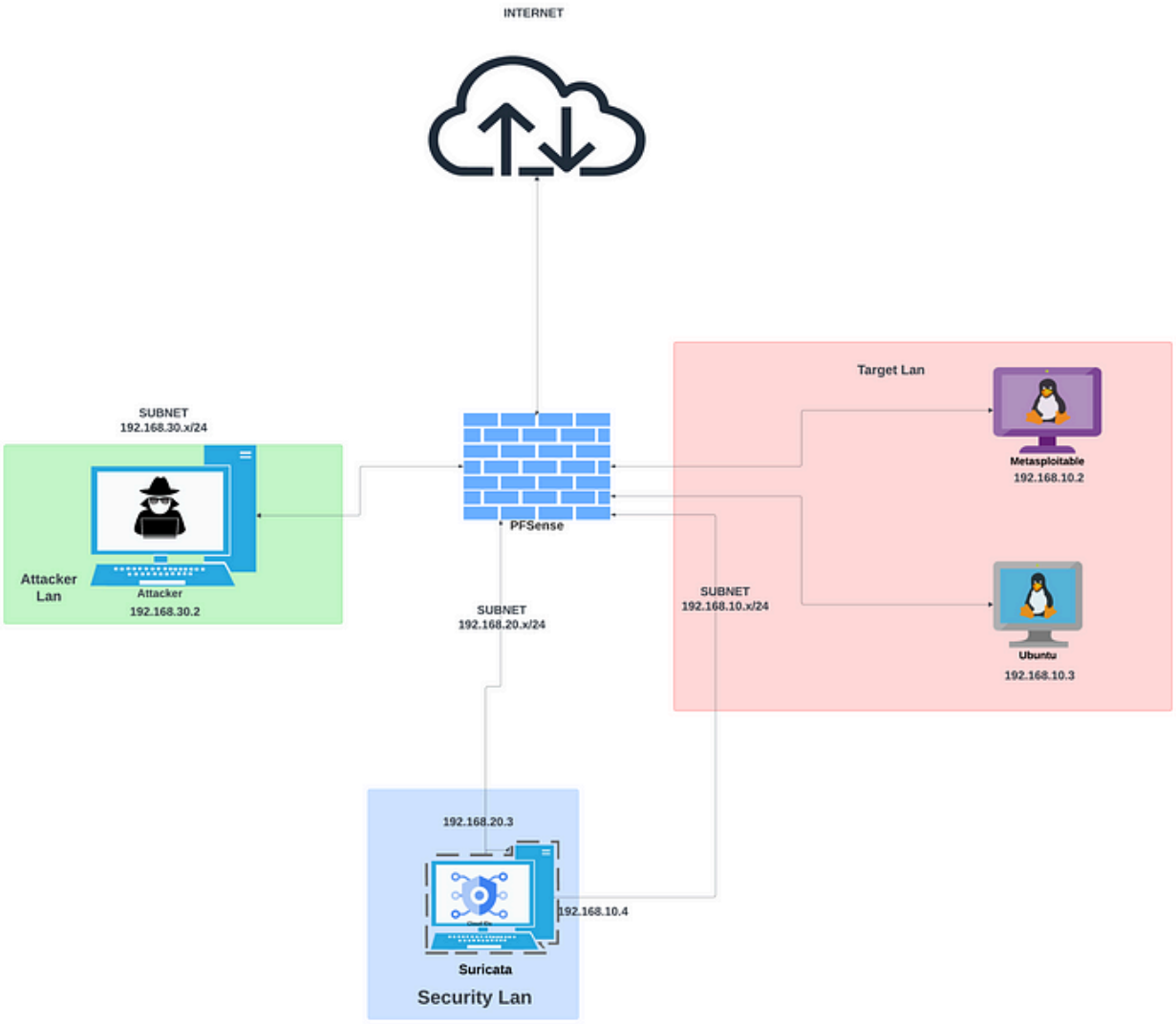
Creating this lab not only allowed me to refresh my networking and virtualization skills but also emphasized the importance of understanding your network to effectively secure and monitor for threats. It's a project I've been eager to share, detailing step-by-step configurations for each system in the simulated home network.

If you are familiar with computer networking, virtualization and basics of operating systems and build your own lab.

Lab Environment:

1. Having a network diagram helps while setting it up, to avoid confusion. Having a blueprint is indeed a good practice.
2. Below is the network diagram I came up with when building up my home network.



3. Networks:

a. Target Lan (192.168.10.x/24):

→ This would include the Metasploitable and Ubuntu Desktop machines.

→ Also, One of the interface of the monitoring device running suricata will be in target lan and configured to run in promisc mode, this helps the interface to capture all the traffic in the target lan.

b. Security Lan (192.168.20.x/24):

→ All the machines for monitoring traffic and threats will have their interface in this subnet, I will have a Ubuntu Machine running suricata and splunk, with one interface in this subnet and other in the target-lan for monitoring.

c. Attacker Lan (192.168.30.x/24):

→ I have kept a kali machine connected to this lan which will simulate the attacks on to my target lan.

Installation:

I assume, you understood the lab environment. I have given the resources on how to install ubuntu and kali linux in virtualbox. I will be demonstrating on how to setup pfsense and splunk cloud.

1. Virtualbox.
2. Ubuntu Desktop.
3. Kali Linux.
4. Pfsense (Just install the file , the configurations for this are described in the below sections).

5. Metasploitable.

Installation and configuring pfsense:

Create a new machine, I have named it Pfsense gateway.

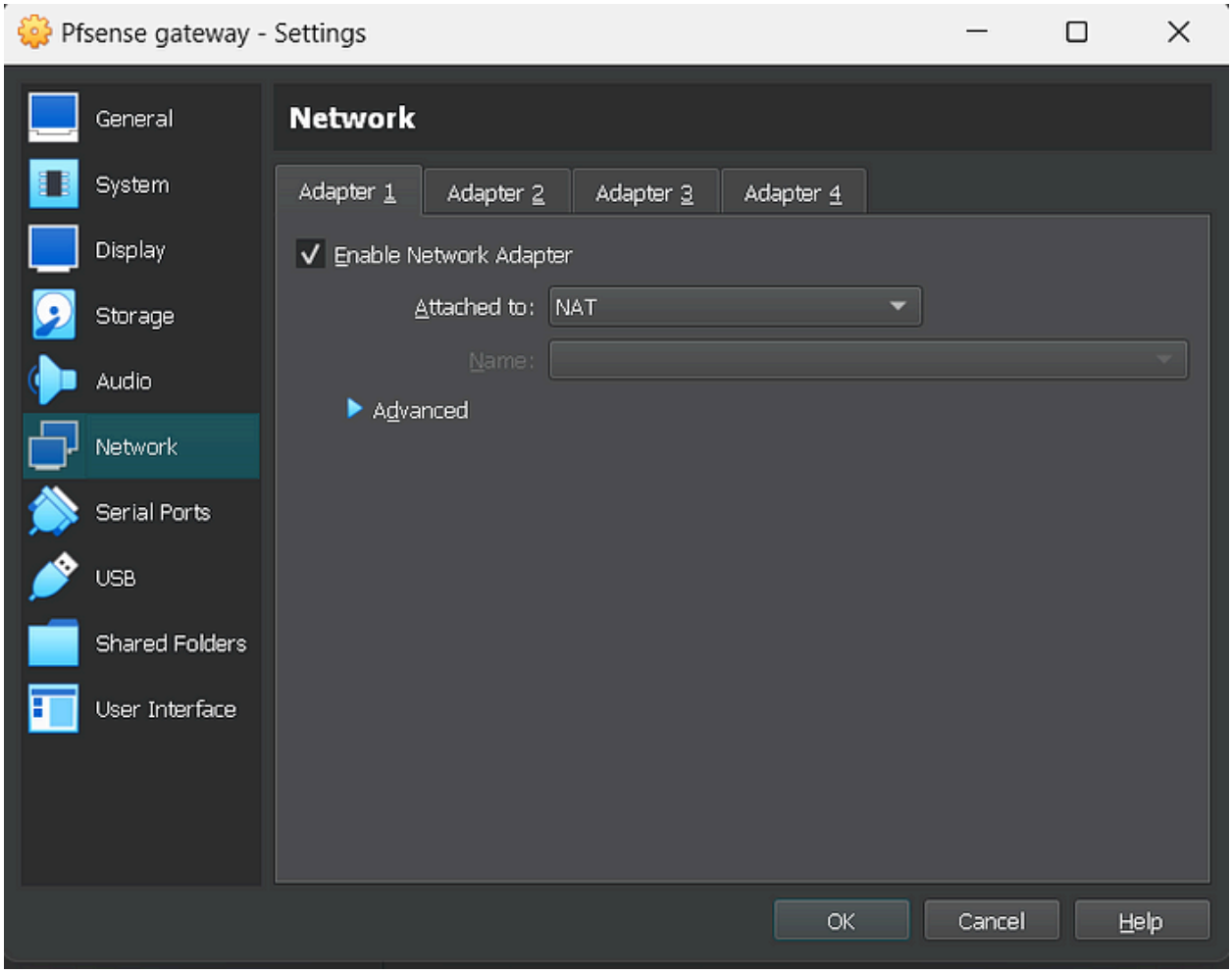
1. Ram:- 2 gb (recommended).
2. CPU- 2 (recommended).
3. Storage:- 20–25 (Default recommended).

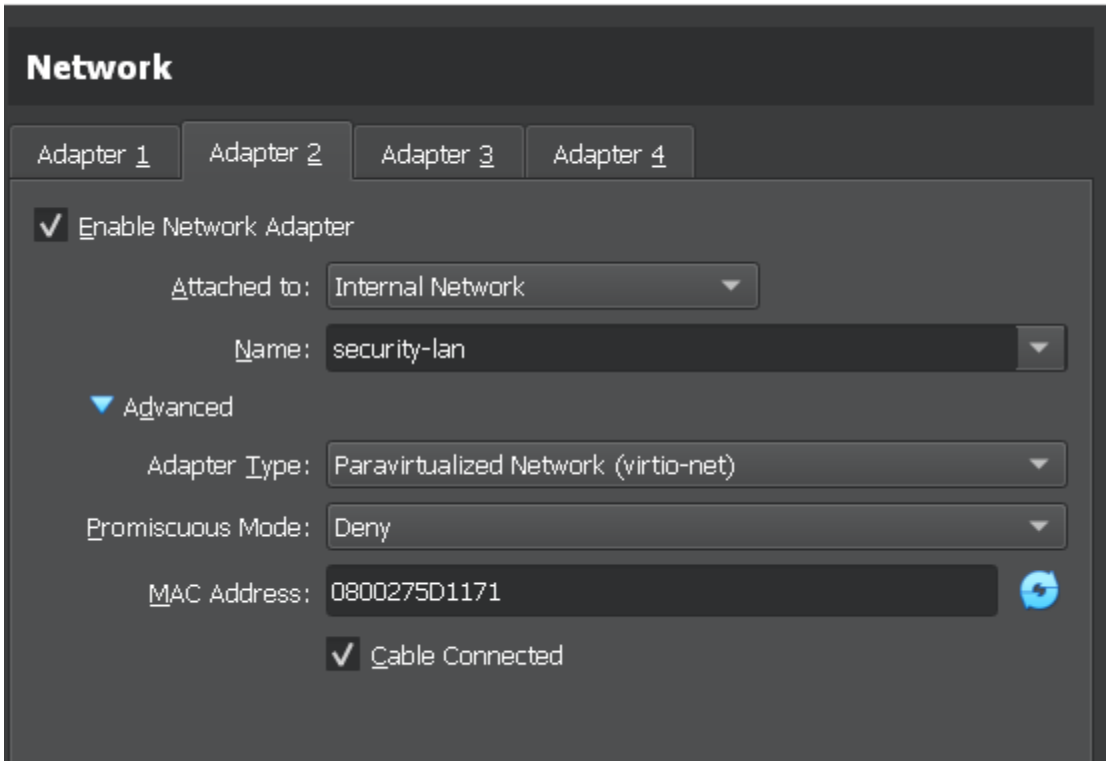
LAN setup:

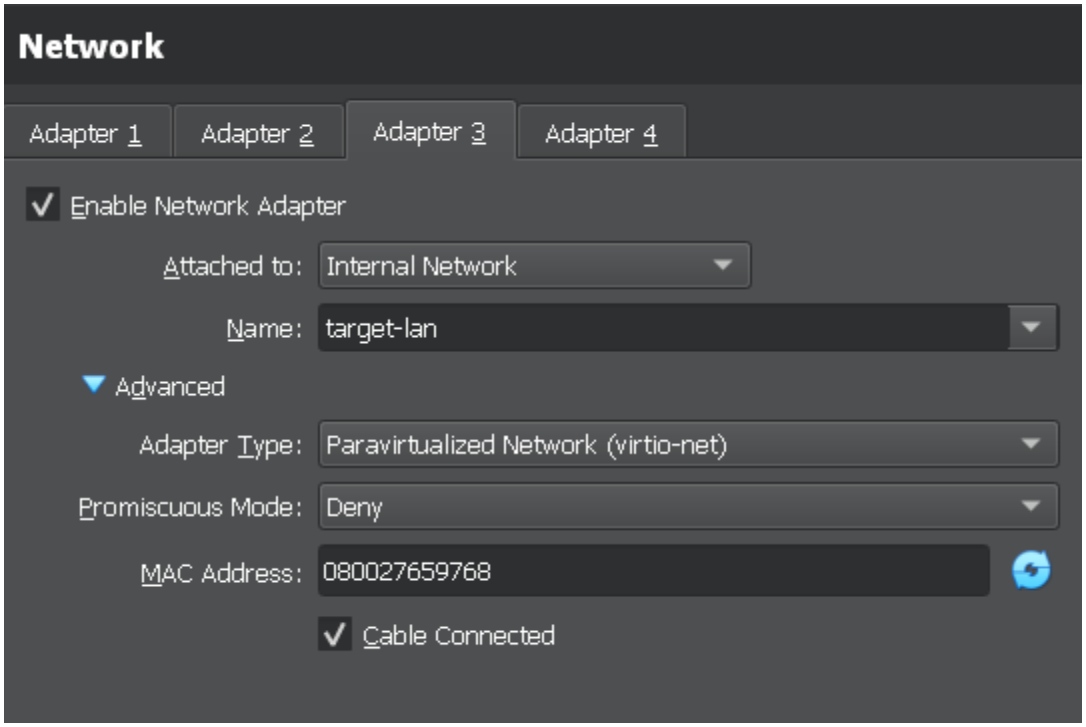
I have created 4 adapters on the machine running pfsense:

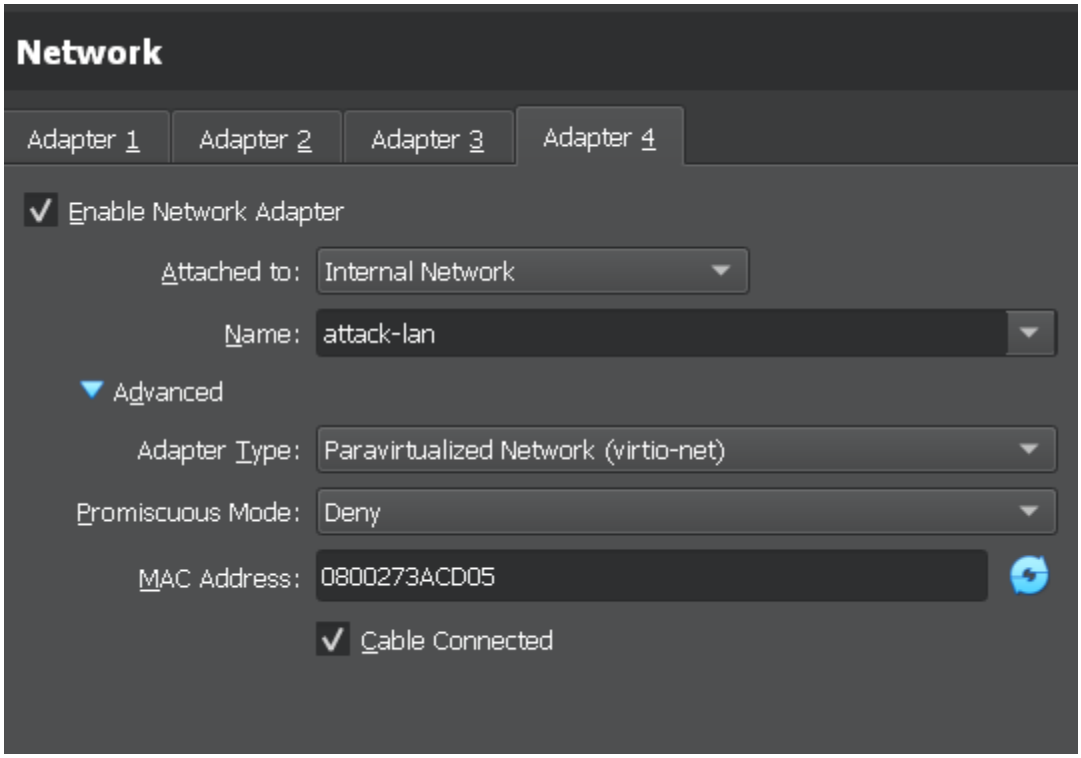
1. Adapter 1 — NAT.
2. Adapter 2 — Security Lan.
3. Adapter 3 — Target Lan.
4. Adapter 4 — Attacker Lan.

check the below screenshots:

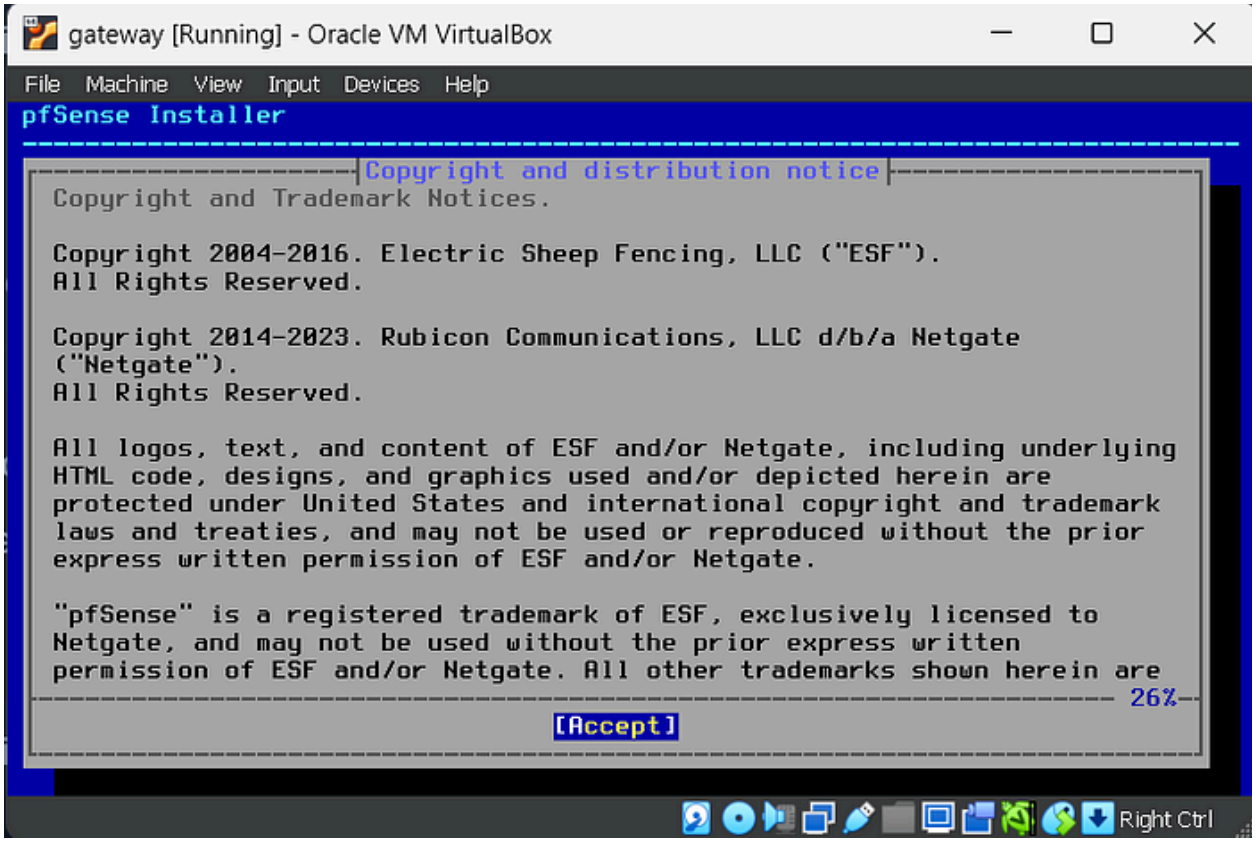

Pfsense gateway - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced
OK
Cancel
Help


Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
security-lan
Advanced
Adapter Type:
Paravirtualized Network (virtio-net)
Promiscuous Mode:
Deny
MAC Address:
0800275D1171
Cable Connected

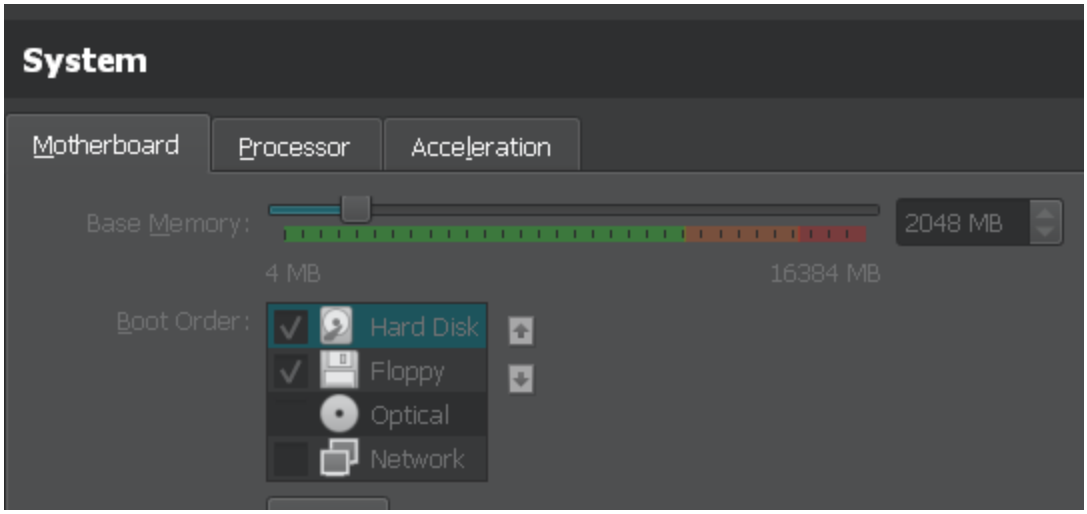

Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
target-lan
Advanced
Adapter Type:
Paravirtualized Network (virtio-net)
Promiscuous Mode:
Deny
MAC Address:
080027659768
Cable Connected



Now start the machine and wait for the copyright section to appear:



Select Install → Auto UFS → BR DOS Partition → Finish → Commit and wait for it to install and then reboot. After rebooting if it prompts for the Copyright page again like above, change the boot order of the virtual machine.

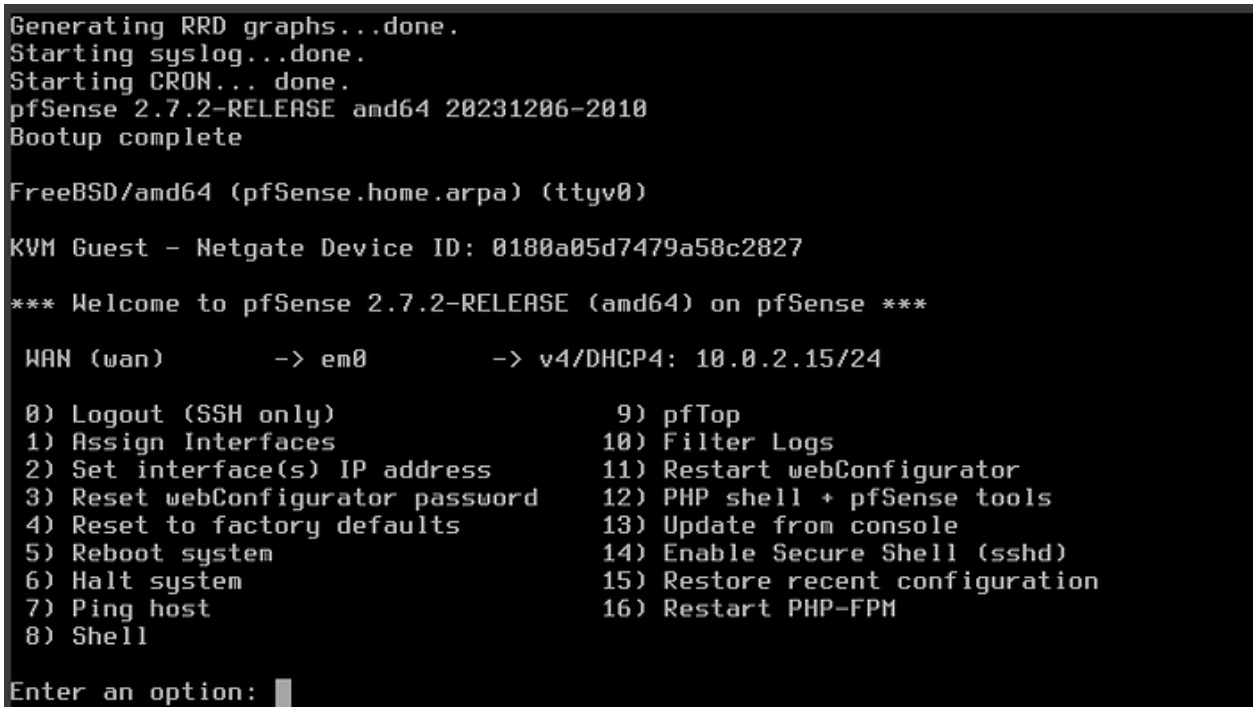


Then start the machine again:

```
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? 2024-07-20T12:16:11.428001+00:00 - php-fpm 38
 - - /rc.linkup: Ignoring link event during boot sequence.
2024-07-20T12:16:15.757194+00:00 - php-fpm 388 - - /rc.linkup: Ignoring link ev
nt during boot sequence.
2024-07-20T12:16:15.760246+00:00 - php-fpm 389 - - /rc.linkup: Ignoring link ev
nt during boot sequence.
em0: link state changed to UP
2024-07-20T12:16:17.514097+00:00 - php-fpm 661 - - /rc.linkup: DHCP Client not
unning on wan (em0), reconfiguring dhclient.
2024-07-20T12:16:32.899874+00:00 - php-fpm 661 - - /rc.newwanip: rc.newwanip: I
fo: starting on em0.
2024-07-20T12:16:32.900235+00:00 - php-fpm 661 - - /rc.newwanip: rc.newwanip: o
 (IP address: 10.0.2.15) (interface: WAN[wan]) (real interface: em0).
pflog0: promiscuous mode enabled


If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 vtnet0 vtnet1 vtnet2 or a):
```

I have set the first adapter to NAT, hence the WAN interface is indeed em0 so enter em0 and then click [Enter].

Then you will be shown the below screen



Assigning Interfaces

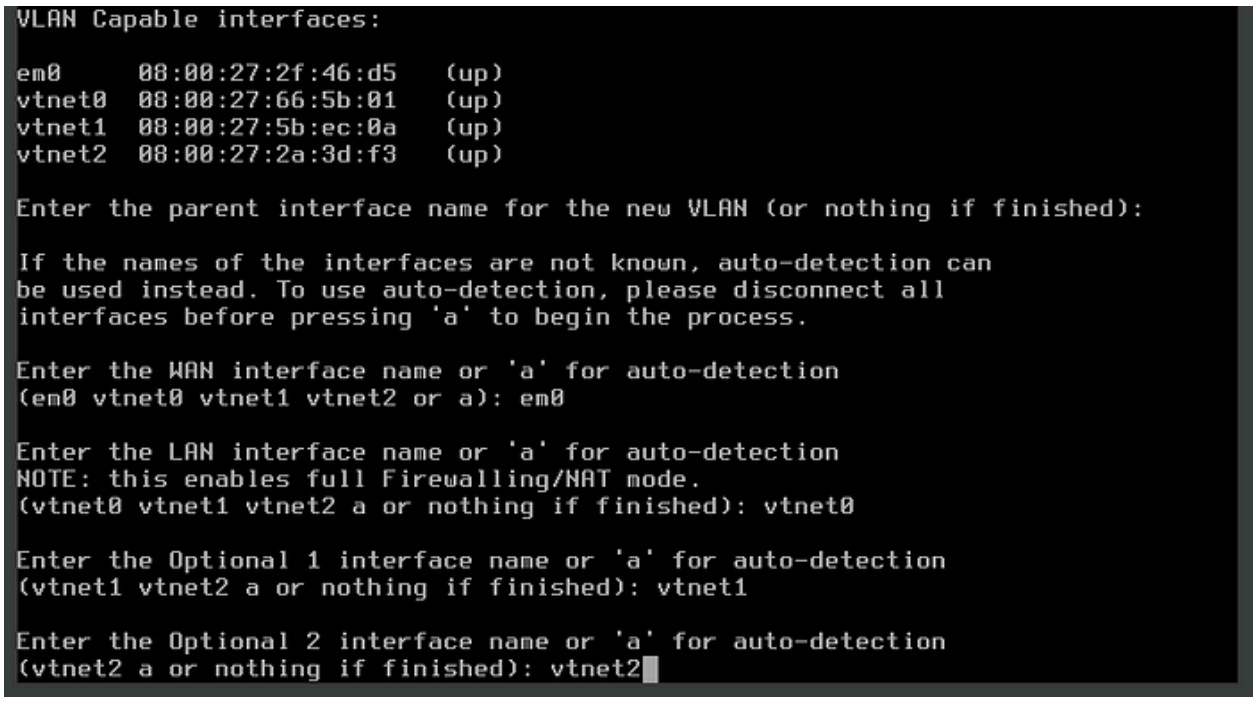
Enter 1 → Should vlan be set up : y → Enter parent interface : [Click Enter] → then set the interface as below image → then proceed with “y”.

Adapter 1(NAT): — em0…(this will be facing the internet).

Adapter 2(Security-Lan):-vtnet0.

Adapter 3(Target-Lan):-vtnet1.

Adapter 4(Attacker Lan):- vtnet2.

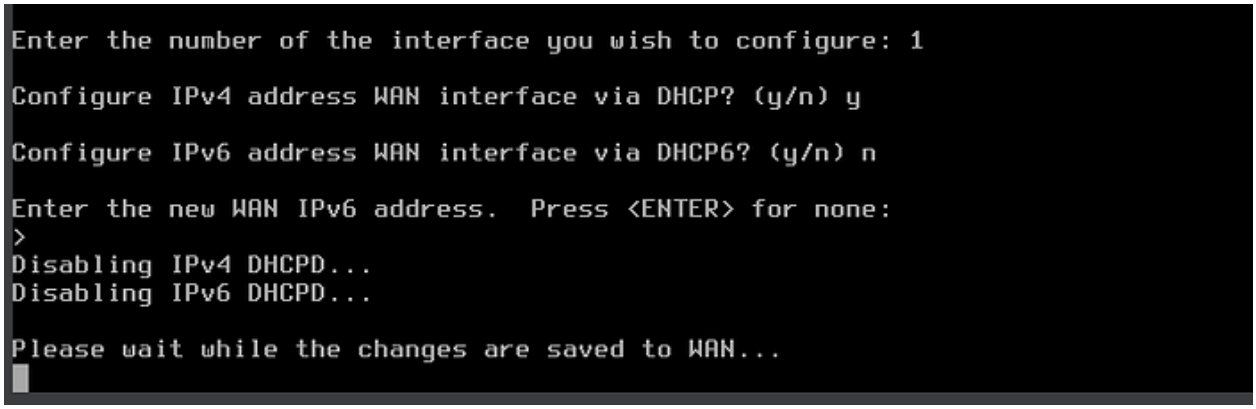


Configuring IP addresses

em0 : Adapter 1 (NAT)

Enter 2 → Enter 1 (for wan interface) → DHCP (ipv4): “y” →

DHCP(ipv6):”n” → [Enter]

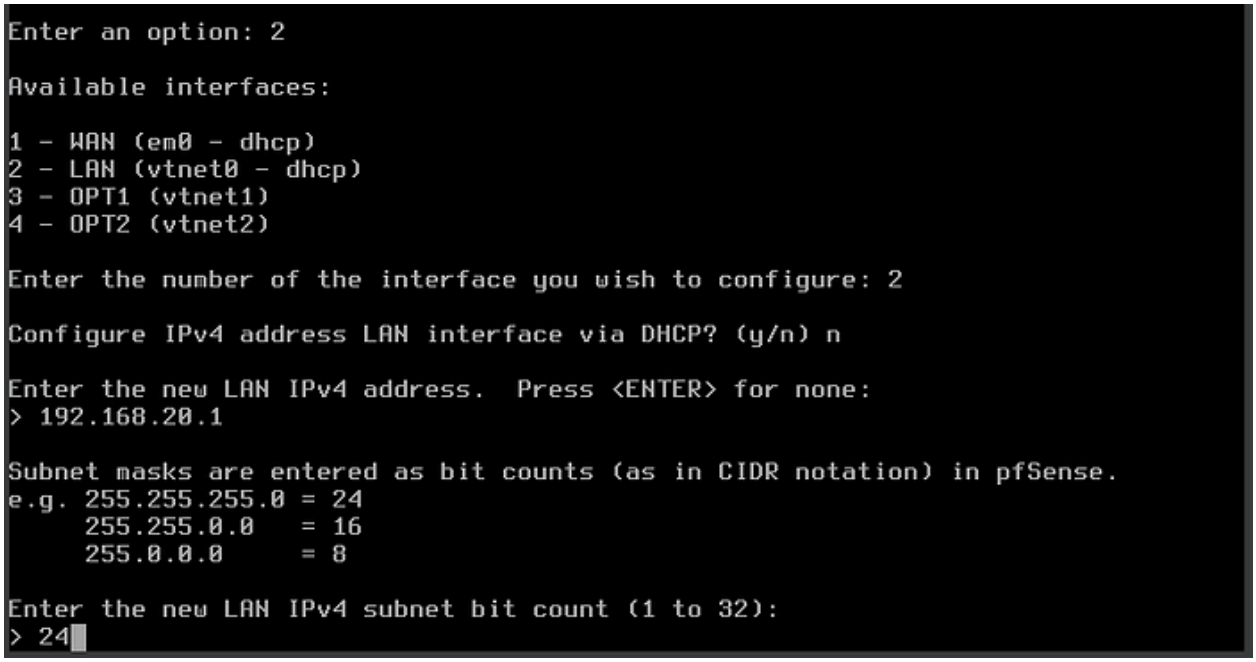


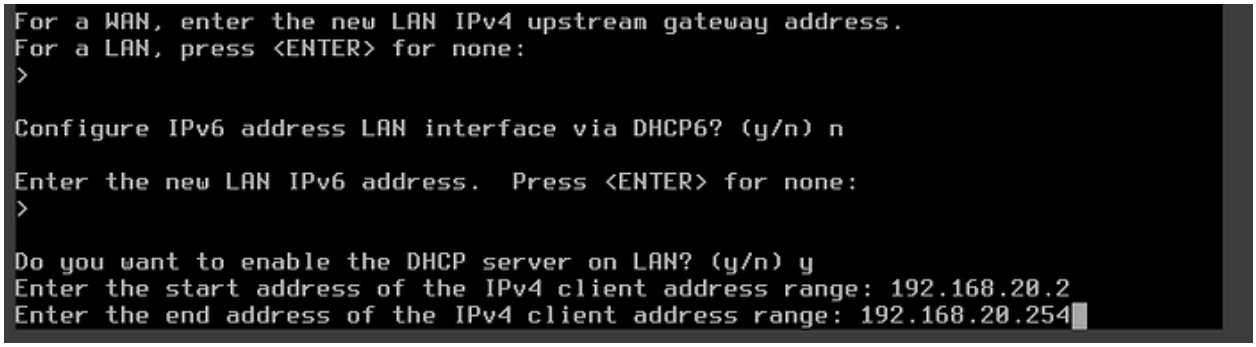
vtnet0 : Adapter 2 (Security Lan)

Enter 2 → DHCP(v4):”n” → 192.168.20.1 → Subnet Mask : 24 →

[ENTER] → DHCP(v6):”n” → [Enter] → Enable DHCP on LAN:”y” →

Start:192.168.20.2 → End:192.168.20.254.





What the above configuration does is, it sets the ip 192.168.20.1 for the vtnet0 interface and subnet 24 (255.255.255.0) which is associated with the Adapter 1 which we named it as Security-Lan in the internal network section in beginning. Then we tell that this interface will act

as dhcp through which our machines connected to this network will get the ip.

Since this is a /24 subnet it will consist of 254 usable address , one is used by the vtnet0 interface i.e 192.168.20.1 and remaining addresses will be leased by the connected machines later.

Repeat the above processes for:

vtnet1: Adapter 3(target-lan)

IPv4 addres: 192.168.10.1.

subnet:/24.

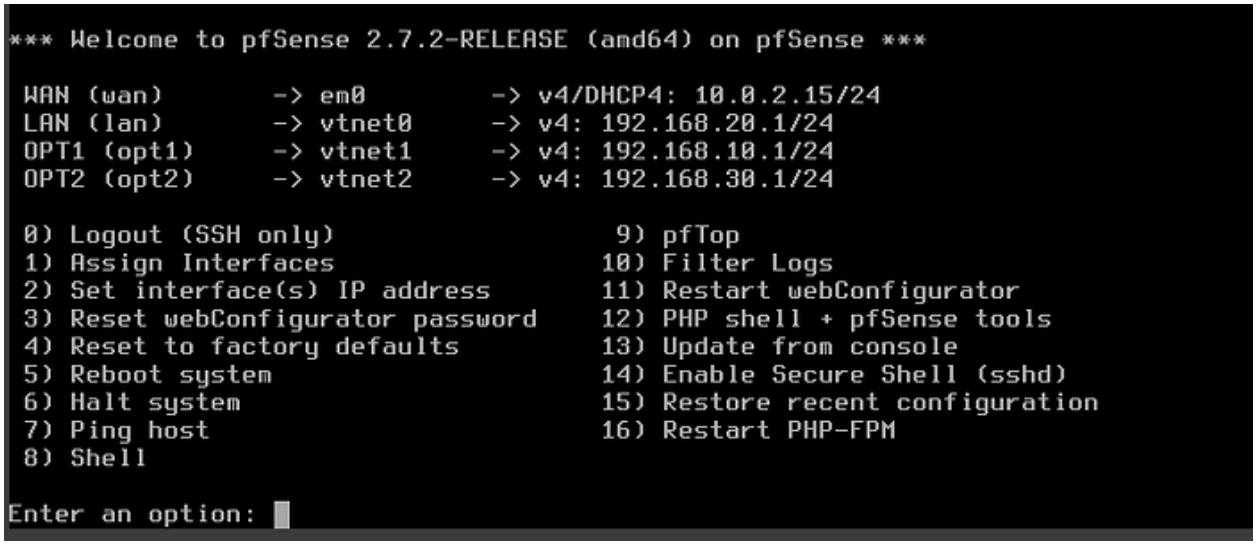
dhcp range:192.168.10.2–254.

vtnet2: Adapter 4 (attacker-lan)

IPv4 addres: 192.168.30.1

subnet:/24

dhcp range:192.168.30.2–254.

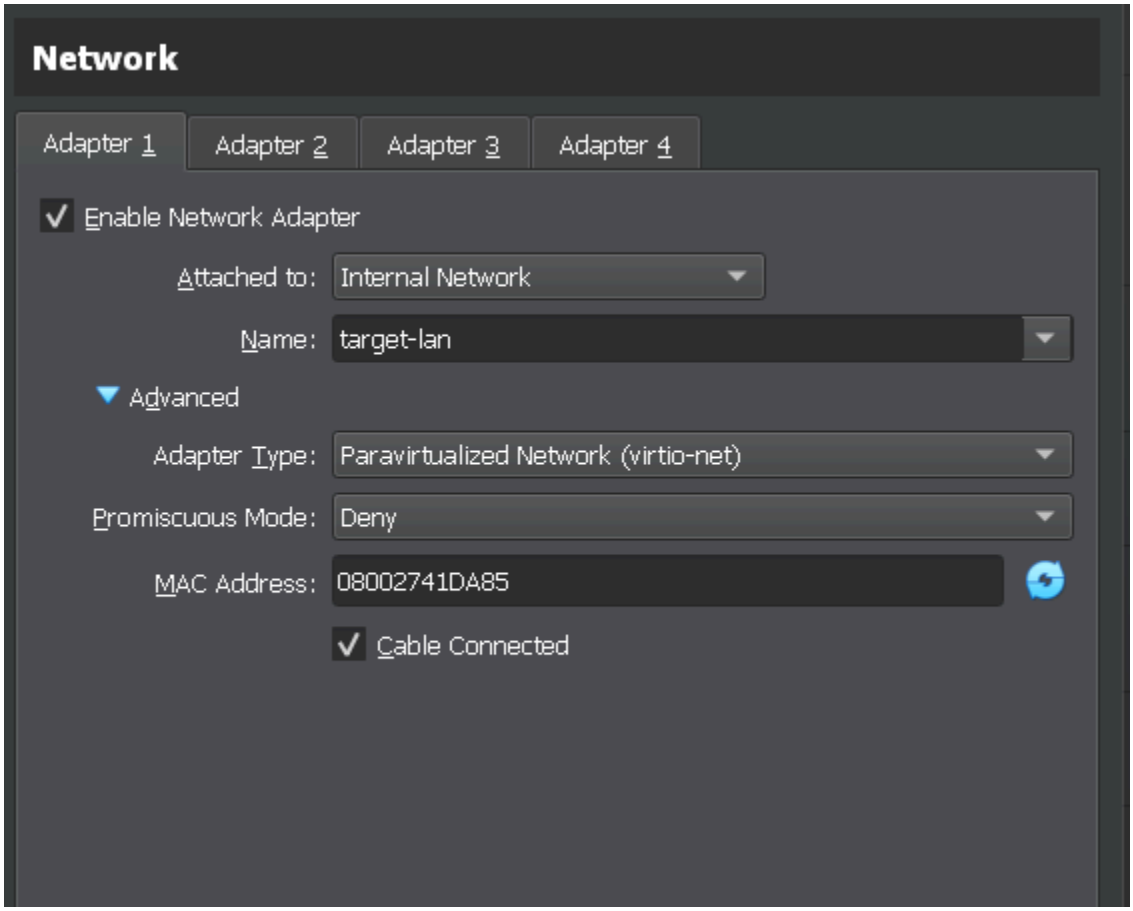


After setting up the ip addresses, the screen should display the interfaces with their ip address same as above.

Connect Machine to their respective LAN:

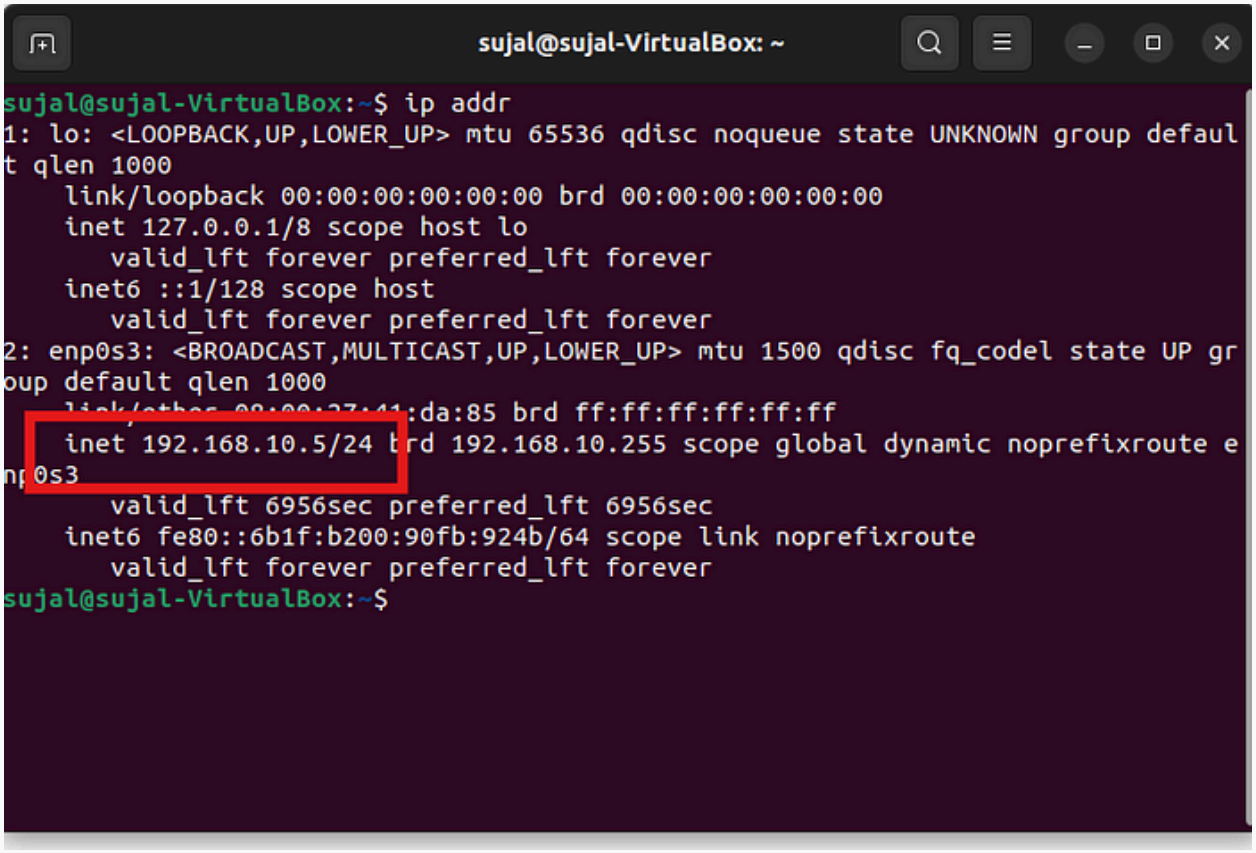
1. Connecting Ubuntu to the Target-Lan:

After installation → Go to machine settings → Set Adapter to Internal Network and target-lan → Save and restart the machine.



To verify if the machine got its ip address from the pfsense dhcp run the below command:

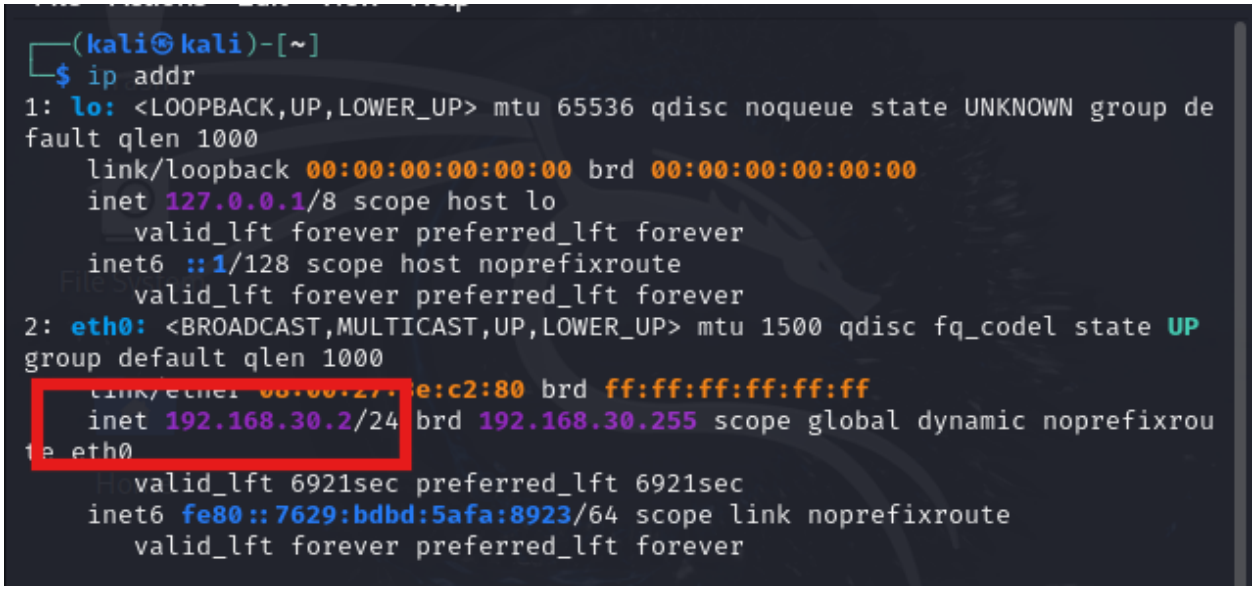
```
ip addr
```



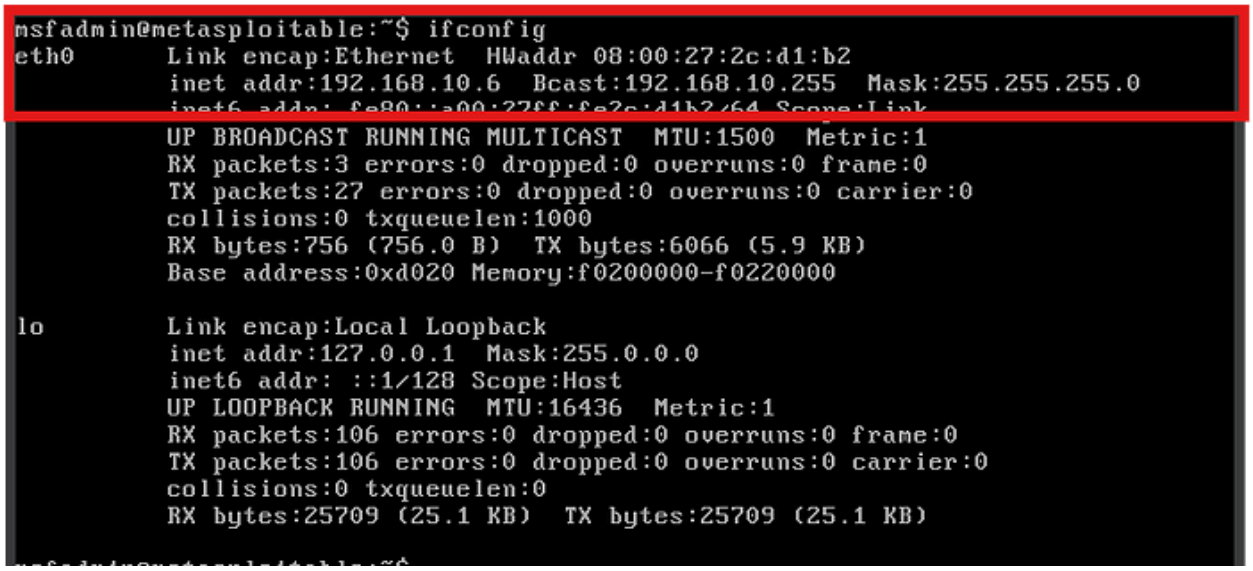
We can see that the interface got its ip as the configured network range for target-lan.

NOTE:- Incase you don’t see any ip address ,run “sudo dhclient [interface name]” from the terminal.

Similarly add the metasploitable machine to target lan and kali linux to attacker lan.



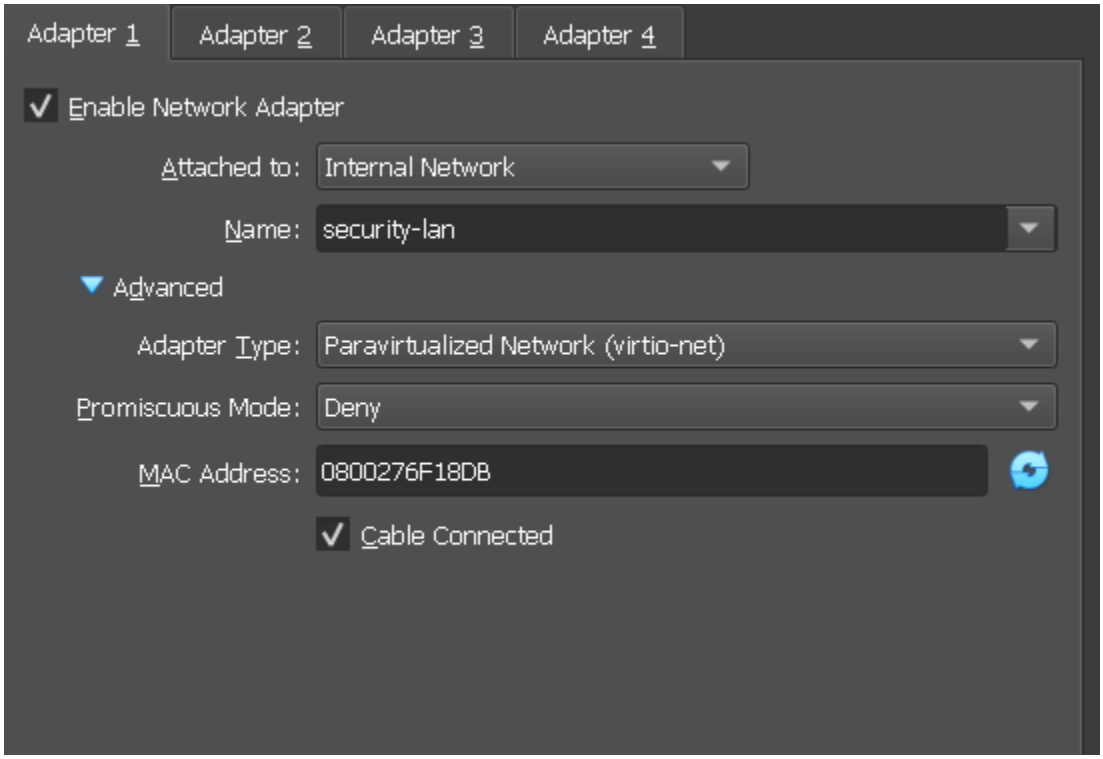
Kali Linux Ip

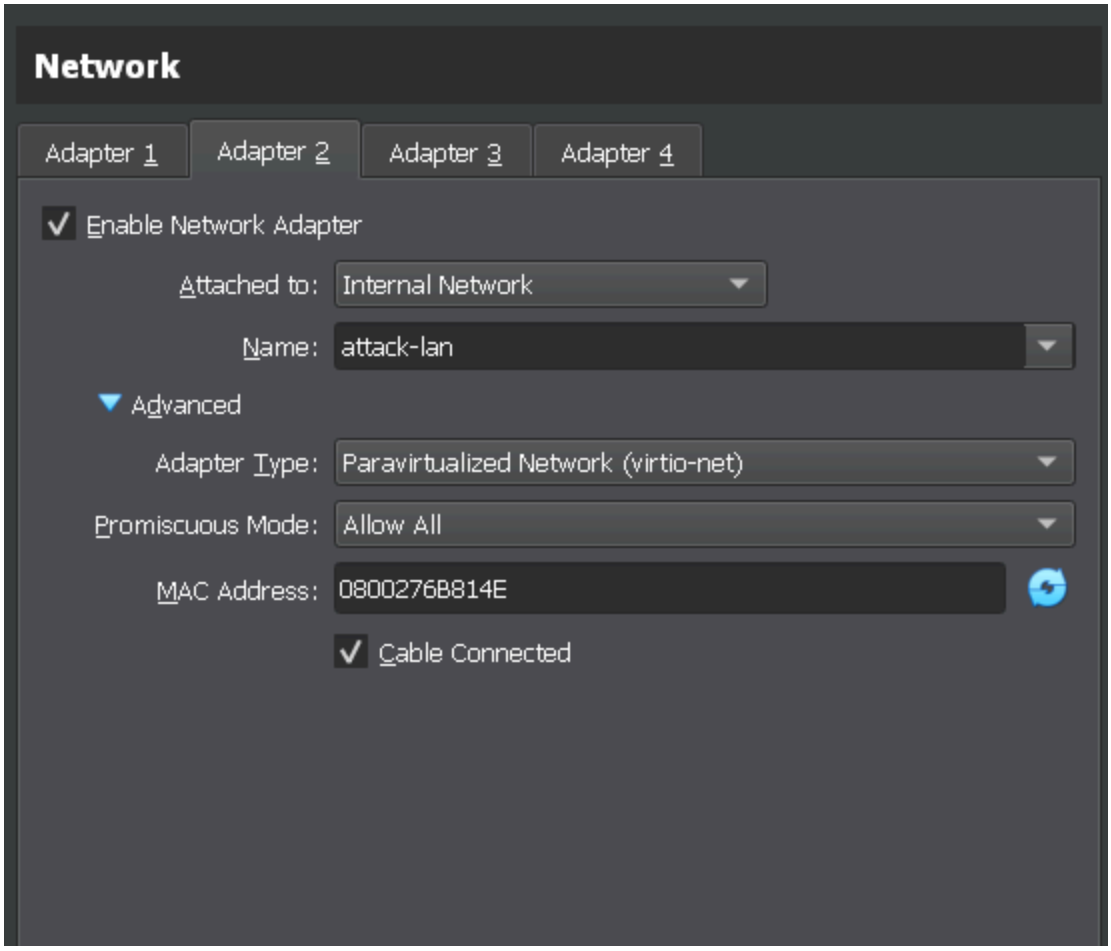


metasploitable ip

Configuring Ubuntu Server running suricata and splunk:

I have named it SOC ANALYST, set 1 adapter of the this machine to the security-lan and other in the target lan in promisc mode.

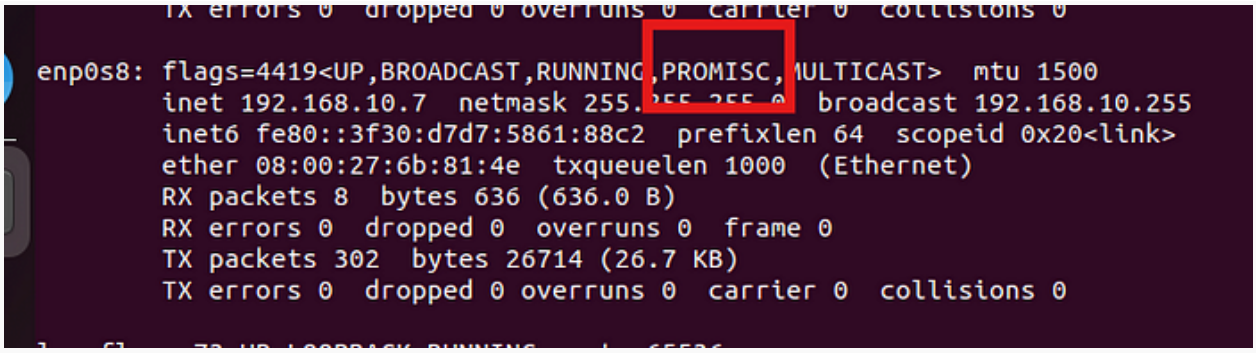





```
sujal@sujal-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.5  netmask 255.255.255.0  broadcast 192.168.20.255
        inet6 fe80::9f7d:c9f3:ff78:ec58  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6f:18:db  txqueuelen 1000  (Ethernet)
        RX packets 52  bytes 5121 (5.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 103  bytes 11717 (11.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.7  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::5750:6fd7:5861:88c2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6b:81:4e  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 384 (384.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 80  bytes 9343 (9.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 188  bytes 16003 (16.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 188  bytes 16003 (16.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sujal@sujal-VirtualBox:~$
```

We need to keep the interface enp0s8 which has the ip 192.168.10.7 in promisc mode, run the below command :

```
sudo ip link set enp0s8 promisc on
```



Phew ! We are done with connecting the machines to the local network.

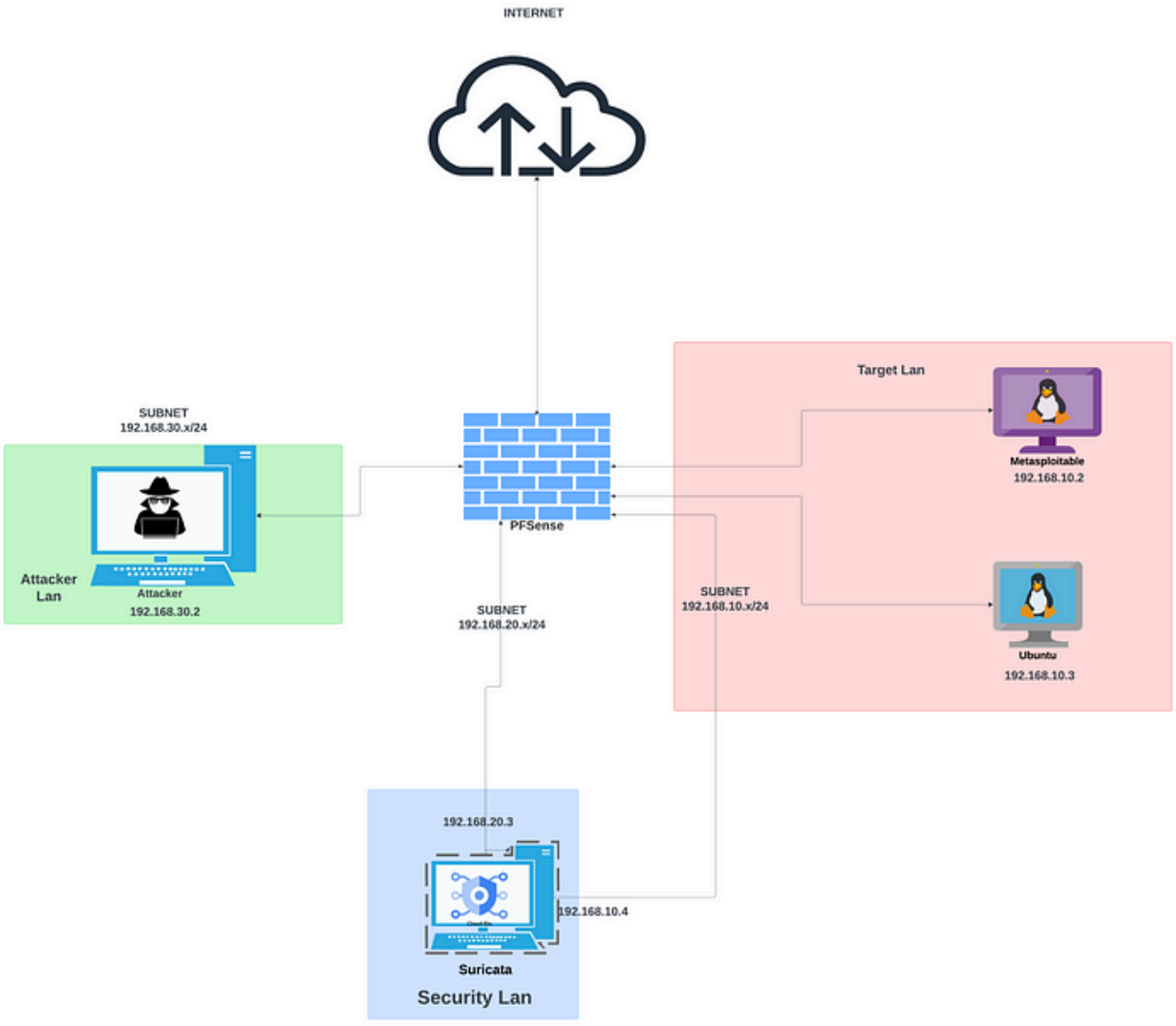
Summary:

1. Ubuntu → Lan: Target , Ip:192.168.10.5 .
2. Metasploitable → Lan:Target , Ip:192.168.10.6
3. Kali Linux → Lan:Attacker , Ip:192.168.30.2
4. SOC Analyst→ Lan:Security , Ip:192.168.20.5

5. Pfsense Wan → Lan:NAT , Ip:10.0.2.15/24
6. PFsense vtnet1 → Lan:Security , Ip:192.168.20.1
7. Pfsense vtnet2 → Lan:Target , Ip:192.168.10.1
8. Pfsense vtnet3 → Lan:Attacker, Ip:192.168.30.1

Next we have to give some of the machines the internet access by configuring firewall rules on pfsense and spin up suricata on the ubuntu machine in the security lan

I will setup the necessary firewall rules to give the internet access to certain machines and spin up suricata on SOC Analyst machine to work as an IDS.

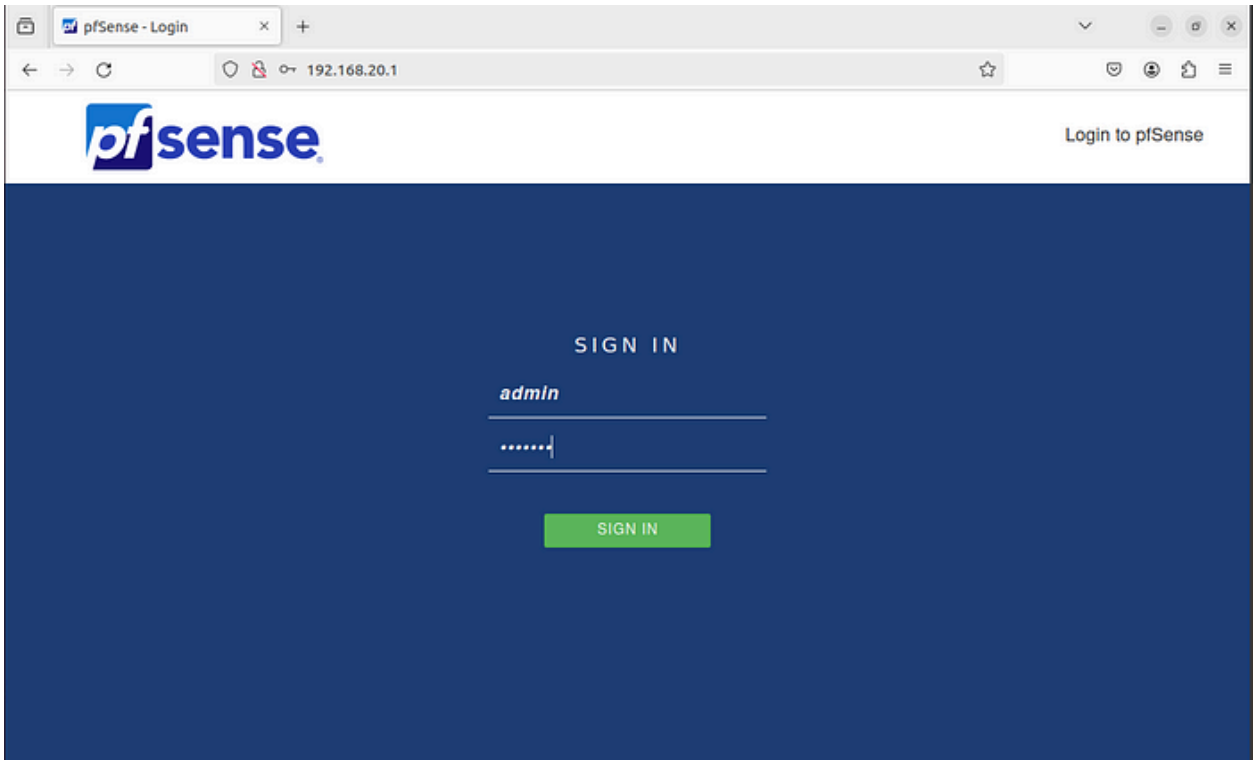


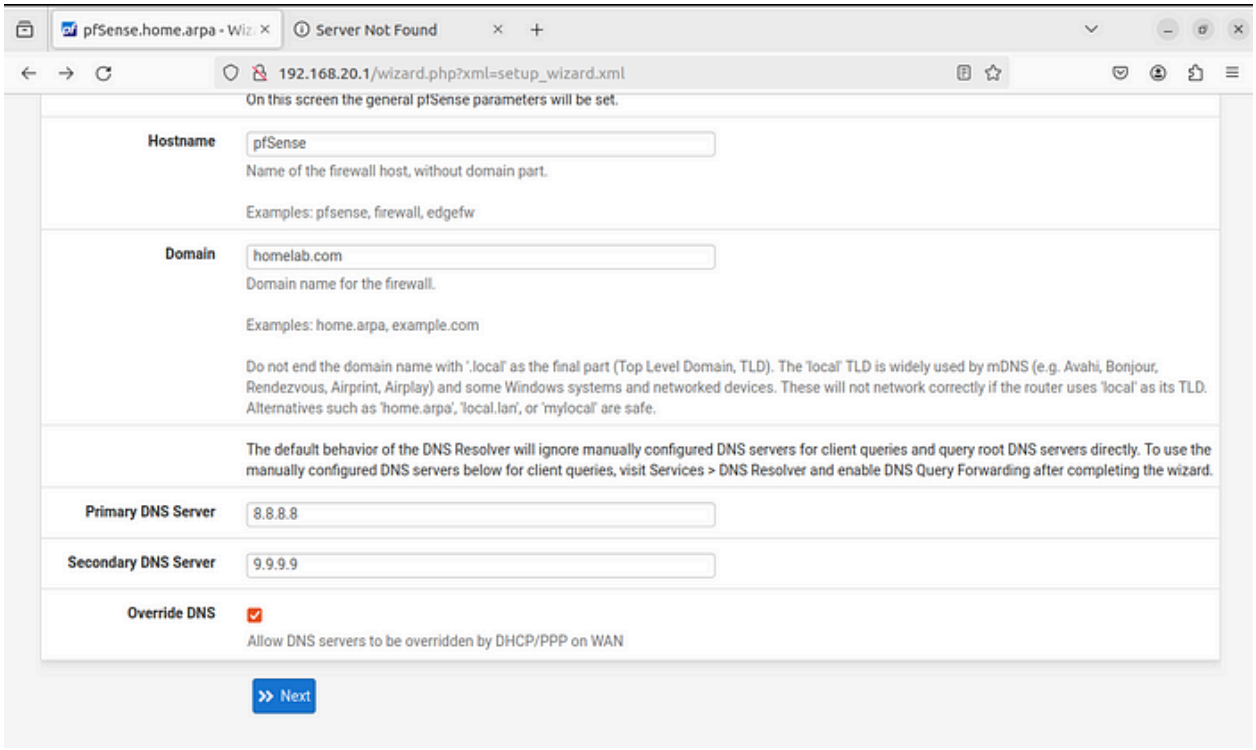
Accessing Pfsense Web GUI

First we need to access the web interface of the pfsense which is by default accessible only by the devices connected to the LAN network, devices connected to WAN / OPT1 / OPT2 are not allowed. That's the

reason, the ubuntu machine in the security lan is connected to LAN network of the pfsense.

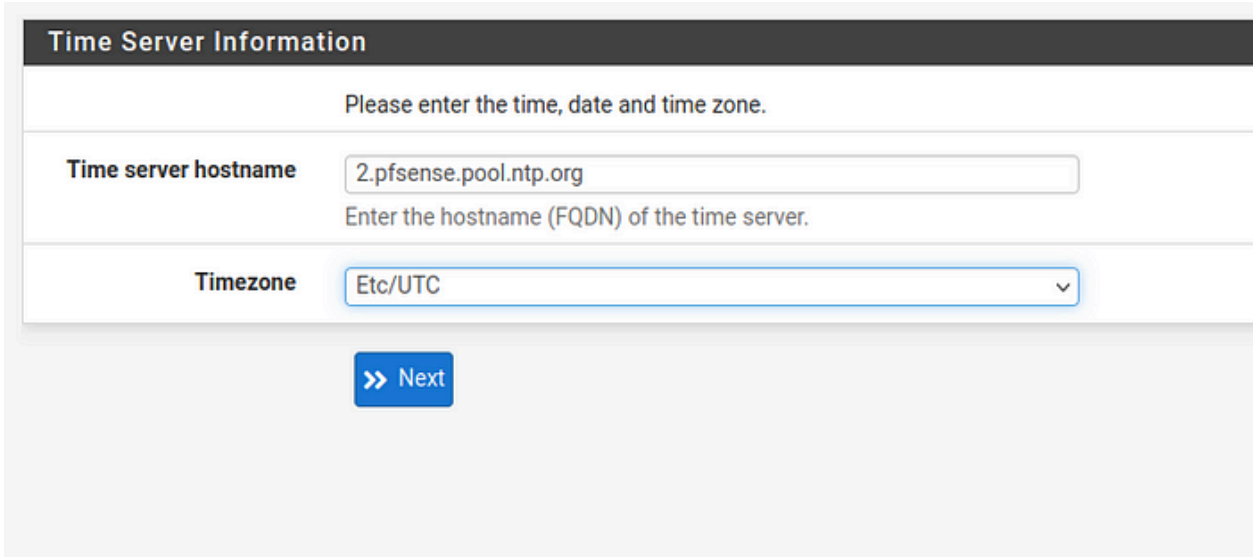
To access the web gui : Open Browser → Enter pfsense ip of the security lan interface (192.168.20.1) → Username:-admin & Password:- pfsense.



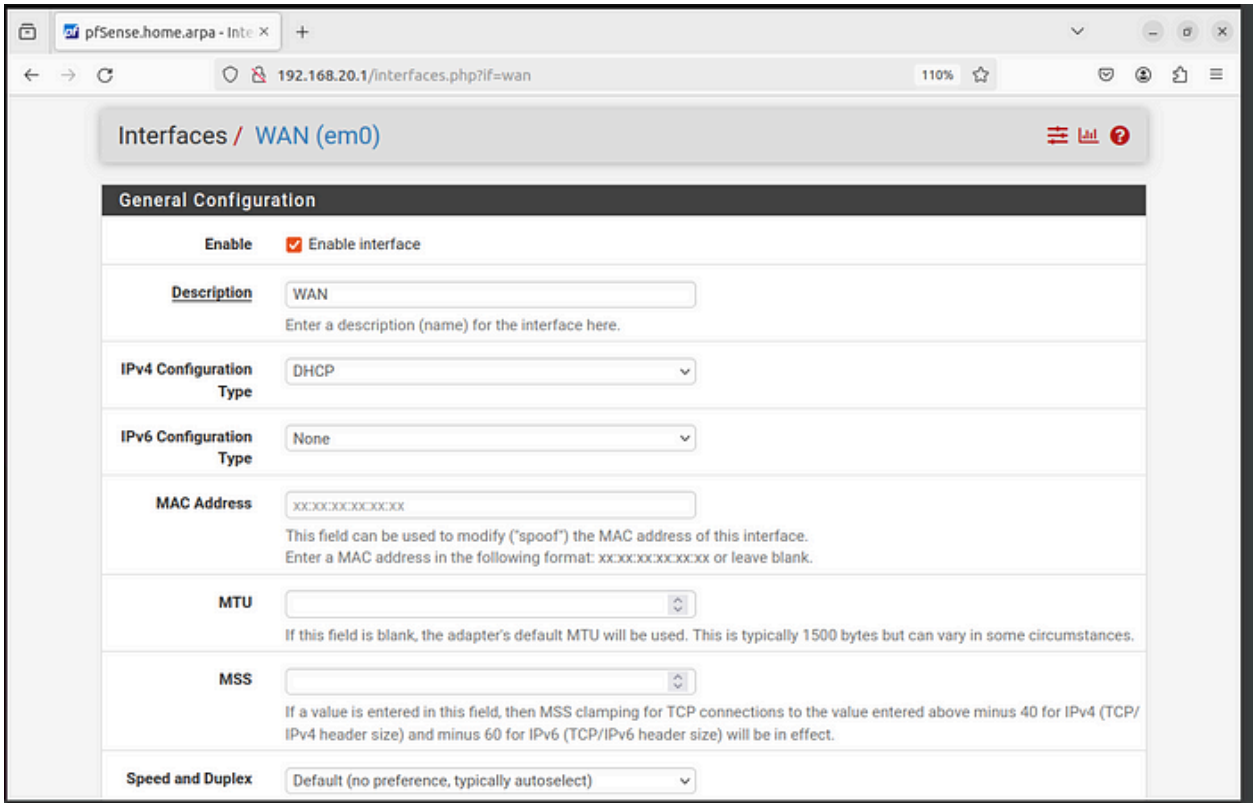


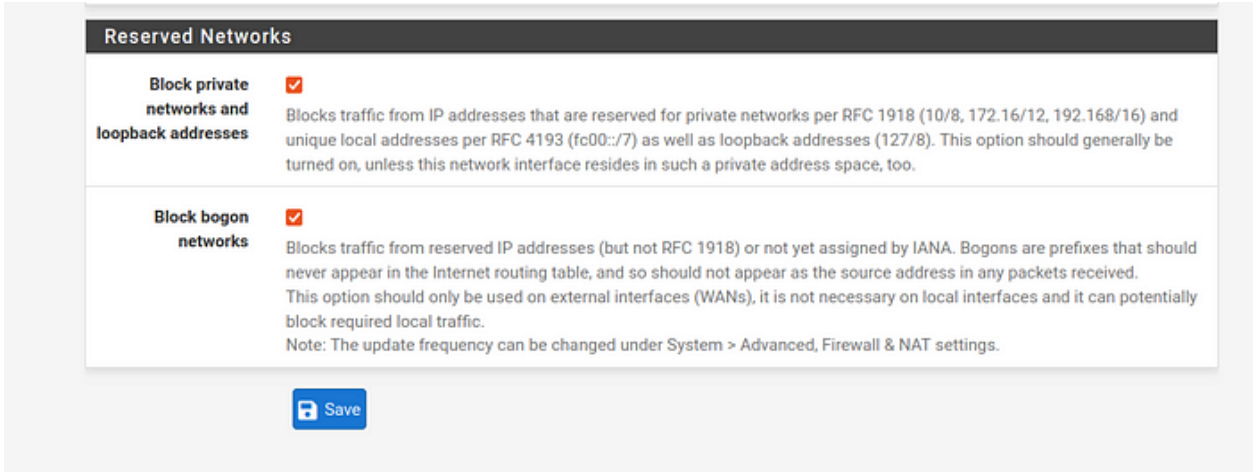
I have set the hostname as default and domain to homelab.com,

primary dns : — 8.8.8.8 and secondary:9.9.9.9



Set the time server to default



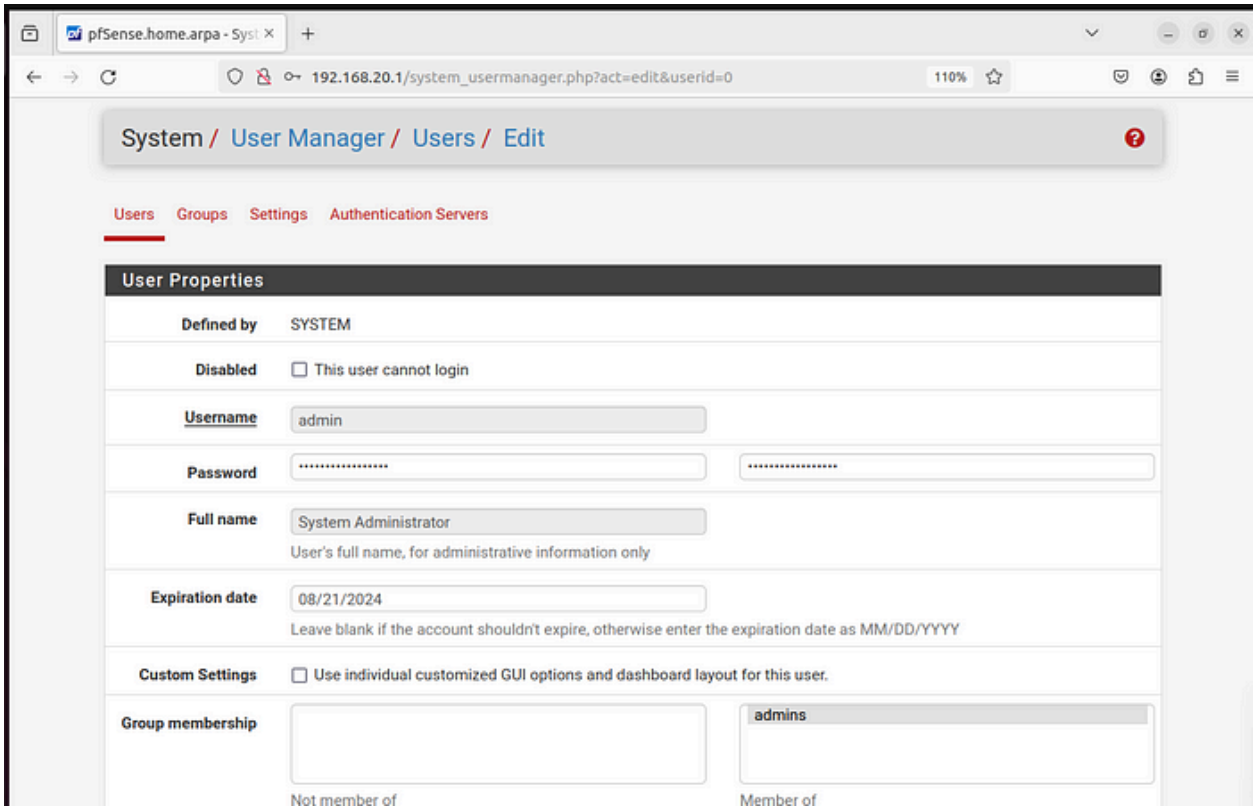


Only set the above sections for the wan interface.

The two options above block private networks:- This will block any incoming packets from the RFC 1918 reserved addresses (private addresses) towards wan interface,because packets to and from the internet with source address set to private ip address is something which should not be allowed since we are using nat.

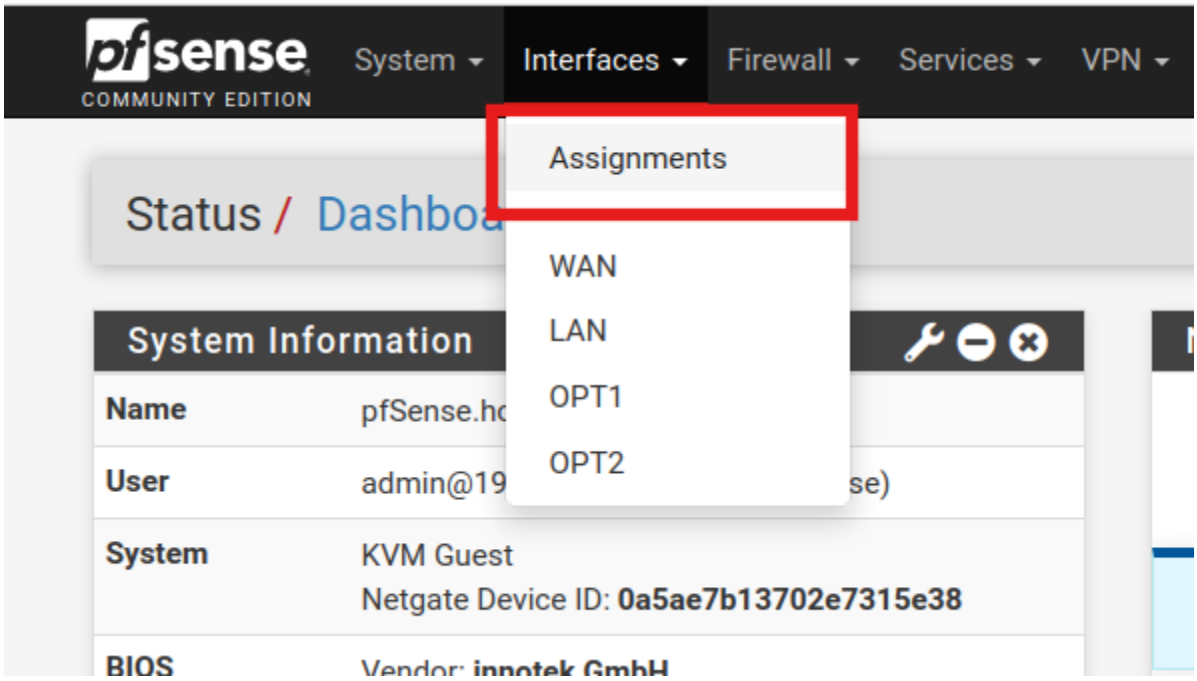
Change admin credentials:

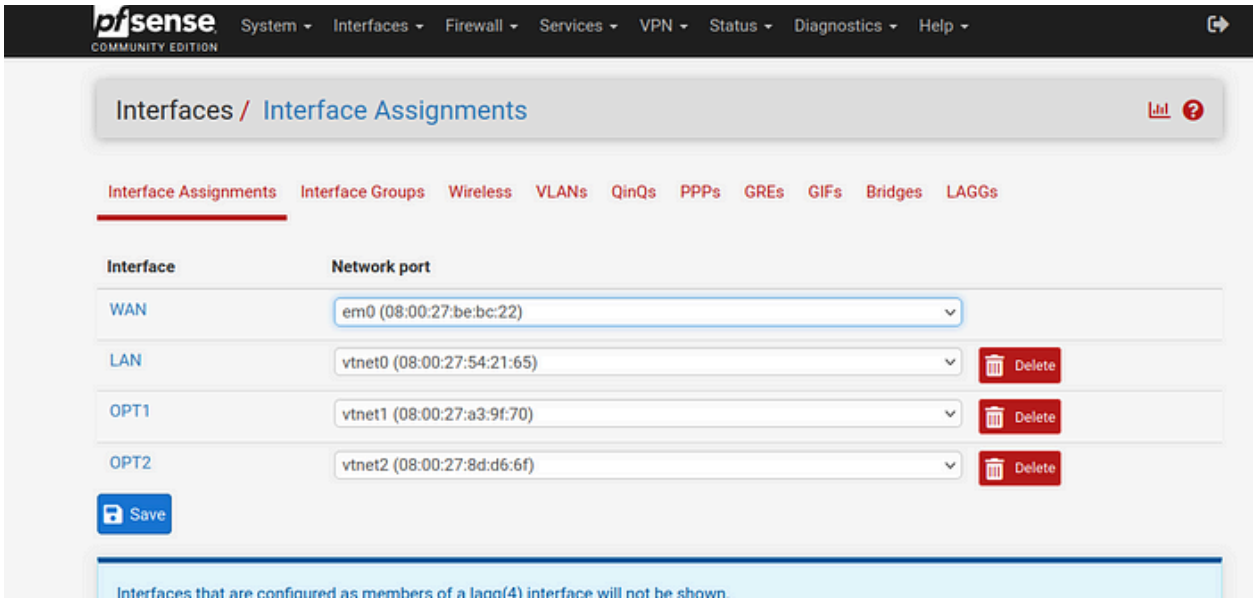
Click on the change admin password poping up at the top of the screen.



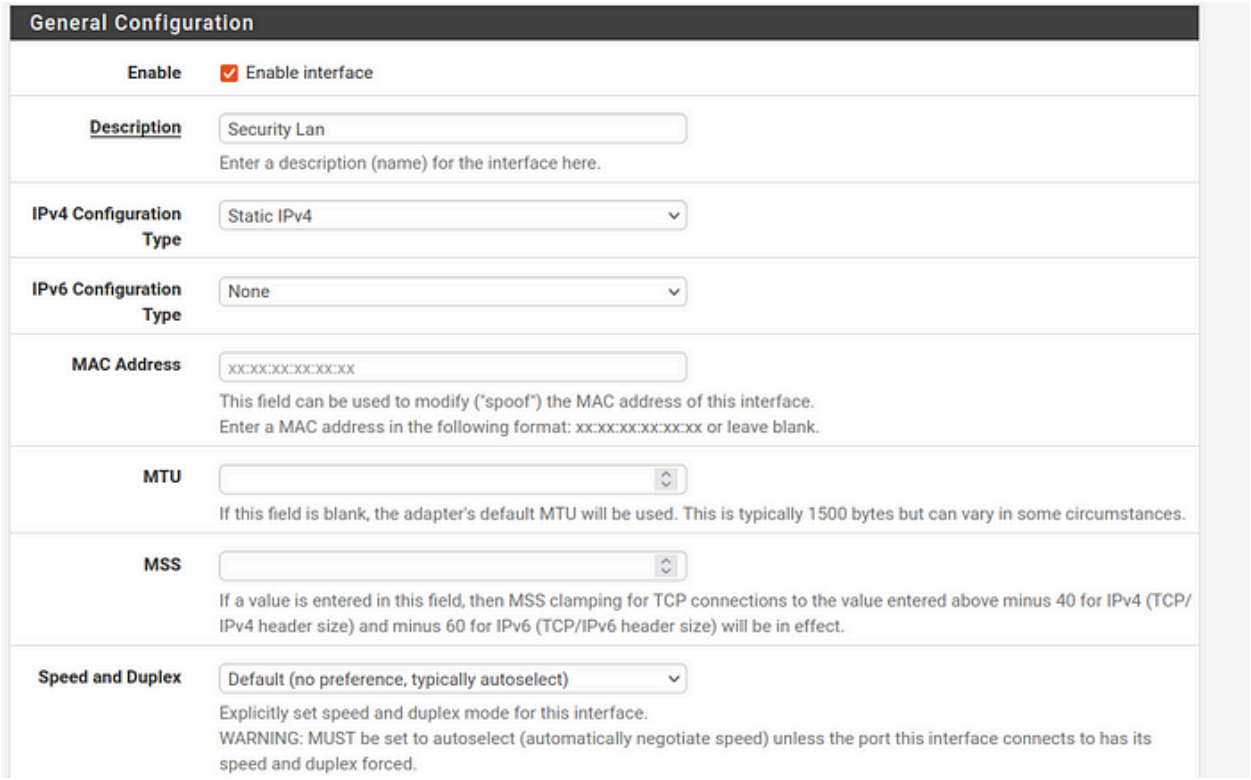
To get the details of the pfsense server go to the dashboard after saving changes. The dashboard shows the status of the pfsense firewall such as cpu type, memory usage, last configuration etc.

Assign Interface Names:-

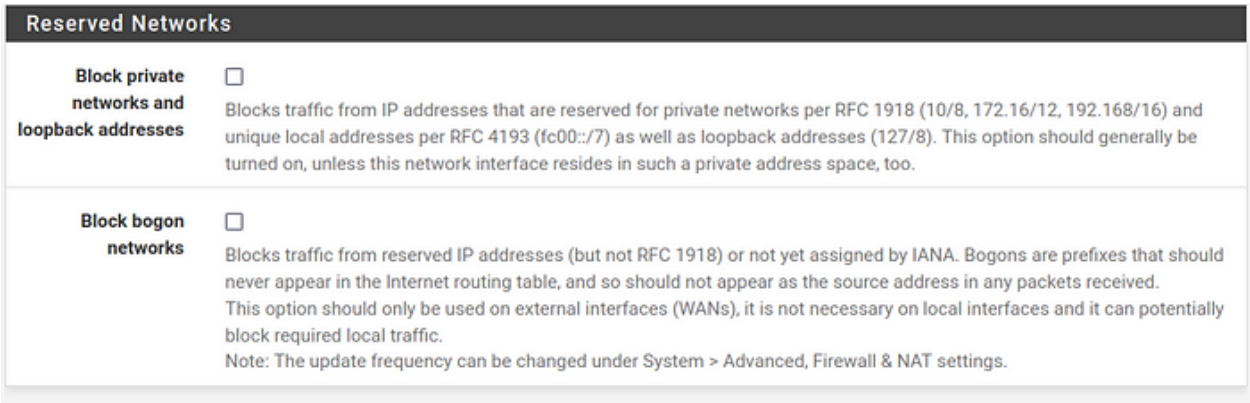




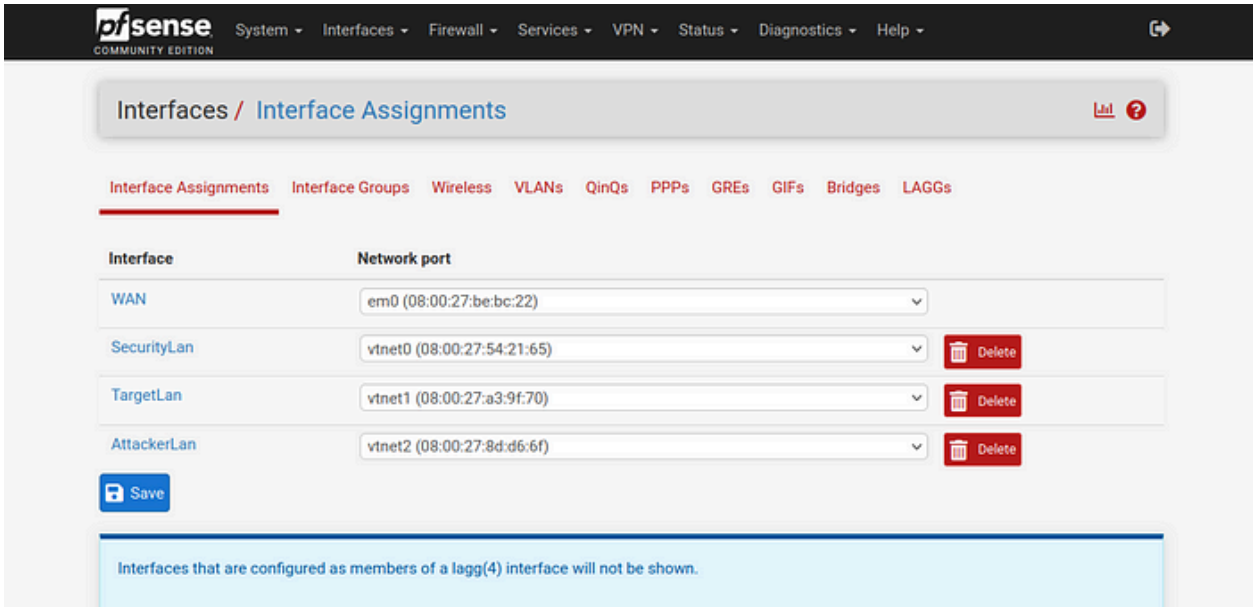
Lets change the name of the LAN interface



I have only changed the name of the Interface to security lan for ease, every other configuration such as ipv4 address, dhcp has been configured at the beginning of setting up pfsense, change the name of other interfaces to their respective LAN name. Uncheck the last two options

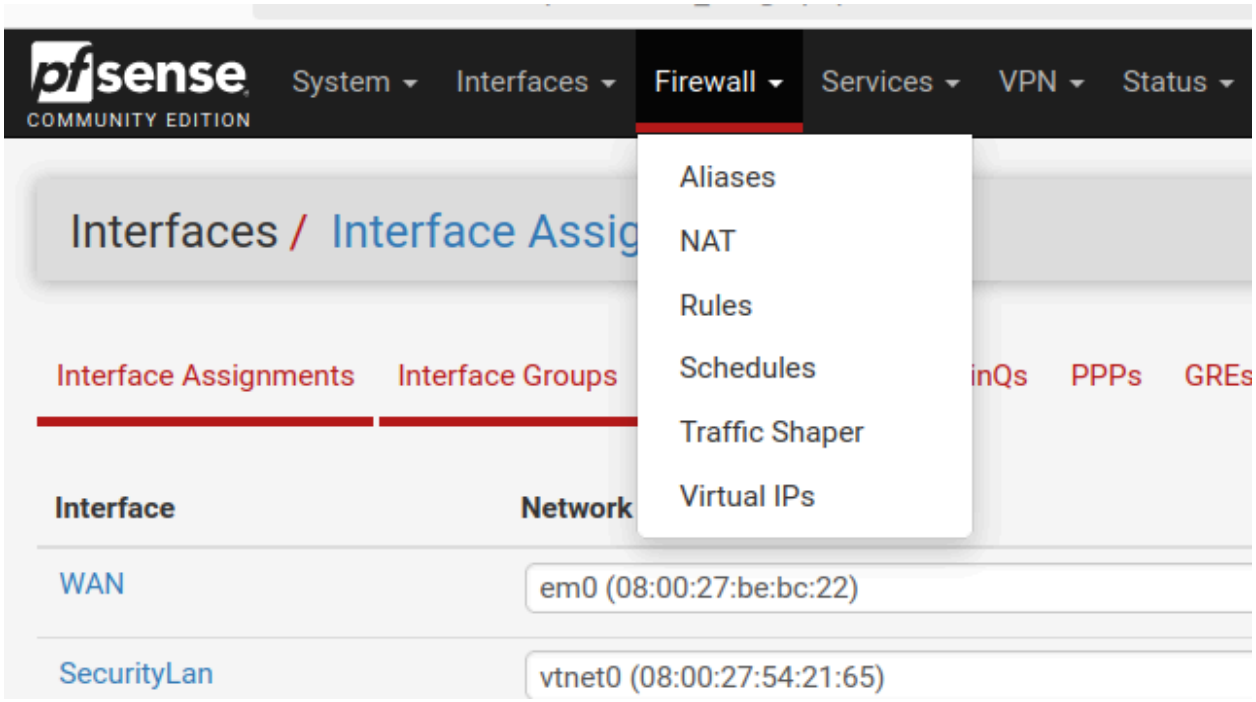


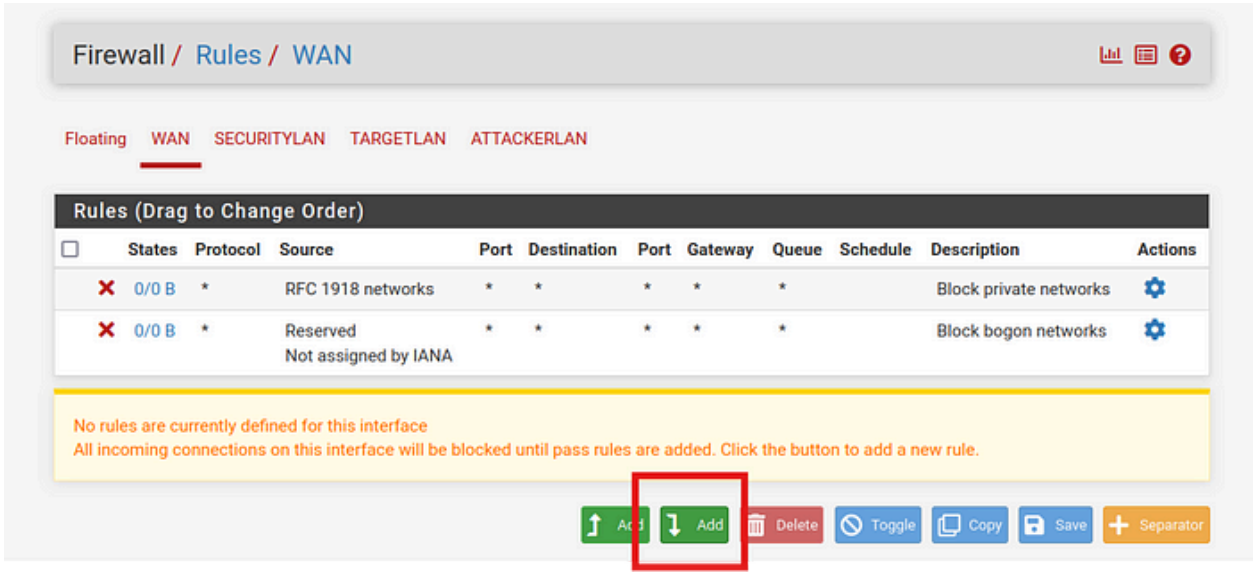
This is a LAN interface so traffic from private ip addresses towards this interfaces should be allowed. Once done click Save and then click Apply changes.



Adding firewall rules through GUI

Click Firewall → Rules → Interface → Add

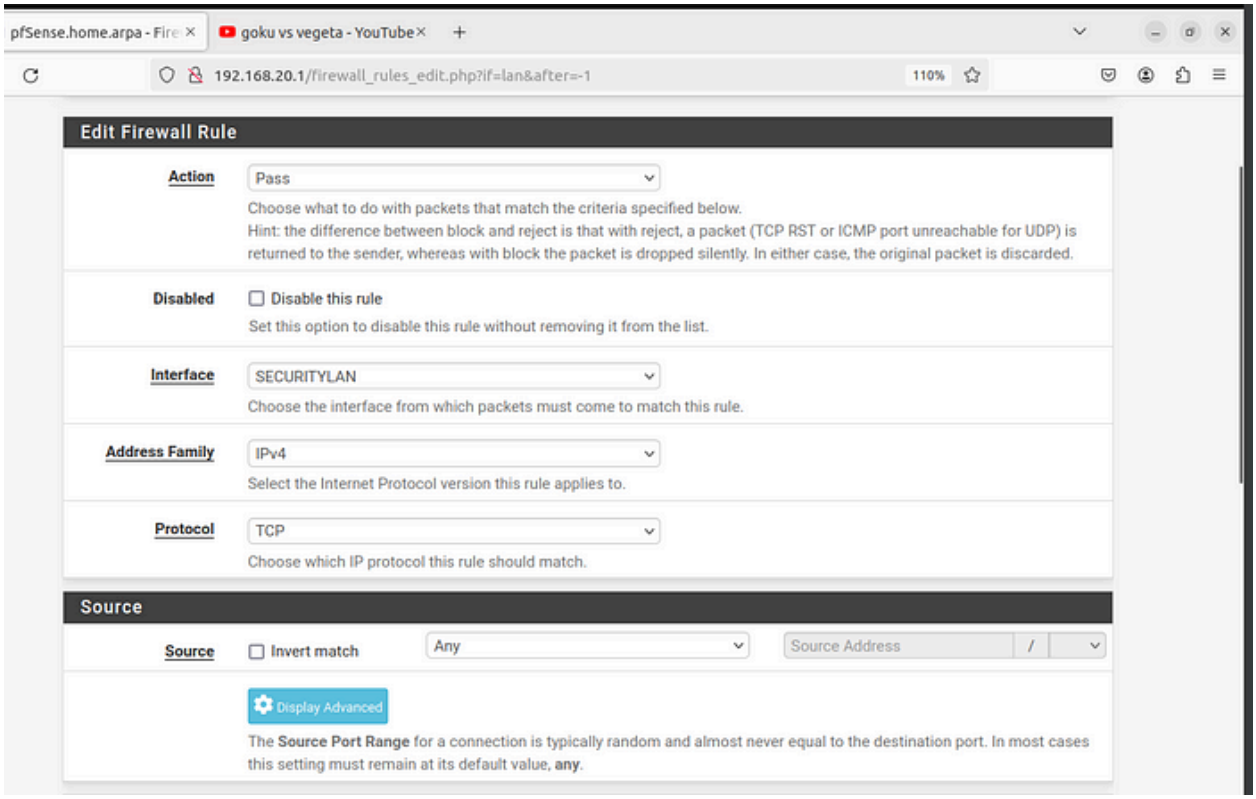


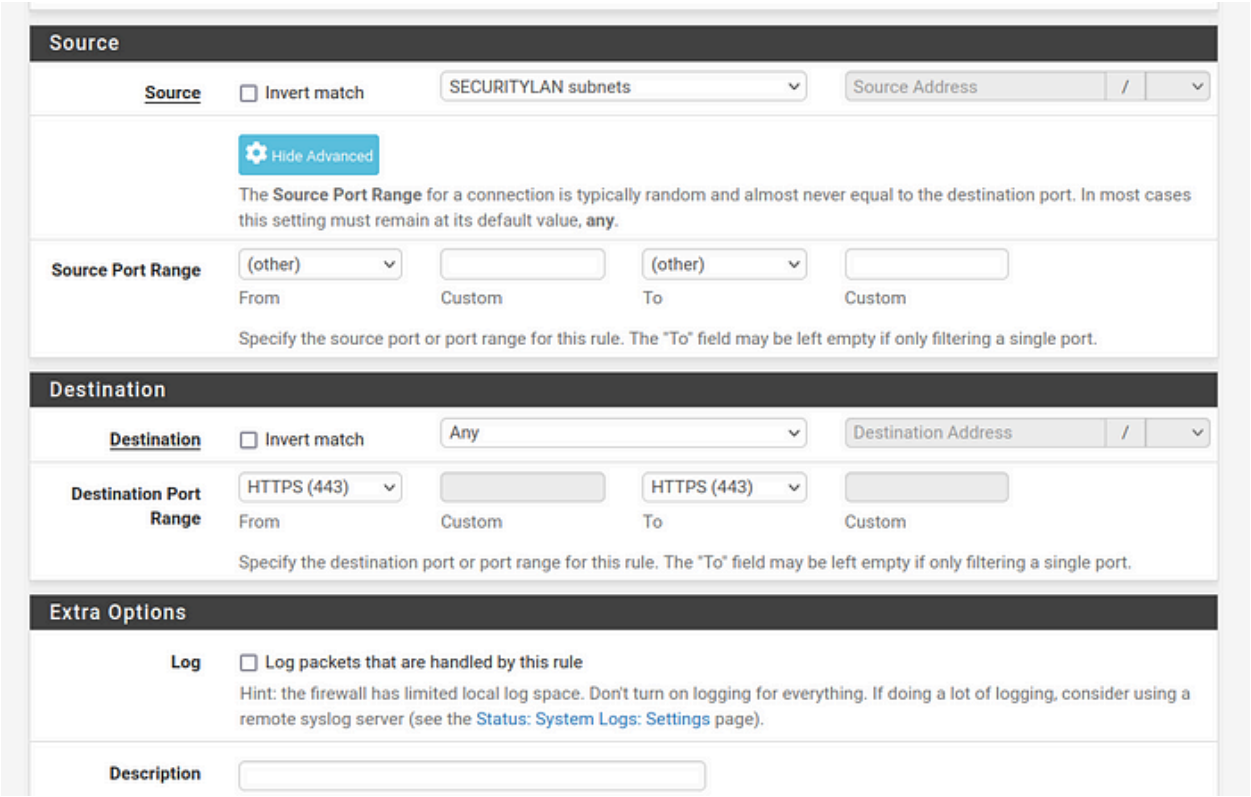


Before adding rules let us first understand the default rules of the pfsense firewall:

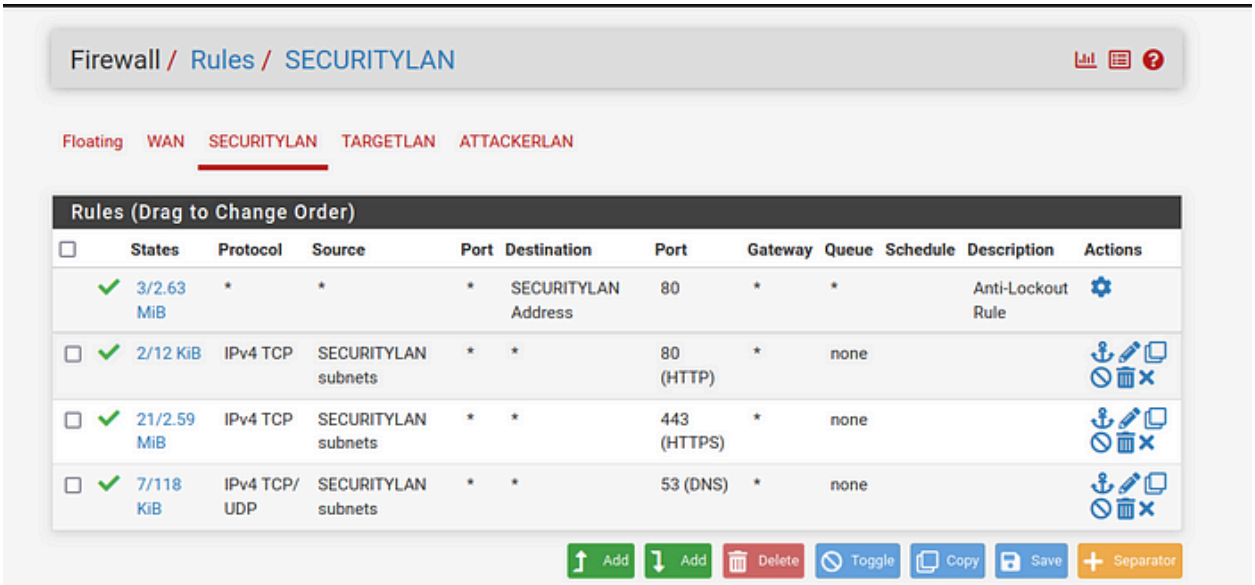
1. Any requests made from outside the LAN to our internal network is blocked, this is ingress filtering. Pfsense will block all the incoming requests towards our network by default.
2. Any requests made from our internal network that is the requests made from our LAN network (renamed to security lan) to the internet will be allowed and the corresponding responses into the lan will be allowed as well, because pfsense run as a stateful firewall which keeps track of the states of network connections made from our network, this is egress filtering i.e filtering outgoing packets.
3. Any other requests to/from our OPT1 and OPT2 LAN are blocked by default until any explicit rule is configured to allow the outgoing traffic from these LAN's.
4. Learn more about pfsense filtering through here.

I will add a rule to allow connections made from our security-lan to destination port listening on port 443.





The description below at each setting, is enough to understand what each setting would help us to achieve.



Lets understand the above rules in short:

Rule 1: This rule is by default and it allows us to access the web interface of the pfsense.

Rule 2: This rule will allow http request from our security-lan from any port to any destination listening on port 80.

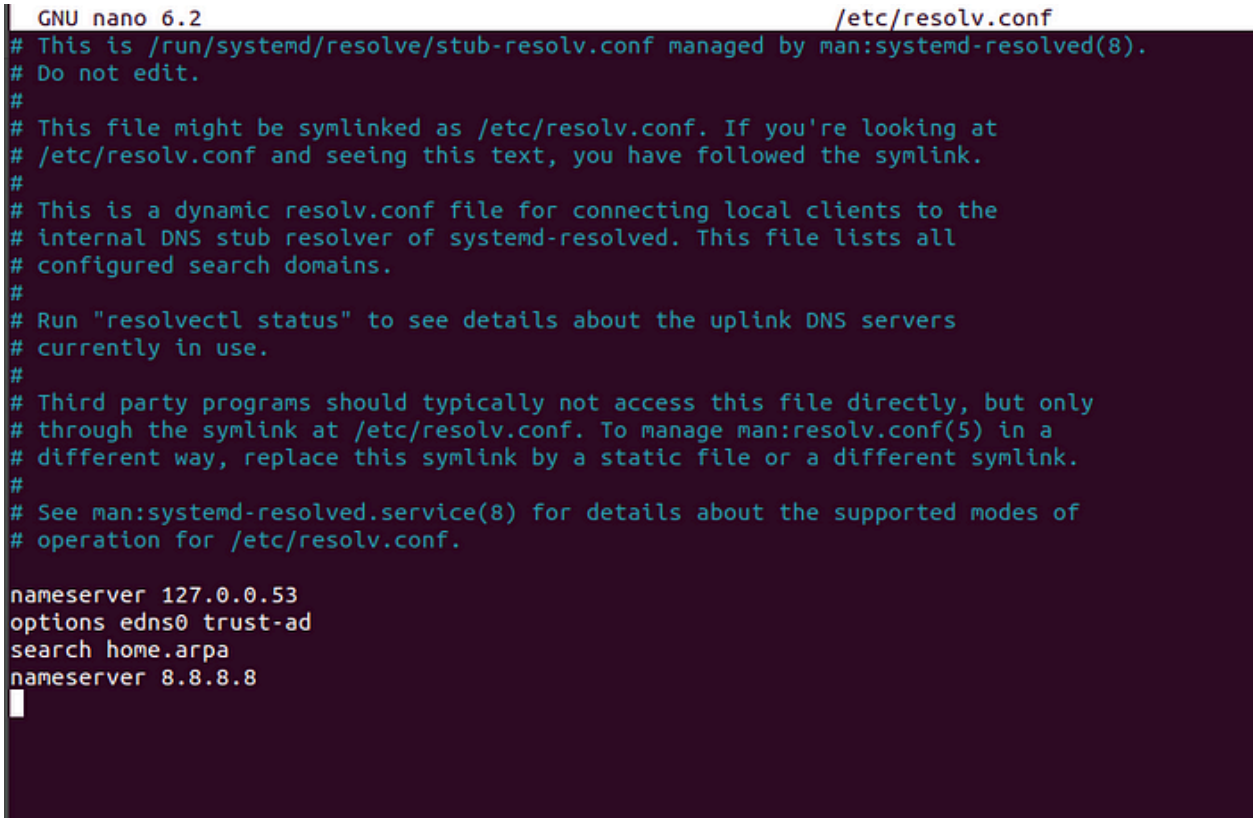
Rule 3:This rule will allow https connections initiated from our security lan to any destination listening on port 443.

Rule 4:This rule will allow any dns queries made from our security lan to any destination listening on port53 for dns queries.

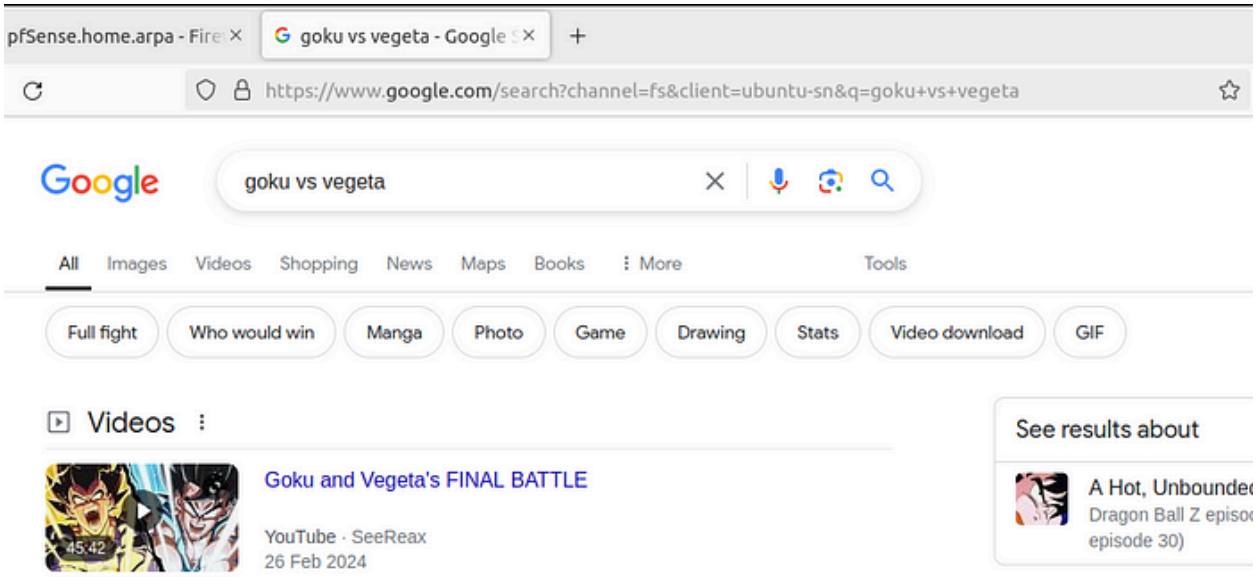
We need to set the name servers in etc/resolv.conf in the machines who needs to surf the internet through browser, open the /etc/resolv.conf file.

```
sudo nano /etc/resolv.conf
```

and then add the nameserver 8.8.8.8 at the bottom of the file, then save your file.



Now let us try to reach the internet through our browser from our ubuntu machine.



That’s great ! It gave us the results.

Lets determine the traffic flows

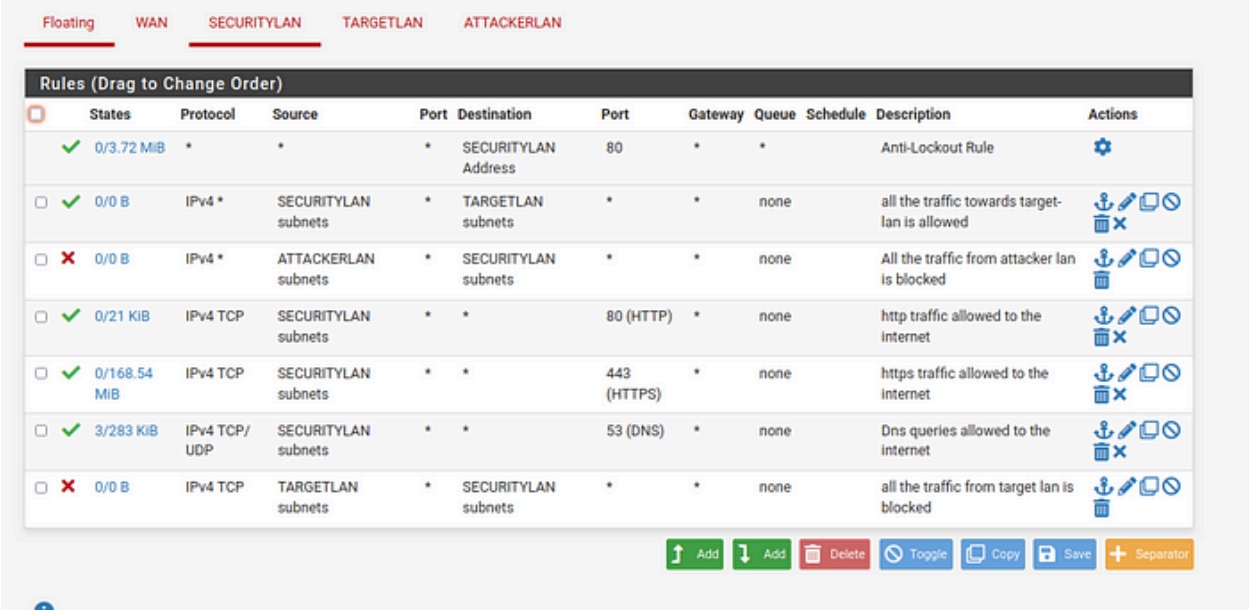
Traffic rules for Inter-Lan communication:

1. Security Lan:- Internet access for outgoing allowed, traffic from attacker-lan is blocked and traffic from target lan *(*except for certain traffic such splunk forwarders to send data to any siem tool for data ingestion if configured in future *)* to security-lan is blocked.

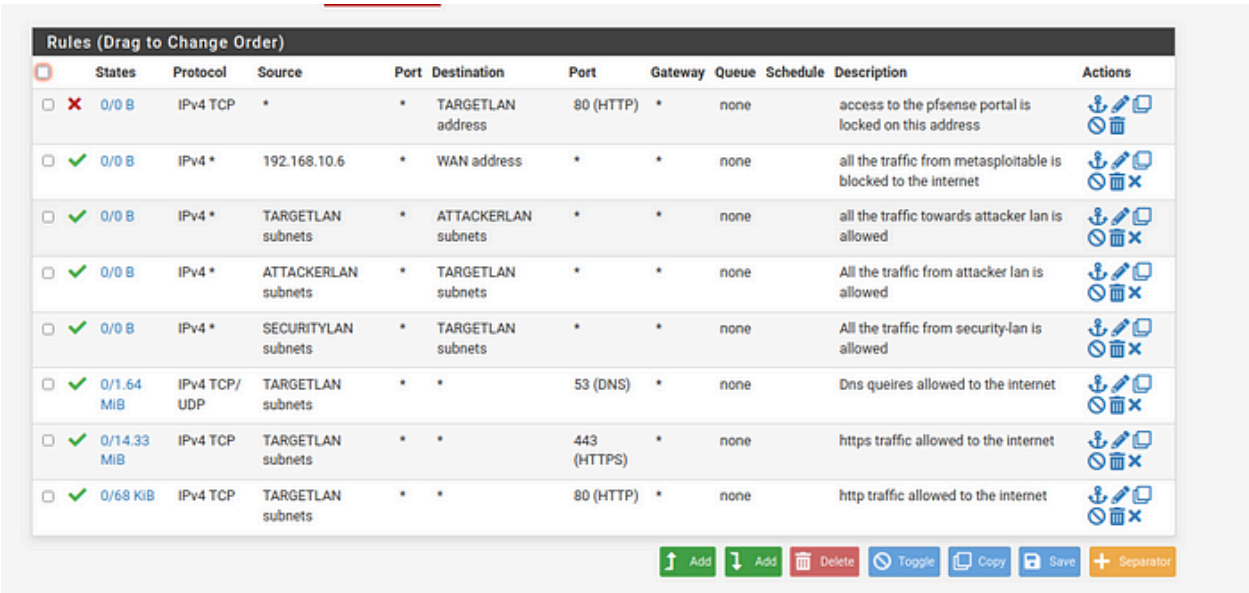
2. Target Lan: Traffic from security-lan and attacker lan allowed to the target lan, traffic from target-lan to attacker lan should be allowed, traffic from target-lan to the internet is allowed.
3. Attacker-Lan: Traffic to internet is allowed (this is necessary to install tools and stuff).
4. WAN:- All the incoming traffic from the internet should be blocked by default, if certain traffic is necessary will be allowed based on requirements.

I hope you can configure the above rules, I have put up the screenshots for every firewall rule configured on each interface with their description:

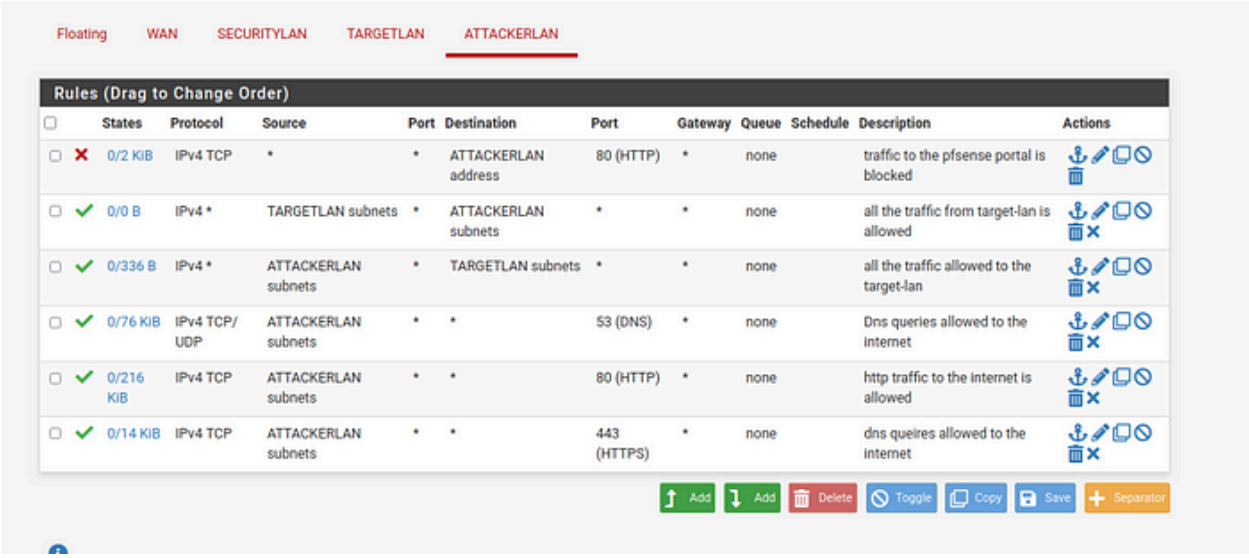
Security-Lan:



Target-Lan



Attacker-lan:



Do test the firewall rules, I have tested the rules and all worked according to the way I expected, if there are any mistakes or you face any issues you can reach me out at my linkedIn.

Setting up suricata:

Open up your SOC Analyst Machine and run:

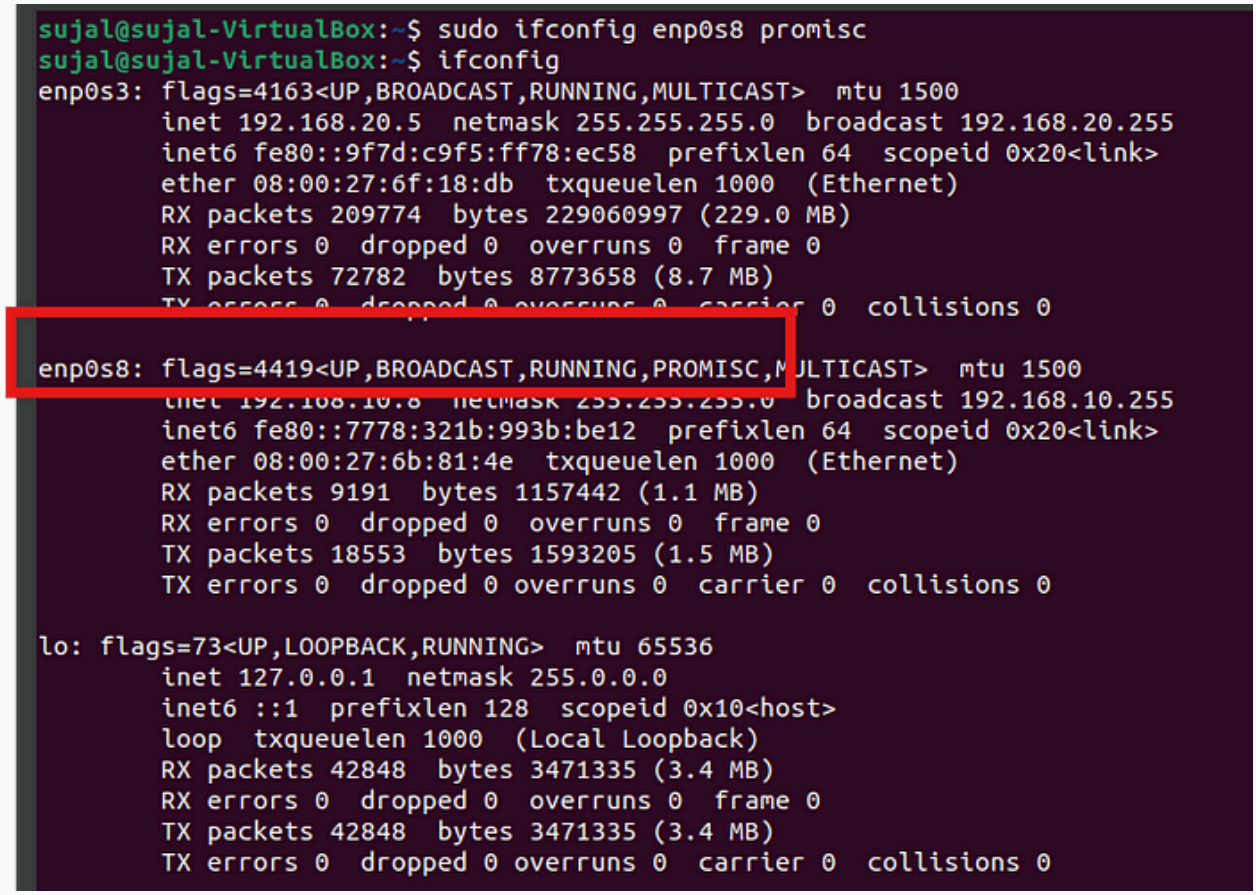
```
sudo apt-get update && sudo apt-get install suricata
```

Once suricata is installed first we need to check few things:

1. The other interface in the target lan which we are going to monitor is in promiscous mode.
2. No communication takes place on that interface.

To put the interface into promisc mode run :

```
sudo ifconfig [interface] promisc
```



To stop communication on promiscous interface:

we will flush the ip it got from dhcp and block all the communications using iptables rule, run:

```
sudo ip addr flush dev [interface]

sudo iptables -A INPUT -i [interface] -j DROP

sudo iptables -A OUTPUT -o [interface] -j DROP

sudo iptables-save
```

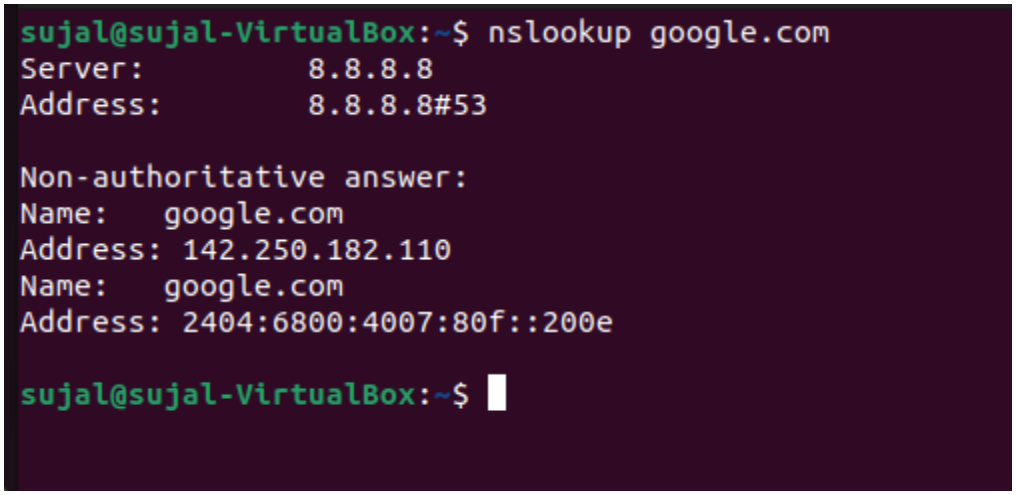
```
sujal@sujal-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
sujal@sujal-VirtualBox:~$
```

```
enp0s8: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet6 fe80::7a15:5287:c1ca:8357  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6b:81:4e  txqueuelen 1000  (Ethernet)
        RX packets 9207  bytes 1160783 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18566  bytes 1595330 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

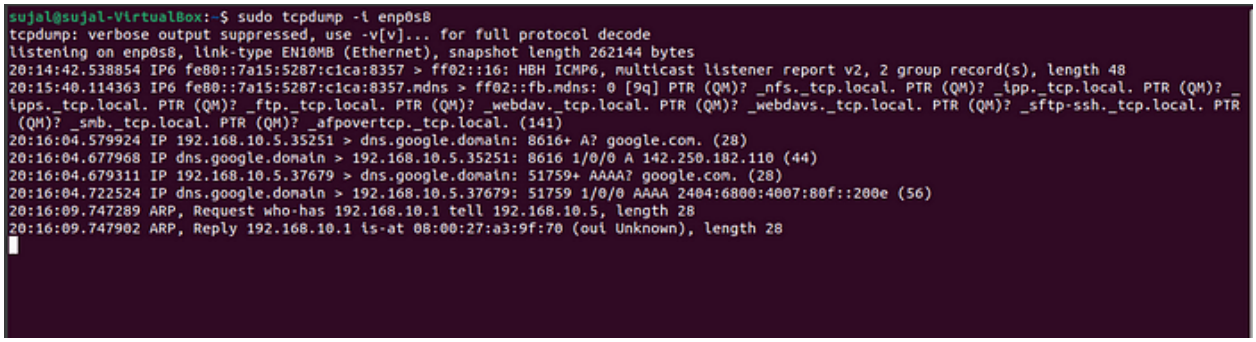
Now to confirm whether we can capture traffic from target-lan from this interface, run tcpdump on the interface in promisc mode.

```
sudo tcpdump -i enp0s8
```

Use one of the machines in target lan to communicate with other hosts or access internet.



Go back to your SOC Analyst machine, and see if the interface captured any traffic



Yahoo! The interface can capture the traffic from the target-lan.

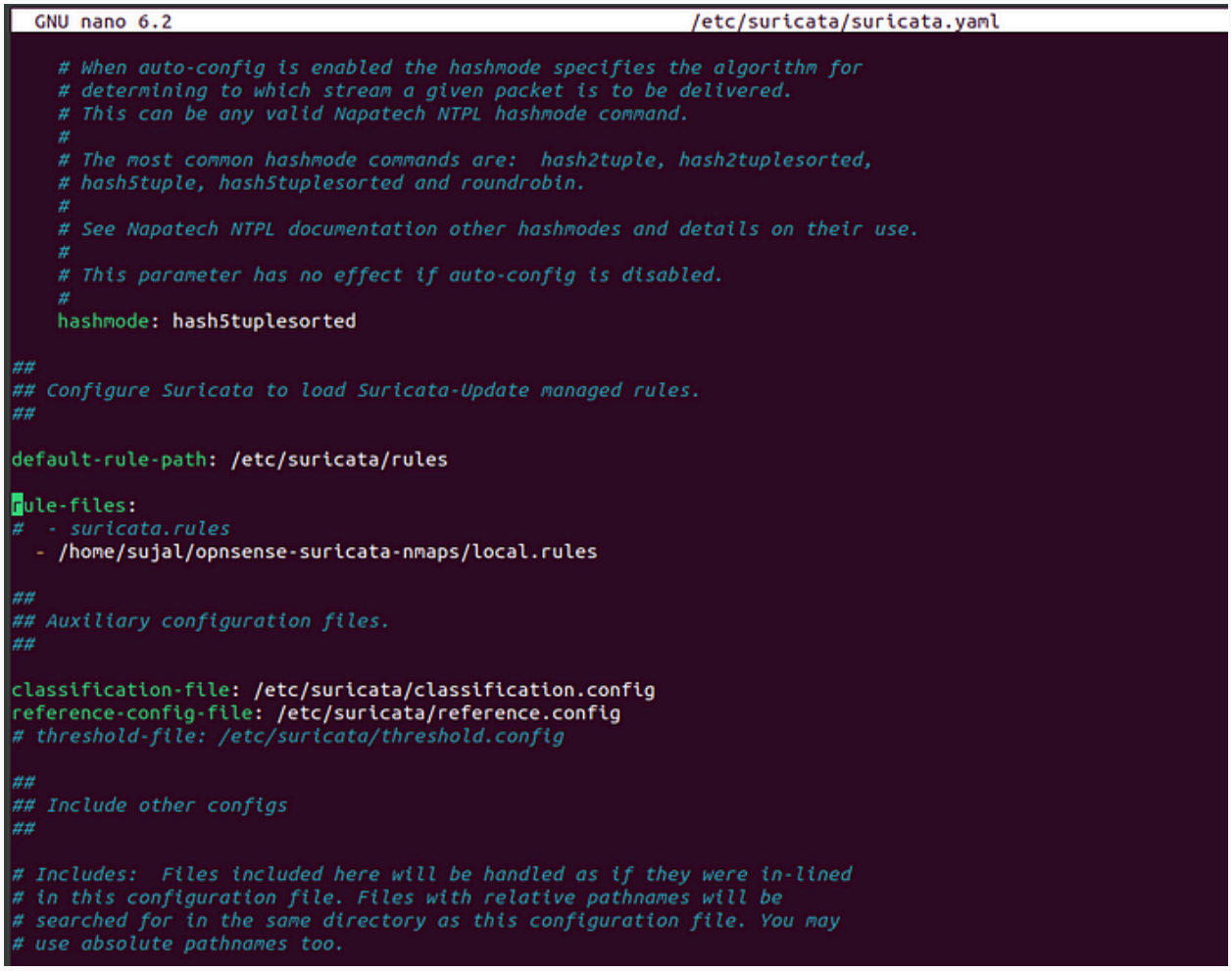
Testing Suricata

I would like you to clone the rules for nmap scans from this repo.

Once cloned copy the path to the local.rules file and put in the

rule-files section of the suricata.yaml file

```
sudo nano /etc/suricata/suricata.yaml
```

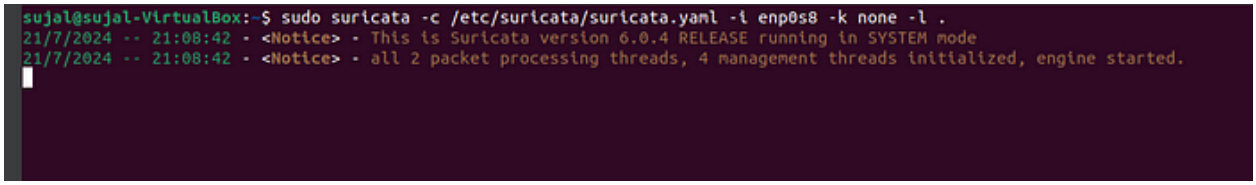


Save it and then spin up suricata on the interface enp0s8.

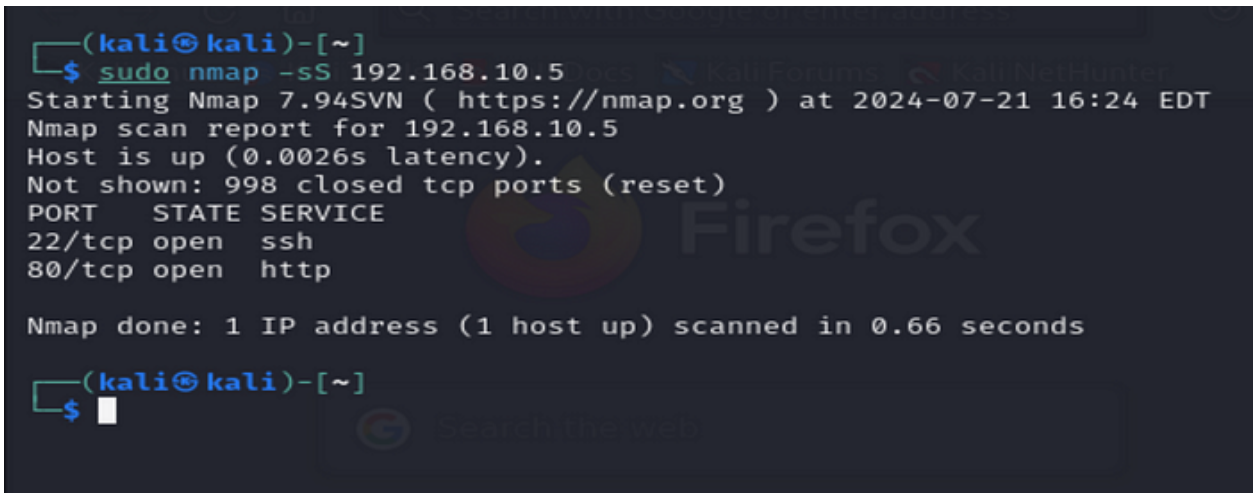
```
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8 -k none -l .
```

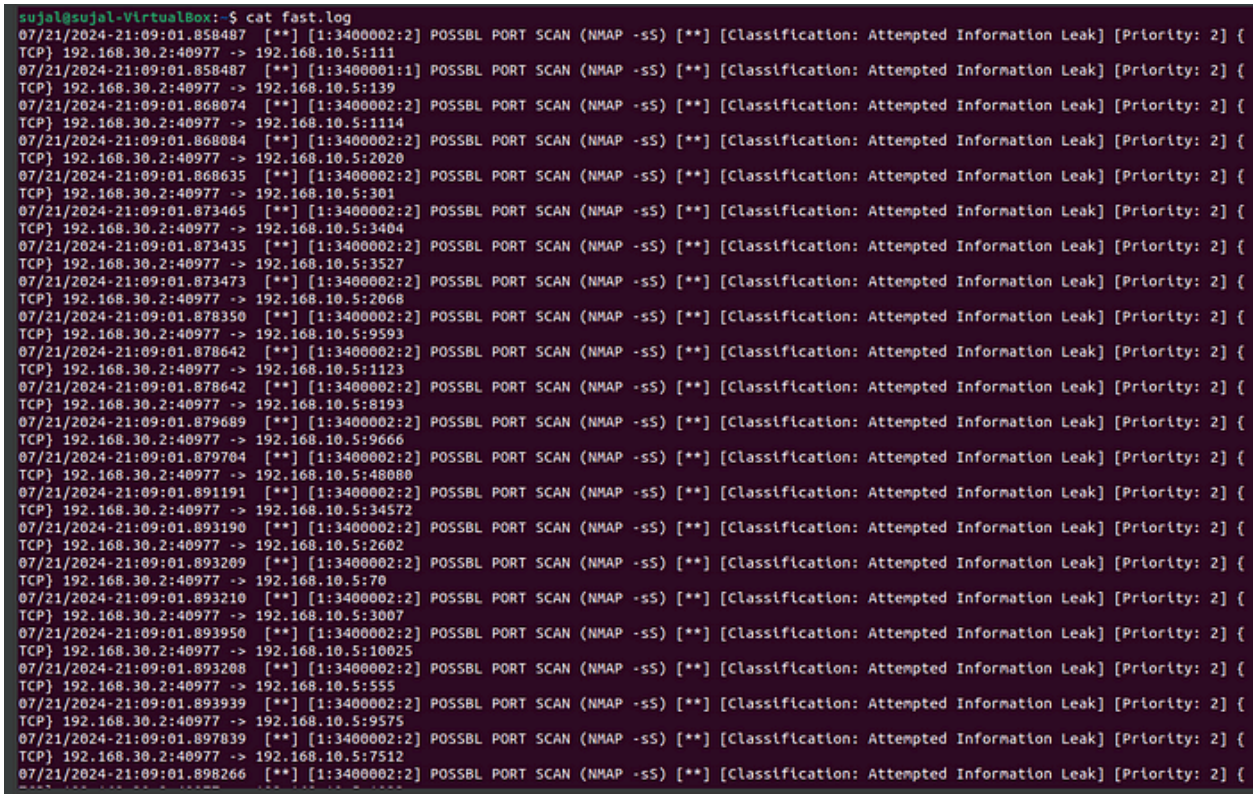
The above command runs suricata with the specified configuration file i.e suricata.yaml (which is made by default on installation) and the

interface (enp0s8) will monitor -k none does the checksum validation and -l . sets the logging to the current directory.



Suricata is monitoring, run nmap from kali linux and then open fast.log to see if it detected any nmap scanning techniques.





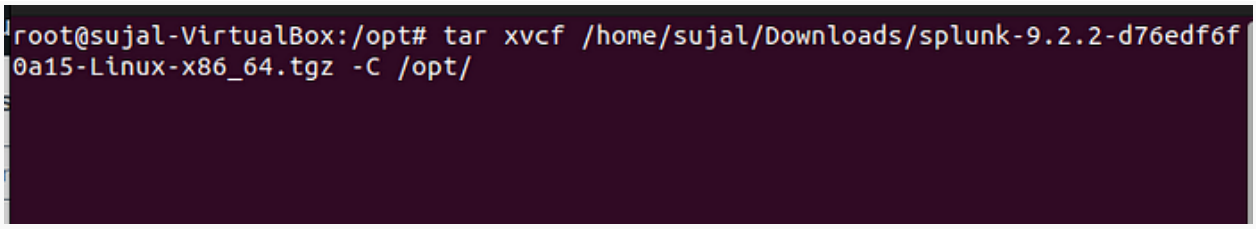
Open the fast.log file, it indeed logged nmap SYN scanning, hence our suricata server is running as an IDS

I will be demonstrating on how to setup splunk server on the SOC Analyst machine and data ingestion into the splunk indexer. To learn more about splunk check here.

Installing Splunk

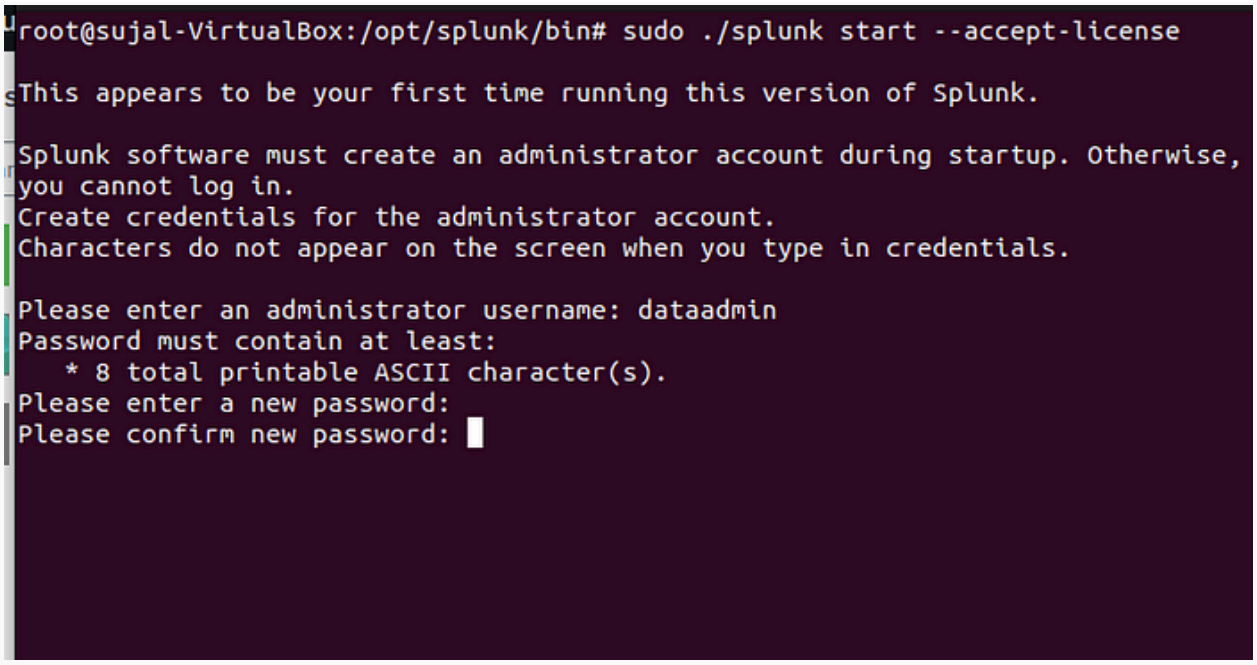
Install splunk from splunk website, after installation run the below command in the directory which the splunk installation file was saved.

```
sudo tar xvzf [splunk tar file] -C /opt/
```

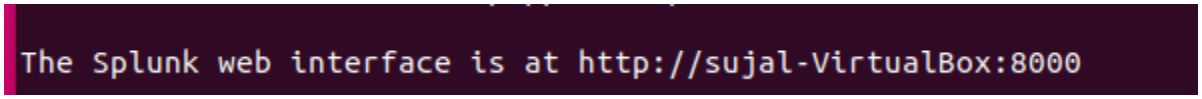


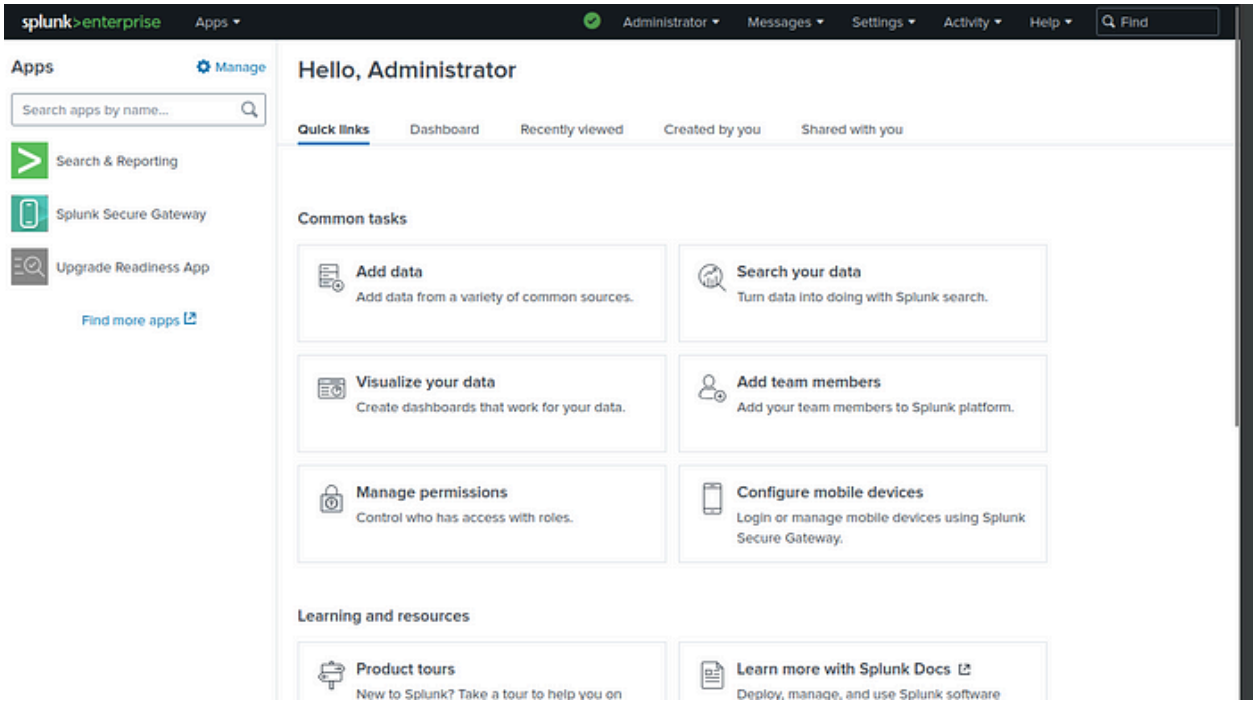
Then start the splunk server with the below command, it will ask for setting admin account and password on initial start of the server.

```
cd /opt/splunk/bin && sudo ./splunk start --accept-license
```



Once done, it will show the uri on which the splunk gui can be accessed, login with the username and password you configured above.

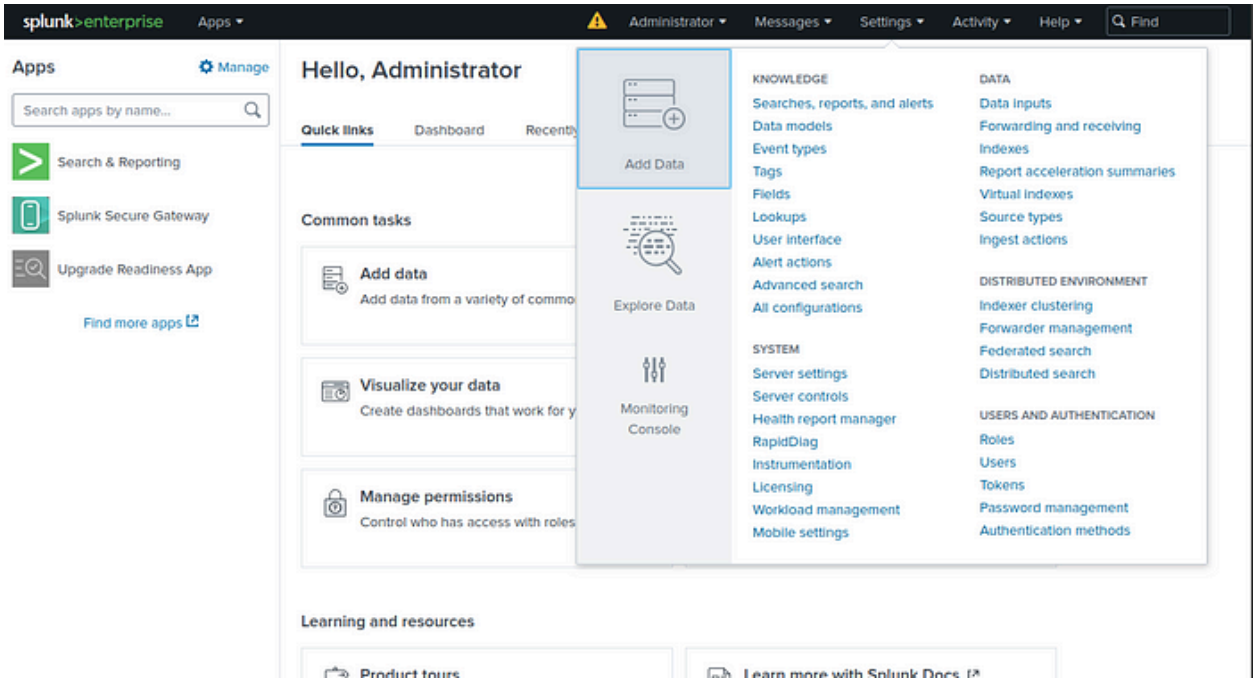


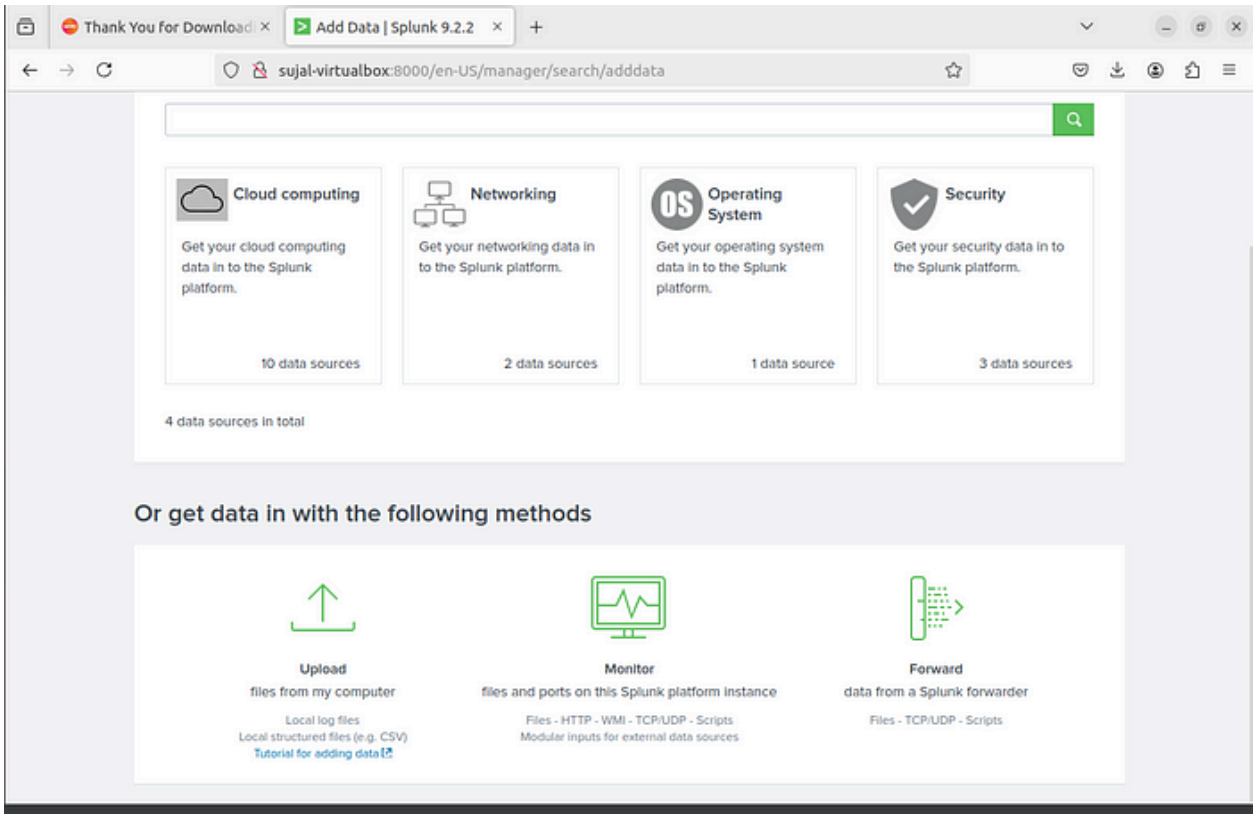


The installation of splunk is successful

Ingesting data to Splunk

Click Settings → Add Data → [Method]


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Manage
Search apps by name...
Search & Reporting
Splunk Secure Gateway
Upgrade Readiness App
Find more apps
Hello, Administrator
Quick links
Dashboard
Add Data
Explore Data
Monitoring Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Federated search
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods
Common tasks
Add data
Visualize your data
Manage permissions
Learning and resources


Thank You for Download
Add Data | Splunk 9.2.2
sujal-virtualbox:8000/en-US/manager/search/adddata
Cloud computing
Get your cloud computing data in to the Splunk platform.
10 data sources
Networking
Get your networking data in to the Splunk platform.
2 data sources
Operating System
Get your operating system data in to the Splunk platform.
1 data source
Security
Get your security data in to the Splunk platform.
3 data sources
4 data sources in total
Or get data in with the following methods
Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data
Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources
Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

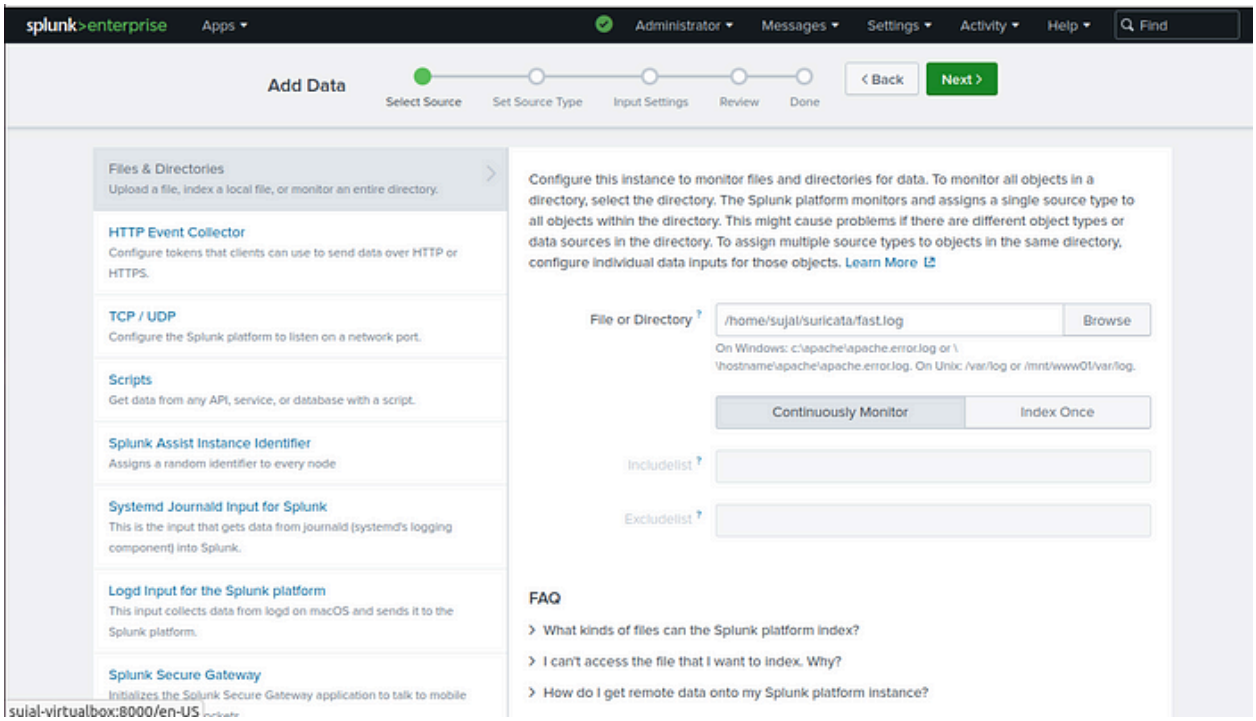
There are guides on the data sources and method types. To learn more about ingestion in splunk check this documentaion.

I will be demonstrating Monitor and Forward method, for the demonstration purpose for monitoring method I will be monitoring the log file generated by suricata on the machine running splunk. I created a directory suricata in my user directory, then spinned up suricata to log the alerts in that directory.

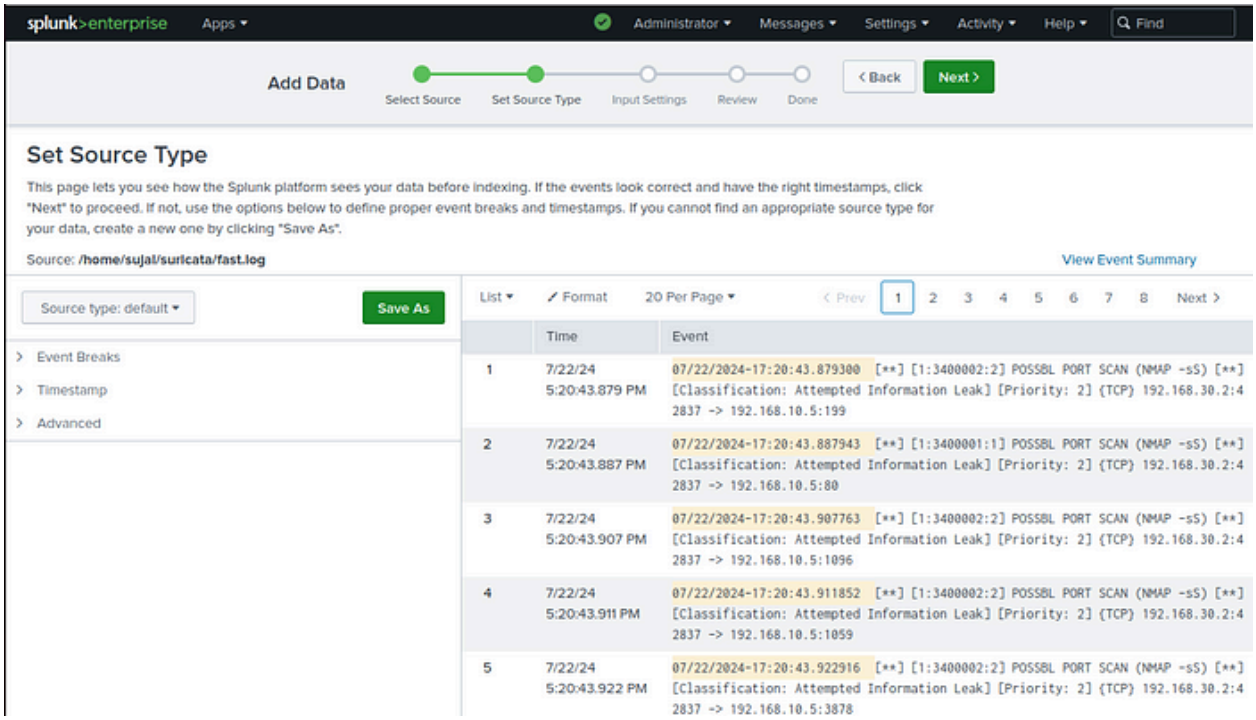
```
sujal@sujal-VirtualBox:~$ mkdir suricata
sujal@sujal-VirtualBox:~$ cd suricata/
sujal@sujal-VirtualBox:~/suricata$ ls
sujal@sujal-VirtualBox:~/suricata$ sudo suricata -c /etc/suricata/suricata.yaml
-i enp0s8 -k none -l .
[sudo] password for sujal:
Sorry, try again.
[sudo] password for sujal:
22/7/2024 -- 17:07:54 - <Notice> - This is Suricata version 6.0.4 RELEASE runnin
g in SYSTEM mode
22/7/2024 -- 17:07:54 - <Notice> - all 2 packet processing threads, 4 management
 threads initialized, engine started.
```

Next spin up your kali machine and perform a SYN Scan with nmap on any one of the machine this will add the logs to the directory specified.

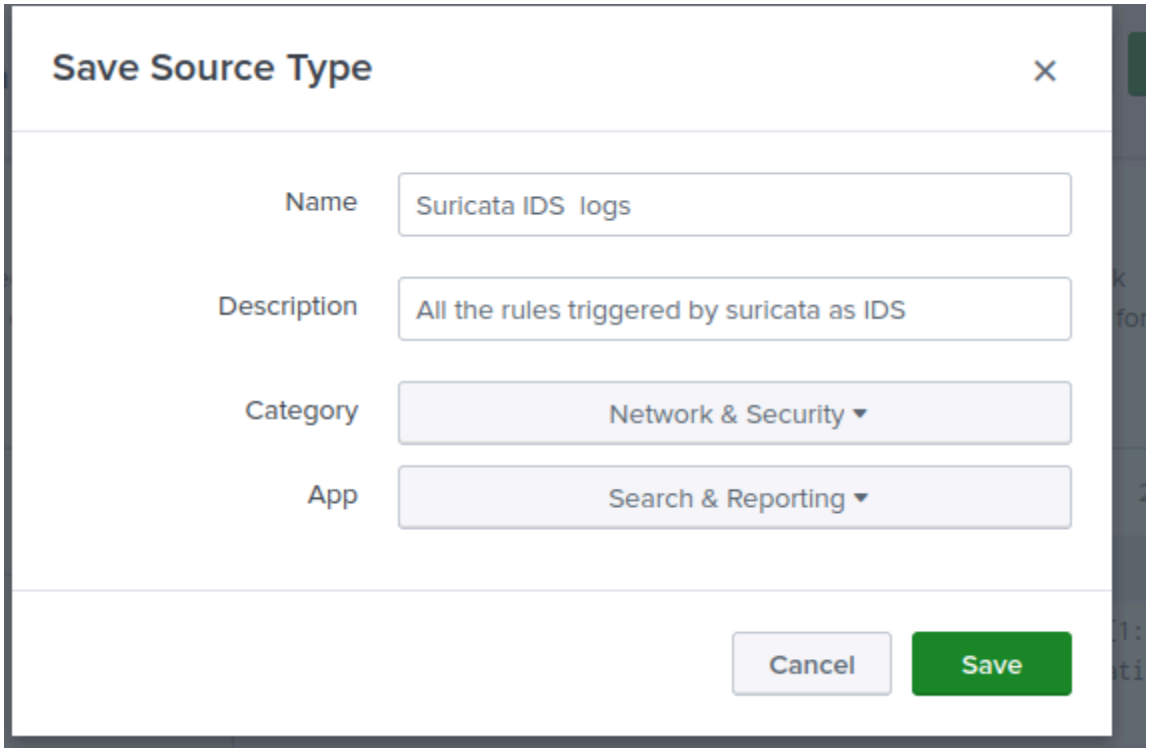
Select Monitoring files and directories.

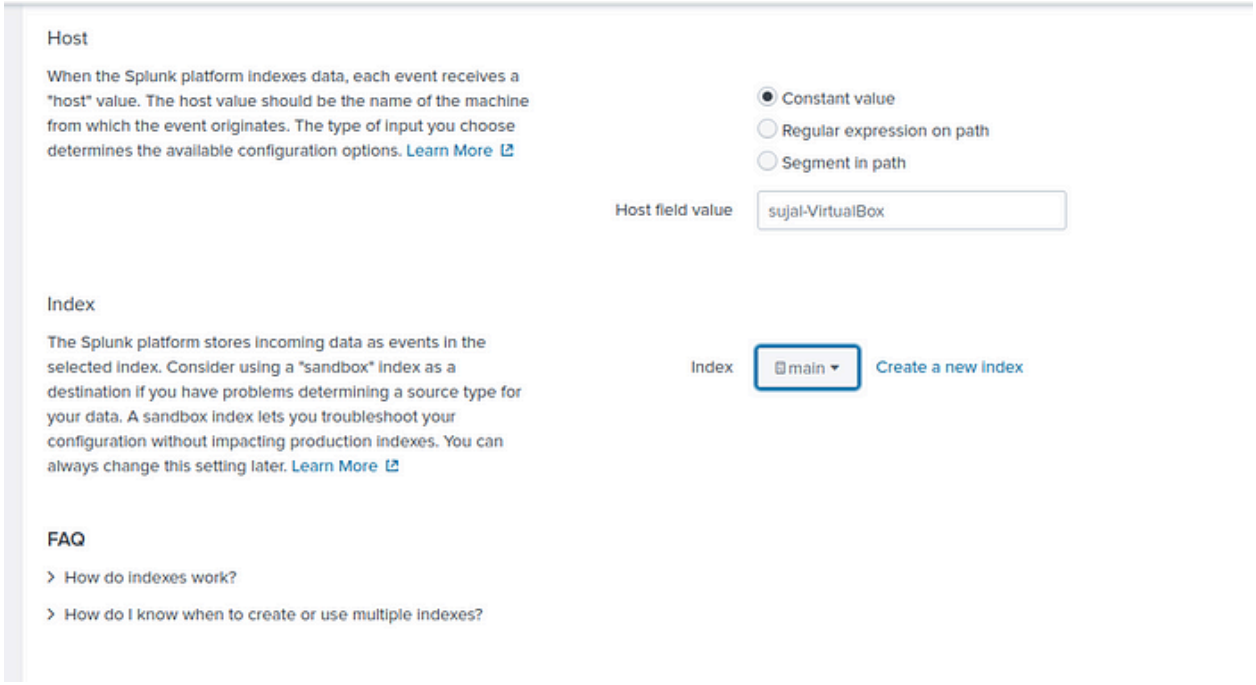


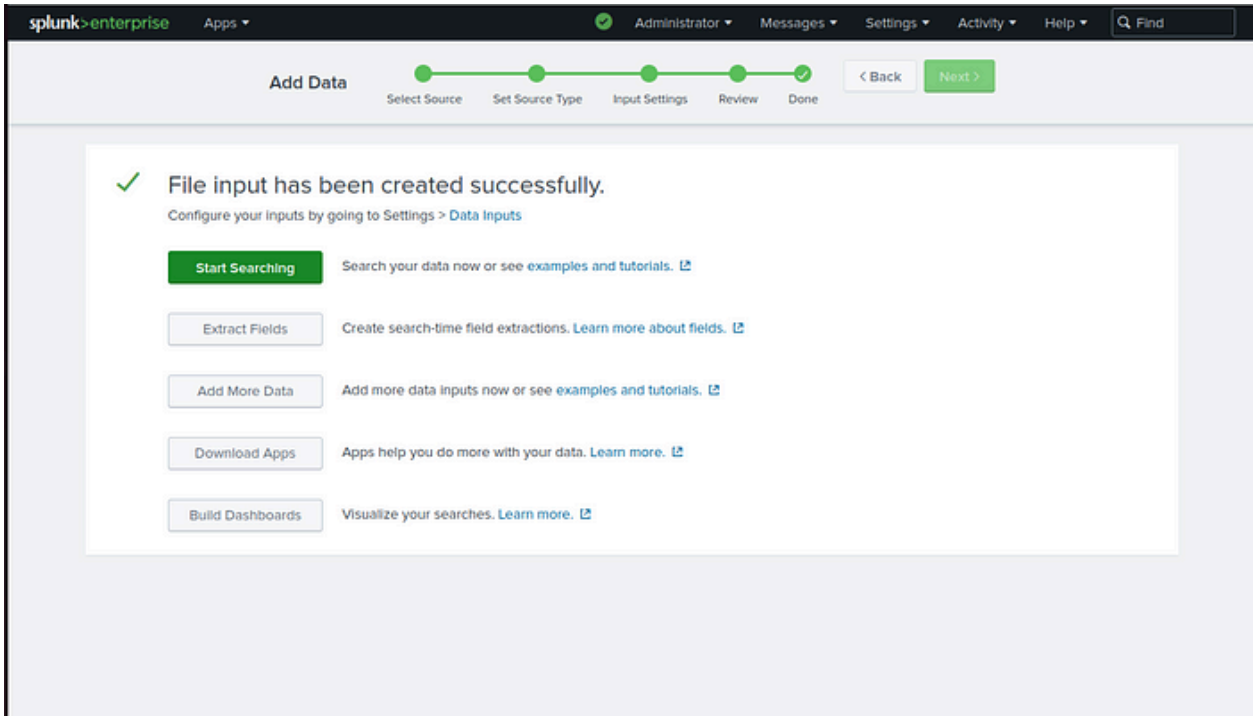
Select continuously monitor option, so that if new data is logged then splunk will index it for us to monitor simultaneously.

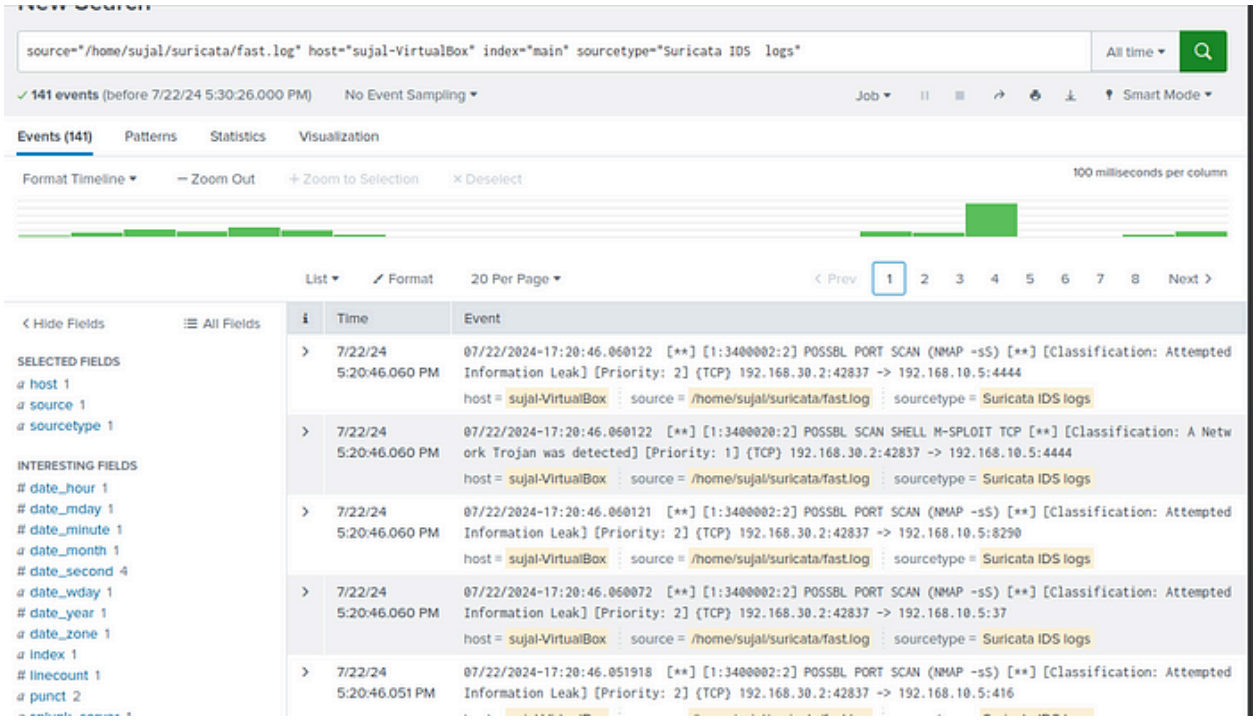


Review if the logs added are in the correct format.


Save Source Type
Name
Suricata IDS logs
Description
All the rules triggered by suricata as IDS
Category
Network & Security
App
Search & Reporting
Cancel
Save

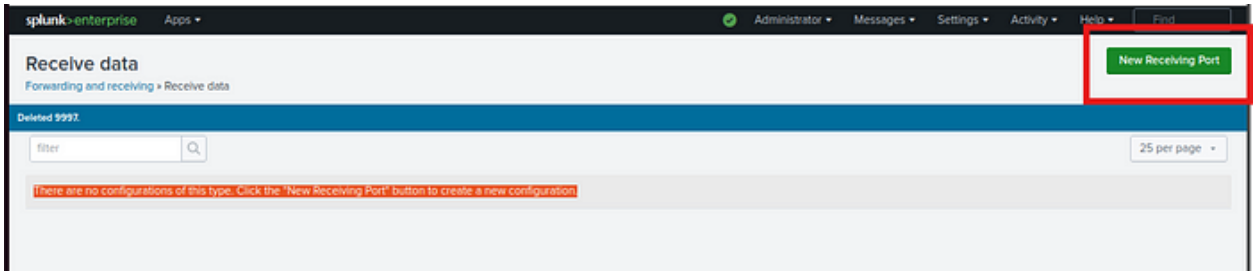

Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
sujal-VirtualBox
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
main
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?

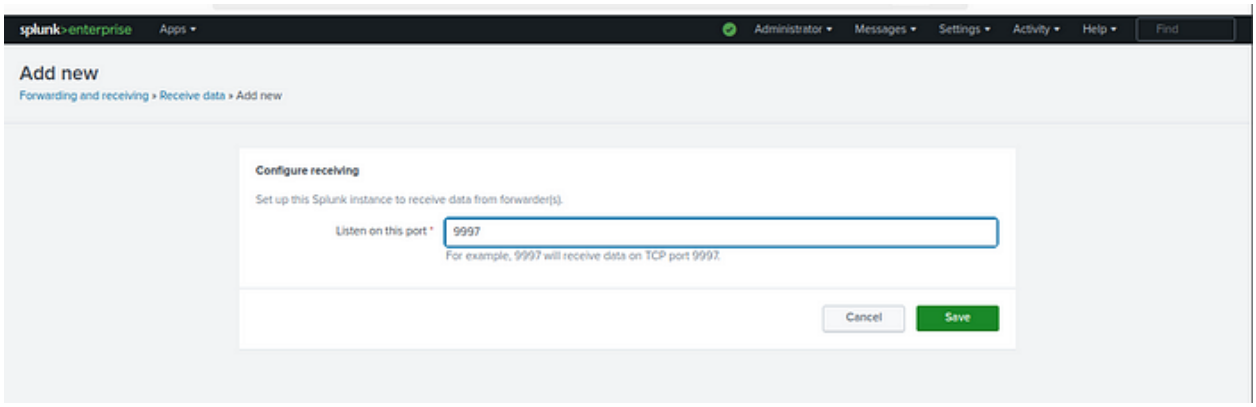

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
File input has been created successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Extract Fields
Create search-time field extractions. Learn more about fields.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.


source="/home/sujal/suricata/fast.log" host="sujal-VirtualBox" index="main" sourcetype="Suricata IDS logs"
All time
141 events (before 7/22/24 5:30:26.000 PM)
No Event Sampling
Job
Smart Mode
Events (141)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 4
a date_wday 1
date_year 1
a date_zone 1
a index 1
linecount 1
a punct 2
Time
Event
7/22/24 5:20:46.060 PM
07/22/2024-17:20:46.060122 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:4444
host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.060 PM
07/22/2024-17:20:46.060122 [**] [1:3400020:2] POSSBL SCAN SHELL M-SPLOIT TCP [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.30.2:42837 -> 192.168.10.5:4444
host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.060 PM
07/22/2024-17:20:46.060121 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:8290
host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.060 PM
07/22/2024-17:20:46.060072 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:37
host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.051 PM
07/22/2024-17:20:46.051918 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:416

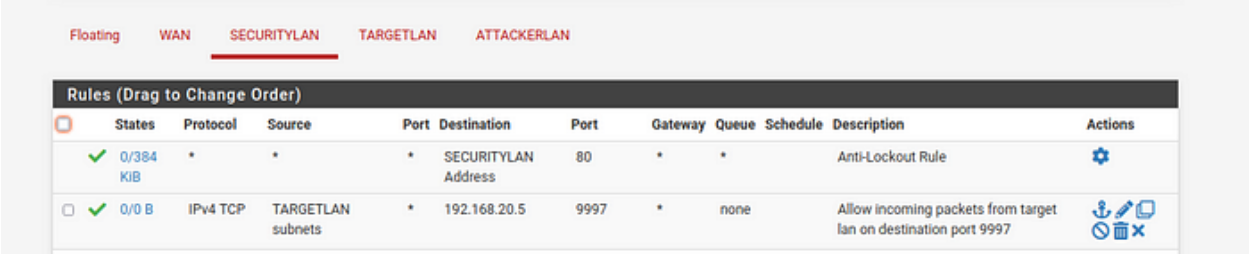
Setting up Universal forwarders.

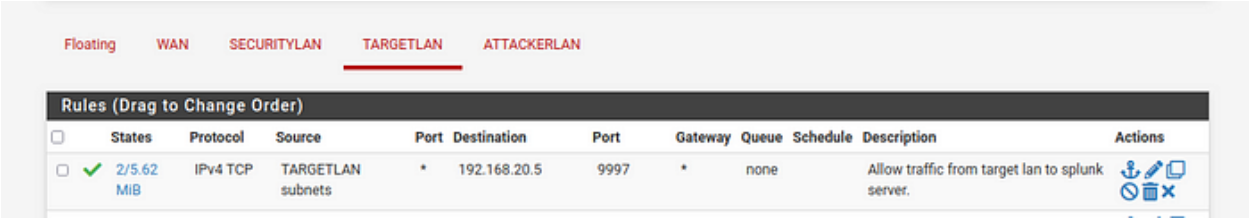
Click Settings → Forwarding and Receiving → Configure Receiving → New Receiving Port → Add port [9997 default].





I will set up a forwarder on ubuntu machine in target lan to forward the data to the splunk server in security lan. Need to add a rule to allow this traffic to security lan through pfsense.





Install the universal forwarder on the target lan machines from here.

Move to the directory where splunk forwarder is downloaded and extract it to the /opt directory.

```
sudo tar xzvf [forwarder file] -C /opt/
```

```
cd /opt/splunkforwarder/bin && sudo ./splunk start --accept-license (start the forwarder)
```

```
sudo ./splunk enable boot-start (to automatically start the splunk service on boot)
```

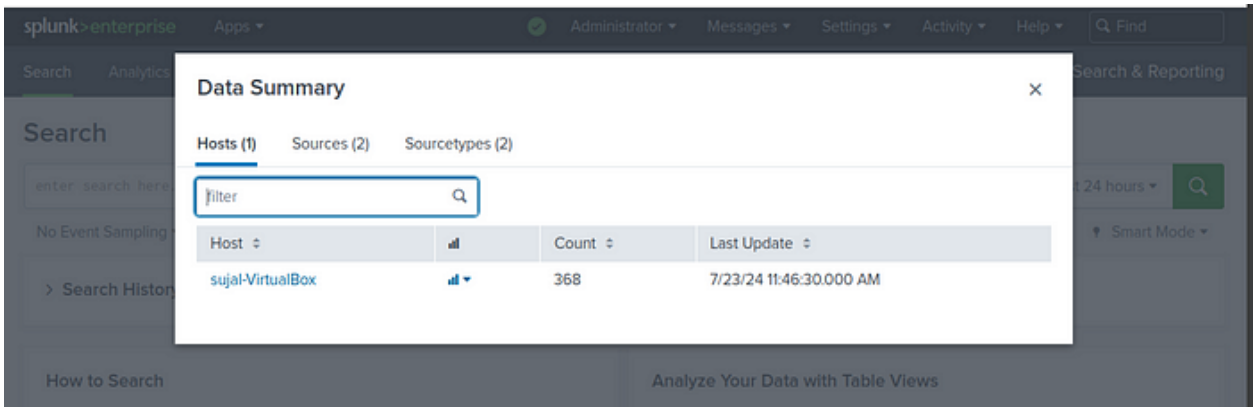
```
sudo ./splunk add forward-server [SOC Analyst IP]:[Receiving Port] (Add a forward server)
```

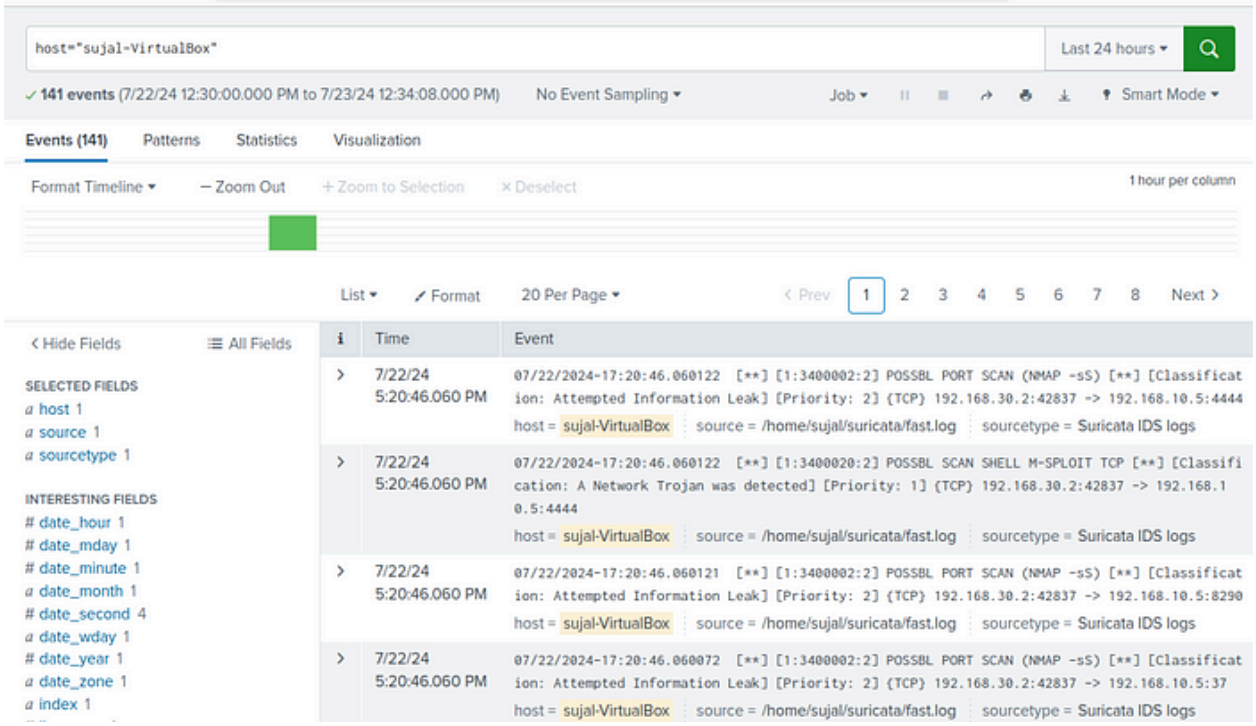
Run the below command to tell the forwarder what data to send.

```
sudo ./splunk add monitor /var/log/auth.log
```

To verify if the data is being forwarded

Click Search & Reporting → Data Summary.





The forwarder is working fine and we can get the data into splunk .

Note : To save resources and avoid storage consumption delete the logs manually or through scripts .

Do add more forwarders to get all the necessary data into your splunk server for monitoring.