

**Research and Testing Two Open Source Firewalls, One of Which is IPTables And Second is pfSense**

**B00106665-Parvaz Ahmed**

**B00106732 –Musab Ali**

*Department of Informatics*

*School of Engineering & Informatics*

*Technological University Dublin, Blanchardstown Campus*

*Dublin 15.*

**Word Limit for Assignment: 2,000: Actual Word Count: 1995**

**Bachelor of Computing**

**IT Business Management**

**22/02/2020**

**Table of Contents**

**Report Overview ....................................................................................................... 3**

**Firewall Defined ........................................................................................................ 3**

**Opensource Firewalls ….............................................................................................. 3**

**Firewall Rules ............................................................................................................. 3**

**IpTables Firewall ....................................................................................................... 4**

**Why IpTables ............................................................................................................. 4**

**Installation and Configuration .................................................................................. 5**

**IpTables Tests ............................................................................................................ 6**

**NMAP Scan and Mitigation ........................................................................................ 7**

**pfSense Firewall ........................................................................................................ 11**

**Why pfSense .............................................................................................................. 12**

**Installation and Configuration ................................................................................... 12**

**pfSense Tests ............................................................................................................. 13**

**NMAP Scan and Mitigation ....................................................................................... 15**

**Iptables and pfSense Comparison .............................................................................. 17**

**Conclusion …………………………………………………….....................................……………………. 18**

**References ……………………………………………………………...................................……………... 18**

**Appendix ……………………………………………………………....................................………………. 18**

**Report Overview**

Firewall is a security mechanism that allows system admins to monitor and manage traffic based on specific rules. They are part of overall network security system along with others. There are many commercial and opensource firewalls available. To choose one of them depends on the requirements of the business. In this report we are discussing ipTables and pfSense firewalls which are one of the best opensource firewalls. Both have their advantages and disadvantages.

**Firewall**

A firewall is a security mechanism that monitors and controls network traffic both incoming and outgoing uses a set of defined rules. It basically acts as barrier between internet users and private networks. A firewall can be implemented as hardware, software or a combination of both. Firewall controls traffic flow between networks based primarily on lay 3 and 4 information (IP and Transport)

**Opensource** **Firewall**

A software that allows its users to analyse and modify/enhance its source code for free under its usage license is known as opensource. One of most popular and widely used opensource firewall are “ipTables” and “pfSense”.

**Firewall Rules**

On LAN 1 created following firewall rules:

* Allow ICMP requests
* Allow DNS request on port 53
* Allow Lan traffic on port 80
* Allow Lan traffic on port 443
* Only Ubuntu Linux allowed to ssh to firewall
* Block SSH to firewall on port 22
* Sniffer block web access
* Block All Lan traffic

**On WAN created following rule:**

* Disable ICMP requests from WAN to LAN1 and OPT1

**On OPT1(second LAN) created following rule:**

* Allowing ICMP requests from OPT1 to LAN1
* Allow ICMP requests from LAN1 to OPT1

**IpTables Opensource Firewall**

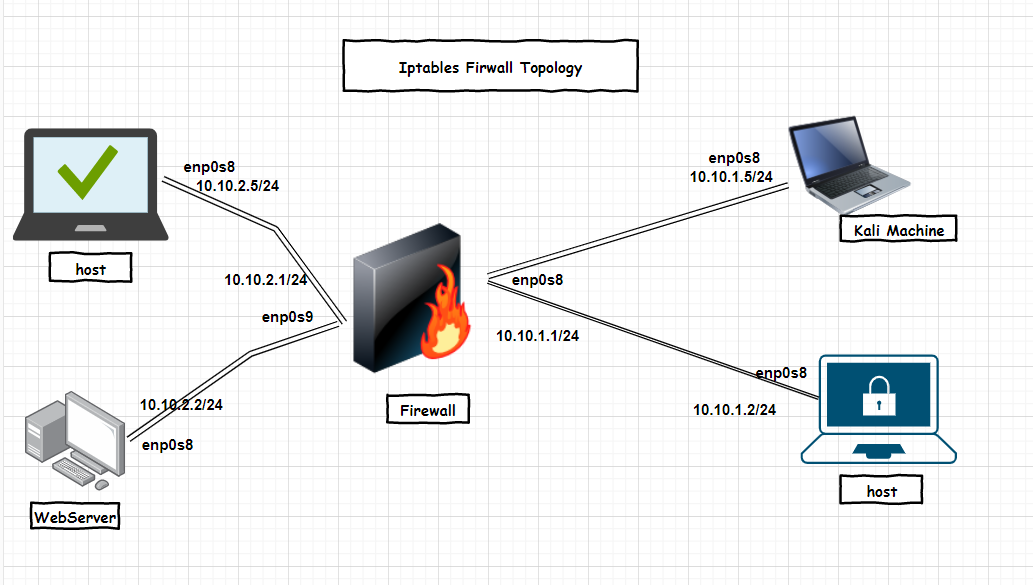
Iptables is used to define the Linux kernel firewall and its part of the netfilter project. Iptables is the front-end of the netfilter, Iptables has a structure which is based on tables, chains and rules. User uses iptables tool to instruct the kernel on how to deal with IP packets that flow through the kernel of the firewall, then Linux machine analyses the IP headers on packets and manipulates it according the iptables rulesets user has already defined.

**Why ipTables**

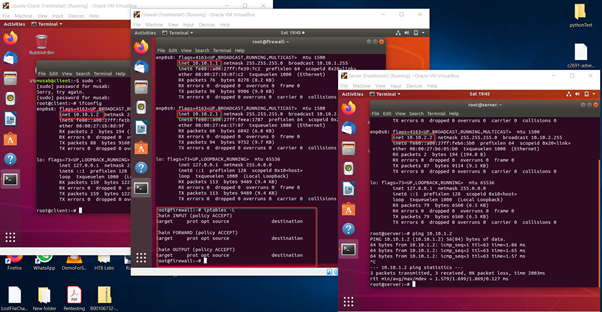
Iptables are advanced tools that come with linux operating systems for network packet filtering, controlling network packets that enter and monitor them till they move through and exit the network stack within the kernel.

**Installation and Configuration**

Our topology which we will be used for our project iptables is as follows:



We have created two different networks which will communicate through the firewall as shown below:

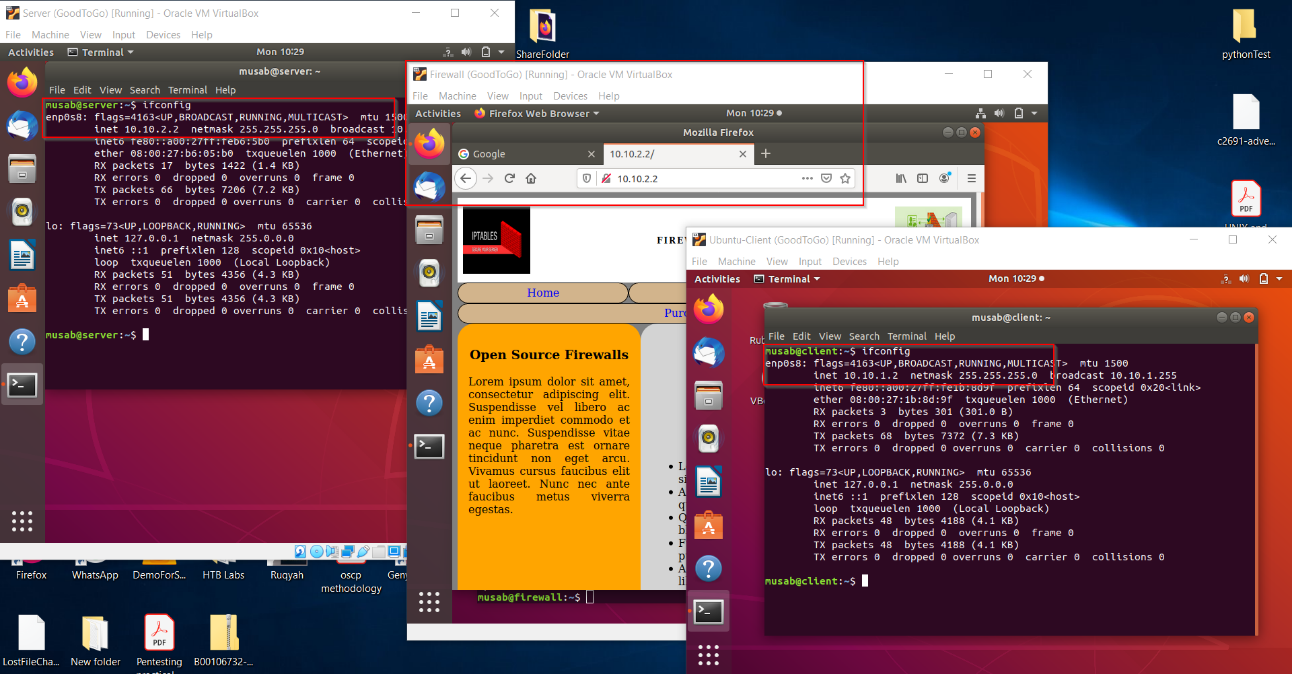


**Firewall Rules**

Initially our iptables rules is empty and these machines can communicate, and all services and ports are accessible which puts the security of the networks at risk. On the left hand of our topology we have a machine which offers services such as web access, file sharing or samba and ftp. We also must allow our network hosts to have icmp ports open so we can ping each other for troubleshooting. But ssh must be limited to only one host. following are the ruleset we will have:

1. Allow ICMP requests
2. Allow DNS request on port 53
3. Allow Lan traffic on port 80
4. Allow Lan traffic on port 443
5. Only one ip will be allowed to ssh webserver

We have created two different networks which will communicate through the firewall as shown below:

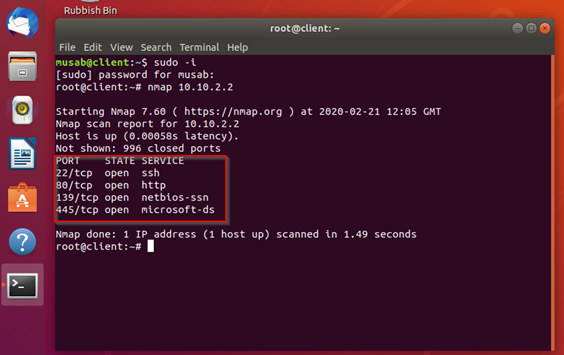


Webserver is of 10.10.2.0/24 network and client host have an IP address of 10.10.1.0/24 network, they are communicating via our firewall which is also our gateway.

**IpTables Tests**

The network is tested with different tools before any rules were set in our firewall, Nessus scan and nmap tests has been conducted and these are the results which came out.

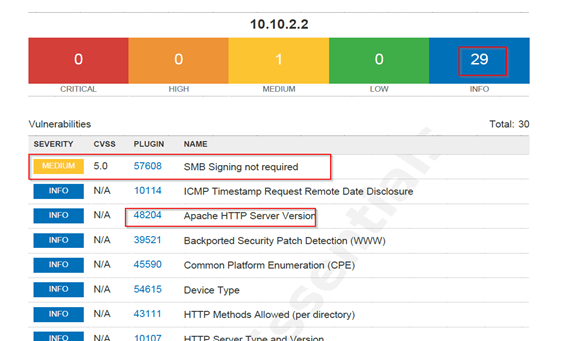
**NMAP Scan and Its Mitigation**



This test shows open ports and the services which runs on them also our Nessus test shows these information, other vulnerabilities and the severity of each vulnerability poses to our network as well as suggestions on how to mitigate them.

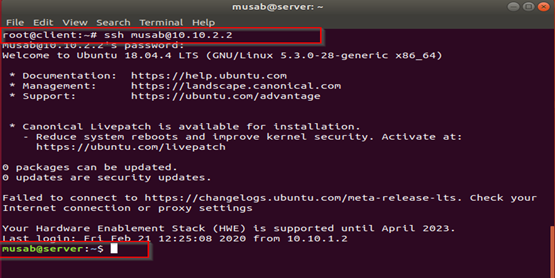
**Nessus Scan prior to firewall rulesets**

Nessus scan was able to collect 29 information on our network prior our firewall rules which can easily lead to more enumeration and an attack at the end on our networks.



**SSH Test**

A client machine on the 10.10.1.0/24 network can access the server on the 10.10.2.0/24 network:



**Mitigation of these open ports and services with the iptables Firewall**

We first set a default rule in our firewall which doesn’t allow any input and forward of packets and only accepts output.

**Default firewall polices**

iptables -P INPUT DROP

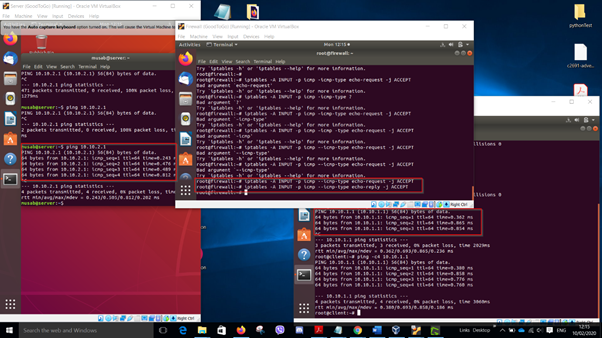
iptables -P OUTPUT ACCEPT

iptables -P FORWARD DROP

and to allow us testing our network and troubleshooting we allow server and client networks to ping each other from every end to the other end.

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

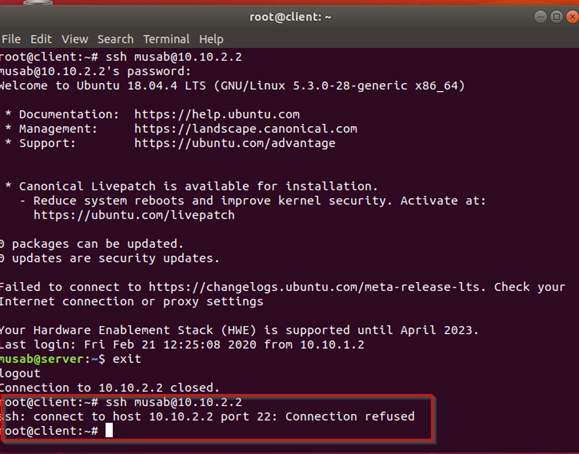


To secure ssh we then restrict any access from network 10.10.1.0/24 to the server network with this rule:

Iptables -A INPUT -s 10.10.1.2/24 -p tcp –dport 22 -j REJECT

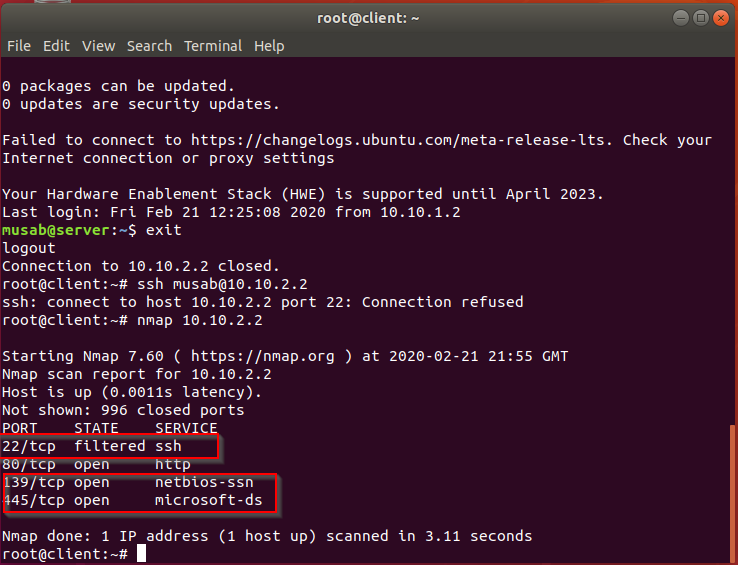
Iptables -A FORWARD -d 10.10.2.2/24 -p tcp –dport 22 -j REJECT

And this is what happened when we tried ssh-ing to server network from the client network



But the client network can still access port 80 our website and icmp. (Help.ubuntu.com, 2020)

Let’s take another test to check if our mitigation worked and the remaining open ports.

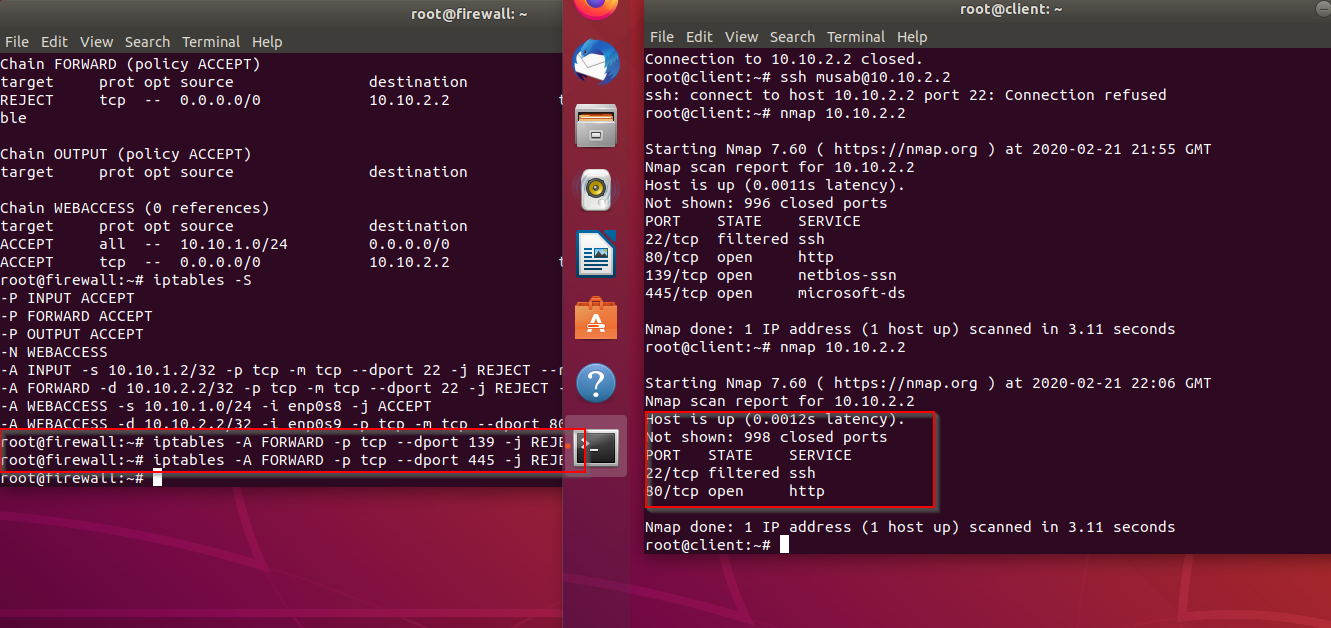


Now we will close samba ports of 445 and 139 using the following iptables rules:

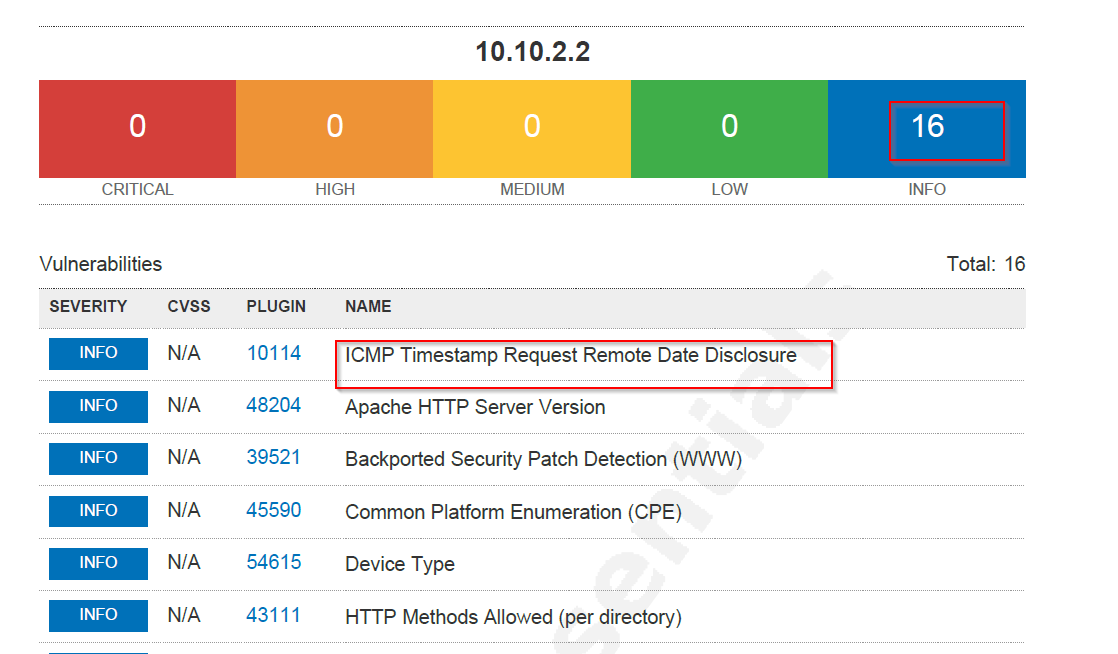
iptables -A FORWARD -p tcp --dport 139 -j REJECT --reject-with tcp-reset

iptables -A FORWARD -p tcp --dport 445 -j REJECT --reject-with tcp-reset

After these rules has been applied smb ports are closed as shown by the following nmap and Nessus tests



The second Nessus scan shows fewer open ports and vulnerabilities after we had mitigated them. With no critical, high, medium or even low severity.



**pfSense** **Opensource** **Firewall**

It is a FreeBSD based Linux distribution that can be install on dedicated hardware (a computer) or on virtual machine. It acts both as firewall and a router. Its iso image comes with a custom kernel that is very easy to install, configure and upgrade through web-based interface which does not required the knowledge of underlying FreeBSD system. A very well-established community support is available on the internet but if one requires dedicated support and service pfSense also offers it through paid membership. Like ipTables, pfSense is also state-full and network-based firewall.

**pfSense** **Opensource** **Firewall**

It is a FreeBSD based Linux distribution that can be install on dedicated hardware (a computer) or on virtual machine. It acts both as firewall and a router. Its iso image comes with a custom kernel that is very easy to install, configure and upgrade through web-based interface which does not required the knowledge of underlying FreeBSD system. A very well-established community support is available on the internet but if one requires dedicated support and service pfSense also offers it through paid membership. Like ipTables, pfSense is also state-full and network-based firewall.

**Why pfSense**

Because of following features, we choose pfSense as our opensource firewall:

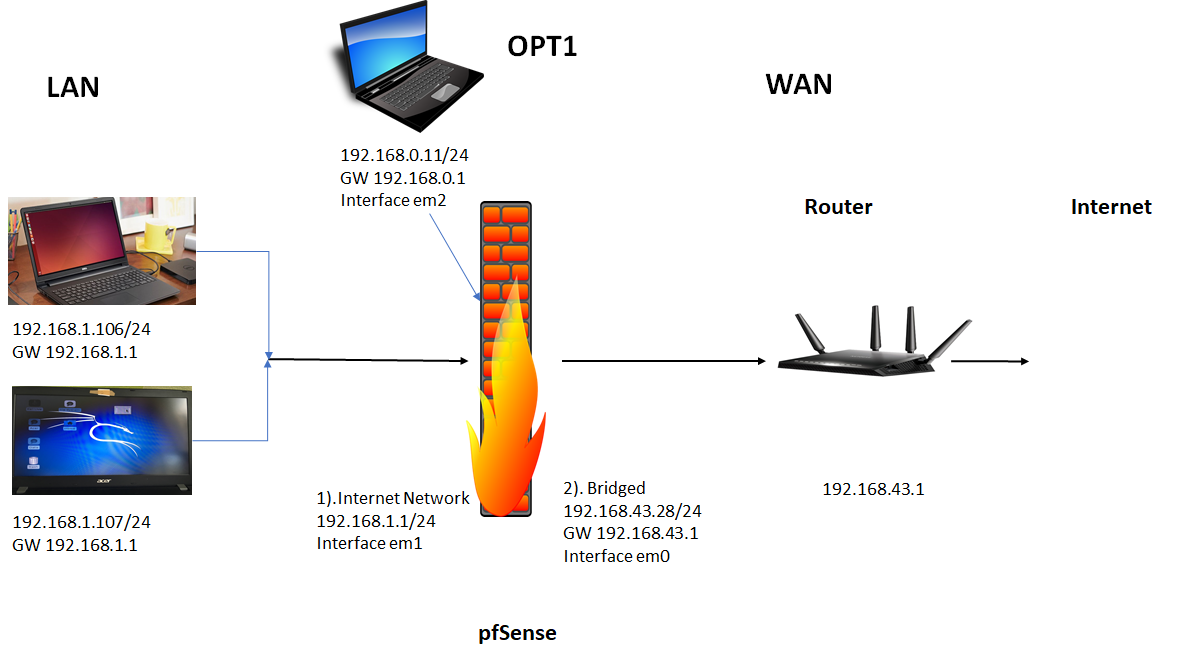
* Ease of set-up firewall rules
* Acts as firewall and router
* Enabling/disabling filtering is very easy
* Can handle multi-LANs/WANs
* Web-based easy to use interface
* Availability of online support and tutorials

These are many more features available in pfSense but because they are not relevant to our project, we are not mentioning them here.

**Installation and Configuration**

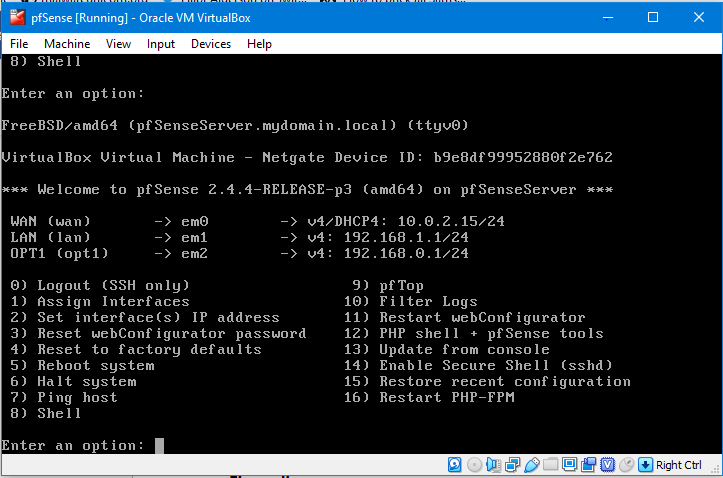
Network Topology

* Two LANs
* One WAN
* pfSense



For the purpose of this report, we downloaded latest version (2.4.4) of pfSense from official site pfsense.org and installed in virtual box but before installing the iso, we changed virtual box’s network adapter settings. For pfSense we created three network adapters: one “bridged” and two “internal network”. For our virtual machines(vms) we have only one adapter that is “internal network” state.

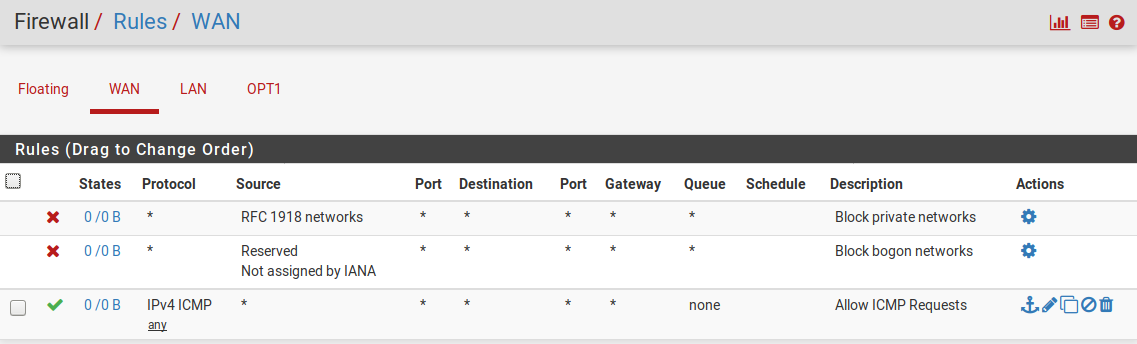
During the installation process, pfSene asks for which interface to attached with WAN, we selected “em0” as our WAN and “em1” as LAN and “em2” as our second LAN named as “OPT1”. Once its installed, we selected option 2 from the menu to give interfaces their ip address.



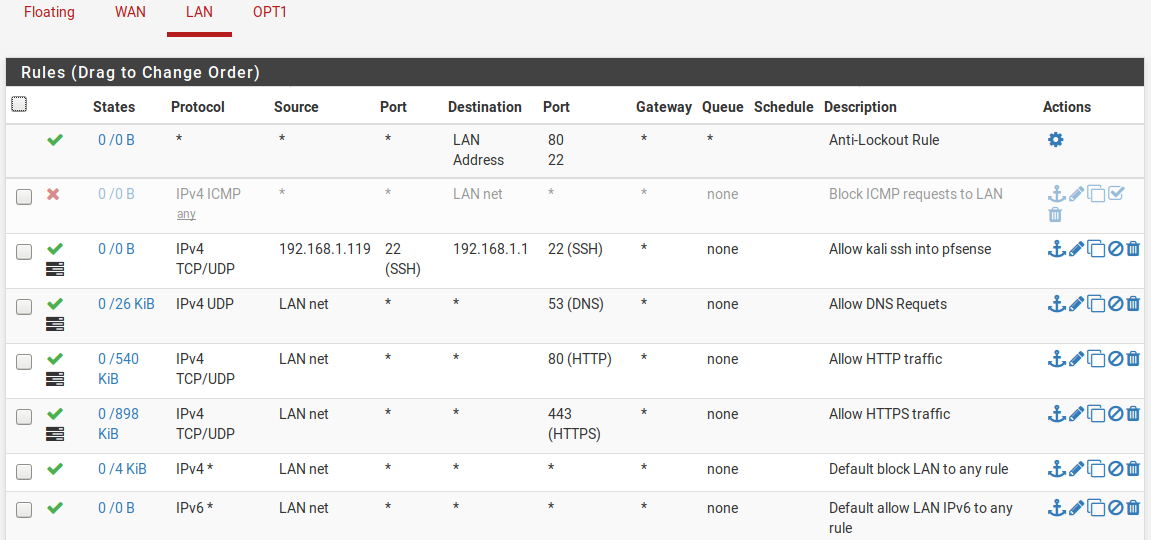
Because pfSense acts both as firewall and router, it gives us the option to set a pool of ip addresses to allocate them to our LANs. Similarly, we installed three vms, two on LAN1 and one on OPT1 for testing purposes.

**pfSense Tests**

It is very easy to create new firewall rules in pfSense. We have created a rule that allows WAN ICMP ping request for both of our LAN networks.



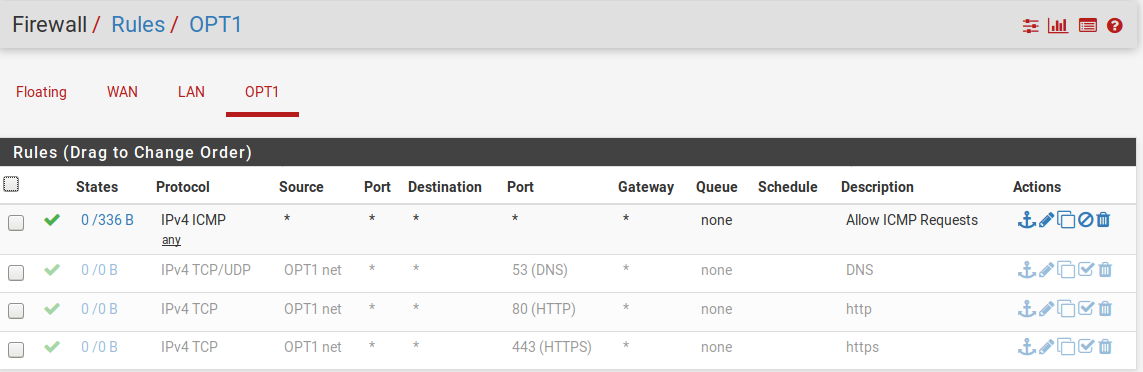
Similarly, under LAN tab there are options to create, copy, disable and delete any firewall rule.



As we can see in the above screenshot, we have created our required rules that are:

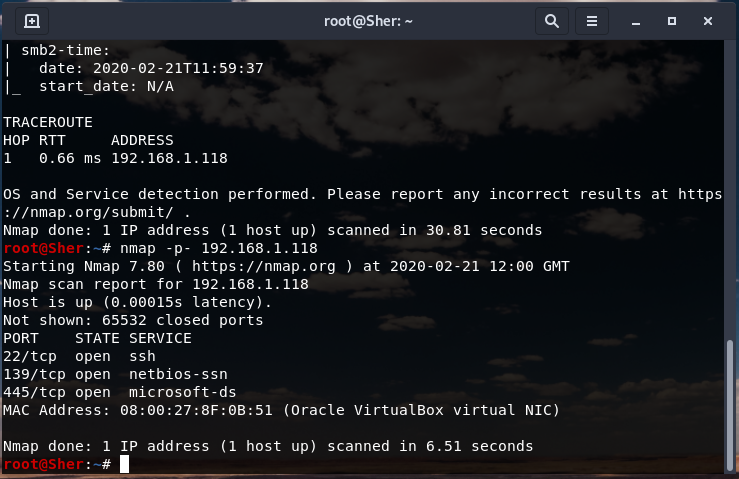
* IP address 192.168.1.119(Ubuntu) is allowed to ssh into pfSense
* Http and https traffic are allowed
* ICMP requested can be blocked from WAN but it is disabled for now

Our second LAN network “OPT1” is only allowed to ping our LAN network.

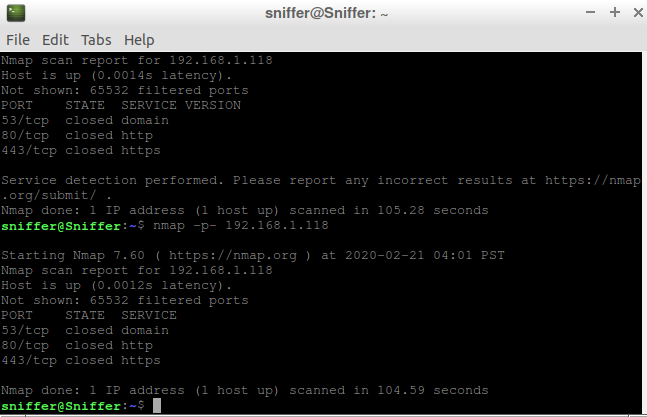


**NMAP Scan and Its Mitigation**

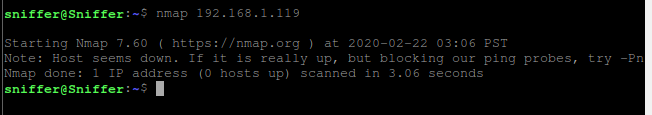
When namp scan is performed form internal network it shows three ports open.



But form our OPT1 network nmap scan shows those ports are closed.

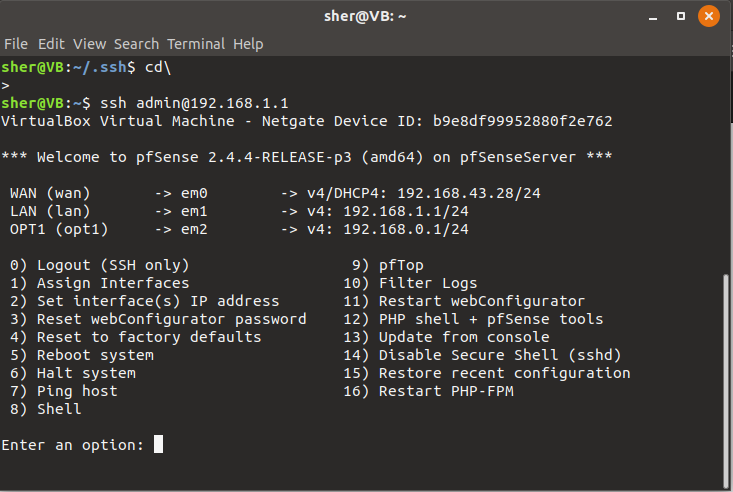


After applying our firewall rulles a nmap scan performed from OPT1 network shows it cannot perform scan.

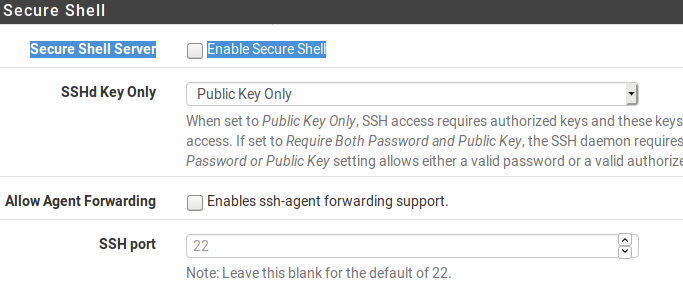


**SSH Test**

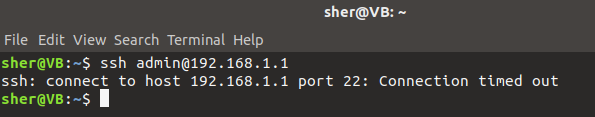
One ip is allowed to ssh into pfSense.



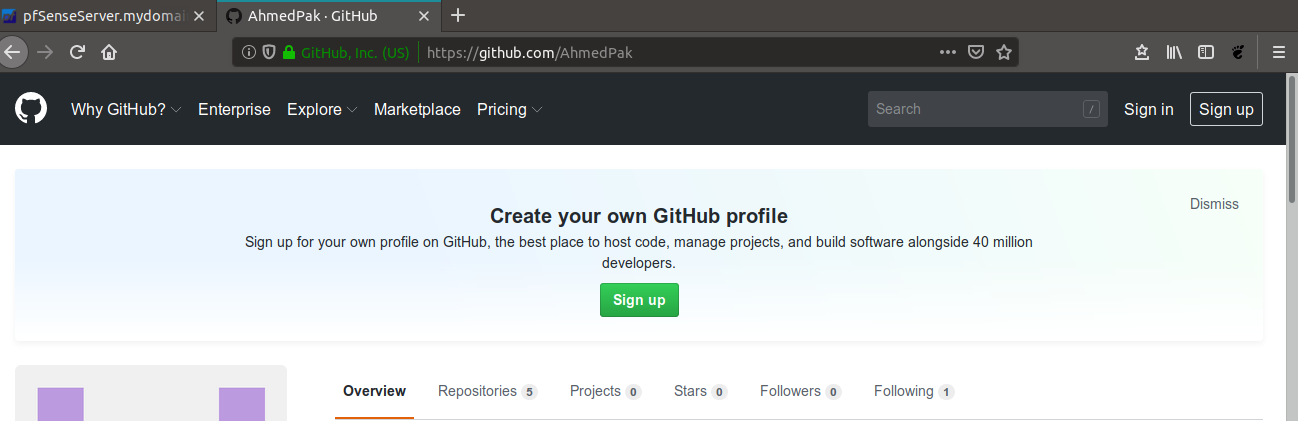
But It can be disapabled from WUI in pfSense.



After disabling SSH access now no machine can ssh into pfSense.



Internet access I.e., traffic on port 53, 80 and 443 is allowed only form LAN network. OPT1 network is not allowed to access internet.



**IpTables and pfSense Comparison**

Both have their advantages and disadvantages. We have enlisted a few of them here:

iptables is more of a command-line firewall where every rule is created through commands and saved as a file which is basically a bunch of commands whereas pfSense is web-based user interface where rules are created through few mouse clicks. pfSense creates configuration file for its tables, lists and variables which can be manipulated at ease.

Second difference between iptables and pfSense is the way they process packets. Each packet must go through all the iptables depending on the source and destination address in that packet. Each iptables has its own rules. It is possible for one packet to jump to another iptables based on a rule set in that iptables. In pfSenes a packet goes through configuration file, if a rule is matched action is taken if not default rule is applied. Rules can be created as need in pfSense. pfSense amends its iptables, lists or variables based on those rules, no need to do manually.

Another difference is the processing speed. As pfSense is stateful firewall, it lets packets bypass rules once a connection is established. This feature speeds up processing of packets but it makes it less secure. In iptables, each packet has to transverse through all the iptables which slows down over all speed of the traffic.

**Conclusion**

Both iptables and pfSense are advance opensource firewall solutions. They have great features and depending on the need of the organisation either can used. Although iptables have very advanced features but its not easy to implements those features whereas pfSense is easy to configure and it is fast but not that secure.

**References**

Iptables. *Man pages.* Available at: https://linux.die.net/man/8/iptables

Help.ubuntu.com. (2020). *Firewall*. [online] Available at: https://help.ubuntu.com/lts/serverguide/firewall.html [Accessed 4 Feb. 2020].

pfSense. Download Available at: https://www.pfsense.org/download/

Sumit Gupta, *OpenBSD pf vs Linux iptables: A Comparison* Available At: <https://www.experts-exchange.com/questions/27724507/pf-vs-iptables.html> [Accessed on 21 Feb 2020]

**Appendix**