Jason Hodge

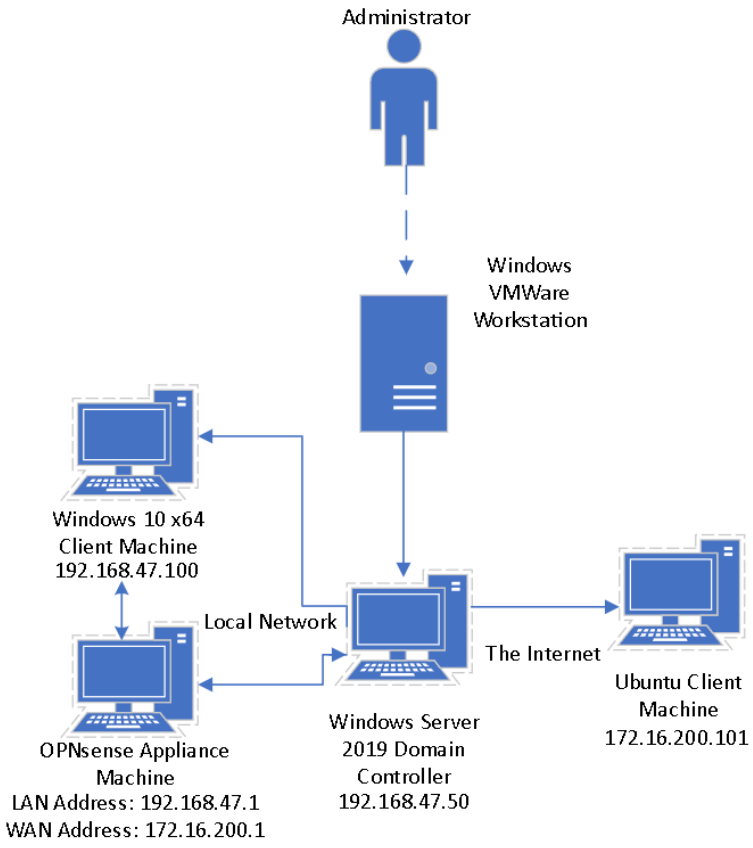
Lab 02 – Your First Pseudo VNF

March 8, 2024

Description:

The primary objective of this lab was to set up an OPNsense virtual machine (VM) and connect it to our existing network of VM's from our previous lab. In doing so I configured the OPNsense appliance accordingly with my existing Windows 2019 Server VM, Windows 10 Client machine, and Ubuntu machine. I set up two different subnets, an internal LAN, and an external WAN. The Windows Server and Client machines stayed on the LAN and the Ubuntu machine moved to the WAN. I configured the proper network configurations and set up the DHCP, NAT, and performed an SSH on the OPNsense machine from my Windows Client. Then I ensured they were all able to communicate with each other when applicable.

Topology:



This is a basic overview of the four virtual machines built in this lab within VMWare Workstation and how they connect with each other.

Key Syntax:

OPNsense:

Username: root or installer

Password: opnsense

Commands:

‘ipconfig /all’: Provides full detailed adapter configuration information (IPv4 address, subnet mask, default gateway, DNS Servers, etc.)

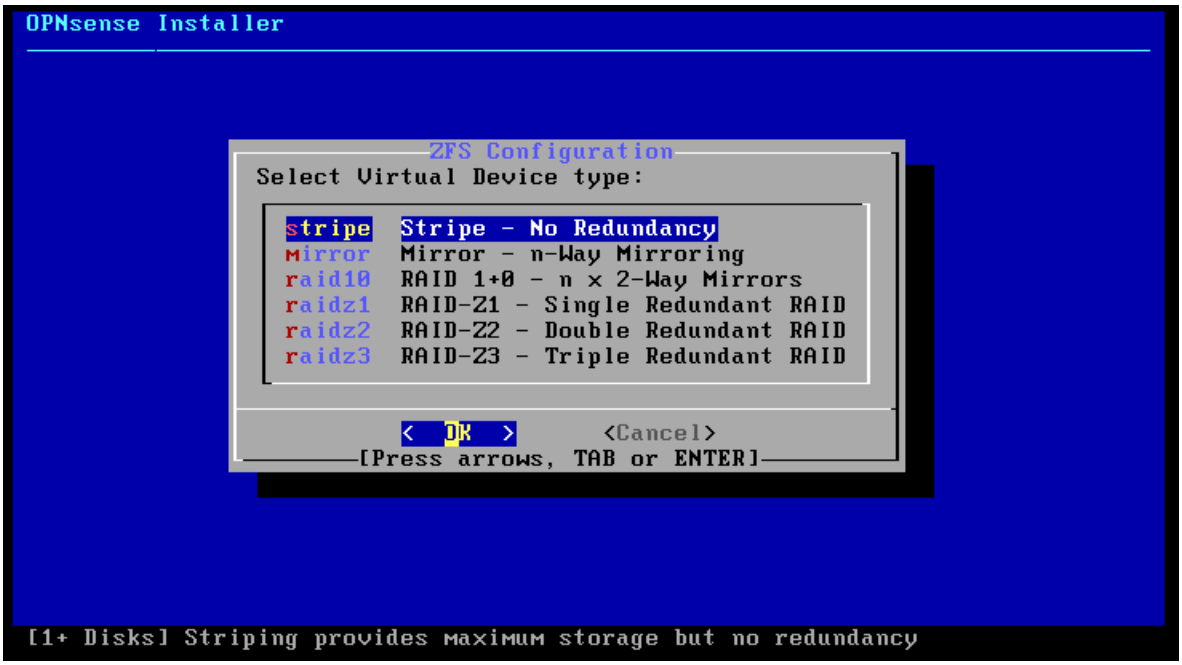
‘Shell command uname -a’: Displays the machine ID, name of the node, OS release number, the system name, and the OS version.

Verification:

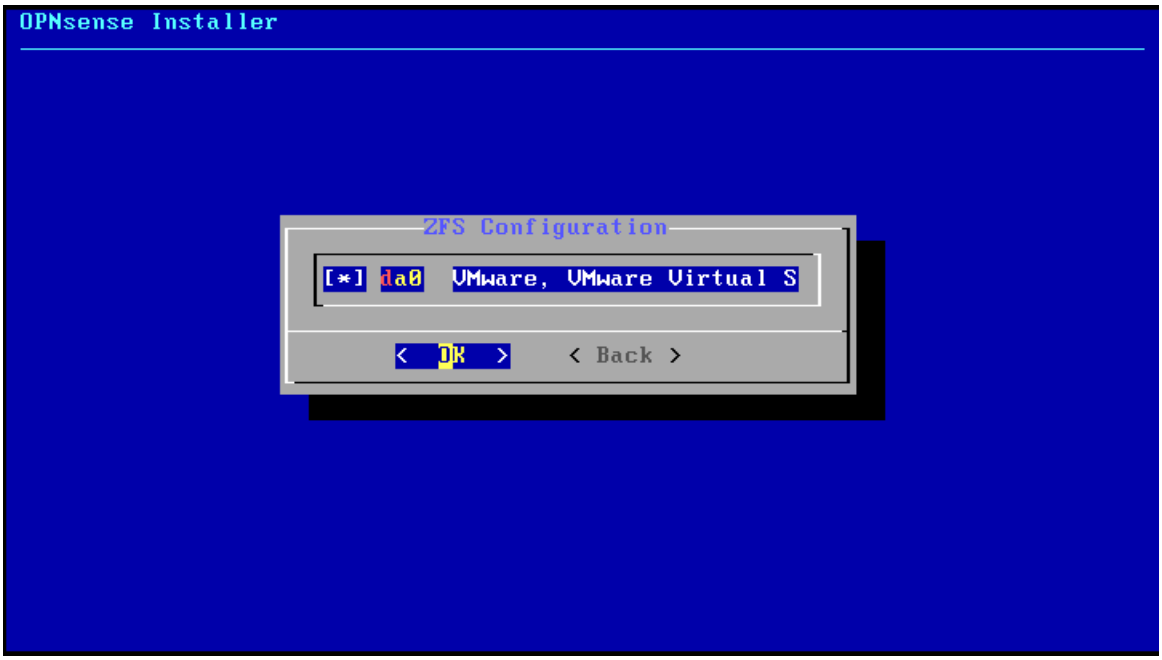
TASK ONE: OPNsense Installation

My OPNsense Appliance VM is up and running.

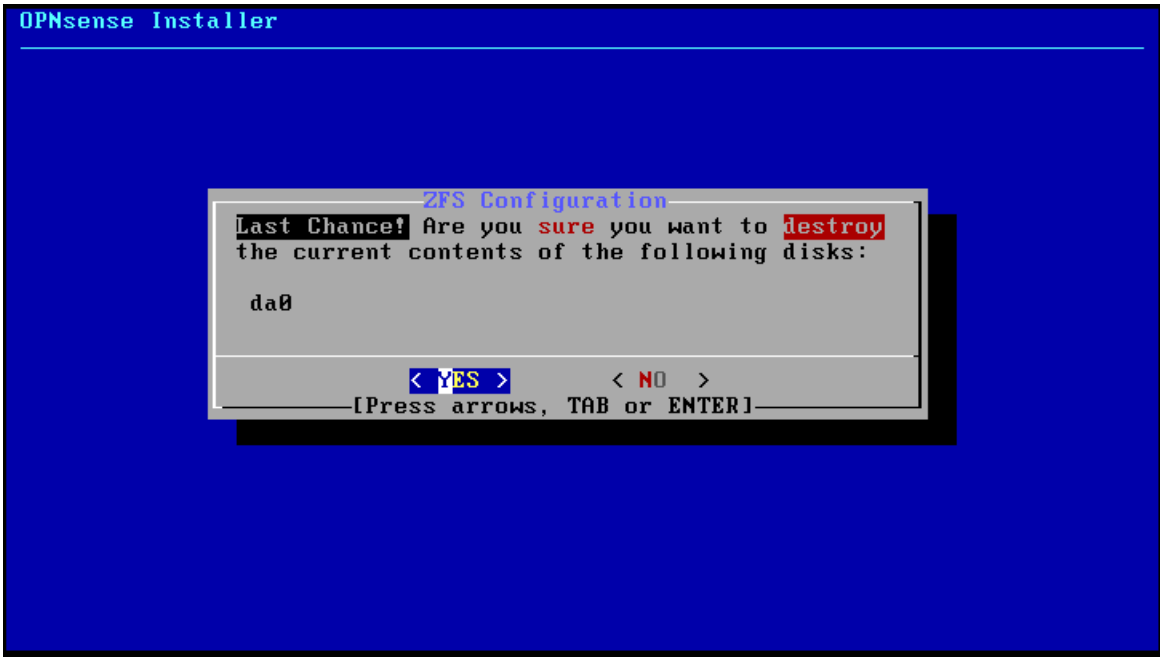
First, I clicked to install ZFS. ZSF is a file system manager that provides data integrity.



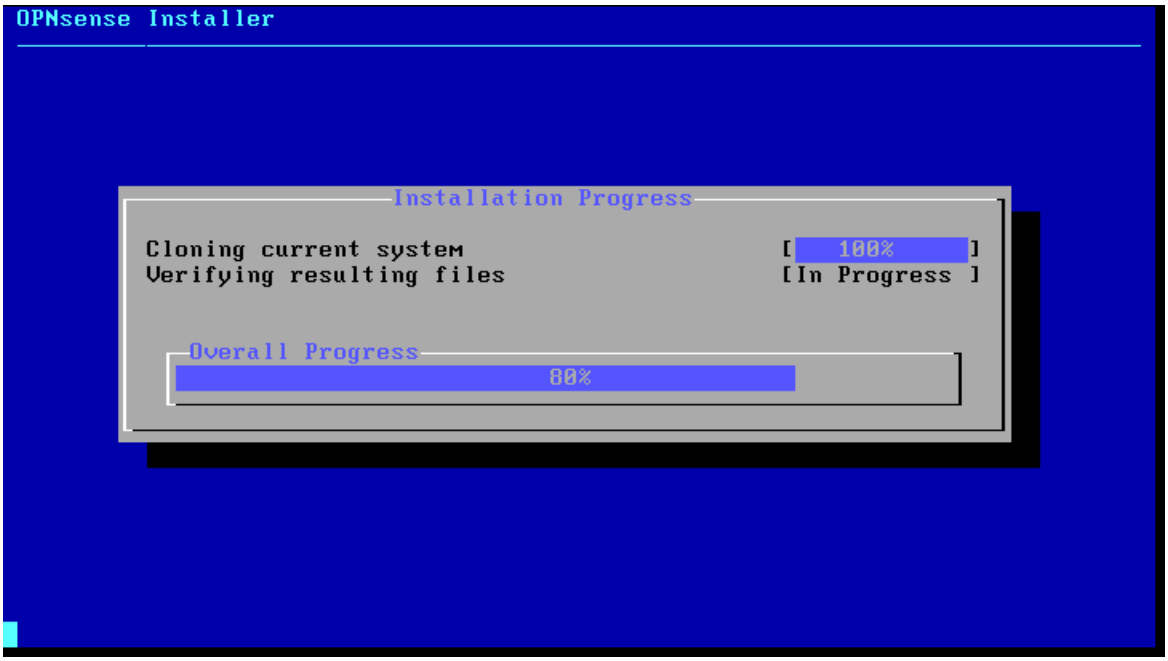
The next option I clicked is “Stripe – No Redundancy” which provides faster speed as well as read and write capabilities because there is no data redundancy as we see with mirroring.



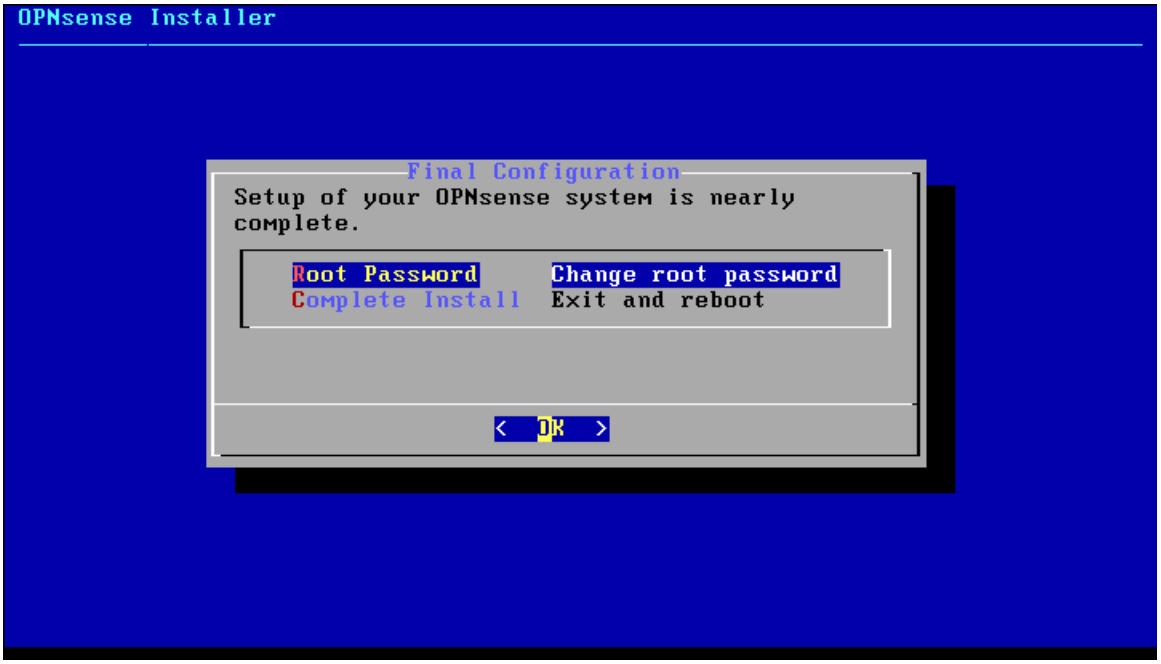
After, I clicked “OK” as there is only one option for where the VM should be stored on the disk.



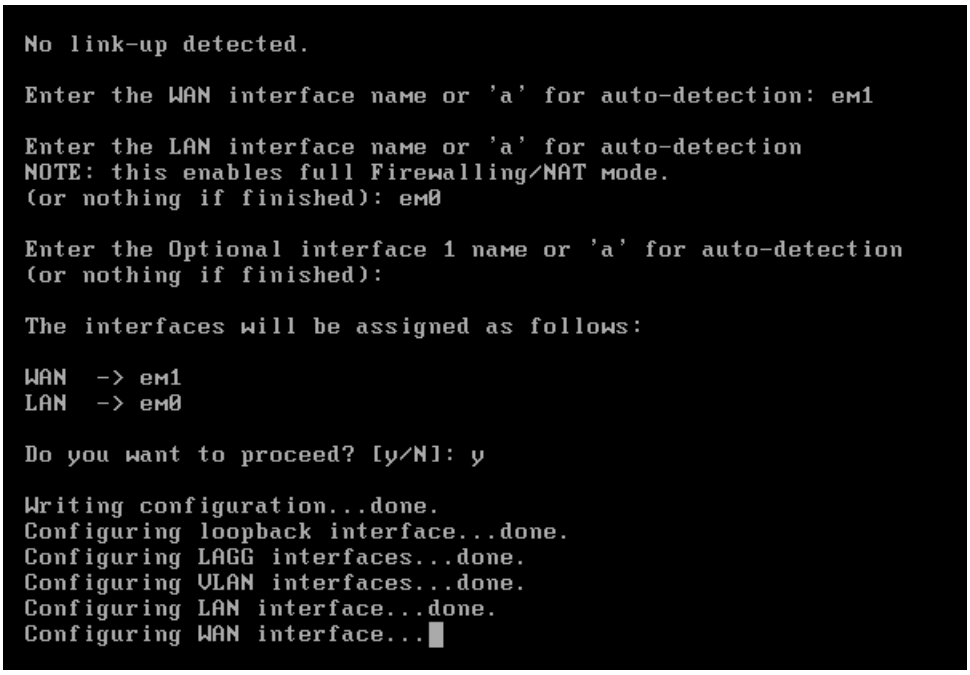
Then, a safety page comes up asking if you are sure you want to destroy any contents on the disk. We click “YES”.



This is the installation of the machine in progress.



Here we can change the root password if we'd like to, but for the purposes of this lab this step was not necessary.



Here I assigned the LAN as em0 and the WAN as em1.

```
  5) Power off system                  12) Update from console
  6) Reboot system                     13) Restore a backup

Enter an option: 2

Available interfaces:

1 - LAN (em0 - static, track6)
2 - WAN (em1 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.47.1


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

I then assigned the IP address subnet 192.168.47.1/24 for the LAN.

```
 HTTPS: SHA256 30 1D BF 10 8B 0F 58 29 AF ED 0F 80 75 0D EF DD
              05 7F 65 A2 D8 14 D1 D7 13 F3 02 78 36 A0 90 5C

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 2

Available interfaces:

1 - LAN (em0 - static)
2 - WAN (em1 - dhcp, dhcp6)

Enter the number of the interface to configure: 2

Configure IPv4 address WAN interface via DHCP? [Y/n] n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.16.200.1
```

Option 2 needs to be selected in order to assign and edit the interfaces.

```
1 - LAN (em0 - static)
2 - WAN (em1 - dhcp, dhcp6)

Enter the number of the interface to configure: 2

Configure IPv4 address WAN interface via DHCP? [Y/n] n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.16.200.1


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? [Y/n] n
```

Next, I needed to assign the WAN the subnet IP address 172.16.200.1/24.

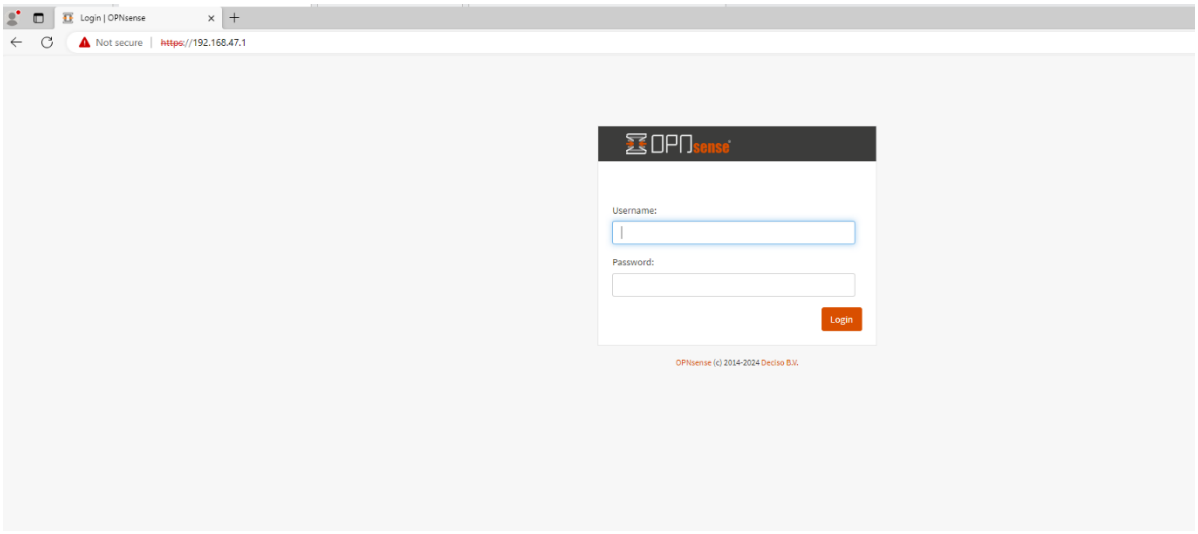
```
Generating /etc/resolv.conf...done.
Generating /etc/hosts...done.
Configuring WAN interface...done.
Setting up routes for wan...done.
Starting Unbound DNS...done.
Configuring firewall.......done.


*** OPNsense.localdomain: OPNsense 24.1 ***

 LAN (em0)       -> v4: 192.168.47.1/24
 WAN (em1)       -> v4: 172.16.200.1/24

 HTTPS: SHA256 30 1D BF 10 8B 0F 58 29 AF ED 0F 80 75 0D EF DD
               05 7F 65 A2 D8 14 D1 D7 13 F3 02 78 36 A0 90 5C

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

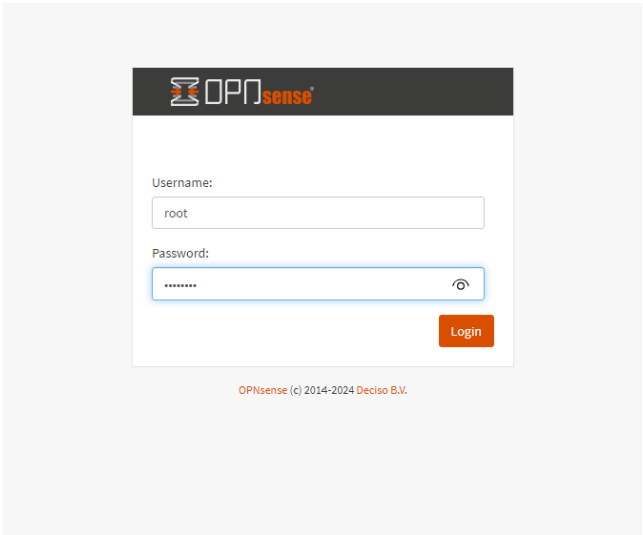
We can now see the LAN and WAN have their proper subnet interfaces assigned.

TASK TWO: Lab Environment VNF and VM Configuration

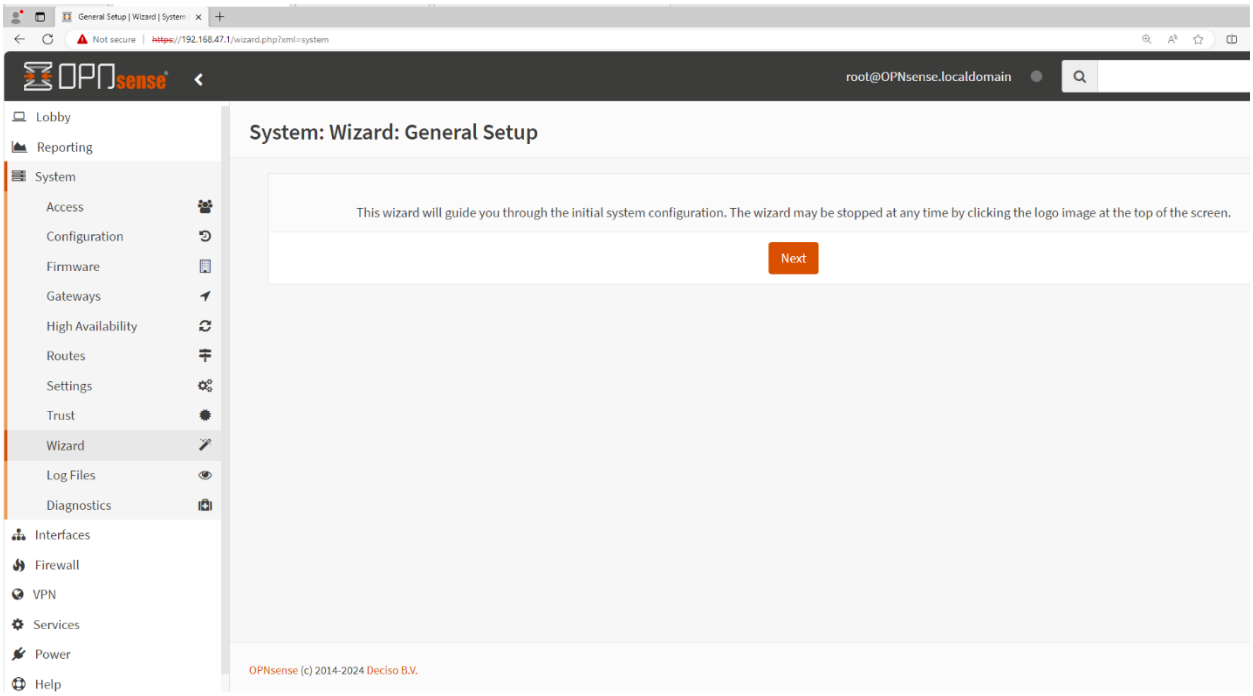
```
C:\Users\Test>ping 192.168.47.1

Pinging 192.168.47.1 with 32 bytes of data:
Reply from 192.168.47.1: bytes=32 time<1ms TTL=64
Reply from 192.168.47.1: bytes=32 time<1ms TTL=64
Reply from 192.168.47.1: bytes=32 time<1ms TTL=64
Reply from 192.168.47.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.47.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Here I pinged the LAN (em0) from my Windows Client machine just to make sure the network is functional.

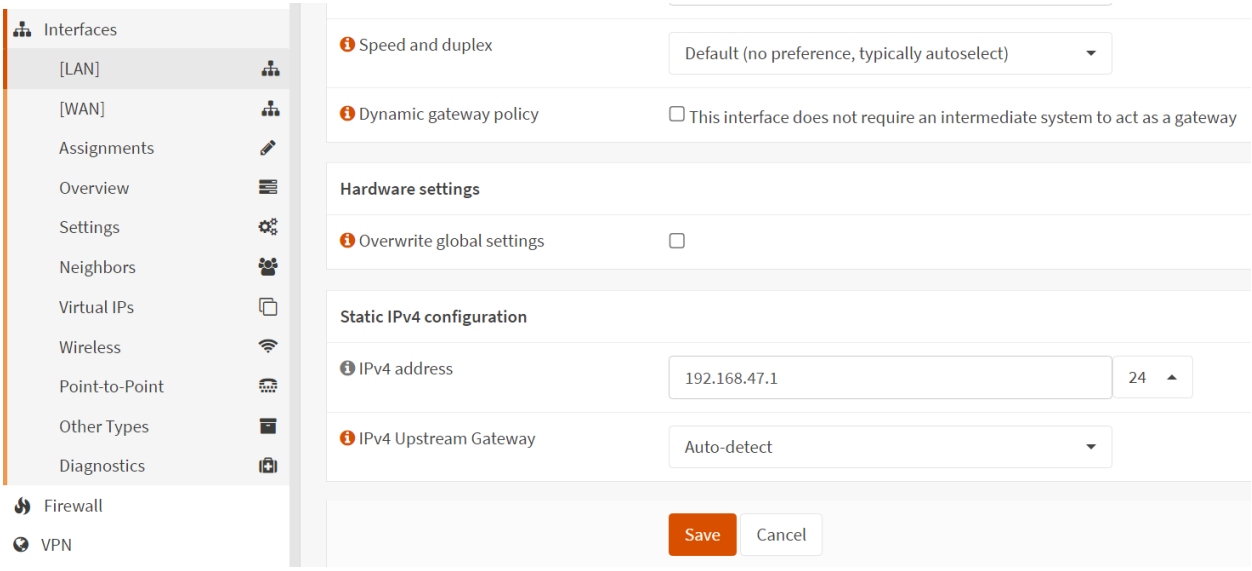




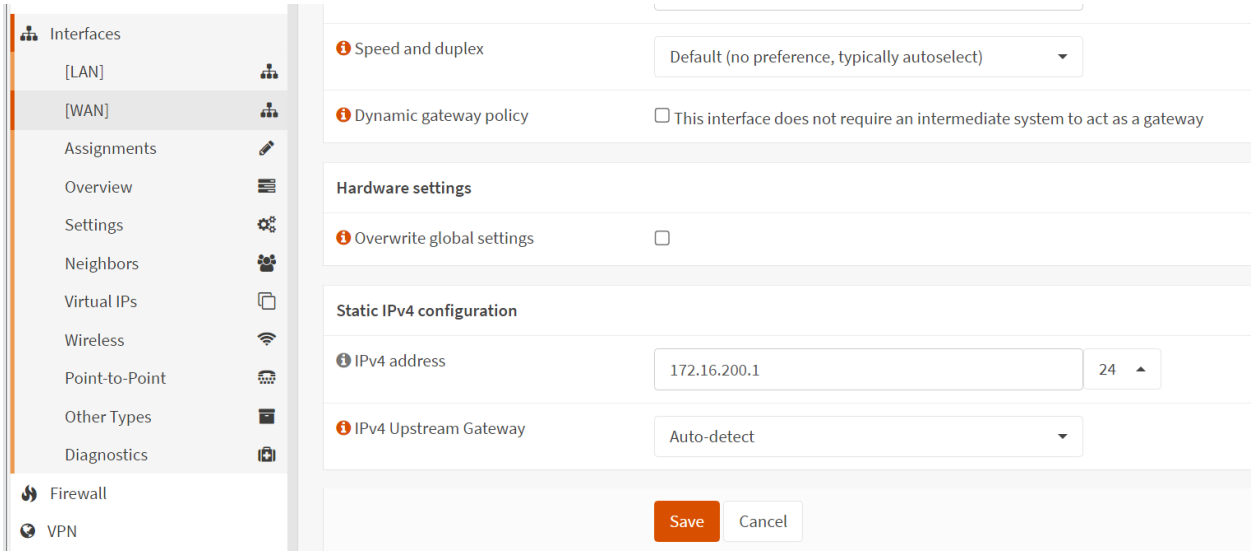
Next I went to the page for the LAN at the address 192.168.47.1 to access the OPNsense GUI.



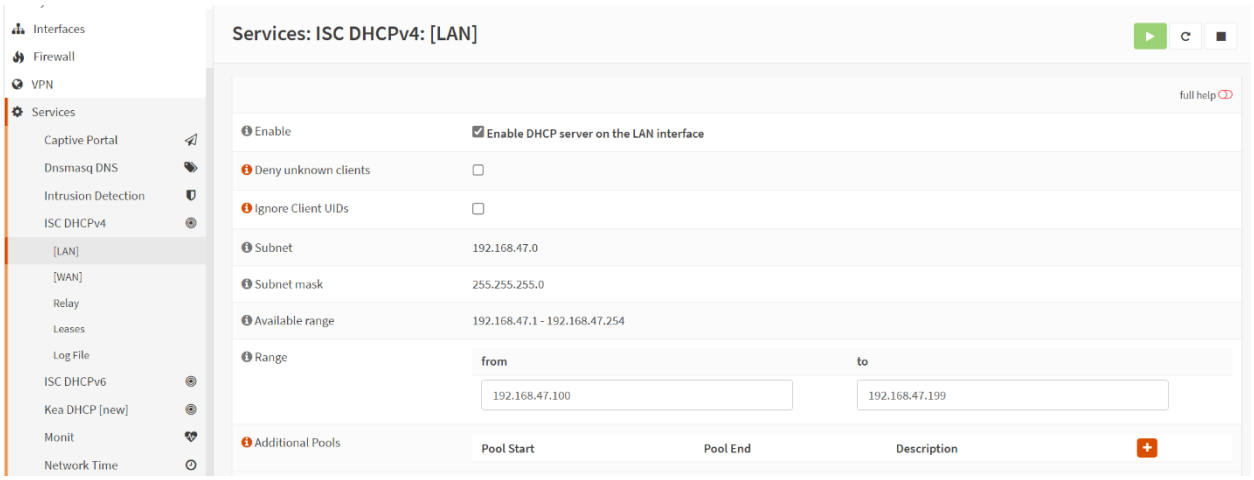
Here is the general system setup wizard.



Here is the configured LAN interface with IPv4 address 192.168.47.1.

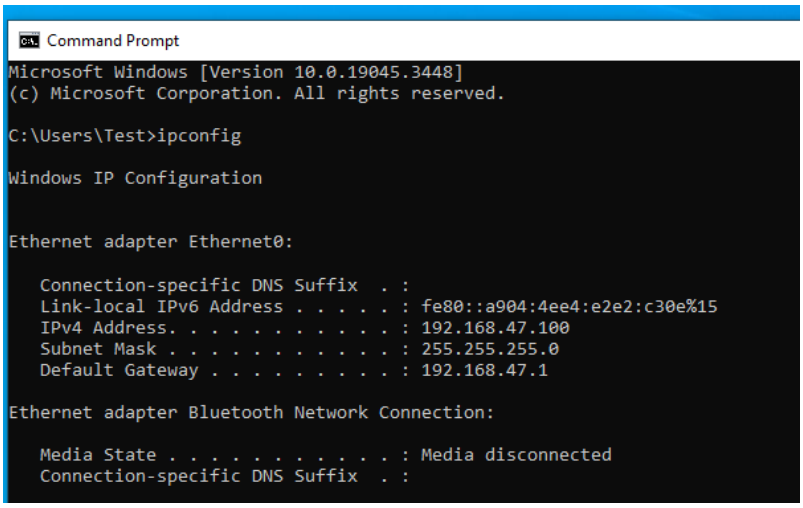


Here is the configured WAN interface with IPv4 address 172.16.200.1.

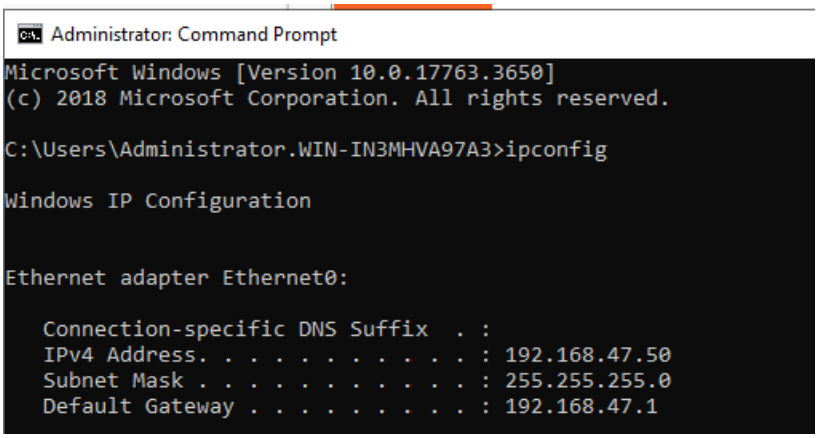


Next, I set up the DHCP LAN service by enabling it and setting the range 192.168.47.100 – 192.168.47.199.

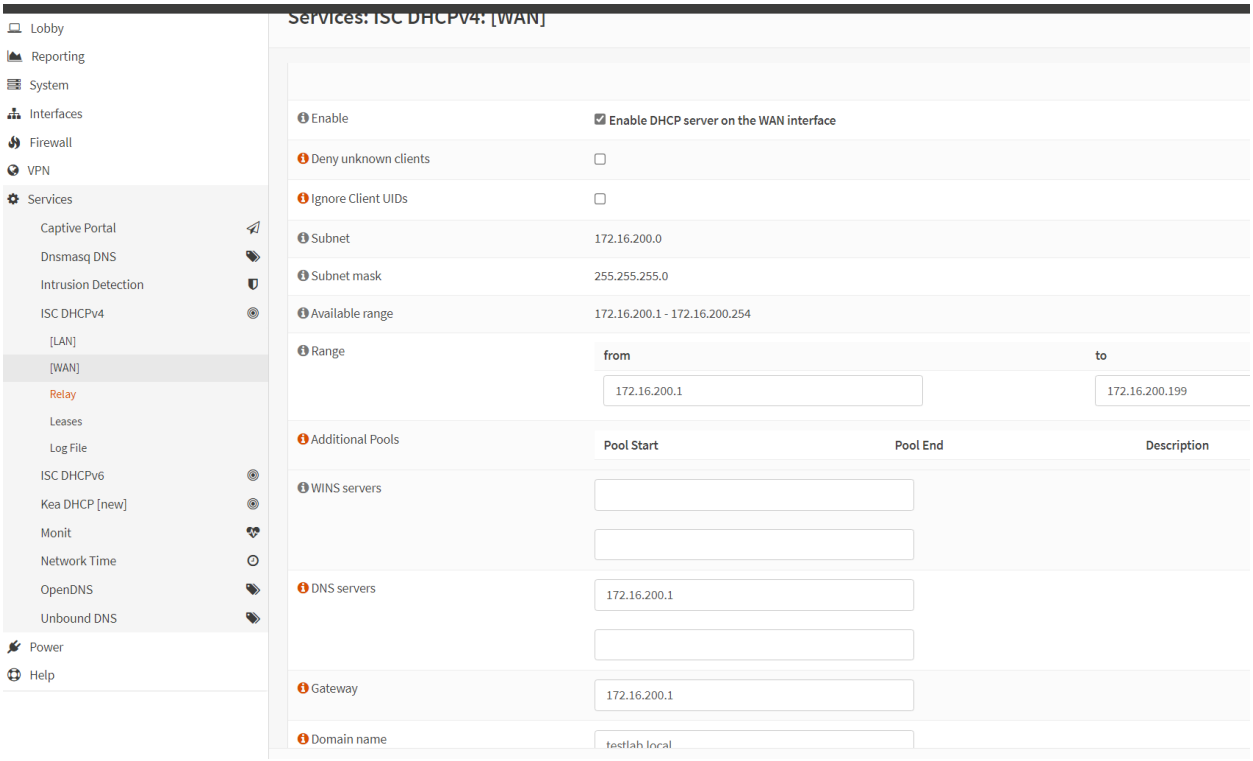
Then I also updated the rest of the relevant LAN information.



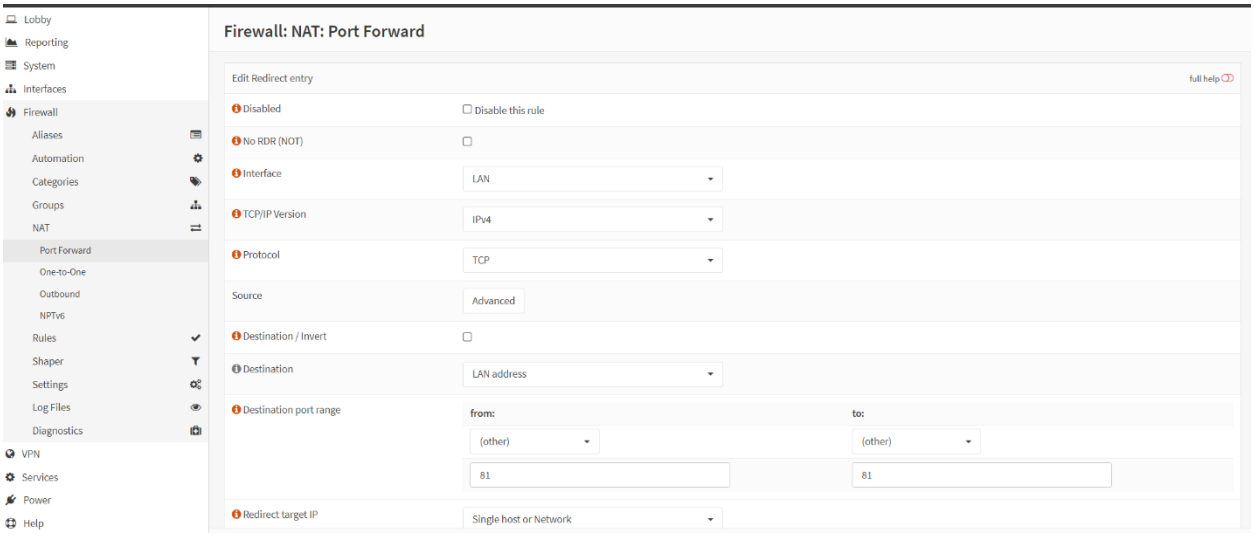
Here we can see the relevant IP configuration information of the Windows Client Machine.



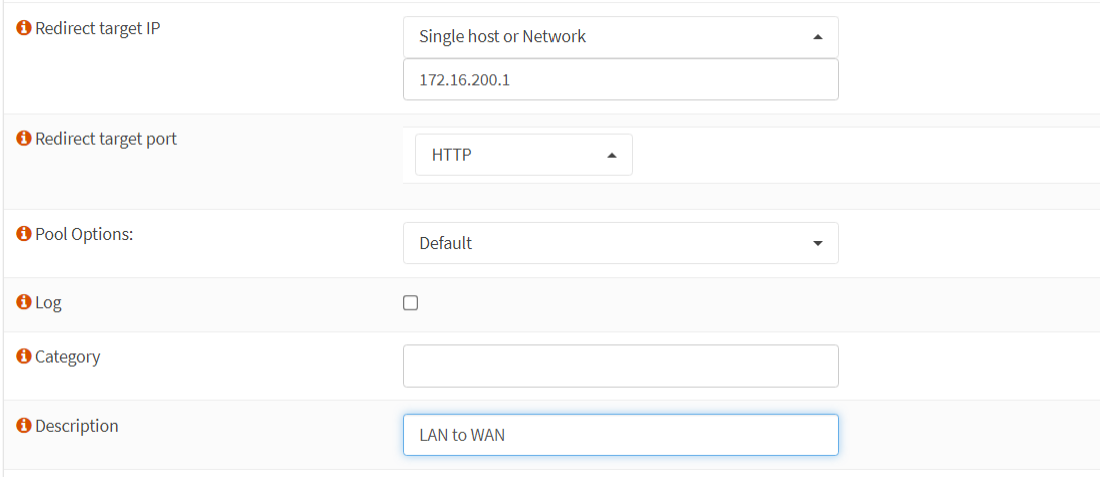
Here we can see the relevant IP configuration information of the Windows Server Machine.



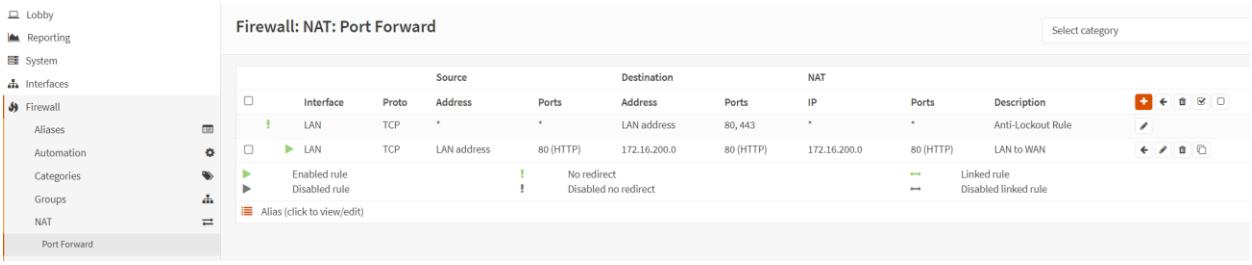
Next, I set up the DHCP WAN service by enabling it and setting the range 172.16.200.1 – 172.16.200.199. I also updated the rest of the relevant WAN information. I completed this part even though there is only one client on this subnet network.



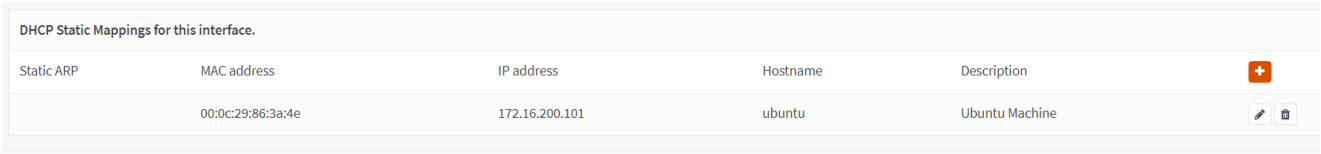
Then I set up a Firewall NAT Port Forward rule to source the traffic from the LAN interface to redirect it to the WAN interface.



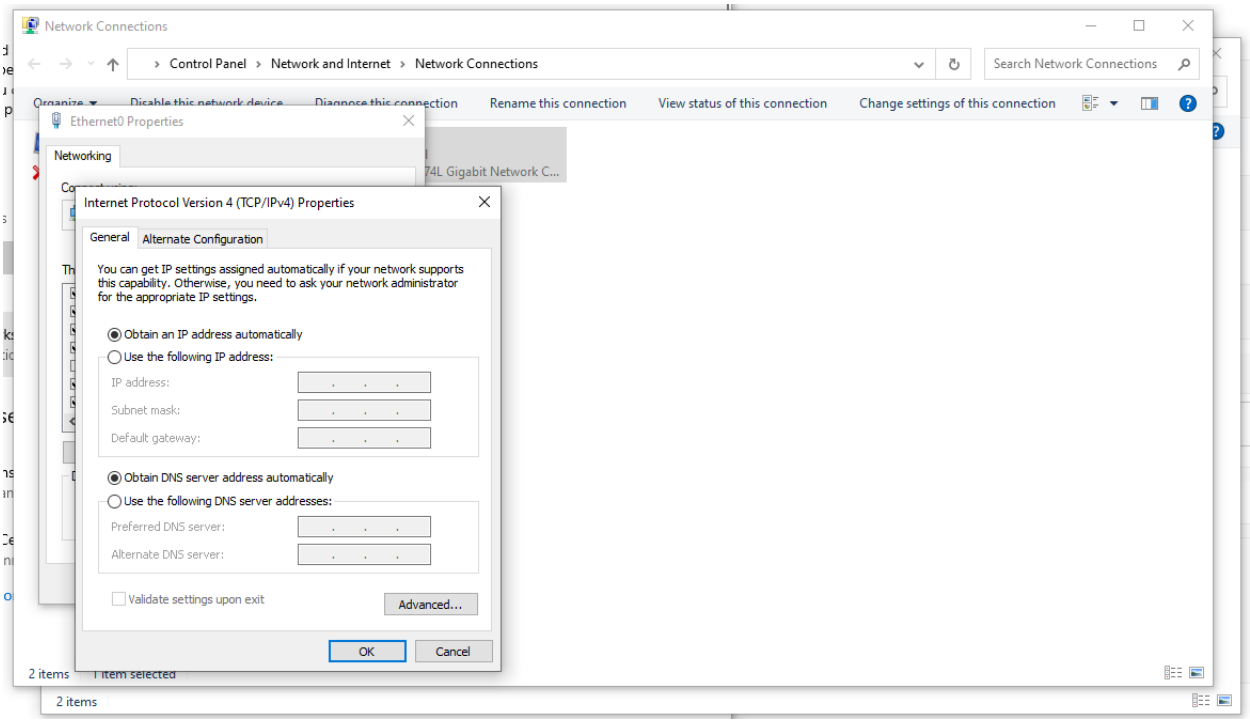
Here we can see the redirect target, our WAN.



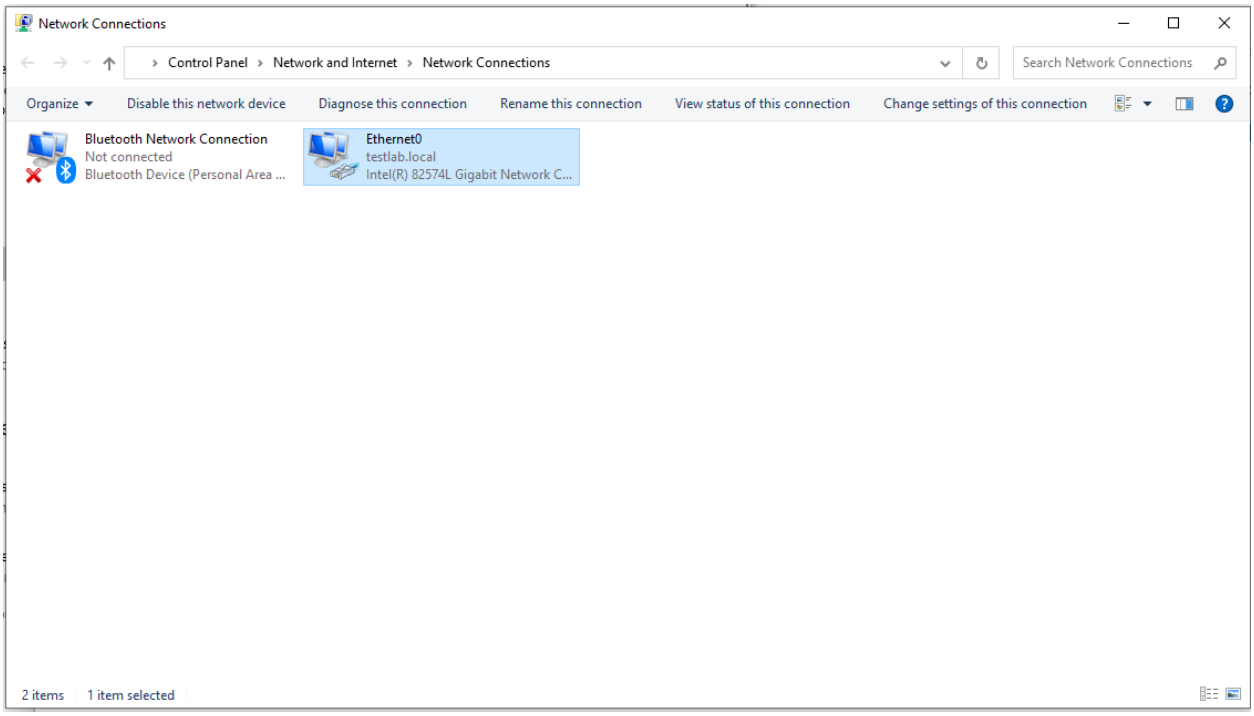
The rule has been created and applied.



I added the Ubuntu Client machine, which is on the WAN network, statically to the DHCP as the IP address 172.16.200.101.



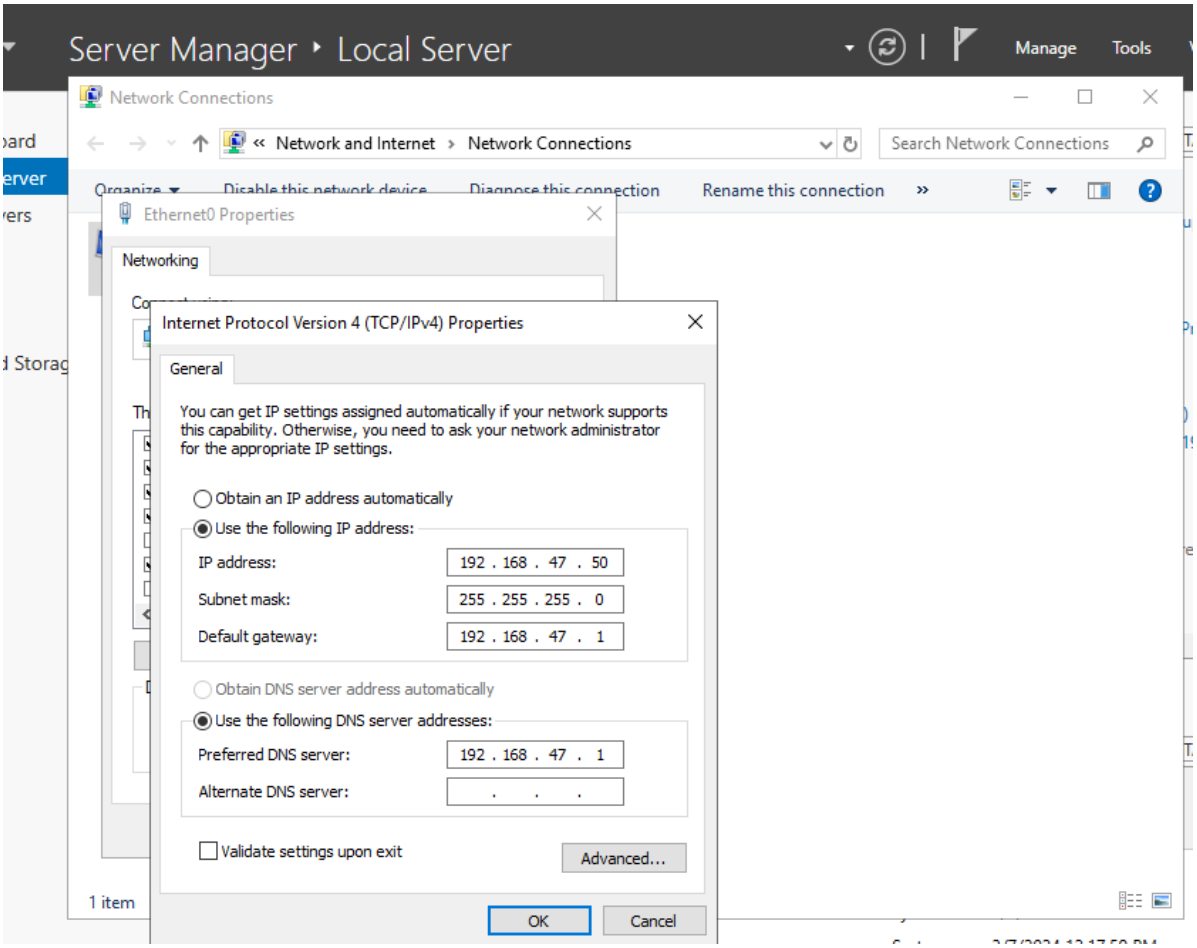
Then I had to verify the windows client can obtain the DHCP address, subnet mask, default gateway, and DNS suffix of testlab.local automatically.



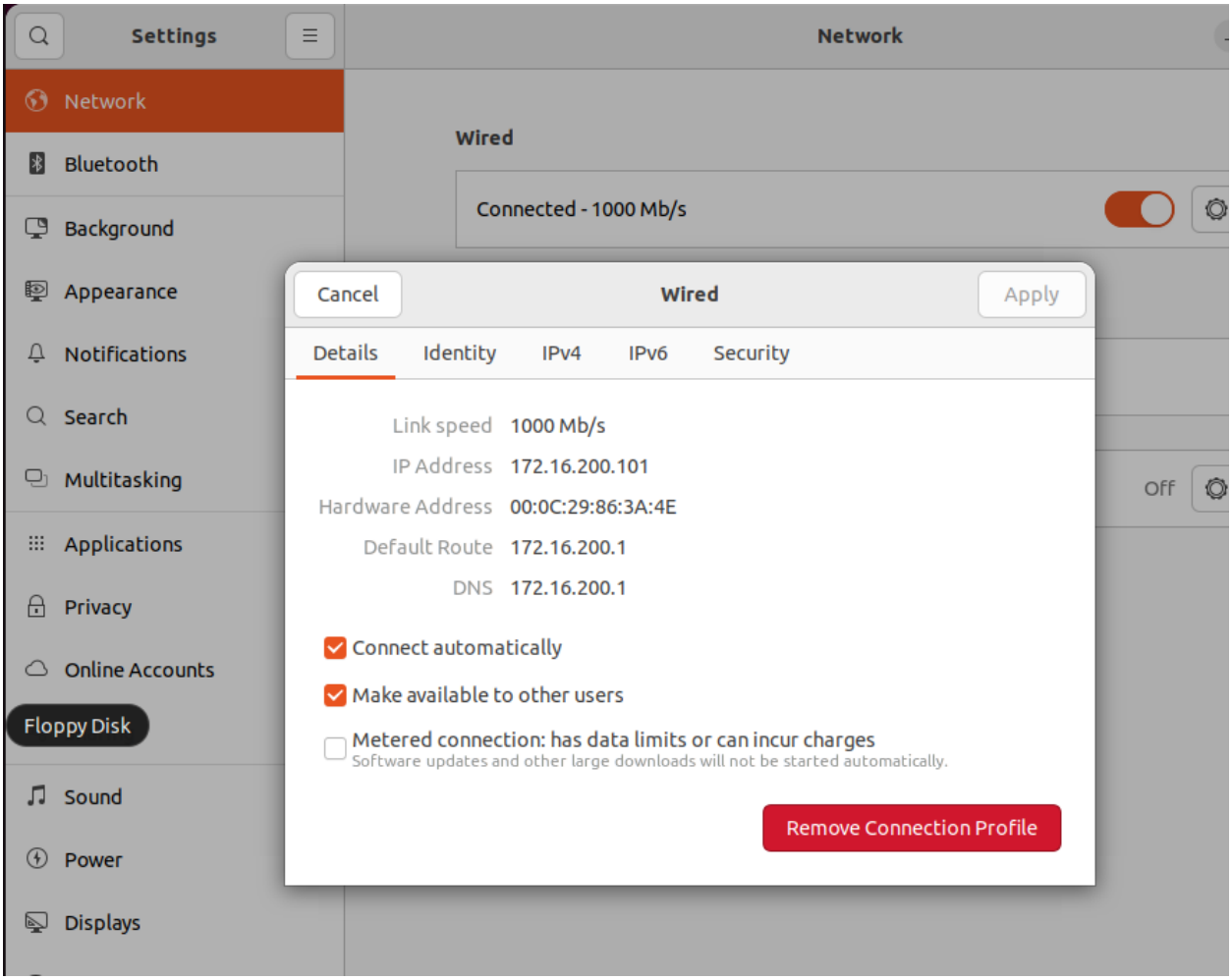
Here we can see it appears to be connected.

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : testlab.local
   Link-local IPv6 Address . . . . . : fe80::677e:2a81:fef:d198%15
   IPv4 Address. . . . . . . . . . . : 192.168.47.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.47.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

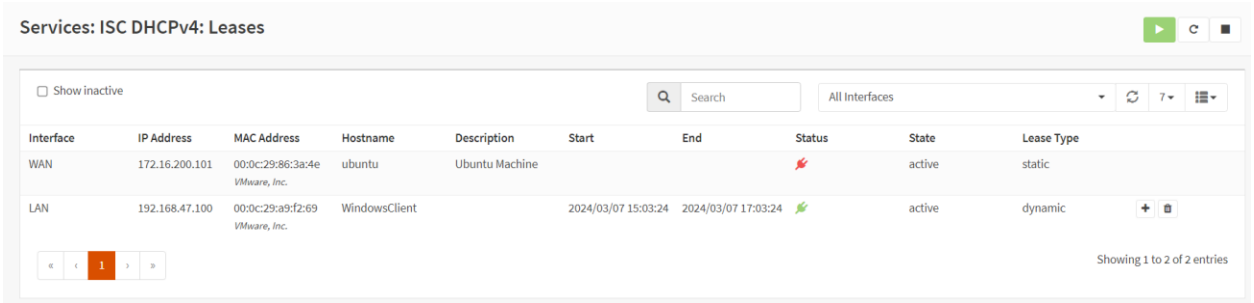
Here we can see the verification that the Windows Client successfully obtained the proper network configurations.



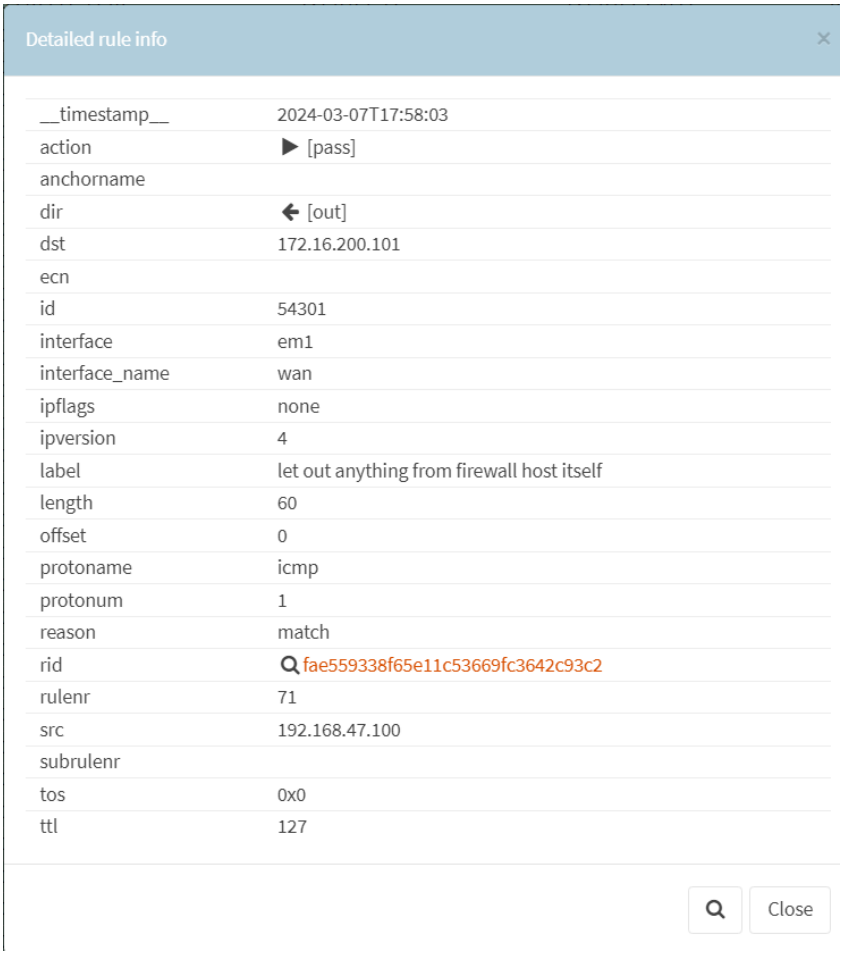
Here we can see the Windows Server is on the proper subnet and DNS server with the proper IP address on the LAN.



The Ubuntu Client machine has the proper subnet and DNS server with the proper IP address on the WAN.



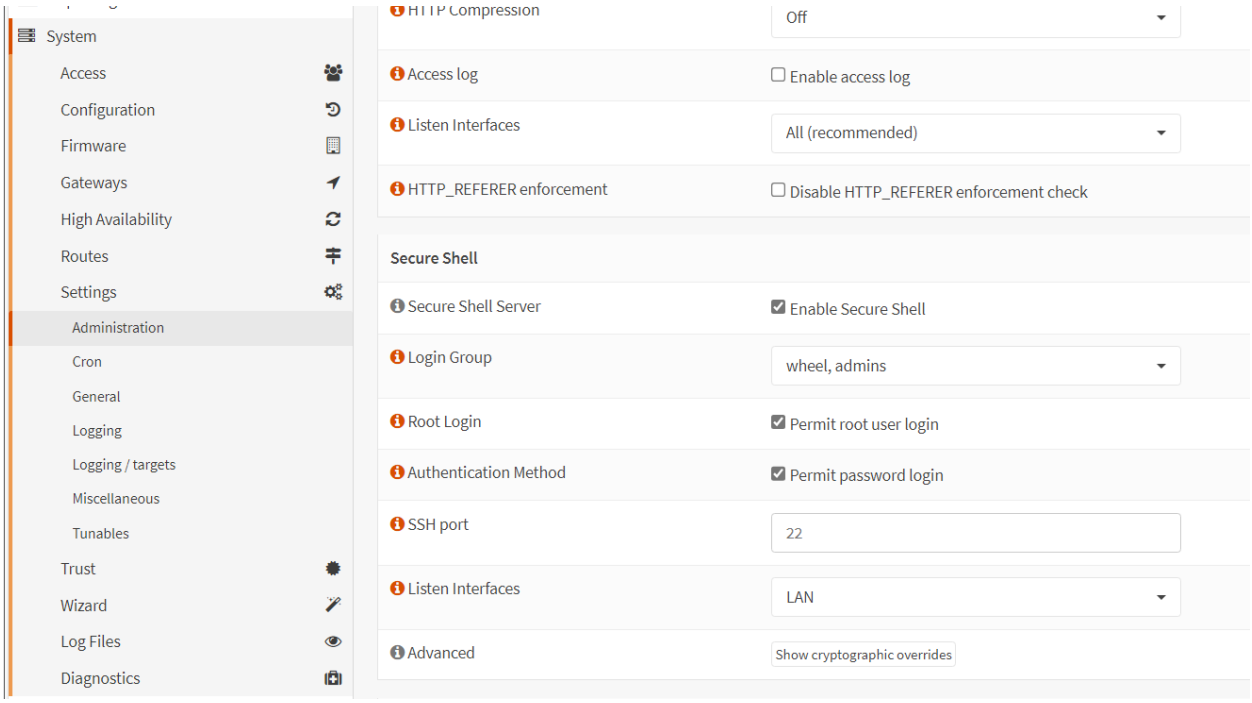
Here we can see both machines are managed by the OPNsense appliance machine.



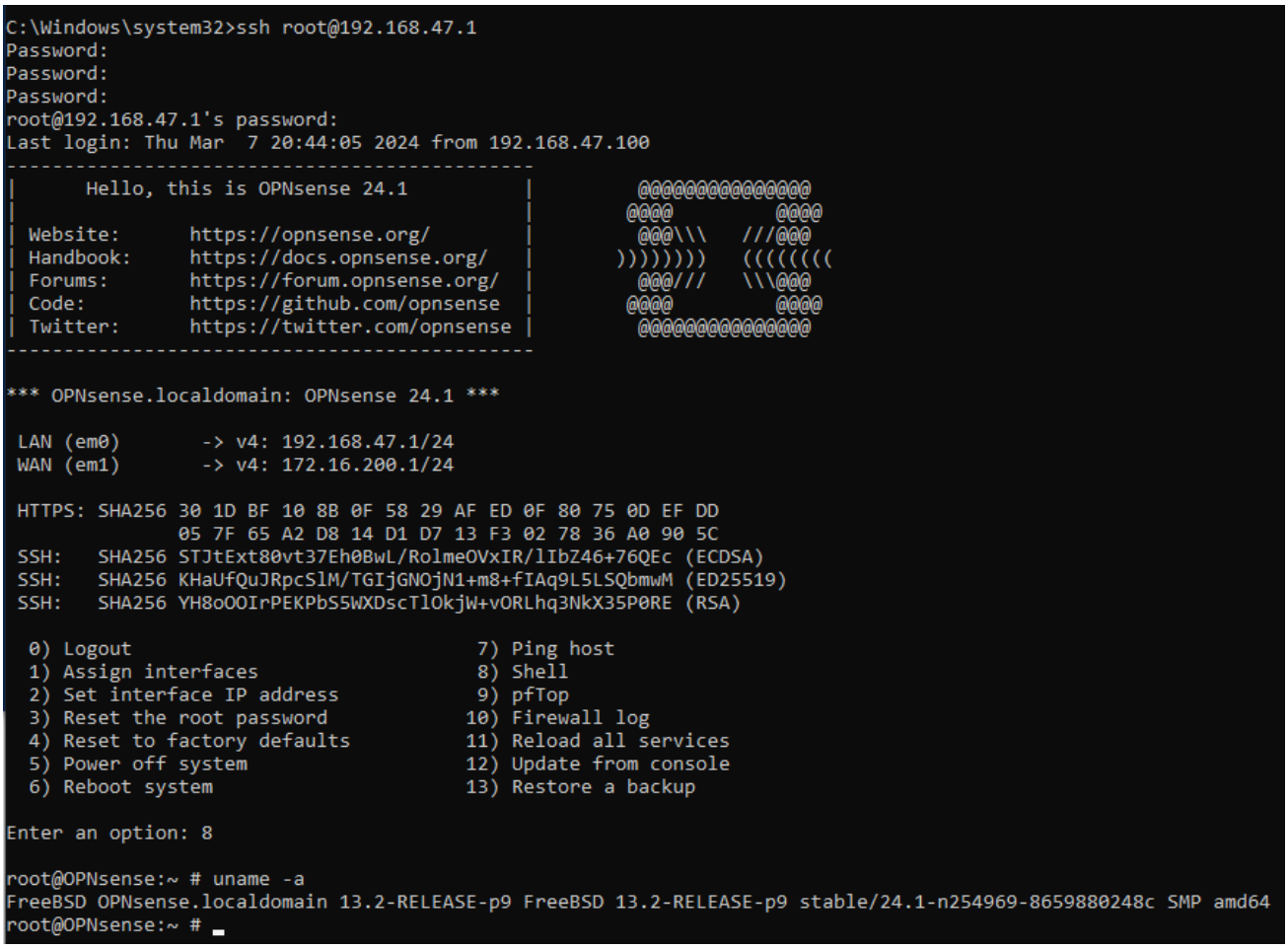
Here we see the LAN internal source address has been transferred to the WAN external address.

```
C:\Windows\system32>ping 172.16.200.101

Pinging 172.16.200.101 with 32 bytes of data:
Reply from 172.16.200.101: bytes=32 time<1ms TTL=128
Reply from 172.16.200.101: bytes=32 time<1ms TTL=128
Reply from 172.16.200.101: bytes=32 time<1ms TTL=128
Reply from 172.16.200.101: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.200.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

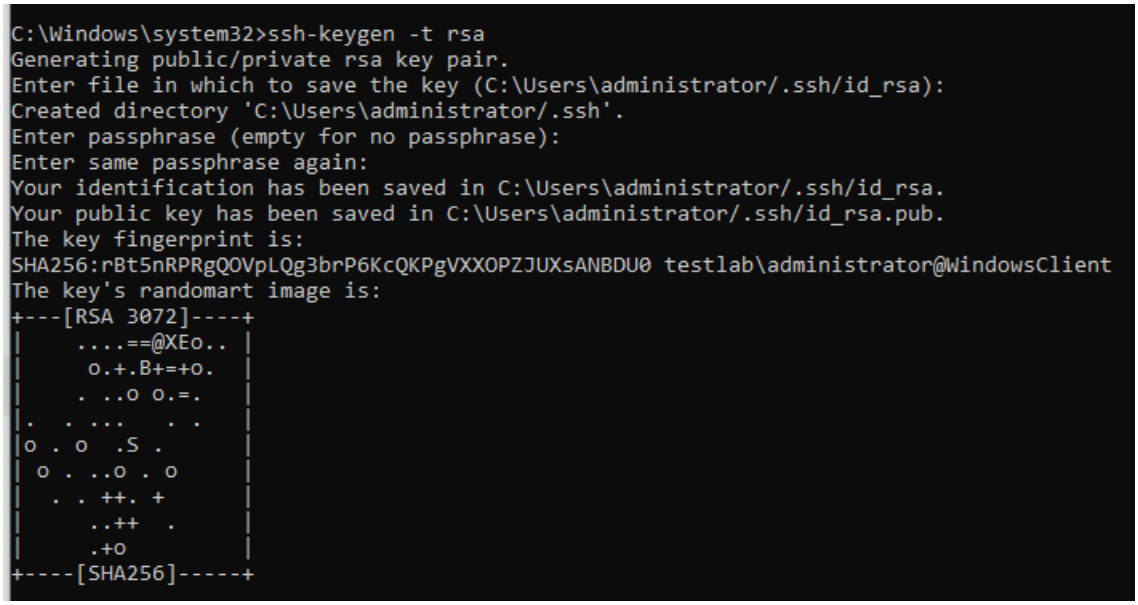
Here we can see the Ubuntu machine can be pinged.



At this point, I went to the administration section of the settings and enabled the secure shell to listen on the LAN interface. I also enabled the root login and password login, which are optional features.



Next, using command prompt I used the command “ssh root@192.168.47.1” to ssh into the OPNsense appliance. Then I opened a shell by entering option 8 and used the “uname -a” command to receive the machine ID, name of the node, OS release number, the system name, and the OS version.



Here I tried the “ssh-keygen -t rsa” command which is used to generate an RSA key which is used for security purposes to better secure our OPNsense appliance.

Conclusion:

This lab was a challenge, but I made it through. I was able to accurately set up the OPNsense Appliance machine and configure it with my three existing virtual machines. I had some trouble along the way with network issues as well as working through configuring my NAT with the proper routing sourcing traffic from the internal LAN (192.168.47.0/24) and translating it to my external WAN (172.16.200.0/24), which both took some time to work through.

References:

https://www.youtube.com/watch?v=h2_cQxTkh3Q&t=1005s

https://www.youtube.com/watch?v=Vegl9azqY9A

https://www.youtube.com/watch?v=HczerqZlw3s

https://docs.opnsense.org/manual/dhcp.html

https://www.zenarmor.com/docs/network-security-tutorials/how-to-configure-opnsense-nat#