

# **LAB 2 – Introduction to Networking**

**By :- Faraz Ahmed**

## Contents

1.	Installing and Configuring pfSenseRouter .....	2
1.1	Installing pfSenseRouter .....	2
1.2	Installing Open-VM-Tools on pfSenseRouter .....	2
2.	Migrating Ubuntu + Windows Desktop Client using CLI .....	3
2.1	For Windows :- .....	3
2.2	For Linux :-.....	5
3.	Subtask: Demonstration of Internet Connectivity for Both Clients .....	7
3.1	Ubuntu Linux.....	7
3.2	Windows 10 .....	10
4.	Additional Tasks .....	14
5.	Appendix A- Developing a Topology .....	18

## 1. Installing and Configuring pfSenseRouter

To understand the installation process for pfSenseRouter is important to all users in the field of cybersecurity especially in system security to configure to a proper network and check for its stability. So, to connect to pfSenseRouter through vSphere we need to follow some steps and commands.

### 1.1 Installing pfSenseRouter

For the installation of pfSenseRouter follow :-

- Right click on pfSenseRouter and select Edit Settings.
- Change CD/DVD drive 1 from Client Device to Datastore ISO File.
- Use the ISO cdr-iscsi4/ISOs/Routers/pfSense-CE-2.7.2-RELEASE amd.iso (that the only latest option available).
- Then click on the run button and then hit refresh.
- Then click on “Launch Web Console” to start pfSenseRouter.
- Now watch video guidance from link  
<https://ub.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=4aa25bbe-c46e-40d0-af66-b1e0017b372c> and follow the instructions.

### 1.2 Installing Open-VM-Tools on pfSenseRouter

- At the pfSenseRouter command prompt, select 13 option to update from Console. Accept all to complete installation.
- At the pfSenseRouter command prompt, select 8 to Shell.
- Type command “pkg install pfSense-pkg-Open-VM-Tools”.
- Then Type command “service -l | grep vmware”.  
If the installation is successful, you will observe 4 listed services starting with “vmware-”.

## 2. Migrating Ubuntu + Windows Desktop Client using CLI

So, now we will connect Win10Client to AdminNet network (managed by the pfSenseRouter LAN interface) and connect UbuntuClient to ServerNet network (managed by the pfSenseRouter OPT1 interface). Now follow the steps to connect them to pfSenseRouter which are :-

- Disable the pfSenseRouter firewall by selecting 8 then type pfctl -d command.
- Configure the client endpoint network interfaces on both Operating Systems (Windows and Linux) using the command line i.e. Terminal or Powershell.

### 2.1 For Windows :-

- Open the “Powershell” application as administrator(as highlighted below).

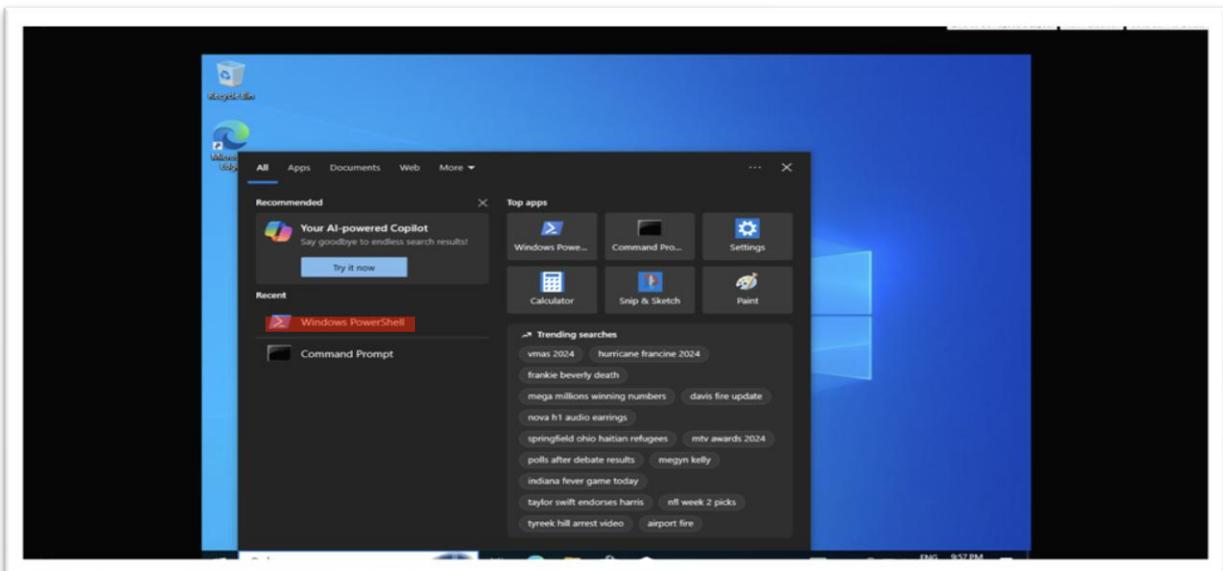


Figure 1: Screenshot of “Powershell” search on Windows 10

- Then type “Get-NetAdaptor -Name \*” as highlighted below.

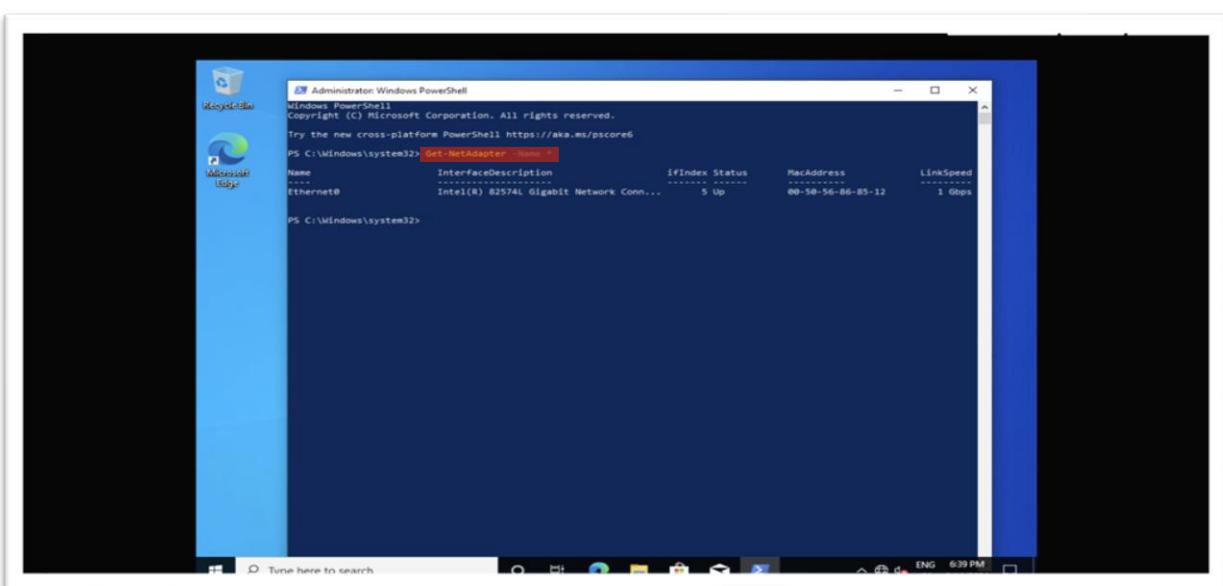


Figure 2: Screenshot of “Get-NetAdaptor -Name \*”

- Now we can observe that the ifIndex network interface value is 5 which will be our “Y”.
- Then type “Remove-NetIPAddress -InterfaceIndex <Y> -Confirm:\$false where <Y> is the ifIndex which is 5 as stated before.
- After that, type “Remove-NetRoute -InterfaceIndex -Confirm:\$false”
- Type “New-NetIPAddress -InterfaceIndex <Y> -IPAddress 10.42.<X>.12 -AddressFamily IPv4 -PrefixLength 24 DefaultGateway 10.42.<X>.1 (as highlighted below) where “X” is our team number in vSphere(which is 32 in my case).

```

Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> Get-NetAdapter -Name *
Name InterfaceDescription IfIndex Status MacAddress LinkSpeed
---- -----
Ethernet# Intel(R) 82574L Gigabit Network Conn... 5 Up 00-50-56-86-85-12 1 Gbps

PS C:\Windows\system32> Remove-NetIPAddress -InterfaceIndex 5 -Confirm:$false
PS C:\Windows\system32> Remove-NetRoute -InterfaceIndex 5 -Confirm:$false
PS C:\Windows\system32> New-NetIPAddress -InterfaceIndex 5 -IPAddress 10.42.32.12 -AddressFamily IPv4 -PrefixLength 24
DefaultGateway 10.42.32.1

IPAddress : 10.42.32.12
InterfaceIndex : 5
InterfaceAlias : Ethernet#
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Tentative
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipLoopBack : False
PolicyStore : ActiveStore

IPAddress : 10.42.32.12
InterfaceIndex : 5
InterfaceAlias : Ethernet#
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Tentative
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipLoopBack : False
PolicyStore : PersistentStore

PS C:\Windows\system32>

```

Figure 3: Screenshot of “New-NetIPAddress-....”

- Now finally type “Set-DnsClientServerAddress -InterfaceIndex <Y> -ServerAddresses (“8.8.8.8”,“8.8.4.4”) as highlighted below.

```

Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> Get-NetAdapter -Name *
Name InterfaceDescription IfIndex Status MacAddress LinkSpeed
---- -----
Ethernet# Intel(R) 82574L Gigabit Network Conn... 5 Up 00-50-56-86-85-12 1 Gbps

PS C:\Windows\system32> Remove-NetIPAddress -InterfaceIndex 5 -Confirm:$false
PS C:\Windows\system32> Remove-NetRoute -InterfaceIndex 5 -Confirm:$false
PS C:\Windows\system32> New-NetIPAddress -InterfaceIndex 5 -IPAddress 10.42.32.12 -AddressFamily IPv4 -PrefixLength 24
DefaultGateway 10.42.32.1

IPAddress : 10.42.32.12
InterfaceIndex : 5
InterfaceAlias : Ethernet#
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Tentative
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipLoopBack : False
PolicyStore : ActiveStore

IPAddress : 10.42.32.12
InterfaceIndex : 5
InterfaceAlias : Ethernet#
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Tentative
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipLoopBack : False
PolicyStore : PersistentStore

PS C:\Windows\system32> Set-DnsClientServerAddress -InterfaceIndex 5 -ServerAddresses ("8.8.8.8","8.8.4.4")
PS C:\Windows\system32>

```

Figure 4: Screenshot of “Set-DnsClientServerAddress”

## 2.2 For Linux :-

- Open the “Terminal” application as highlighted below.

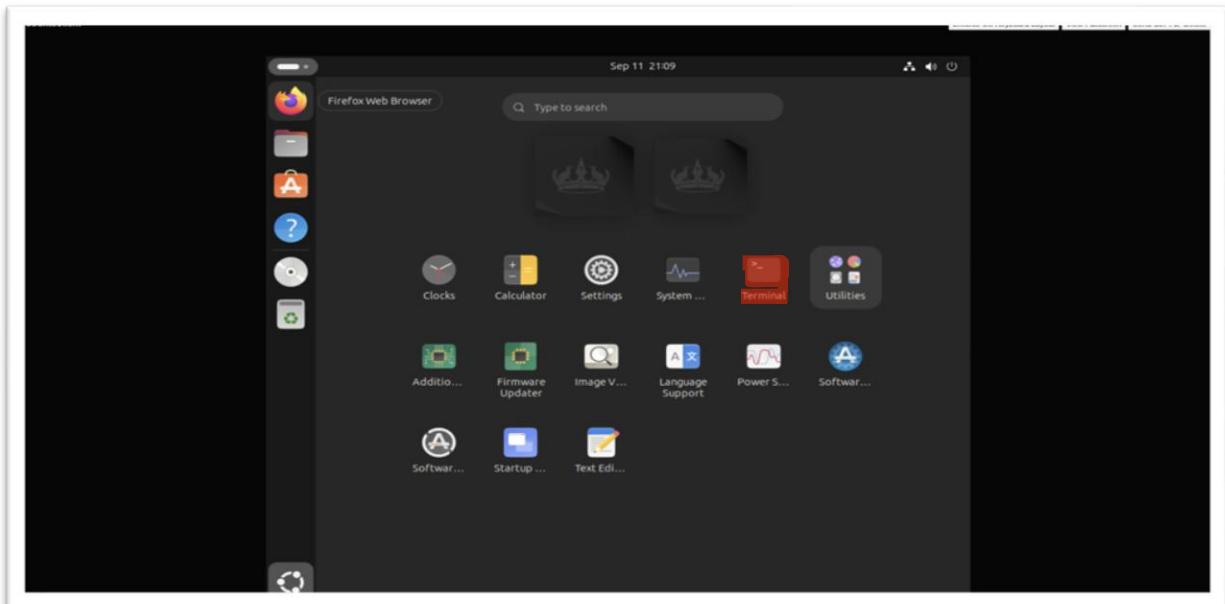


Figure 5: Screenshot of “Terminal” search on Linux

- Then type “sudo nano /etc/netplan/01-network-manager-all.yaml”
- Then edit the file like it is shown below

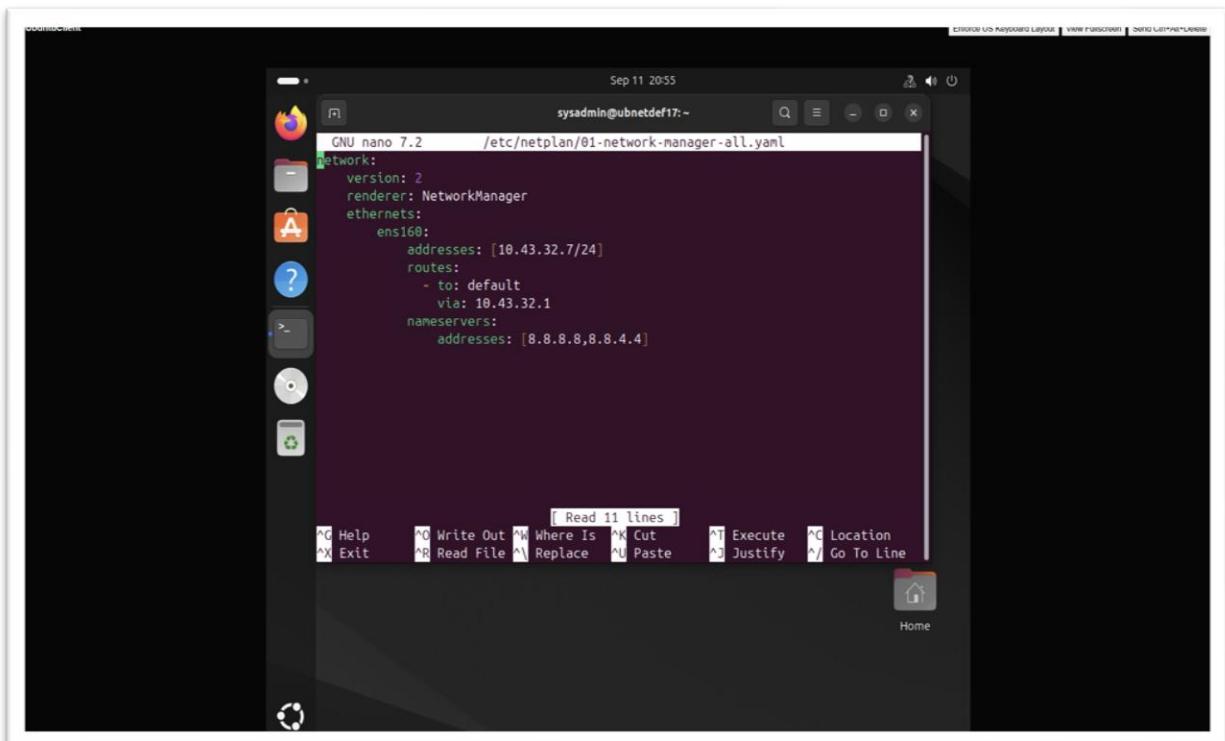


Figure 6: Screenshot of Content we need to edit

- To save the file, press “ctrl + O” and press “ctrl + X”.
- After that type “sudo netplan generate”.

- And type “sudo netplan apply”(highlighted on figure 8). If there is no output then its successful.

Note :- as you can see below that we get many warning messages as an output which is of no use so in order to remove it type “sudo chmod 700 /etc/netplan/01-network-manager-all.yaml” (as highlighted below) and enter the password after that.

```

sysadmin@ubnetdef17:~$ sudo netplan apply
[sudo] password for sysadmin:
** (generate:3578): WARNING **: 20:57:58.164: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
** (generate:3578): WARNING **: 20:58:53.554: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
** (process:3712): WARNING **: 20:58:54.723: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
** (process:3712): WARNING **: 20:58:55.116: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.

```

Figure 7: Screenshot of “sudo netplan apply”

- So as we can see that we get a clean output as shown below (figure 8).

```

sysadmin@ubnetdef17:~$ sudo netplan apply

```

Figure 8: Screenshot of Final Output without any warning messages

### 3. Subtask: Demonstration of Internet Connectivity for Both Clients

We will demonstrate the internet connectivity for both clients i.e. Windows 10 and Ubuntu Linux by using commands in CLI applications like Terminal, PowerShell, etc.

#### 3.1 Ubuntu Linux

- Launch the “Terminal” application as highlighted below.

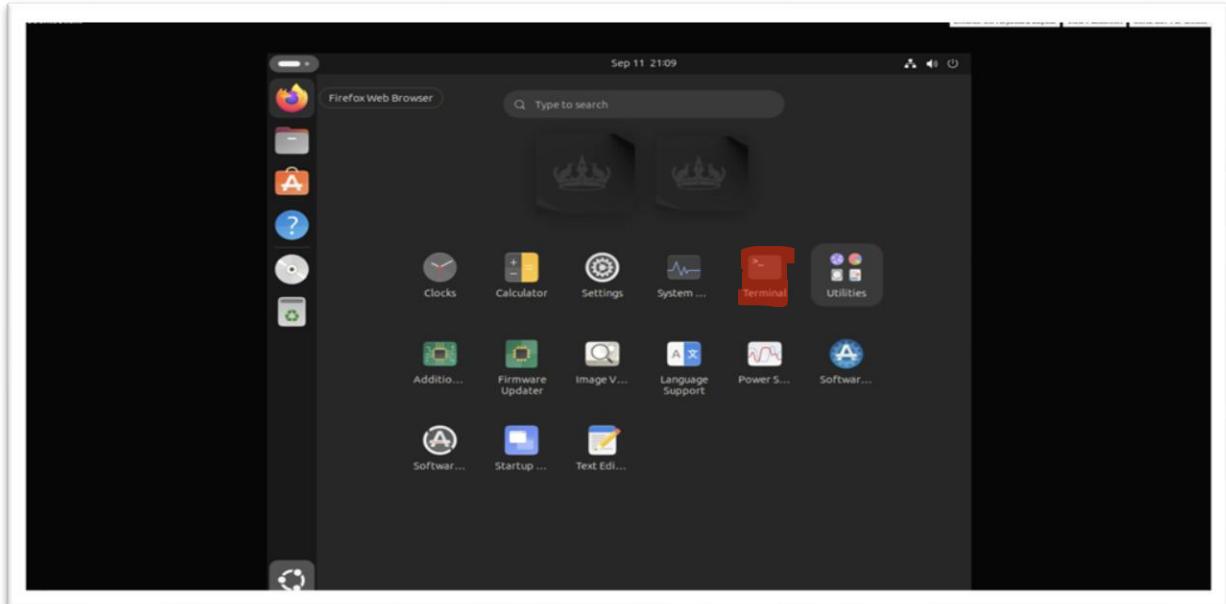


Figure 9: Screenshot of “Terminal” search on Linux

- The first command we wrote is – “**ip r**” (as highlighted below) which means ip route. It is a table about the paths which network packets takes to reach its destination. So, this helps us to find best paths and any blocked network paths.

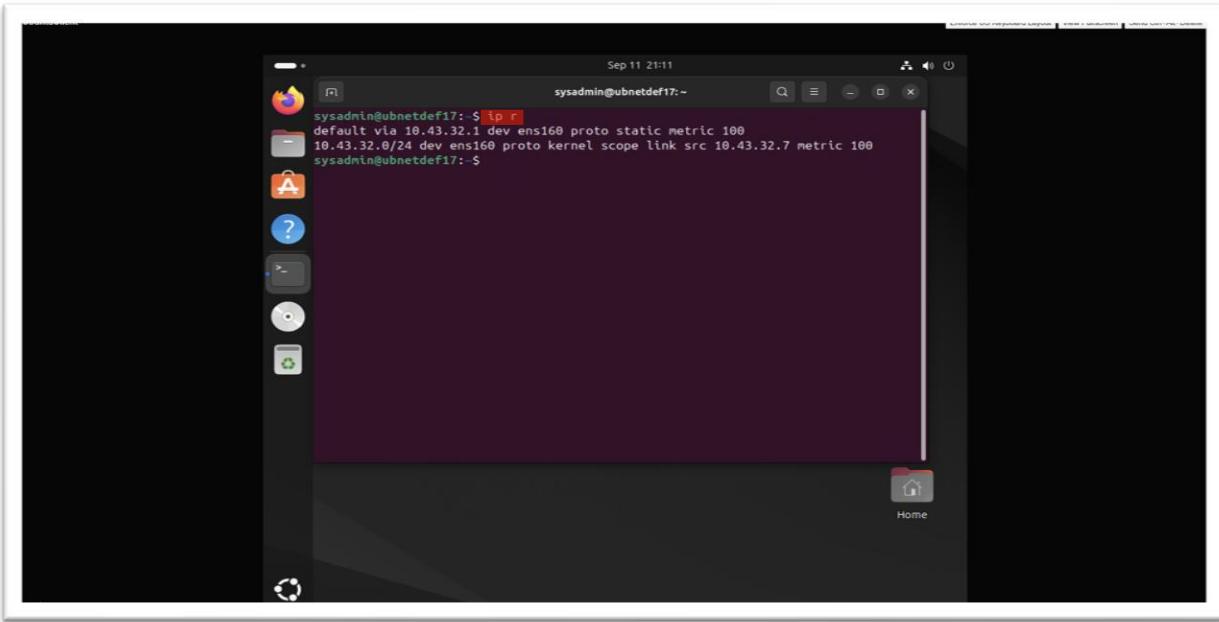


Figure 10: Screenshot of “ip r”

- Then ping the corresponding default gateway IP: 10.42.<X>.1 and 10.43.<X>.1 (as shown below) where <X> is the vSphere team number which is 32 in my case.

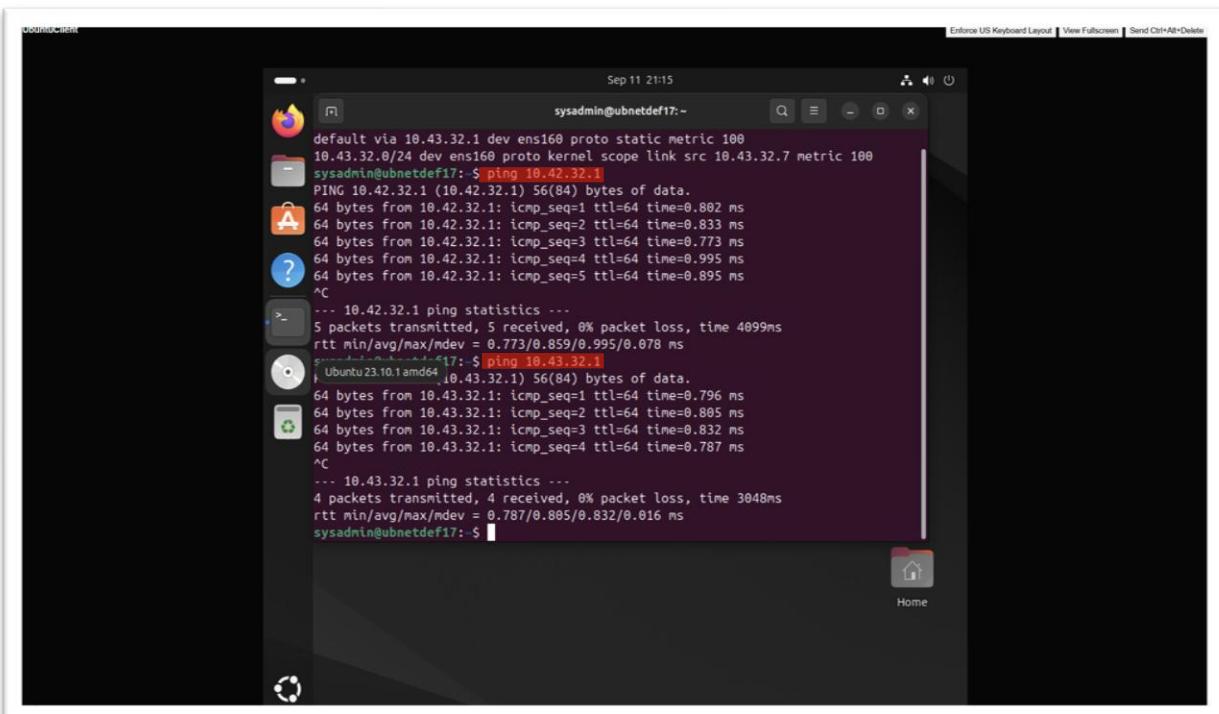


Figure 11: Screenshot of ping both Default Gateway

- Then ping the Gretzky Enterprise gateway IP: 192.168.254.254 as highlighted below.

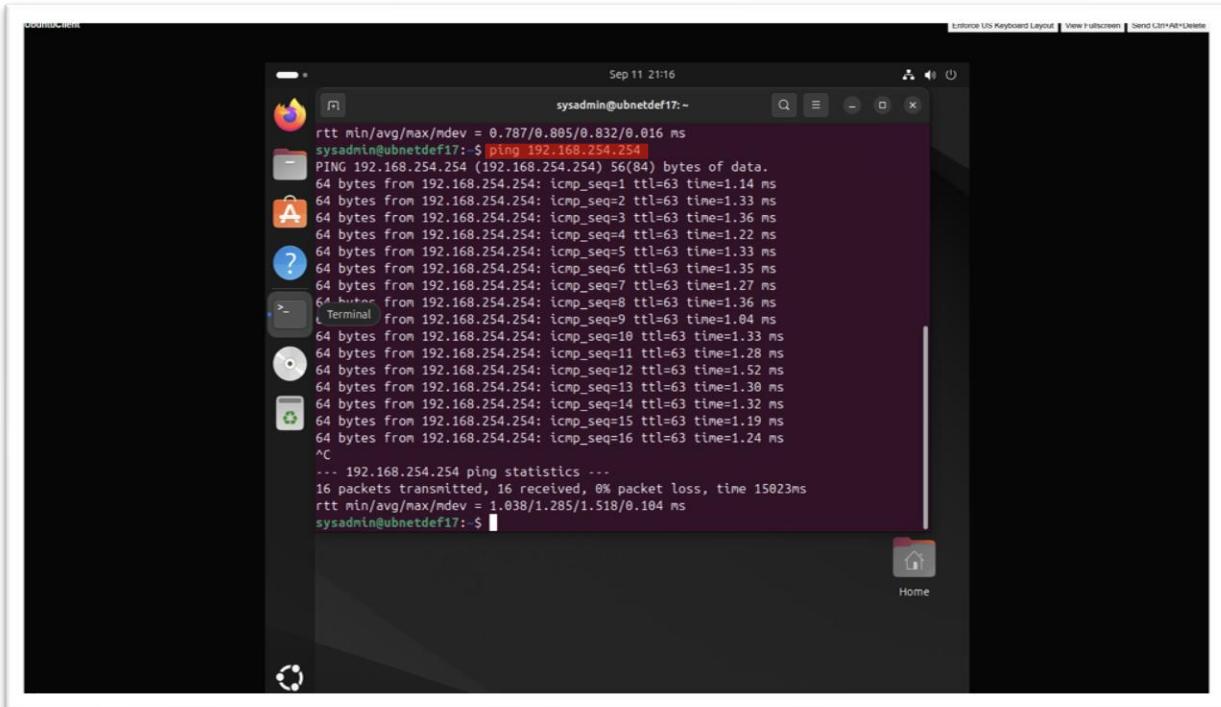


Figure 12: Screenshot of ping Gretzky Enterprise gateway

- Now ping Google DNS IP: 8.8.8.8 .

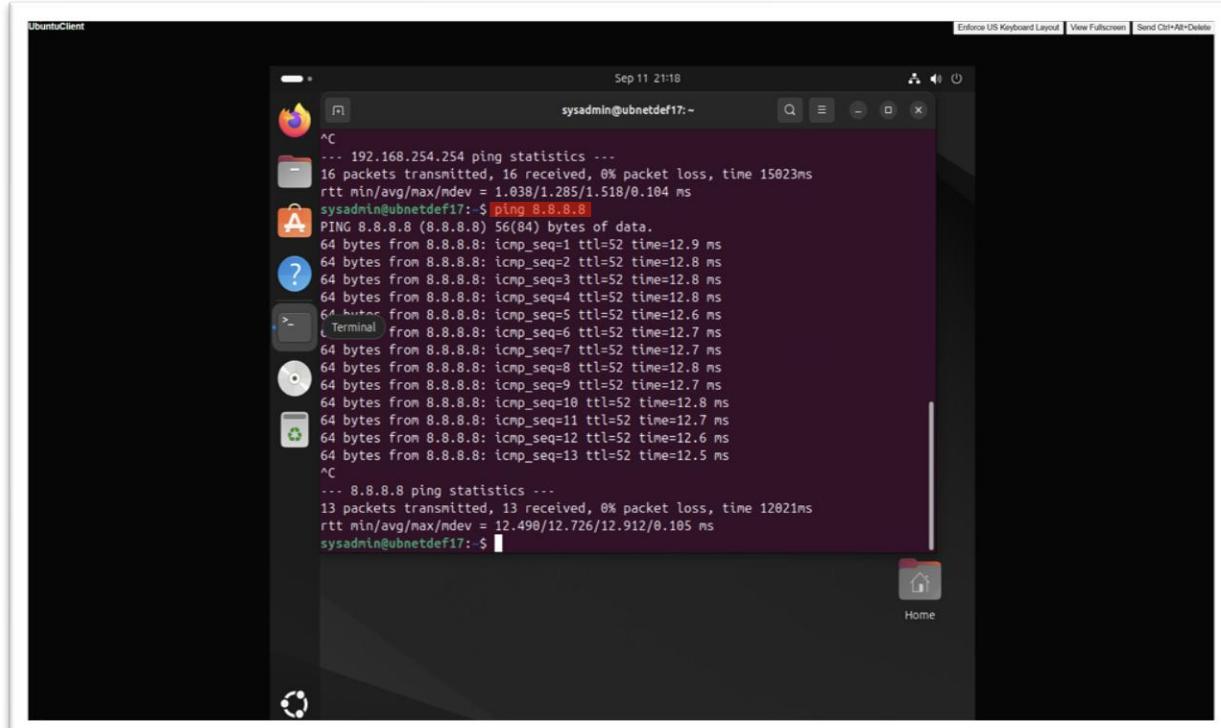
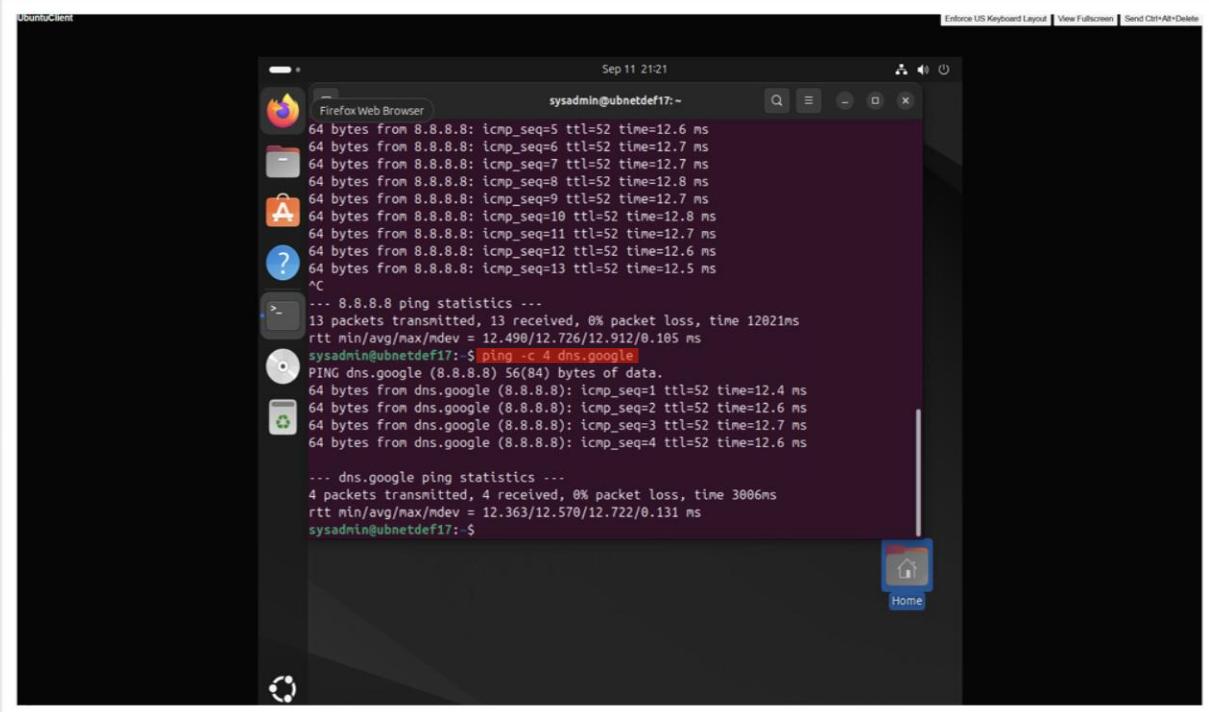


Figure 13: Screenshot of ping Google

- And ping Google DNS domain: dns.google as highlighted below .



```
Sep 11 21:21
sysadmin@ubnetdef17:~$ ping -c 4 dns.google
PING dns.google (8.8.8.8) 56(84) bytes of data.
64 bytes from dns.google (8.8.8.8): icmp_seq=1 ttl=52 time=12.4 ms
64 bytes from dns.google (8.8.8.8): icmp_seq=2 ttl=52 time=12.6 ms
64 bytes from dns.google (8.8.8.8): icmp_seq=3 ttl=52 time=12.7 ms
64 bytes from dns.google (8.8.8.8): icmp_seq=4 ttl=52 time=12.6 ms

--- dns.google ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 12.363/12.570/12.722/0.131 ms
sysadmin@ubnetdef17:~$
```

Figure 14: Screenshot of ping Google DNS Domain

### 3.2 Windows 10

- Launch the “Command Prompt” application as observed below.

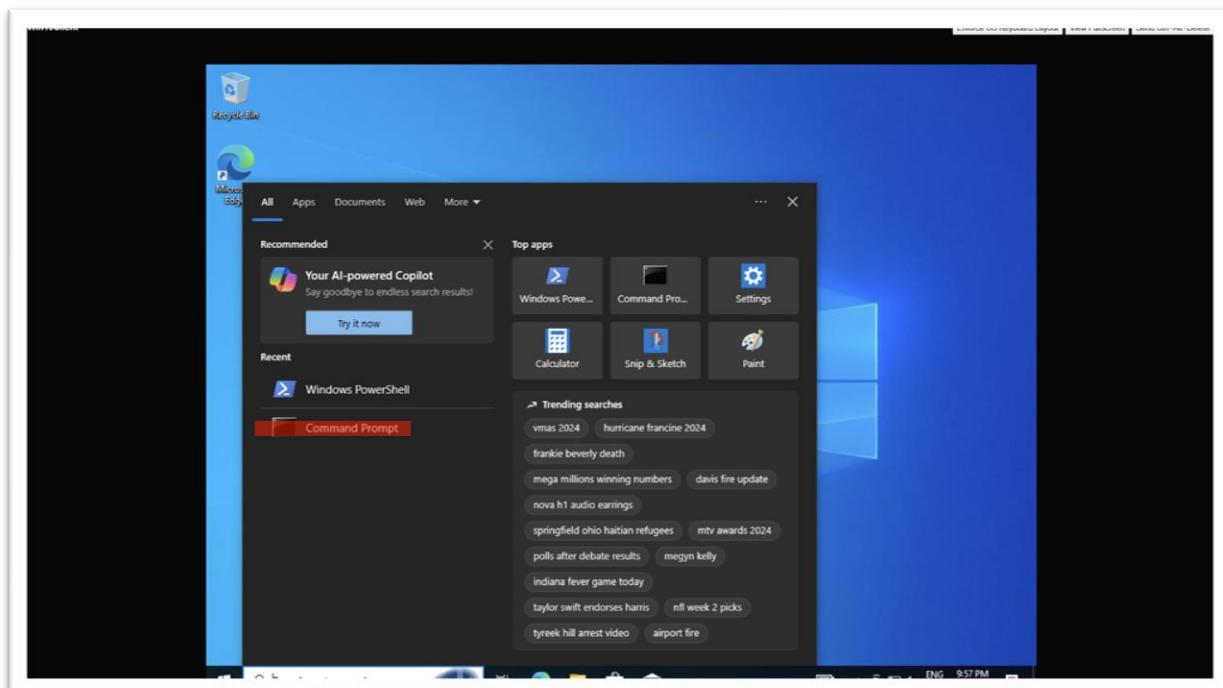


Figure 15: Screenshot of “Command Prompt” search on Windows 10

- The first command we write is – ipconfig (as highlighted below) which is used to display information about our network configuration and DNS settings. So, by entering the command, we get our IP Address, Subnet Mask, and default Gateway.

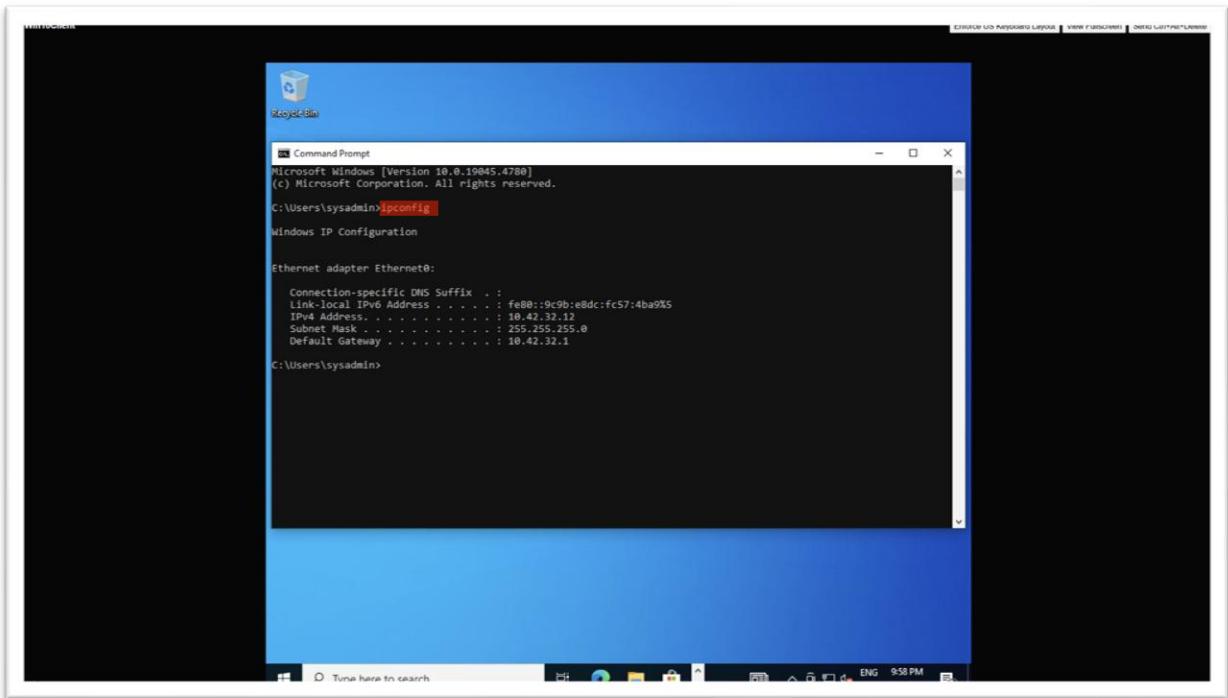


Figure 16: Screenshot of “ipconfig”

- Then ping the corresponding default gateway IP: 10.42.<X>.1 and 10.43.<X>.1 (as shown below) where <X> is the vSphere team number which is 32 in my case.

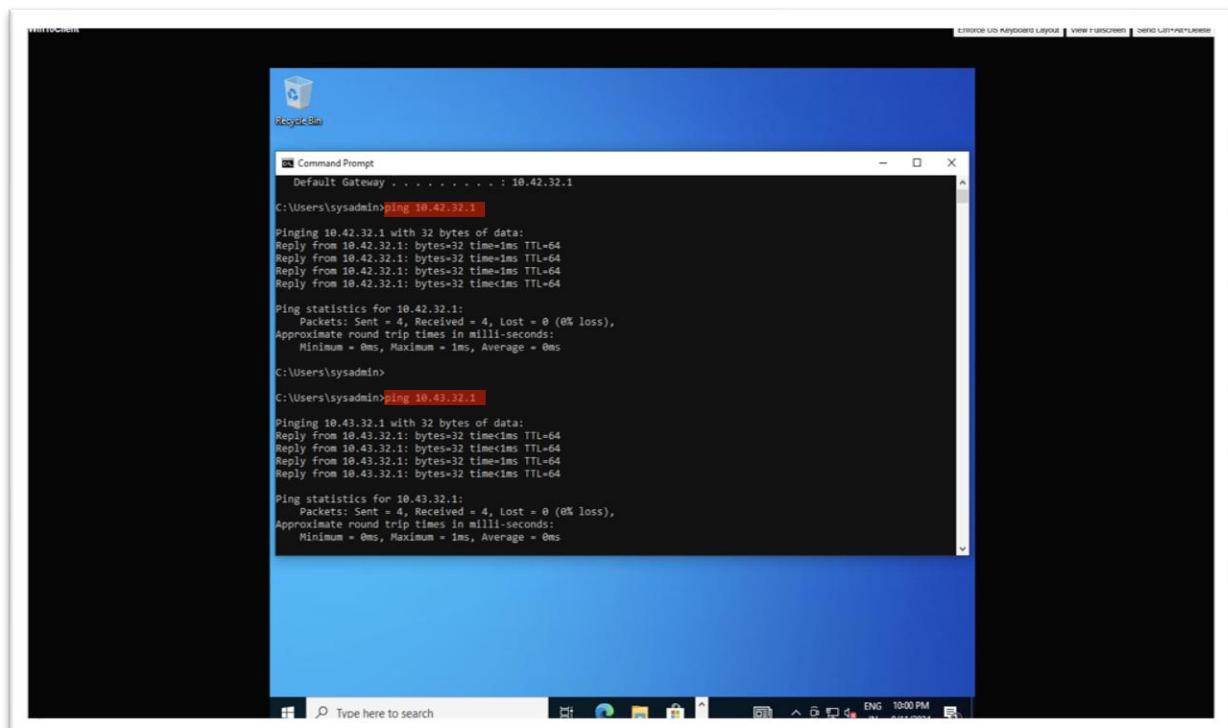


Figure 17: Screenshot of ping both Default Gateway

- Then ping the Gretzky Enterprise gateway IP: 192.168.254.254 as highlighted below.

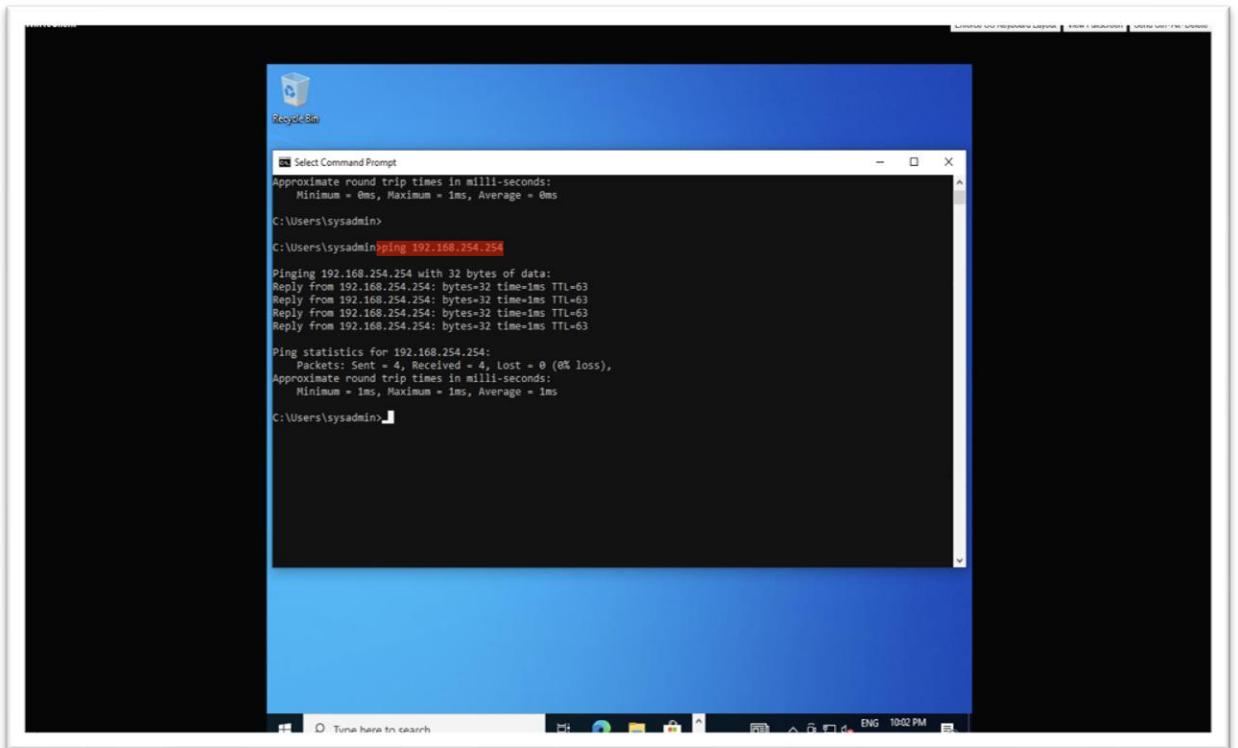


Figure 18: Screenshot of ping Gretzky Enterprise Gateway

- Now ping Google DNS IP: 8.8.8.8 .

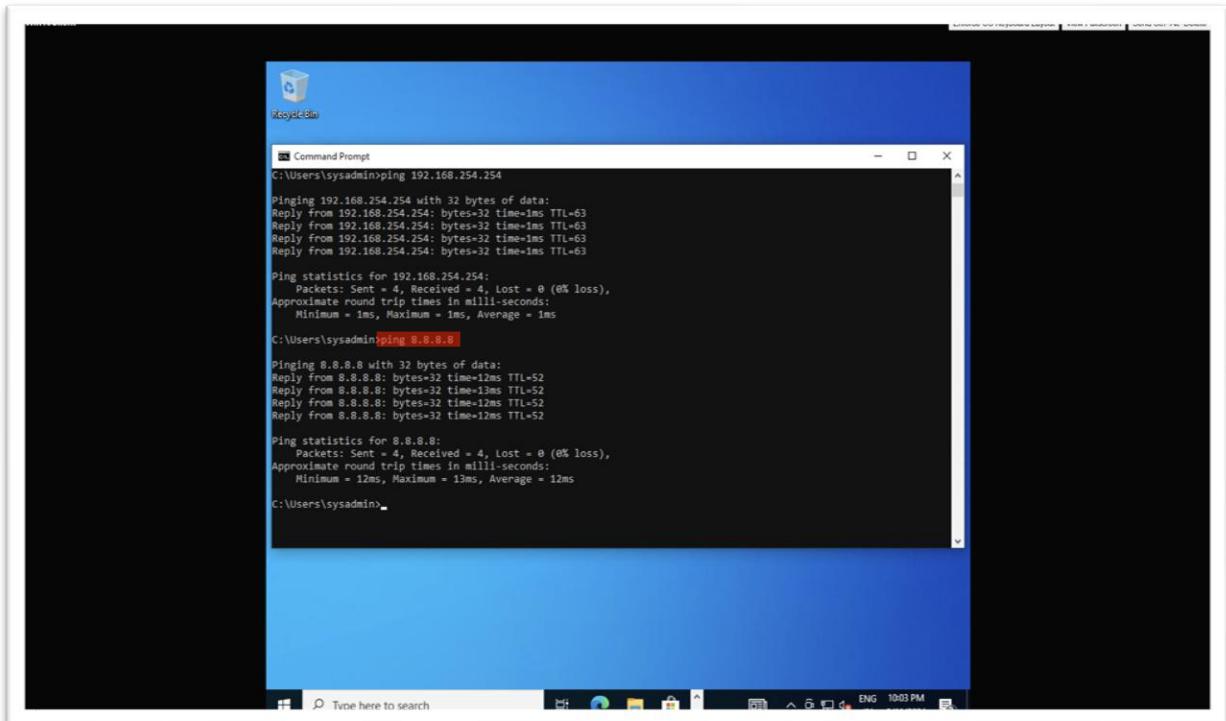


Figure 19: Screenshot of ping Google

- And ping Google DNS domain: dns.google as highlighted below .

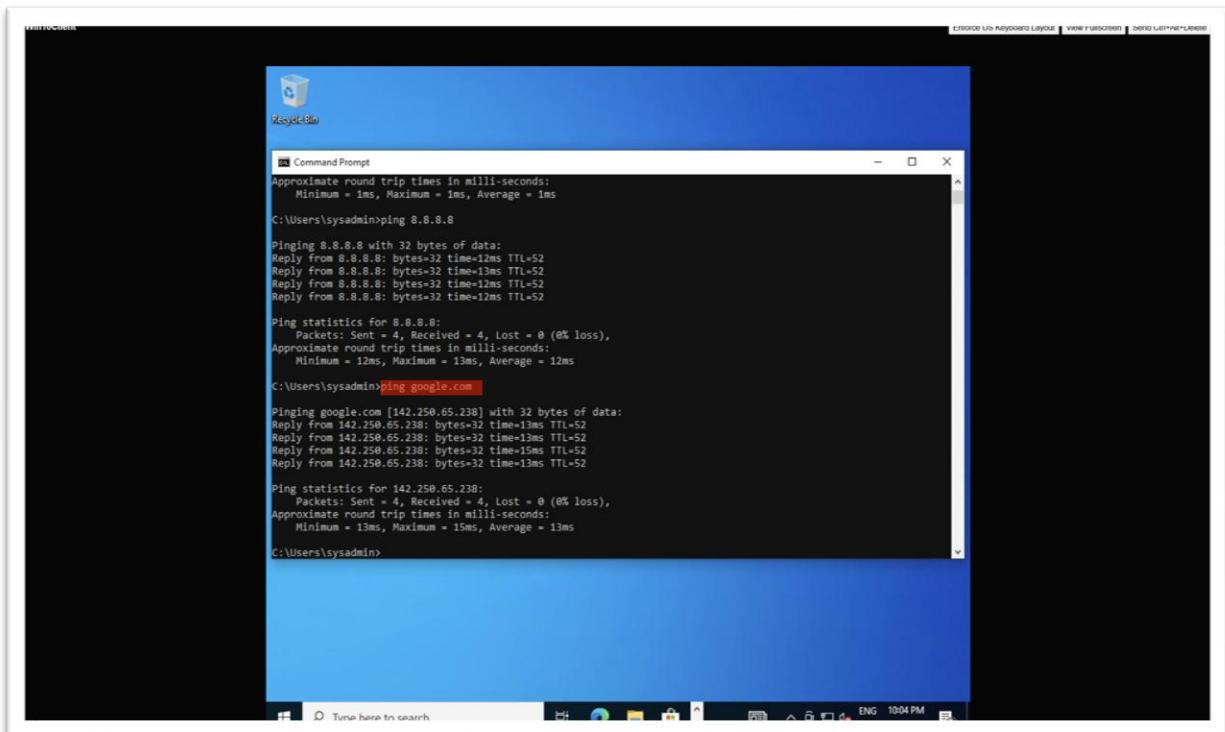


Figure 20: Screenshot of ping Google DNS Server

- Now navigate to any website which showcase our IP address like in below and note down your IPv4.

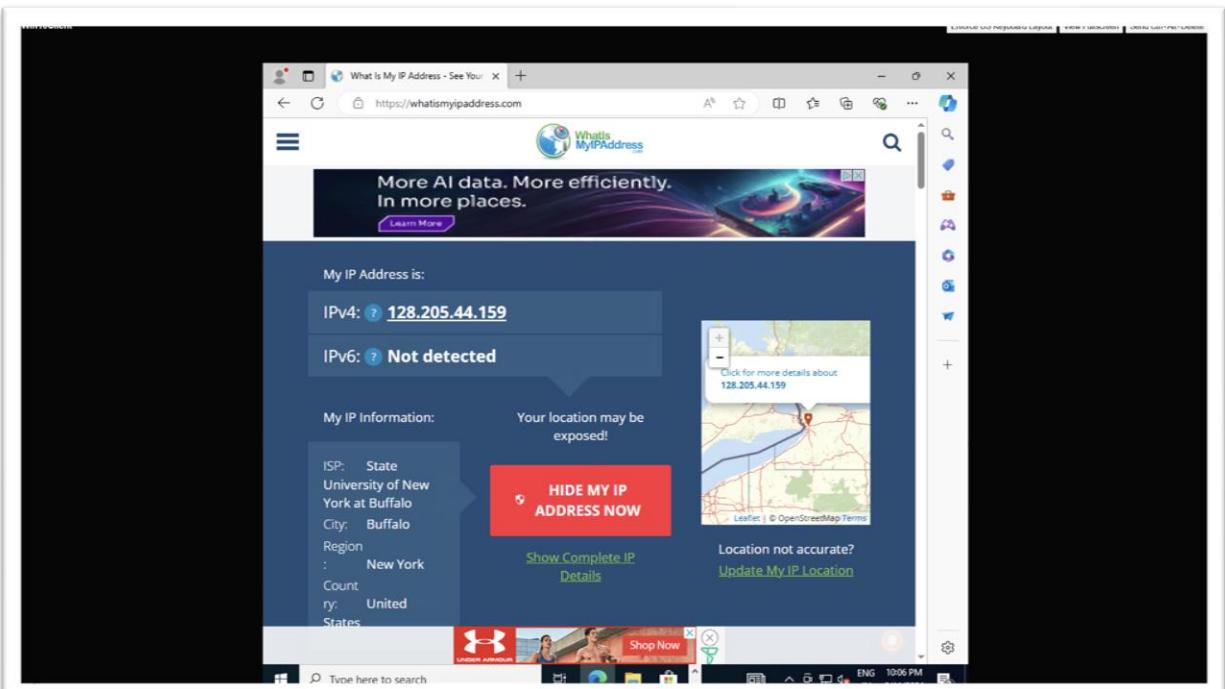


Figure 21: Screenshot of IP Address

## 4. Additional Tasks

- Access our pfSenseRouter web configurator GUI. This can be accessed within our browser from the Win10Client by entering 10.42.X.1 as the URL with “X” being your team number in vSphere.
- The credentials for logging on are: username: admin and password: pfsense  
Note: disable the firewall on pfSenseRouter with pfctl -d.
- Now, change the different interface names to their respective values like for:  
em0: External  
em1: AdminNet  
em2: ServerNet

You can see from below that we change em0 in Figure 22 to External in Figure 23.

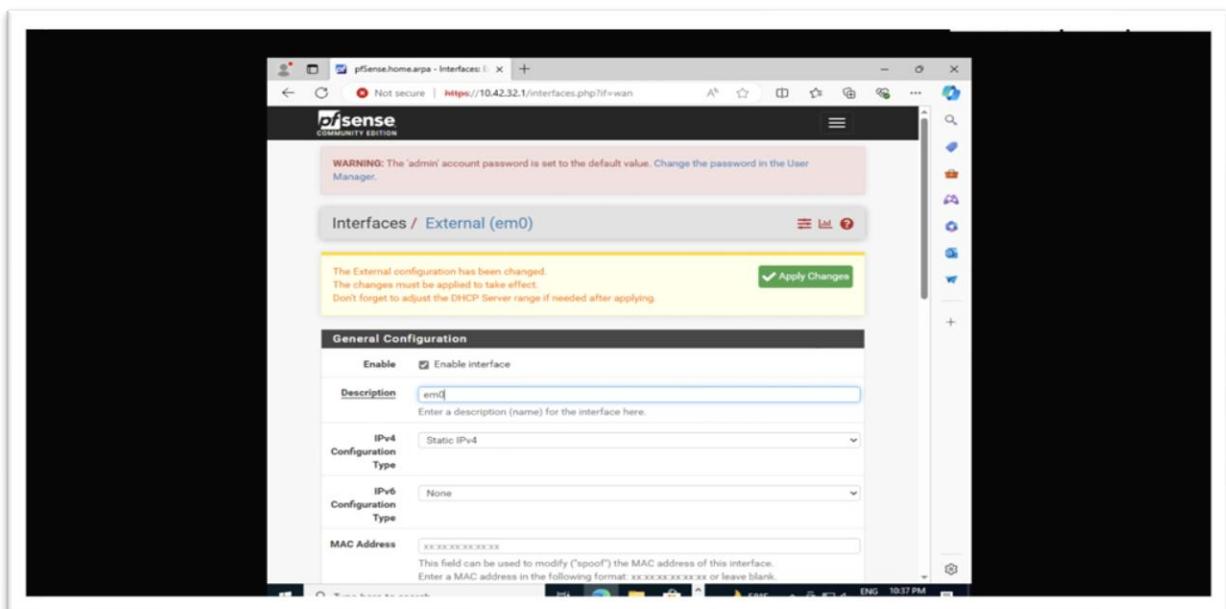


Figure 22: Screenshot of Renaming em0

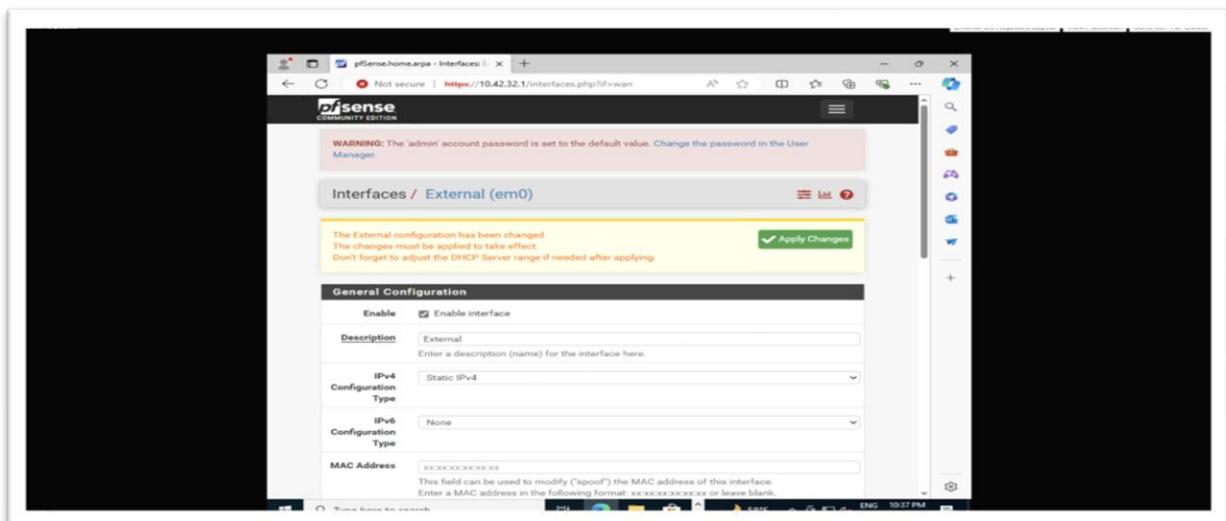


Figure 23: Screenshot of Changing em0 to External

Now repeat the same steps for em1,en2 and renaming it to AdminNet and ServerNet as shown below in figure 24 and 25.

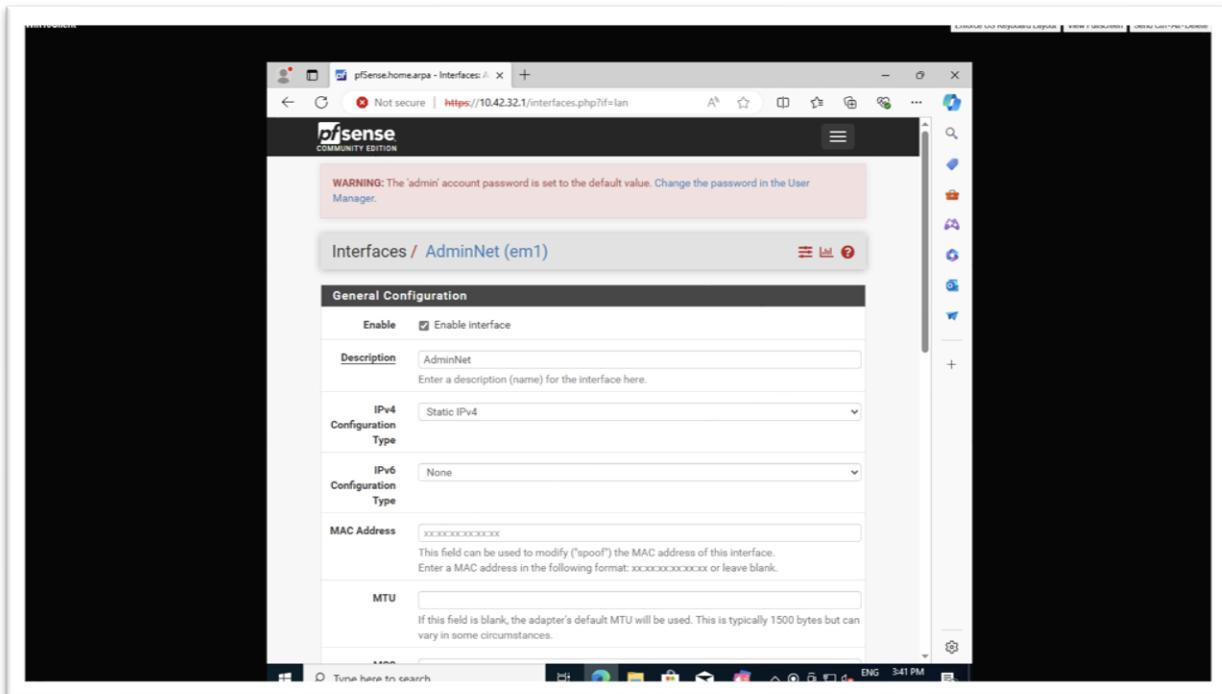


Figure 24: Screenshot of em1 replaced to AdminNet

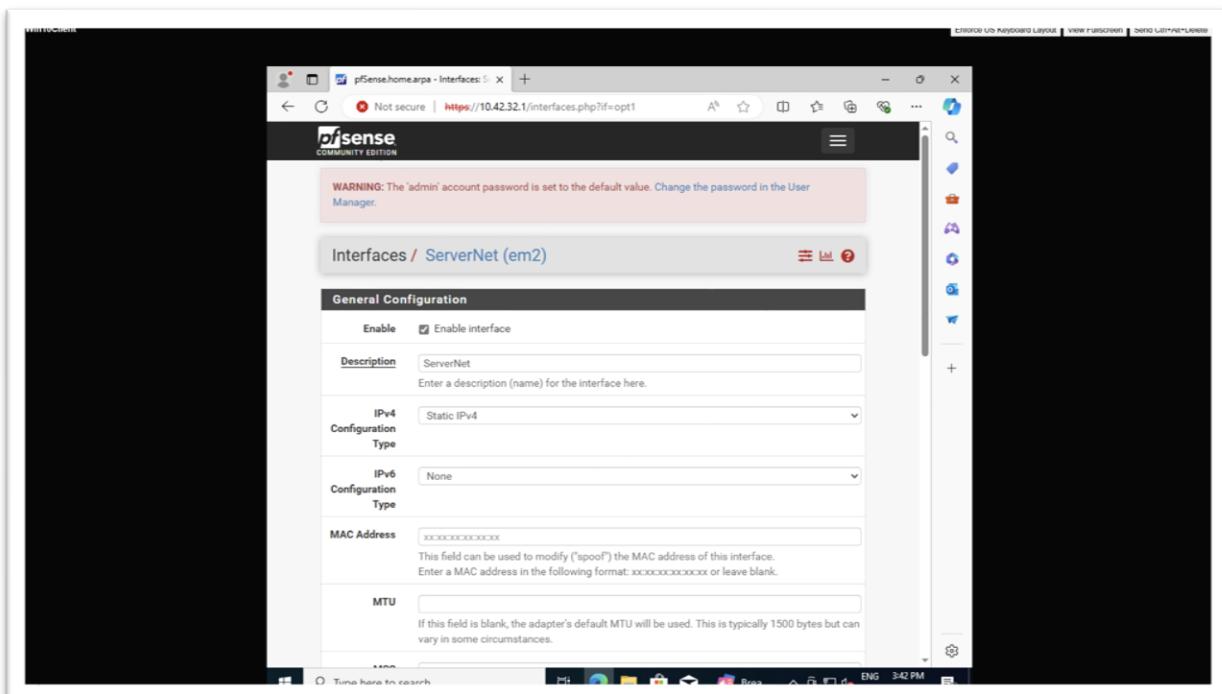


Figure 25: Screenshot of em2 replaced to ServerNet

- Now under system, select the built in package manager to install Suricata to your pfSenseRouter.

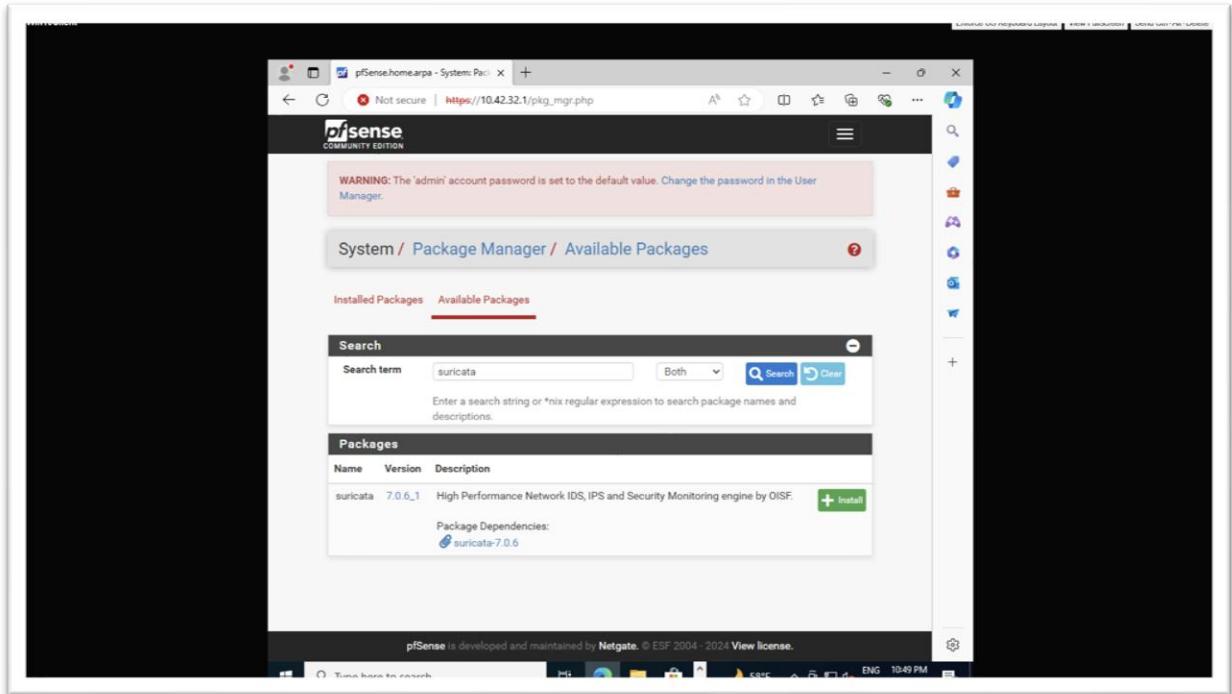


Figure 26: Screenshot of Installation of Suricata

- After that, Suricata can be accessed under the services section after it is installed. Then configure the “captured files retention period” to be 14 days(as highlighted below) under log management.

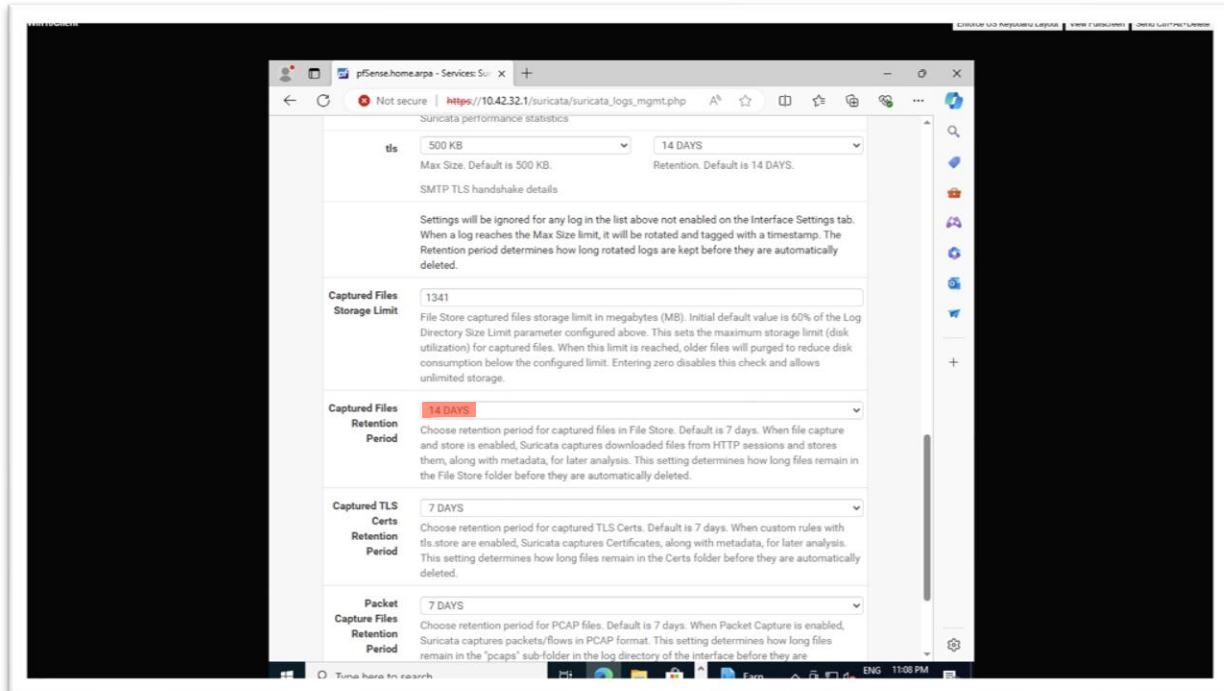


Figure 27: Screenshot of “Captured Files Retention Period”

- Lastly, add an interface by clicking “ADD” and save External (em0) device.

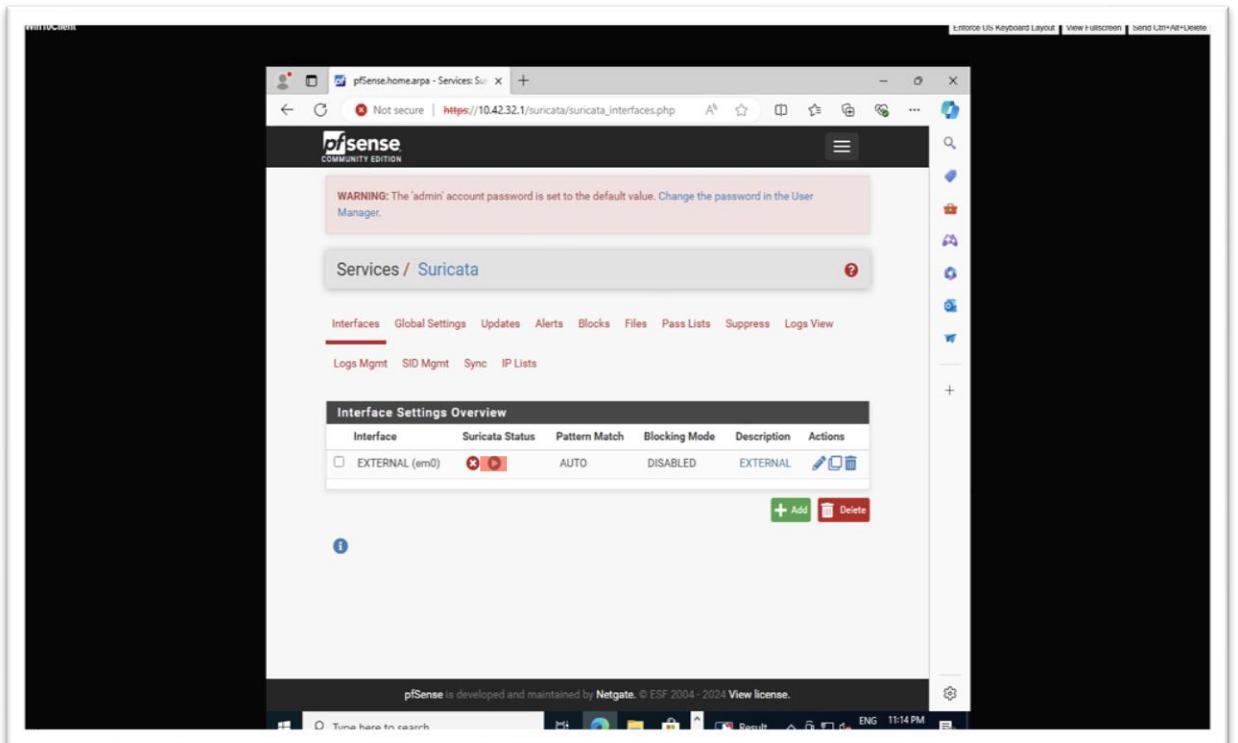


Figure 28: Screenshot of Suricata Run Service

- Then, press the play button highlighted above to turn on Suricata in pfSenseRouter.
- This will happen after turning it on. (watch figure 29)

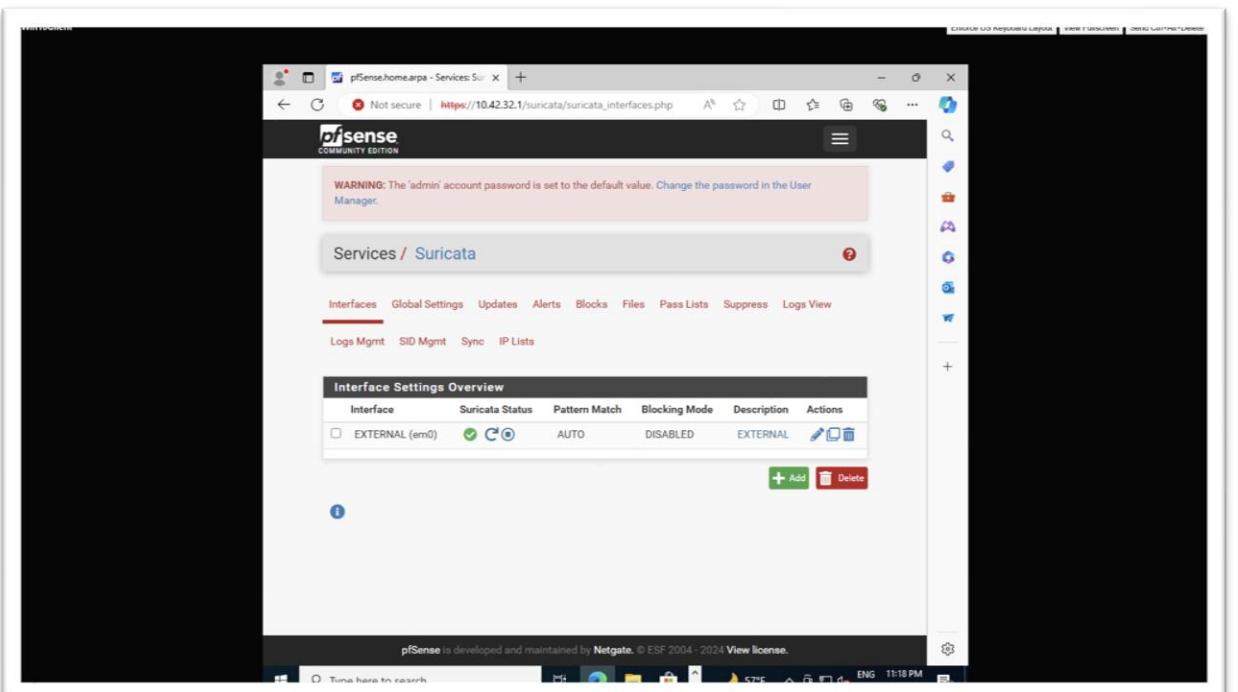


Figure 29: Screenshot of Suricata running

## 5. Appendix A- Developing a Topology

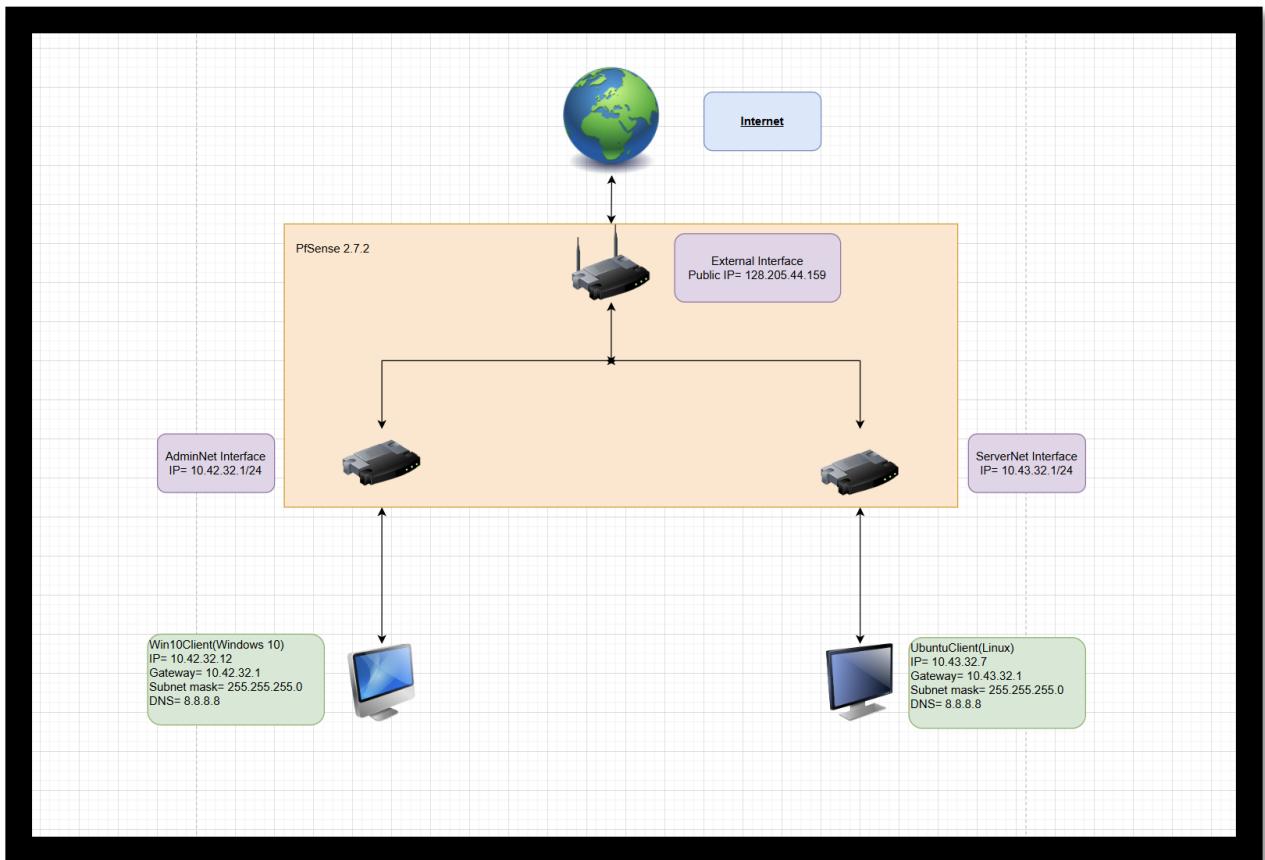


Figure 30: Screenshot of The Topology

- In the above Topology, for Network Device, there are three different interfaces in this network devices:
  - External Interface- connected to Internet
  - AdminNet Interface
  - ServerNet Interface
- Now, for Endpoint Devices, there are two devices:
  - Windows Device which is connected to AdminNet Interface.
  - Linux Device which is connected to ServerNet Interface.

## Appendix B- Complete External Topology

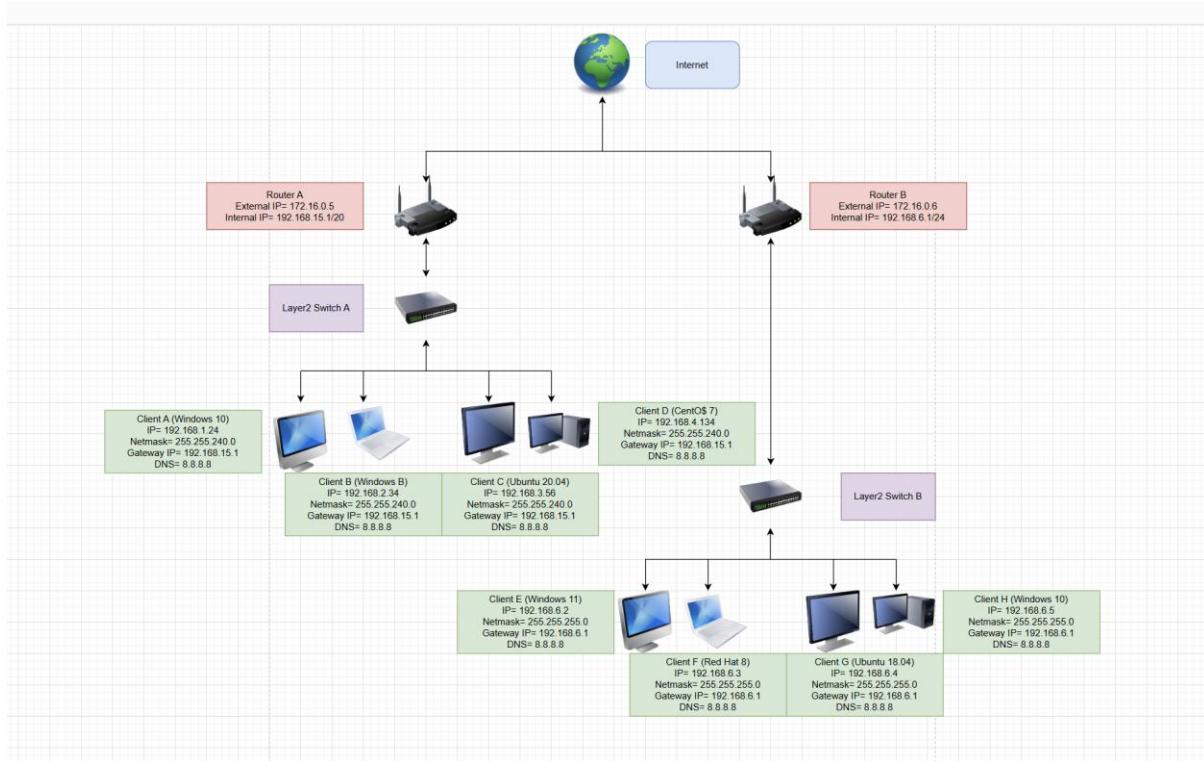


Figure 31: Complete External Topology