojan used by cybercriminals to commit online banking fraud. Since 2010 [67], various malware families evolved from Feodo such as Cridex, Dridex, Geode, Heodo, and Emotet. ConstructZilla has many IOT devices [68] within the office. In the case that any of those devices were to end up connecting to our network and through either user error or malicious intent there was a compromise, then that would leave the test environment vulnerable. Having the FEODO botnet tracker enabled will help to prevent the network from being compromised even if other devices on the network are compromised. Another software package we thought to include in this project was pfblocker. Pfblocker will allow us to provide our client with additional security measures and we used the software to set up a GEOIP access limiter [69]. Currently, we have our GeoIP list set to deny any inbound requests that do not originate from North America. We implemented this after establishing there would be no foreign traffic running to our network and this is a very simple way to stop malicious traffic.



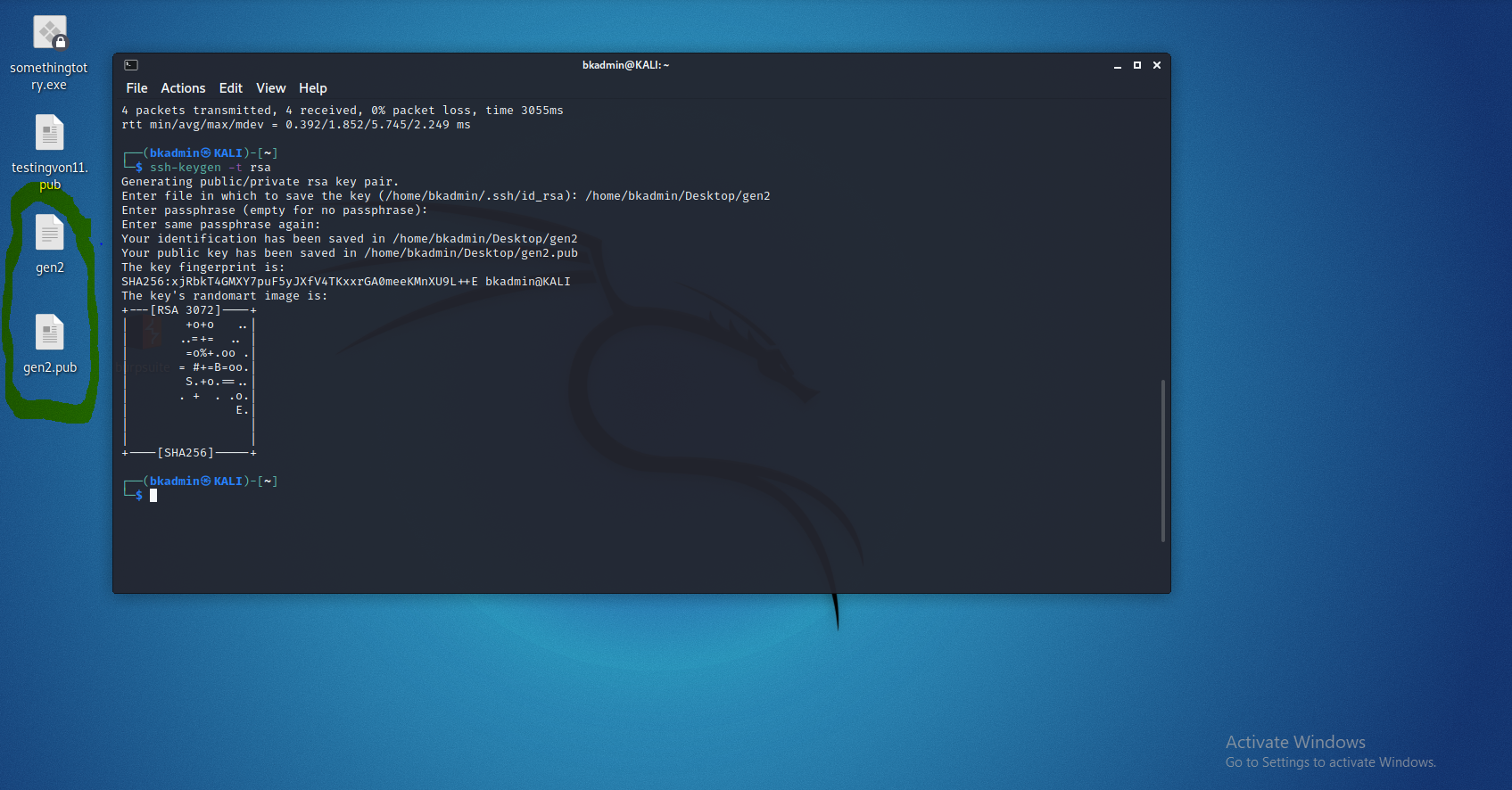
|  |
| --- |
| Fig 10: GEOIP blocking rules |

During another meeting and project review with ConstructZilla, we were asked to set up SSH for using a public-key authentication [70] only. Public key encryption is a security feature that utilizes a pair of generated keys [71] to enhance security beyond that of a password; easily forgotten or leaked by users or hackers and occasionally brute force [72] discovered in the case of simple passwords. To start with the process from a broad perspective, encryption [73] is a process in which information is distorted, seemingly randomized or otherwise hidden. There are two types of encryption [74]: symmetric and asymmetric. Symmetric encryption is the easiest to implement through the use of a password. I.e., one password is used to both lock and unlock or scramble and decipher. SSH can’t use symmetric encryption [75], since SSH involves transferring data over the network to another machine which could then be viewed by a malicious third party. Both parties must know the password to unlock the data, so with symmetric encryption there’s no way to transfer the locked data over the network and the password to unlock that data while ensuring that the password isn’t being leaked.

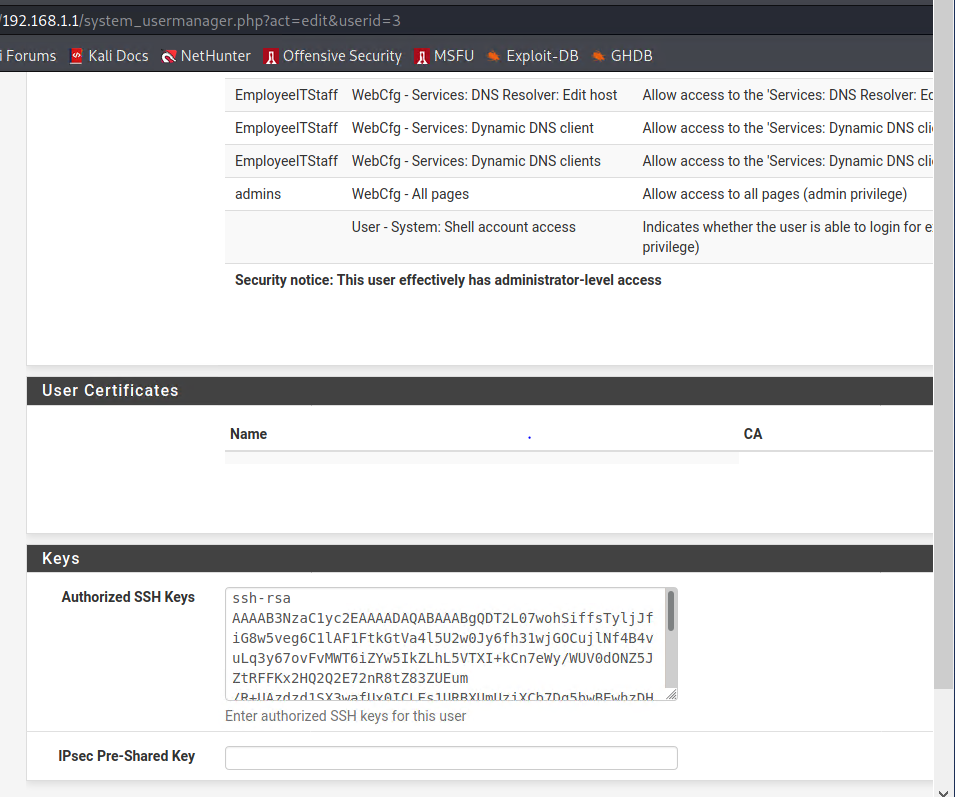


|  |
| --- |
| Fig 11: Diagram depicting SSH process [76] |

This is why SSH uses the asymmetric method of public-key encryption. Public-key encryption is a type of asymmetric encryption. Instead of a single key being used to lock and unlock, we use two. A public key and a private key. A public key is a lot like a mailbox on a street whereas a private key is a lot like the key that unlocks that mailbox. With a public key, information can be encrypted. With a private key, information can be decrypted. This ensures users can obtain locked information from anyone who chooses to encrypt it to them but only the owner of the private key can unlock the information. RSA encryption [77] is one of the more well-known algorithms for deriving keys and the SSH implemented through Kali uses an RSA-derived algorithm. SSH will function with RSA by deriving its client-side public key to encrypt data and its client-side private key to decrypt data. Likewise, on the server, SSH will generate its public key and private key. Once this is complete, the client machine can encrypt information with the server’s public key and upon receiving the encrypted information, our server can decrypt it using its private key. This is how SSH maintains security over the network and prevents third parties from viewing locked data. SSH is not perfect but it highly improves the security of communication over a network. To set up SSH on the project, we first generate the public-private key pair. Then, the public key is added to the server. Once that was complete, users could SSH into the network using their private key.



|  |
| --- |
| Fig 12: Generating keys |

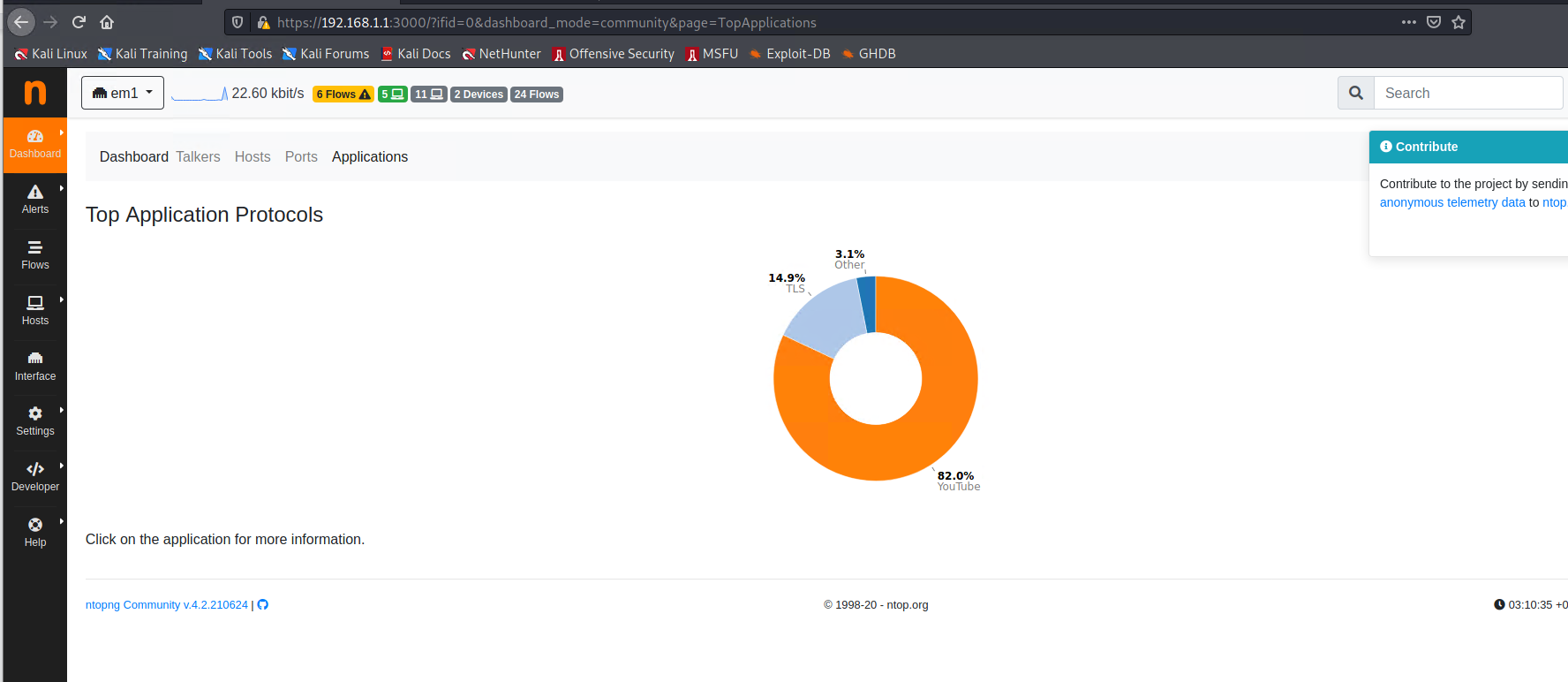


|  |
| --- |
| Fig 13: Adding keys to server |

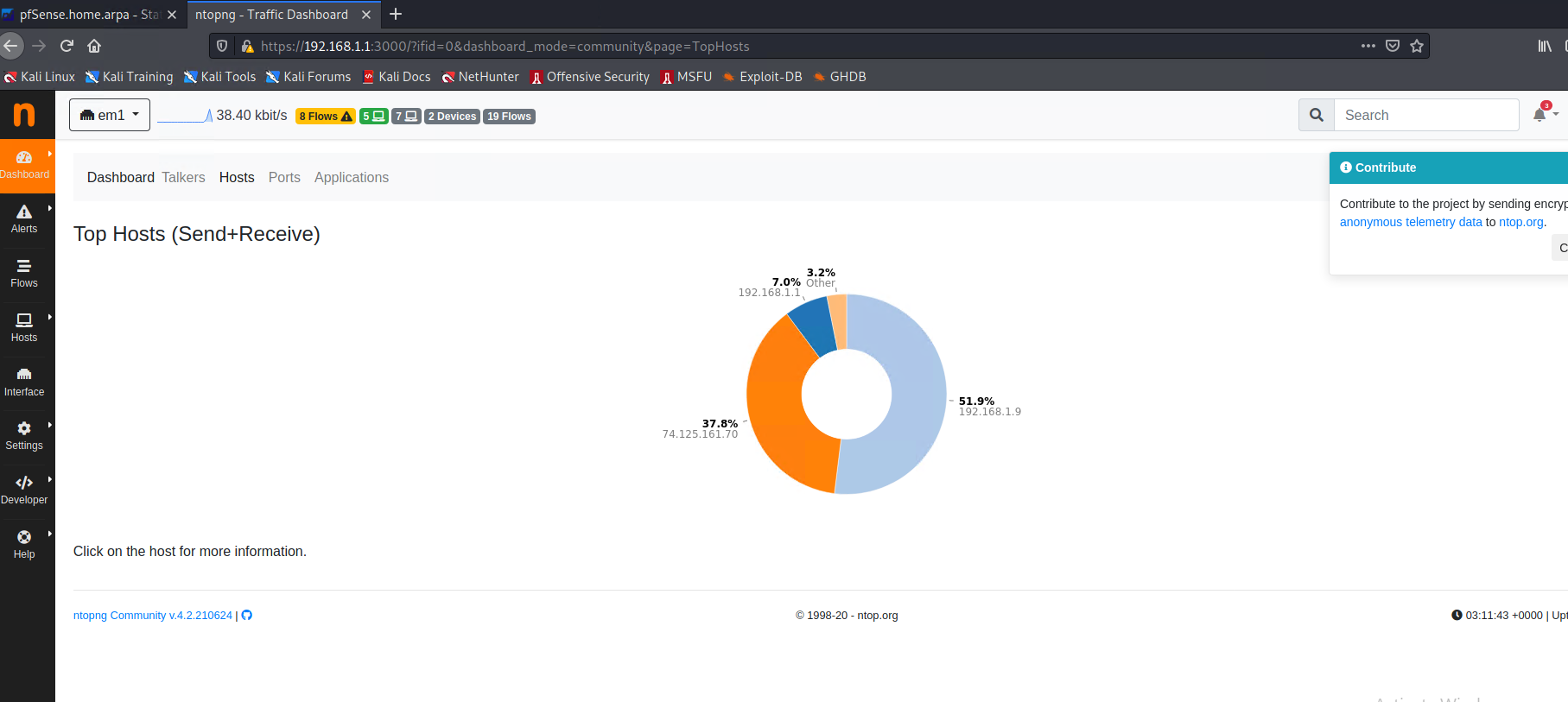
## Testing

### NtopNG

NTOPNG was first in the test process. We opened a web console and visited a few websites to verify NtopNG was functioning correctly.



|  |
| --- |
| Fig 14: ntopng filter by application network usage |

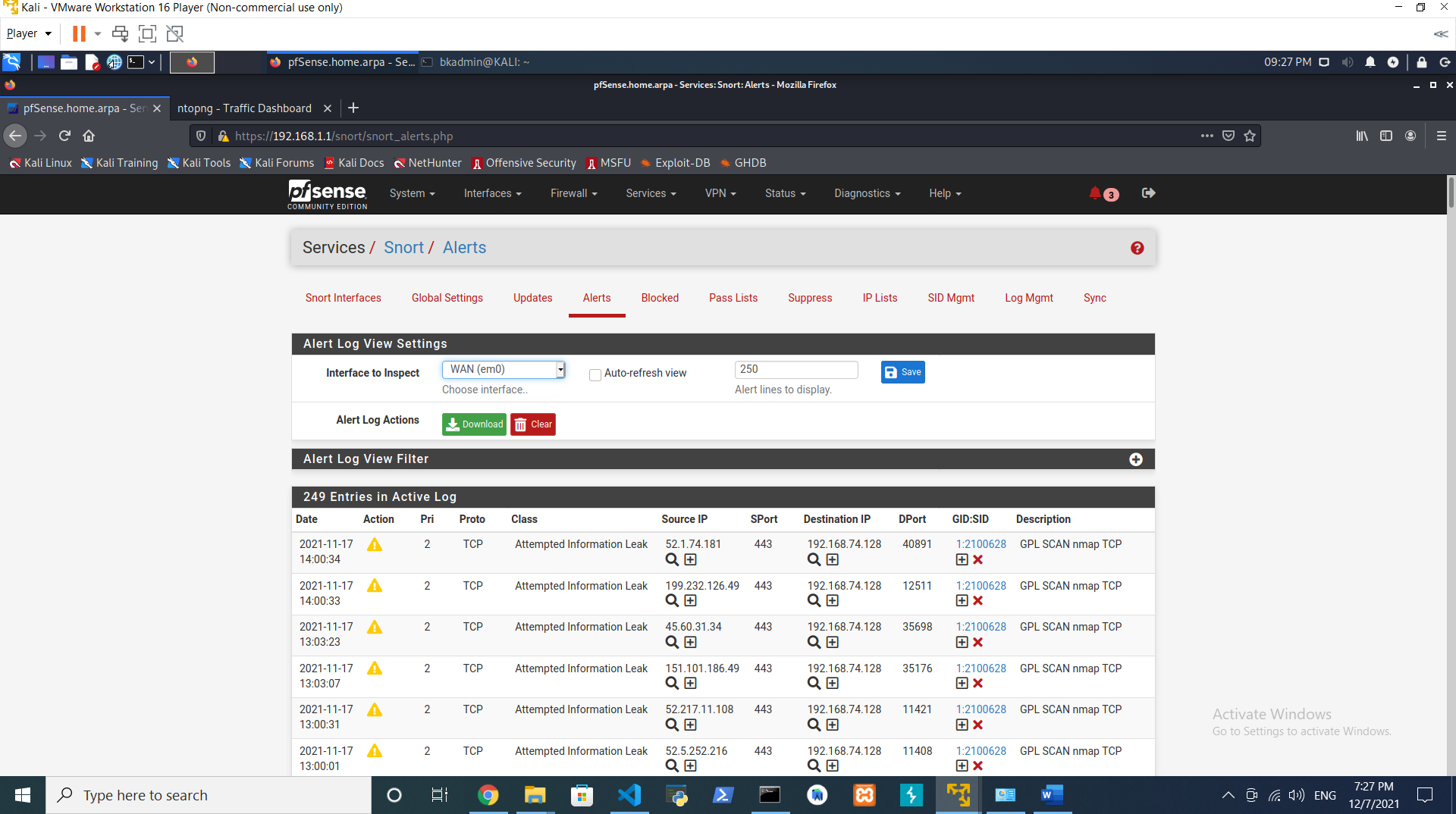


|  |
| --- |
| Fig 15: ntopng filter by hosts |

As verified above, NtopNG is picking up networking traffic and filtering it into metrics that are viewable inside of our Pfsense interface.

### Snort

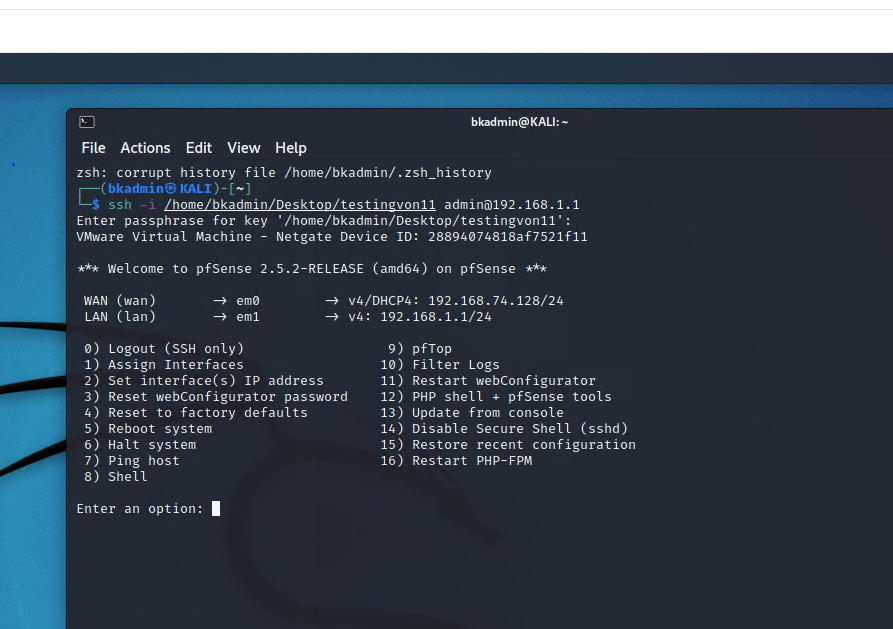
Testing for Snort was a very important step as many IDS’ are known for false positives and false negatives. To avoid any conflicts we wanted to make sure that malicious traffic is indeed being picked up by our IDS. To test for this, we ran an NMAP scan for open ports on the WAN interface of the Pfsense router. We checked the Snort logs and verified the traffic was being discovered and logged.



|  |
| --- |
| Fig 16: Snort captures NMAP running scans on the network |

### SSH

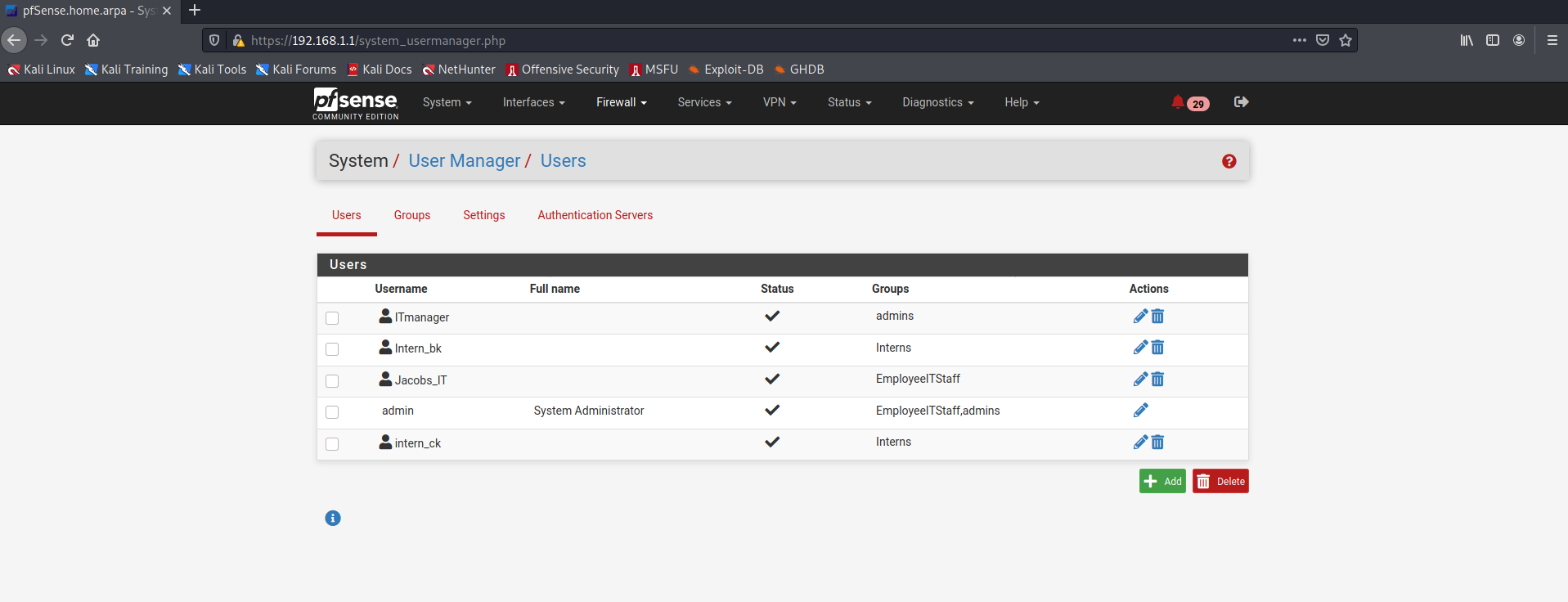
To test SSH using PKI, the public and private key pairs were generated and placed into the pfsense firewall. Private keys were assigned to a user account and this mechanism was tested for functionality by signing in using that private key. The log in was achieved successfully.



|  |
| --- |
| Fig 17: SSH user login successful |

## Administration

At this point, the users needed a way to access this system. There were two custom groups created, interns and IT staff. The interns group is able to learn but at the same time not edit any configurations. IT Staff have access to be able to edit configurations such as VLAN, wireless and MAC address tables but still do not have full admin rights. It is good practice to not assign full admin privileges to user accounts. If a breach happens on a user account then the attacker will be able to do anything on the system. After designing the group structure 5 user accounts were created: 1 Admin user account, 2 Intern user accounts, 1 IT manager user account, and 1 general IT user account.



|  |
| --- |
| Fig 18: User Account Information |

## Documentation & Training

Nearing completion of the project, it was time to construct the user documentation and determine proper staff training. We created documentation for crucial configurations such as authentication with SSH over a public key only. This documentation saves the internal IT staff at ConstructZilla time, and effort. With our documentation their team will learn a new skill in a short period of time. They can also use this documentation to train any new staff that may join the company. The team trained the IT staff on stateful firewalls, their features and why an organization would want to use a stateful firewall over a stateless firewall. We trained staff on how to login to Pfsense using the web GUI, how to create users and delete accounts that should not be active. While training the staff aspects of mission critical components of the system such as snort and where to check for logs was discussed. The team has been trained on how to access the ntopng admin console and why a separate account is needed to access this page. The team was made aware of the importance of locking down the ntopng page, since sensitive information is shown about the network and the type of traffic it is generating. ConstructZillas current IT staff consists of mostly developers who have no knowledge of networking. The team was trained on aspects of DHCP such as how to add machines and remove machines as well as on how to increase your scope in the case where more machines are needed. The team was trained on how to mitigate themselves from ARP spoofing attacks. They were shown how to tie an IP to a MAC address so that if the MAC of a certain IP changes it will not be allowed on to the network. The IT staff was trained on the importance of why they must do this and a demo was shown of an ARP attack so that they are well aware of how easy it is for this attack to occur.

# 4. Ethical Issues

When designing systems in which multiple users are on the same machine, ethical issues can arise. While there were no ethical dilemmas posed during the design or implementation phases of this project, the issue that remained was proper instruction of the staff on ethical behaviors using cyber security knowledge and software. The goal of any cyber security professional ought to be to protect a network from malicious parties; it should not be the goal to use this knowledge for malicious intent. There was great consideration in the documentation and training phase in which we discussed concepts of “ethical hacking.” We made it a point to talk about white/black hat hacking and laws surrounding privacy of information. While security education is highly important, the proper usage of that education is equally as important.

# 5. Business v Budget

We balanced business concerns by implementing a test environment that, while small, still achieves the same goals as a large-scale network implementation. The client originally wanted to go with a large-scale system but when met with the budget requirements for that size network, ConstructZilla was hesitant to continue with the project. To avoid losing the client and to help the client achieve their network implementation goals, we advised a small-scale trial system which came in far under the budget of the original idea the client proposed. This system is both scalable and useful, as well as being easy to maintain, reset and control. Since we’re working with VM technology, we knew that if this project worked as the client anticipated, it would be easier to set up more iterations of this project throughout the company without the overhead of costly physical topology.

# 6. Closing Thoughts

From a prior background in penetration testing and since the client was using this system as a testing ground specifically for training in network setup and cyber security, it was decided to go with some common, important staples in a network. Pfsense, an easy firewall with a good interface to learn on which allows users to interact with different methods in which they can prepare for and prevent attacks. Snort, a great tool that can be used as a teaching tool for network security by capturing specific network traffic. Additionally, with knowledge of encryption, it was understood how important SSH was and how public key encryption could benefit the system.

Citations

[1] Azure.microsoft.com. 2021. *What Is a Virtual Machine and How Does It Work | Microsoft Azure*. [online] Available at: <https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/#overview> [Accessed 10 December 2021].

[2] "Virtual Machine", *VMware*, 2021. [Online]. Available: https://www.vmware.com/topics/glossary/content/virtual-machine. [Accessed: 10- Dec- 2021].

[3]J. Shamir, "5 Benefits of Virtualization", *Ibm.com*, 2021. [Online]. Available: https://www.ibm.com/cloud/blog/5-benefits-of-virtualization. [Accessed: 10- Dec- 2021].

[4]"Enable Hyper-V on Windows 10", *Docs.microsoft.com*, 2021. [Online]. Available: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v. [Accessed: 10- Dec- 2021].

[5]"What is dynamic memory allocation (in virtualization)? - Definition from WhatIs.com", *SearchServerVirtualization*, 2021. [Online]. Available: https://searchservervirtualization.techtarget.com/definition/dynamic-memory-allocation. [Accessed: 10- Dec- 2021].

[6]"Understanding Clones", *Vmware.com*, 2021. [Online]. Available: https://www.vmware.com/support/ws5/doc/ws\_clone\_overview.html. [Accessed: 10- Dec- 2021].

[7]"What is a Virtual Machine Snapshot (VM Snapshot)? - Definition from Techopedia", *Techopedia.com*, 2021. [Online]. Available: https://www.techopedia.com/definition/16821/virtual-machine-snapshot-vm-snapshot. [Accessed: 10- Dec- 2021].

[8]*Virtualhackinglabs.com*, 2021. [Online]. Available: https://www.virtualhackinglabs.com/labs/penetration-testing-lab/. [Accessed: 10- Dec- 2021].

[9]M. Lee and M. Lee, "With Virtual Machines, Getting Hacked Doesn’t Have to Be That Bad", *The Intercept*, 2021. [Online]. Available: https://theintercept.com/2015/09/16/getting-hacked-doesnt-bad/. [Accessed: 10- Dec- 2021].

[10]"What is the Difference Between Type 1 and Type 2 Hypervisor - Pediaa.Com", *Pediaa.Com*, 2021. [Online]. Available: https://pediaa.com/what-is-the-difference-between-type-1-and-type-2-hypervisor/. [Accessed: 10- Dec- 2021].

[11]"Understanding and using Hyper-V hypervisor scheduler types", *Docs.microsoft.com*, 2021. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/manage-hyper-v-scheduler-types. [Accessed: 10- Dec- 2021].

[12]P. home, c. support and </form>, "What is a Hypervisor? Types of Hypervisors Explained (1 & 2)", *Knowledge Base by phoenixNAP*, 2021. [Online]. Available: https://phoenixnap.com/kb/what-is-hypervisor-type-1-2. [Accessed: 10- Dec- 2021].

[13]"Type 1 and Type 2 Hypervisors: What Makes Them Different", *Medium*, 2021. [Online]. Available: https://medium.com/teamresellerclub/type-1-and-type-2-hypervisors-what-makes-them-different-6a1755d6ae2c. [Accessed: 10- Dec- 2021].

[14]"Type-1 vs Type-2 Hypervisor", *vembu.com*, 2021. [Online]. Available: https://www.vembu.com/blog/type-1-and-type-2-hypervisor/. [Accessed: 10- Dec- 2021].

[15]I. Education, "hypervisors", Ibm.com, 2021. [Online]. Available: https://www.ibm.com/cloud/learn/hypervisors. [Accessed: 10- Dec- 2021].

[16]I. Education, "hypervisors", *Ibm.com*, 2021. [Online]. Available: https://www.ibm.com/cloud/learn/hypervisors. [Accessed: 10- Dec- 2021].

[17]“What is Esxi?: Bare metal hypervisor: ESX,” *VMware*, 06-Dec-2021. [Online]. Available: https://www.vmware.com/products/esxi-and-esx.html. [Accessed: 10-Dec-2021].

[18]Scooley, “Introduction to hyper-V on Windows 10,” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. [Accessed: 10-Dec-2021].

[19]“Citrix hypervisor - server virtualization and management software - citrix,” *Citrix.com*. [Online]. Available: https://www.citrix.com/products/citrix-hypervisor/. [Accessed: 10-Dec-2021].

[20]“Download VMware Workstation player,” *VMware*, 06-Dec-2021. [Online]. Available: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html. [Accessed: 10-Dec-2021].

[21]“Microsoft,” *Microsoft Support*. [Online]. Available: https://support.microsoft.com/en-us/topic/description-of-windows-virtual-pc-262c8961-90e5-1125-654f-d87cd5ba16f8. [Accessed: 10-Dec-2021].

[22]“Welcome to Virtualbox.org!,” *Oracle VM VirtualBox*. [Online]. Available: https://www.virtualbox.org/. [Accessed: 10-Dec-2021].

[23]Djohn, “Clone a virtual machine,” *Clone a Virtual Machine*. [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-C86E7n.d.-85A9-4D85-AEBB-135AA5648554.html. [Accessed: 10-Dec-2021].

[24]“VMware workstation 5.0,” *Network Address Translation (NAT)*. [Online]. Available: https://www.vmware.com/support/ws5/doc/ws\_net\_configurations\_nat.html. [Accessed: 10-Dec-2021].

[25]“VMware workstation 3.2,” *Host-Only Networking*. [Online]. Available: https://www.vmware.com/support/ws3/doc/ws32\_network6.html. [Accessed: 10-Dec-2021].

[26]“VMware workstation 4,” *Bridged Networking*. [Online]. Available: https://www.vmware.com/support/ws4/doc/network\_bridged\_ws.html. [Accessed: 10-Dec-2021].

[27]A. Hooper, “Business benefits of virtual machines and virtualization,” *IT Support Guys*, 14-Jul-2021. [Online]. Available: https://itsupportguys.com/it-blog/business-benefits-of-virtual-machines-and-virtualization/. [Accessed: 10-Dec-2021].

[28]“The 2020 State of Virtualization Technology,” *Marketing*. [Online]. Available: https://www.spiceworks.com/marketing/reports/state-of-virtualization/. [Accessed: 10-Dec-2021].

[29] Migration, “Install a guest operating system manually,” *Install a Guest Operating System Manually*. [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-F8A9B904-0DB3-4858-85EC-4864D38056D1.html. [Accessed: 10-Dec-2021].

[30]C. Hoffman, “Dual booting explained: How you can have multiple operating systems on your computer,” *How*, 04-Jul-2017. [Online]. Available: https://www.howtogeek.com/187789/dual-booting-explained-how-you-can-have-multiple-operating-systems-on-your-computer/. [Accessed: 10-Dec-2021].

[31]“4 reasons 'virtualization' software saves money,” *eMazzanti Technologies*, 26-Jun-2020. [Online]. Available: https://www.emazzanti.net/4-reasons-virtualization-saves-money/. [Accessed: 10-Dec-2021].

[32]“Open source security,” *pfSense® - World's Most Trusted Open Source Firewall*. [Online]. Available: https://www.pfsense.org/. [Accessed: 10-Dec-2021].

[33]“Anti-spoofing,” *MANRS*, 09-Apr-2019. [Online]. Available: https://www.manrs.org/isps/guide/antispoofing/. [Accessed: 10-Dec-2021].

[34]“PfSense plus content filtering,” *Netgate*. [Online]. Available: https://www.netgate.com/pfsense-plus-applications/content-filtering. [Accessed: 10-Dec-2021].

[35]“What is IP address spoofing: Attack definition & anti-spoofing measures: Imperva,” *Learning Center*, 30-Sep-2020. [Online]. Available: https://www.imperva.com/learn/ddos/ip-spoofing/. [Accessed: 10-Dec-2021].

[36]“What is IP spoofing? | cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/. [Accessed: 10-Dec-2021].

[37]“What is a distributed denial-of-service (ddos) attack ...” [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Accessed: 10-Dec-2021].

[38]Kaspersky, “What is an IP address – definition and explanation,” *www.kaspersky.com*, 05-Jul-2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address. [Accessed: 10-Dec-2021].

[39]Kaspersky, “What is an IP address – definition and explanation,” *www.kaspersky.com*, 05-Jul-2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address. [Accessed: 10-Dec-2021].

[40] L. Williams, “Types of IP addresses: What is, full form of IP,” *Guru99*, 07-Oct-2021. [Online]. Available: https://www.guru99.com/types-of-ip-addresses.html. [Accessed: 10-Dec-2021].

[41]“What is TCP/IP? | cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/. [Accessed: 10-Dec-2021].

[42]Techopedia, “What is internet protocol version 4 (ipv4)? - definition from Techopedia,” *Techopedia.com*, 12-Dec-2017. [Online]. Available: https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4. [Accessed: 10-Dec-2021].

[43]ipv6 Created: 04 Jan 2011 - Last updated: 09 Aug 2019 — ipv4, “Understanding IP addressing and CIDR charts,” *RIPE Network Coordination Centre*. [Online]. Available: https://www.ripe.net/about-us/press-centre/understanding-ip-addressing. [Accessed: 10-Dec-2021].

[44] “Frequently asked questions (FAQ) on IPv6 adoption and ipv4 exhaustion,” *Internet Society*, 28-Sep-2021. [Online]. Available: https://www.internetsociety.org/deploy360/ipv6/faq/. [Accessed: 10-Dec-2021].

[45] *Stateless address autoconfiguration*. [Online]. Available: https://www.ibm.com/docs/en/i/7.2?topic=concepts-stateless-address-autoconfiguration. [Accessed: 10-Dec-2021].

[46] “Dynamic Host Configuration Protocol,” *Wikipedia*, 05-Dec-2021. [Online]. Available: https://en.wikipedia.org/wiki/Dynamic\_Host\_Configuration\_Protocol. [Accessed: 10-Dec-2021].

[47] JasonGerend, “Dynamic Host Configuration Protocol (DHCP),” *Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top. [Accessed: 10-Dec-2021].

[48] “How dora works? Dora process in details.,” *Skillsire*, 23-Nov-2020. [Online]. Available: https://www.skillsire.com/read-blog/432\_how-dora-works-dora-process-in-details.html. [Accessed: 10-Dec-2021].

[49] “Unicast,” *Wikipedia*, 23-Nov-2021. [Online]. Available: https://en.wikipedia.org/wiki/Unicast. [Accessed: 10-Dec-2021].

[50] M. E. Shacklett, A. Novotny, and K. Gerwig, “TCP/IP: What is TCP/IP and how does it work?,” *SearchNetworking*, 13-Jul-2021. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/TCP-IP. [Accessed: 10-Dec-2021].

[51] “An overview of HTTP - http: MDN,” *HTTP | MDN*. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview. [Accessed: 10-Dec-2021].

[52]“Learning made easy,” *dummies*. [Online]. Available: https://www.dummies.com/category/articles/windows-33532. [Accessed: 10-Dec-2021].

[53] “Indiana University,” *Indiana University Knowledge Base*. [Online]. Available: https://kb.iu.edu/d/aayd. [Accessed: 10-Dec-2021].

[54] “Gateways¶,” *Routing - Gateways | pfSense Documentation*. [Online]. Available: https://docs.netgate.com/pfsense/en/latest/routing/gateways.html. [Accessed: 10-Dec-2021].

[55] Rowell and RowellWi-Fi expert. Coffee addict ☕️. Tech nerd. Business owner., “MAC address table on Cisco Switches,” *Rowell Dionicio*, 12-Dec-2020. [Online]. Available: https://rowelldionicio.com/mac-address-table-cisco-switches-ccnp-encor/. [Accessed: 10-Dec-2021].

[56]“Address resolution protocol,” *Wikipedia*, 05-Dec-2021. [Online]. Available: https://en.wikipedia.org/wiki/Address\_Resolution\_Protocol. [Accessed: 10-Dec-2021].

[57] “Sysadmin's Guide to Network Services,” *MSP360 Blog*. [Online]. Available: https://www.msp360.com/resources/blog/sysadmins-guide-to-network-services/. [Accessed: 10-Dec-2021].

[58] “Ntop,” *ntop*, 03-Dec-2021. [Online]. Available: https://www.ntop.org/. [Accessed: 10-Dec-2021].

[59] “Ntopng,” *ntop*, 04-Dec-2021. [Online]. Available: https://www.ntop.org/products/traffic-analysis/ntop/. [Accessed: 10-Dec-2021].

[60] “Reject versus drop – which to use?,” *Core Sentinel*, 15-Oct-2020. [Online]. Available: https://www.coresentinel.com/reject-versus-drop/. [Accessed: 10-Dec-2021].

[61] “Snort 3 is available!,” *Snort*. [Online]. Available: https://www.snort.org/. [Accessed: 10-Dec-2021].

[62]“Open source,” *Wikipedia*, 09-Dec-2021. [Online]. Available: https://en.wikipedia.org/wiki/Open\_source. [Accessed: 10-Dec-2021].

[63] “Snort review including alternatives,” *Comparitech*, 25-Oct-2021. [Online]. Available: https://www.comparitech.com/net-admin/snort-review/. [Accessed: 10-Dec-2021].

[64] “Snort-network intrusion detection and prevention system,” *Fortinet*. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/snort. [Accessed: 10-Dec-2021].   
[65]S. Shea, “What is openappid? - definition from whatis.com,” *SearchSecurity*, 12-Aug-2014. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/OpenAppID. [Accessed: 10-Dec-2021].

[65] “Configuring the Snort package¶,” *Packages - IDS / IPS - Configuring the Snort Package | pfSense Documentation*. [Online]. Available: https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html. [Accessed: 10-Dec-2021].

[66] *What are community rules?* [Online]. Available: https://www.snort.org/faq/what-are-community-rules. [Accessed: 10-Dec-2021].

[67] “About,” *Feodo Tracker*. [Online]. Available: https://feodotracker.abuse.ch/about/. [Accessed: 10-Dec-2021].

[68] A. Ltd., “What are IOT devices,” *Arm*. [Online]. Available: https://www.arm.com/glossary/iot-devices. [Accessed: 10-Dec-2021].

[69] L. Green and byL. Green, “How to setup PFBLOCKERNG,” *Protectli*, 30-Jun-2020. [Online]. Available: https://protectli.com/kb/how-to-setup-pfblockerng/. [Accessed: 10-Dec-2021].

[70] “Using public keys for authentication,” *WinSCP*, 06-Dec-2021. [Online]. Available: https://winscp.net/eng/docs/public\_key. [Accessed: 10-Dec-2021].

[71]“Using Puttygen,” *WinSCP*, 06-Dec-2021. [Online]. Available: https://winscp.net/eng/docs/ui\_puttygen. [Accessed: 10-Dec-2021].   
[72] “What is social engineering? examples and,” *Webroot*. [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering. [Accessed: 10-Dec-2021].

[72] Kaspersky, “Brute Force attack: Definition and examples,” *www.kaspersky.com*, 05-Jul-2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/brute-force-attack. [Accessed: 10-Dec-2021].

[73]“What is Data Encryption? Definition, best practices & more,” *Digital Guardian*, 01-Dec-2020. [Online]. Available: https://digitalguardian.com/blog/what-data-encryption. [Accessed: 10-Dec-2021].

[74] “What types of encryption are there?,” *ICO*. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-types-of-encryption-are-there/. [Accessed: 10-Dec-2021].

[75] DigitalOcean, “Understanding the SSH encryption and connection process,” *DigitalOcean*. [Online]. Available: https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process. [Accessed: 10-Dec-2021].

[76]“SSH Secure Shell Home Page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, how-tos.,” *SSH Secure Shell home page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, how-tos.* [Online]. Available: https://www.ssh.com/academy/ssh. [Accessed: 10-Dec-2021].

[77] “RSA algorithm,” *Wikipedia*, 02-Sep-2021. [Online]. Available: https://simple.wikipedia.org/wiki/RSA\_algorithm. [Accessed: 10-Dec-2021].

[78] *IETF*. [Online]. Available: https://www.ietf.org/rfc/rfc4432.txt. [Accessed: 10-Dec-2021].