CORPORATE NETWORK DESIGN

PERSONAL PROJECT REPORT

by

ĐỖ KHẮC VĨ

Ho Chi Minh city
11/2024

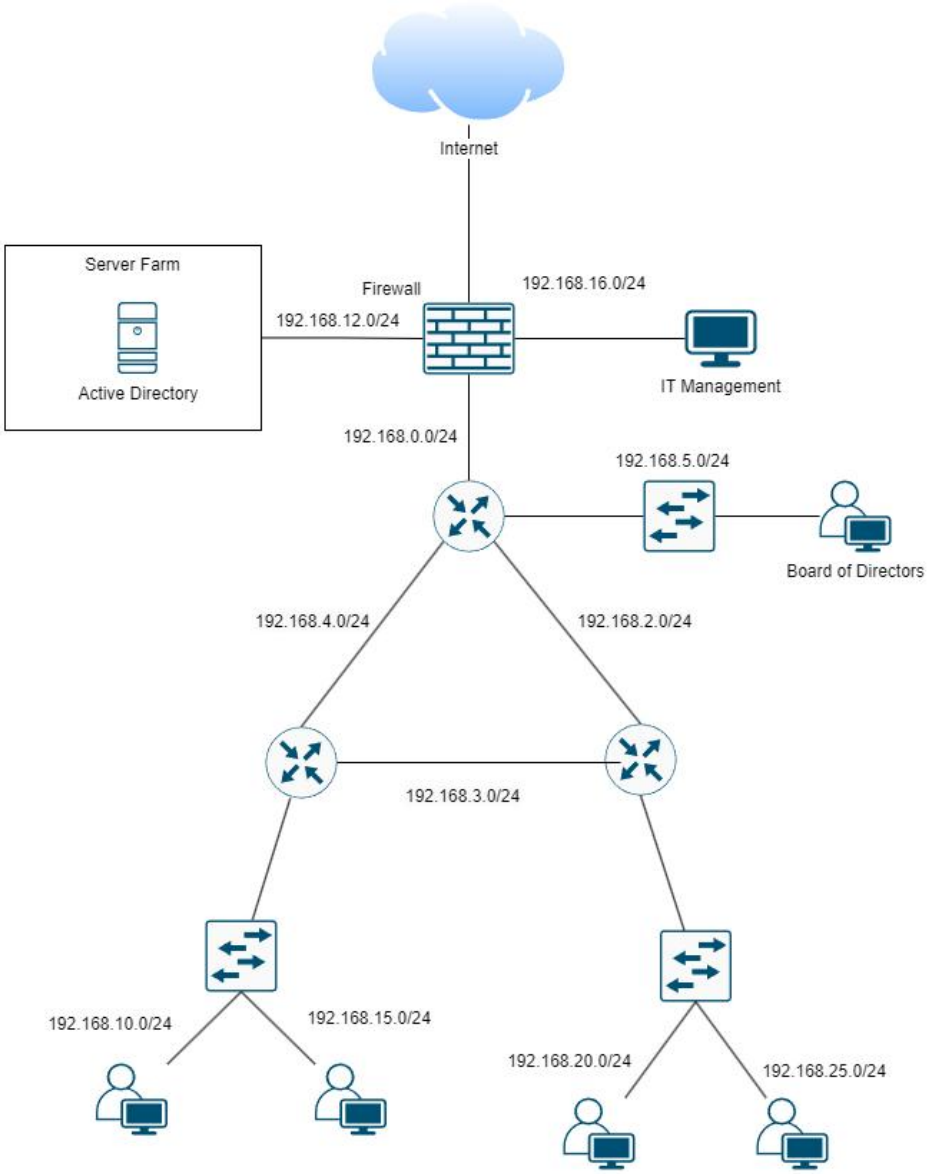
Declaration by Author

This is to declare that this report has been written by me. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I aver that if any part of the report is found to be plagiarized, I shall take full responsibility for it.

Đỗ Khắc Vĩ

Table of Contents

1. Introduction



Project Title: Corporate Network Design

Objective: The primary objective of this project is to design, implement, and document a scalable and secure corporate network infrastructure that efficiently connects all organizational units while ensuring data integrity, availability, and confidentiality.

Project Deliverables:

- Network Topology Design:

A hierarchical network design connecting various organizational departments, including IT Management, the Board of Directors, and end-users.

Logical segmentation of the network into subnets for effective traffic management and improved security.

- Subnet Allocation:

  192.168.0.0/24: Connect the LAN to the firewall.

  192.168.12.0/24: Server Farm hosting Active Directory services.

  192.168.16.0/24: IT Management segment.

  192.168.5.0/24: Board of Directors segment.

  192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24: Branch connectivity to downstream subnets.

  192.168.10.0/24, 192.168.15.0/24, 192.168.20.0/24, 192.168.25.0/24: End-user devices.

- Security Features:

  Deployment of a firewall between the Internet and the internal network for threat mitigation.

  Segmentation of critical servers (Active Directory) to a dedicated subnet for added security.

- Routing and Switching:

  Deployment of routers and switches for core, distribution, and access layers.

  Configuration of inter-VLAN routing to facilitate communication between subnets.

The software I use for this project includes:

VMware® Workstation 17 Pro 17.6.1.

Windows Server 2019.

Windows 10.

Ubuntu 20.04.6 Desktop.

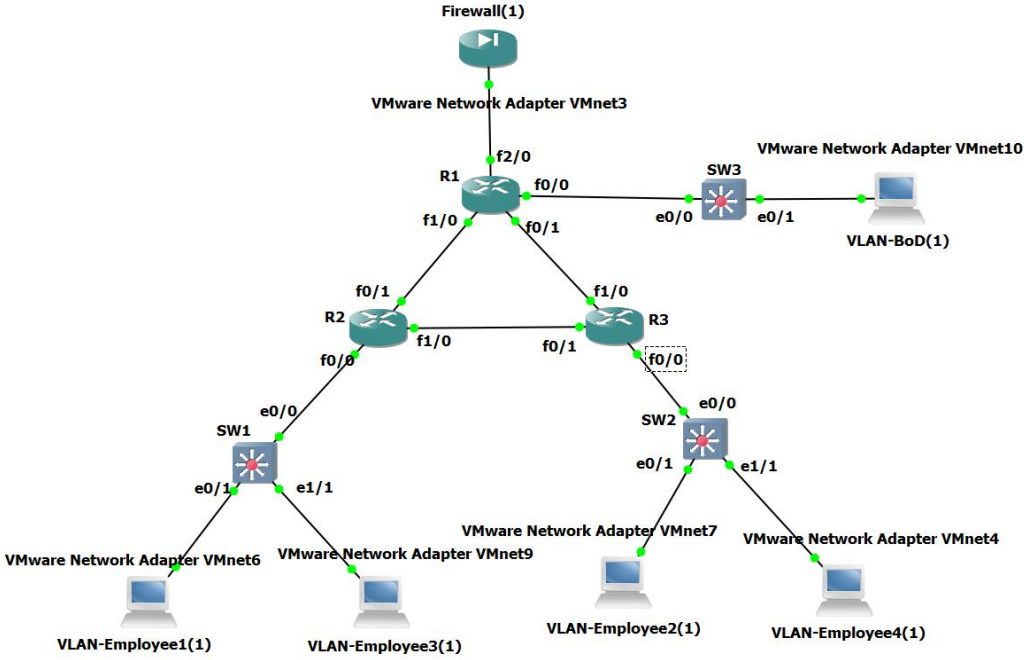
Firewall OPNsense 24.7.

GNS3 2.1.21.

Router: Cisco IOS Software (C3725-AdvEnterpriseK9-M), Version 12.4(15)T14.

Switch: Cisco IOS Software, Linux Software (i86bi_LinuxL2-AdvEnterpriseK9-M), Version 15.2.

2. Establishing the network
2.1. LAN
2.1.1. Fundamental Configuration



This image provides a detailed representation of how the network is structured and appears within the GNS3 simulation environment, showcasing the various components and their connections.

I will begin with the configuration of router R1.

First and foremost, configure the console password and enable password to enhance security and allow the IT team to access the router via SSH in the future.

Console password:

R1#configure terminal
R1(config)#line console 0
R1(config-line)#password vurtle123
R1(config-line)#login
R1(config-line)#exit

Enable password:

R1(config)#enable password vurtle123

Line VTY password:

R1(config)#line vty 0 4
R1(config-line)#password vurtle123
R1(config-line)#login
R1(config-line)#exit

Typically, the passwords should be different for enhanced security; however, for simplicity in this project, I will use the same password.

Next, I will configure the IP addresses for the interfaces based on the topology shown above.

```
R1(config)#interface f2/0
R1(config-if)#ip address 192.168.0.10 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface f1/0
R1(config-if)#ip address 192.168.4.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface f0/1
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

2.1.2. Routing protocol

Once all the interfaces have been assigned IP addresses, proceed with configuring the OSPF routing protocol.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.0.0 0.0.0.255 area 0
R1(config-router)#network 192.168.2.0 0.0.0.255 area 0
R1(config-router)#network 192.168.4.0 0.0.0.255 area 0
R1(config-router)#network 192.168.5.0 0.0.0.255 area 0
R1(config-router)#default-information originate always
```

The final command tells the router to advertise a default route (0.0.0.0/0) into the routing protocol, regardless of whether there is an existing default route in the routing table. The always keyword forces the router to continuously send the default route, even if the router does not have a default route itself.

Now I set the default route:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.254
```

0.0.0.0 0.0.0.0: This specifies the destination network and subnet mask for the default route. The address 0.0.0.0 with a subnet mask of 0.0.0.0 means that this route matches any destination IP address, effectively making it a default route. It tells the router that if it does not know where to send a packet (i.e., the destination network is not in its routing table), it should send the packet to the specified next hop.

192.168.0.2: This is the next-hop IP address, which is the IP address of the next router or gateway that will handle the packet.

One more command that should be configured is

```
R1(config-router)#passive-interface f0/0
```

This command will prevents the router from transmitting routing updates to interface f0/0.

Now, apply the same configuration to the two other routers.

R2

```
R2#configure terminal
R2(config)#line console 0
R2(config-line)#password vurtle123
R2(config-line)#login
R2(config-line)#exit
R2(config)#enable password vurtle123
R2(config)#line vty 0 4
R2(config-line)#password vurtle123
R2(config-line)#login
R2(config-line)#exit
R2(config)#interface f1/0
R2(config-if)#ip address 192.168.3.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.4.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Now, I need to configure subinterfaces, which are logical divisions of a physical interface. These are commonly used for purposes such as:

- Enabling VLAN (Virtual LAN) routing in a Router-on-a-Stick configuration.
- Assigning distinct networks or IP addresses to a single physical interface.
- Managing traffic for different subnetworks.

This configuration is required because the interface is connected to two VLANs.

```
R2(config)#interface f0/0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int f0/0.1
R2(config-subif)#encapsulation dot1Q 10
R2(config-subif)#ip add 192.168.10.254 255.255.255.0
R2(config-subif)#int f0/0.2
R2(config-subif)#encapsulation dot1Q 15
R2(config-subif)#ip add 192.168.15.254 255.255.255.0
```

interface f0/0.1:

Access the subinterface 1 of FastEthernet 0/0 for configuration.

encapsulation dot1Q 10:

Specify the VLAN ID (10) using 802.1Q encapsulation. This command is required for distinguishing traffic for different VLANs.

ip address 192.168.10.1 255.255.255.0:

Assign an IP address to the subinterface, allowing it to route traffic for this VLAN or subnet.

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.4.0 0.0.0.255 area 0
R2(config-router)#network 192.168.3.0 0.0.0.255 area 0
R2(config-router)#network 192.168.10.0 0.0.0.255 area 0
R2(config-router)#network 192.168.15.0 0.0.0.255 area 0
R2(config-router)#passive-interface f0/0.1
R2(config-router)#passive-interface f0/0.2
```

Apply the same configuration from R2 to router R3.

R3

```
R3#configure terminal
R3(config)#line console 0
R3(config-line)#password vurtle123
R3(config-line)#login
R3(config-line)#exit
R3(config)#enable password vurtle123
R3(config)#line vty 0 4
R3(config-line)#password vurtle123
R3(config-line)#login
R3(config-line)#exit
R3(config)#interface f1/0
R3(config-if)#ip address 192.168.2.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface f0/1
R3(config-if)#ip address 192.168.3.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface f0/0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#int f0/0.1
R3(config-subif)#encapsulation dot1Q 20
R3(config-subif)#ip add 192.168.20.254 255.255.255.0
R3(config-subif)#int f0/0.2
R3(config-subif)#encapsulation dot1Q 25
R3(config-subif)#ip add 192.168.25.254 255.255.255.0
```

R3(config)#router ospf 1
R3(config-router)#network 192.168.2.0 0.0.0.255 area 0
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.20.0 0.0.0.255 area 0
R3(config-router)#network 192.168.25.0 0.0.0.255 area 0
R3(config-router)#passive-interface f0/0.1
R3(config-router)#passive-interface f0/0.2

R1

R1(config)#interface f0/0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int f0/0.1
R1(config-subif)#encapsulation dot1Q 5
R1(config-subif)#ip add 192.168.5.254 255.255.255.0

2.1.3. VLAN

Next, I will configure VLANs on the switches, starting with SW1. Set password like the routers.

SW1#configure terminal
SW1(config)#enable password vurtle123
SW1(config)#line console 0
SW1(config-line)#password vurtle123
SW1(config-line)#login
SW1(config-line)#exit
SW1(config)#line vty 0 4
SW1(config-line)#password vurtle123
SW1(config-line)#login
SW1(config-line)#exit

These are the interfaces of the switch. I will assign Ethernet0/1 to Ethernet0/3 to VLAN 10 and Ethernet1/1 to Ethernet1/3 to VLAN 15.

```
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Serial4/0              unassigned      YES unset  administratively down down
Serial4/1              unassigned      YES unset  administratively down down
Serial4/2              unassigned      YES unset  administratively down down
Serial4/3              unassigned      YES unset  administratively down down
Serial5/0              unassigned      YES unset  administratively down down
Serial5/1              unassigned      YES unset  administratively down down
Serial5/2              unassigned      YES unset  administratively down down
Serial5/3              unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

SW1(config)#vlan 10
SW1(config-vlan)#exit
SW1(config)#vlan 15
SW1(config-vlan)#exit
SW1(config)#interface range e0/1-3
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#interface range e1/1-3
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 15
SW1(config-if-range)#exit

interface range e1/1-3:

This command accesses a range of interfaces (Ethernet 1/1 to Ethernet 1/3) on the switch for batch configuration. Any commands applied afterward will affect all the specified interfaces.

switchport mode access:

Sets the selected interfaces to operate as access ports. Access ports are used to connect end devices like PCs, printers, or servers to the switch. This ensures the interface cannot participate in VLAN trunking.

switchport access vlan 15:

Assigns the interfaces to VLAN 15. All traffic sent or received on these interfaces will now be associated with VLAN 15.

SW1(config)#interface e0/0
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk

This command configures the Ethernet0/0 interface to act as a trunk. The trunk port allows traffic for multiple VLANs to pass through, with 802.1Q tags identifying the VLAN for each frame. This setup is used to connect the switch the a router R1.

Now, apply the same configuration on SW2 and SW3.

SW2

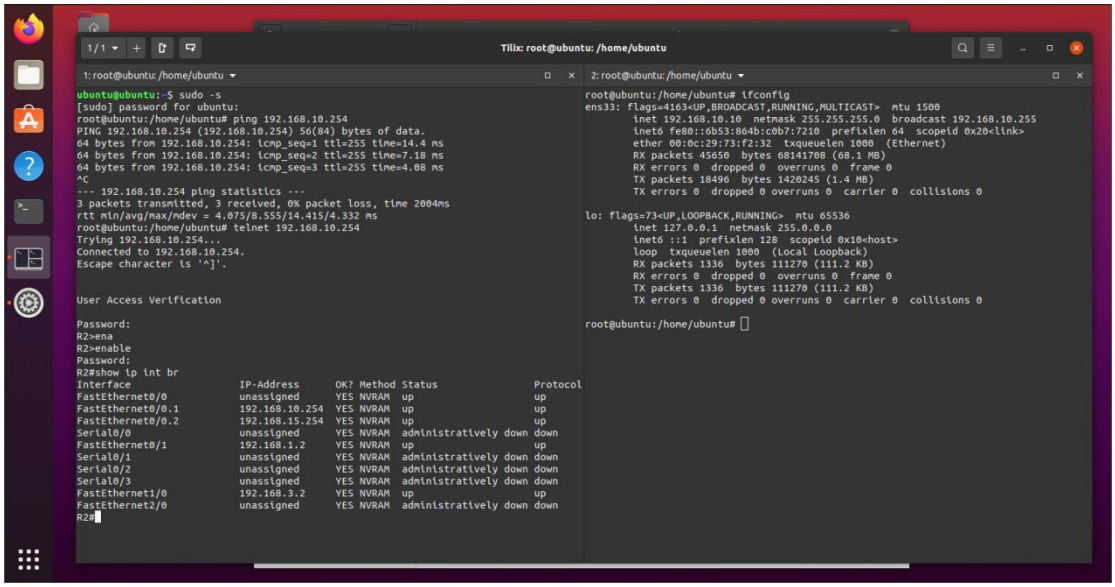
SW2#configure terminal
SW2(config)#enable password vurtle123
SW2(config)#line console 0
SW2(config-line)#password vurtle123
SW2(config-line)#login
SW2(config-line)#exit
SW2(config)#line vty 0 4
SW2(config-line)#password vurtle123
SW2(config-line)#login

SW2(config-line)#exit
SW2(config)#vlan 20
SW2(config-vlan)#exit
SW2(config)#vlan 25
SW2(config-vlan)#exit
SW2(config)#interface range e0/1-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
SW2(config-if-range)#exit
SW2(config)#interface range e1/1-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 25
SW2(config-if-range)#exit
SW2(config)#interface e0/0
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk

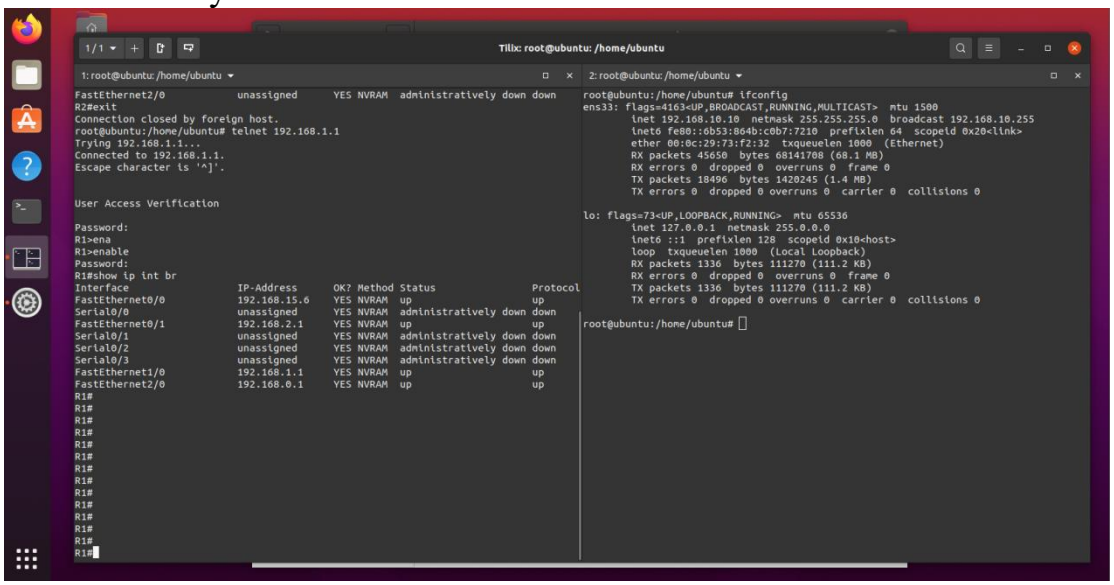
SW3

SW3#configure terminal
SW3(config)#enable password vurtle123
SW3(config)#line console 0
SW3(config-line)#password vurtle123
SW3(config-line)#login
SW3(config-line)#exit
SW3(config)#line vty 0 4
SW3(config-line)#password vurtle123
SW3(config-line)#login
SW3(config-line)#exit
SW3(config)#vlan 5
SW3(config-vlan)#exit
SW3(config)#interface range e0/1-3
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 5
SW3(config-if-range)#exit
SW3(config)#interface e0/0
SW3(config-if)#switchport trunk encapsulation dot1q
SW3(config-if)#switchport mode trunk

Using an Ubuntu machine, I have been able to access the Telnet service of the switch.



And any device in the network that I want to connect to.



2.1.4. NAT

Now, configure NAT on R1 to enable the network to access the Internet.

R1(config)#access-list 1 permit any
R1(config)#ip nat inside source list 1 interface f2/0 overload
R1(config)#interface f2/0
R1(config-subif)#ip nat outside
R1(config)#interface f1/0
R1(config-subif)#ip nat inside
R1(config)#interface f0/1
R1(config-subif)#ip nat inside
R1(config)#int f0/0.1

R1(config-subif)#ip nat inside

2.1.5. Access Control List

Once the network has internet access, I will configure a set of Access Control List (ACL) rules to restrict traffic between users.

The purpose of the rules is to allow all traffic by default and deny only unnecessary traffic. Here, I will use Named Extended ACL for ease of management.

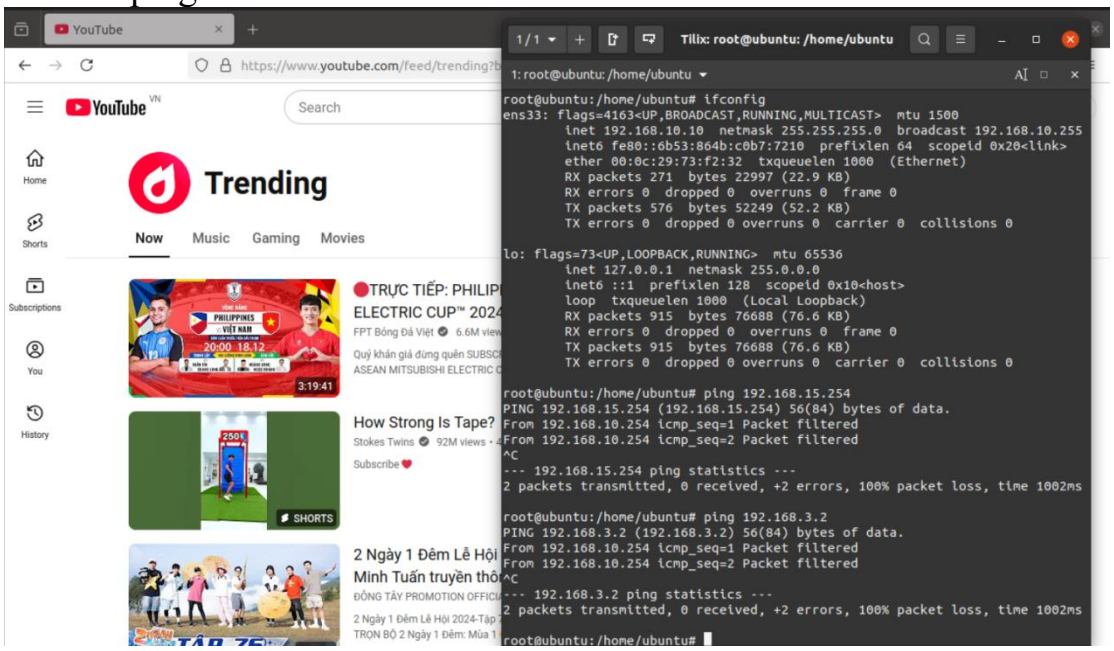
R2(config)#ip access-list extended vlan10
R2(config-ext-nacl)#deny ip any 192.168.0.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.2.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.3.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.4.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.5.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.10.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.15.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.20.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.25.0 0.0.0.255
R2(config-ext-nacl)#permit ip any any
R2(config-ext-nacl)#exit

These rules will restrict devices in the 192.168.10.0 network from connecting to other networks within the LAN but will still allow them to access services from other networks and the Internet.

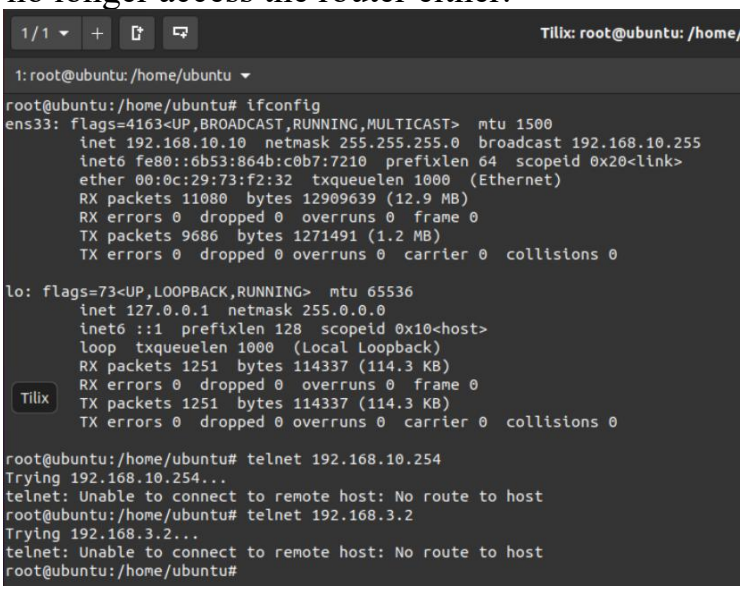
Now, apply them to the interface.

R2(config)#interface f0/0.1
R2(config-subif)#ip access-group vlan10 in

The device can no longer ping other networks within the LAN but can still ping and access websites on the Internet.



It can no longer access the router either.



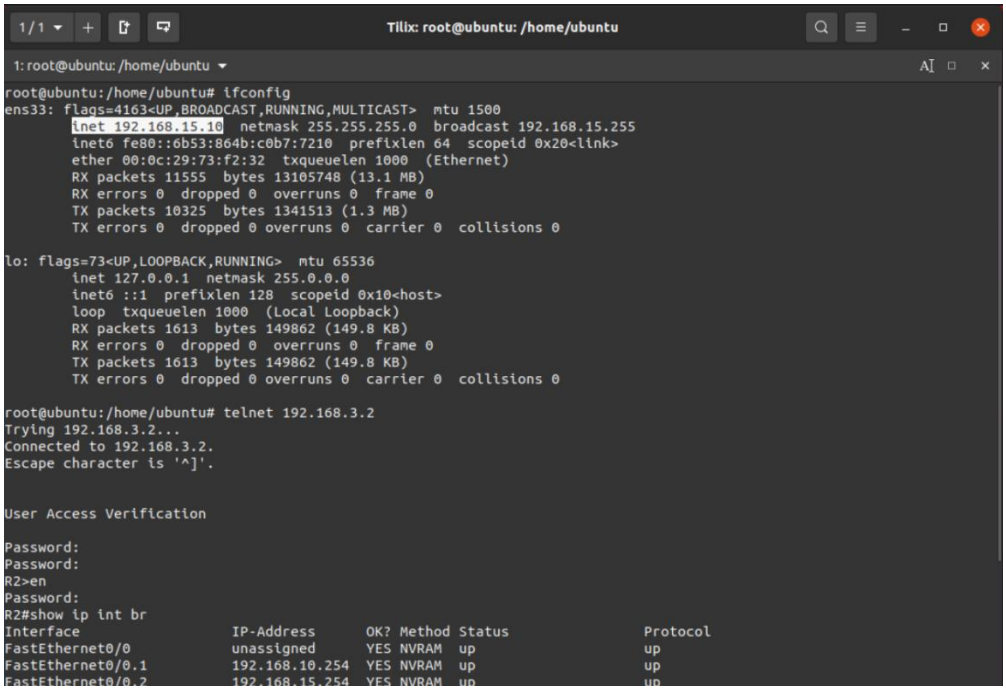
Apply the same rule to the VLAN 15.

R2(config)#ip access-list extended vlan15
R2(config-ext-nacl)#deny ip any 192.168.0.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.2.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.3.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.4.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.5.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.10.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.15.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.20.0 0.0.0.255
R2(config-ext-nacl)#deny ip any 192.168.25.0 0.0.0.255
R2(config-ext-nacl)#permit ip any any

But now let's say VLAN 15 can access to the router. I will add a rule that allows VLAN 15 to telnet to the routers and switches.

R2(config-ext-nacl)#5 permit tcp any any eq 23
R2(config-ext-nacl)#exit
R2(config)#interface f0/0.2
R2(config-subif)#ip access-group vlan15 in

The "5" before the command is necessary because, without it, the rule would be added to the end of the list. This would place it after other restrictive rules, causing it to be inactive.



Apply the same rule as VLAN 10 to other VLANs on other routers.

R3

R3(config)#ip access-list extended vlan20
R3(config-ext-nacl)#deny ip any 192.168.0.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.2.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.3.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.4.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.5.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.10.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.15.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.20.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.25.0 0.0.0.255
R3(config-ext-nacl)#permit ip any any
R3(config-ext-nacl)#exit
R3(config)#interface f0/0.1
R3(config-subif)#ip access-group vlan20 in
R3(config-subif)#exit
R3(config)#ip access-list extended vlan25
R3(config-ext-nacl)#deny ip any 192.168.0.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.2.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.3.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.4.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.5.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.10.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.15.0 0.0.0.255

R3(config-ext-nacl)#deny ip any 192.168.20.0 0.0.0.255
R3(config-ext-nacl)#deny ip any 192.168.25.0 0.0.0.255
R3(config-ext-nacl)#permit ip any any
R3(config)#interface f0/0.2
R3(config-subif)#ip access-group vlan25 in

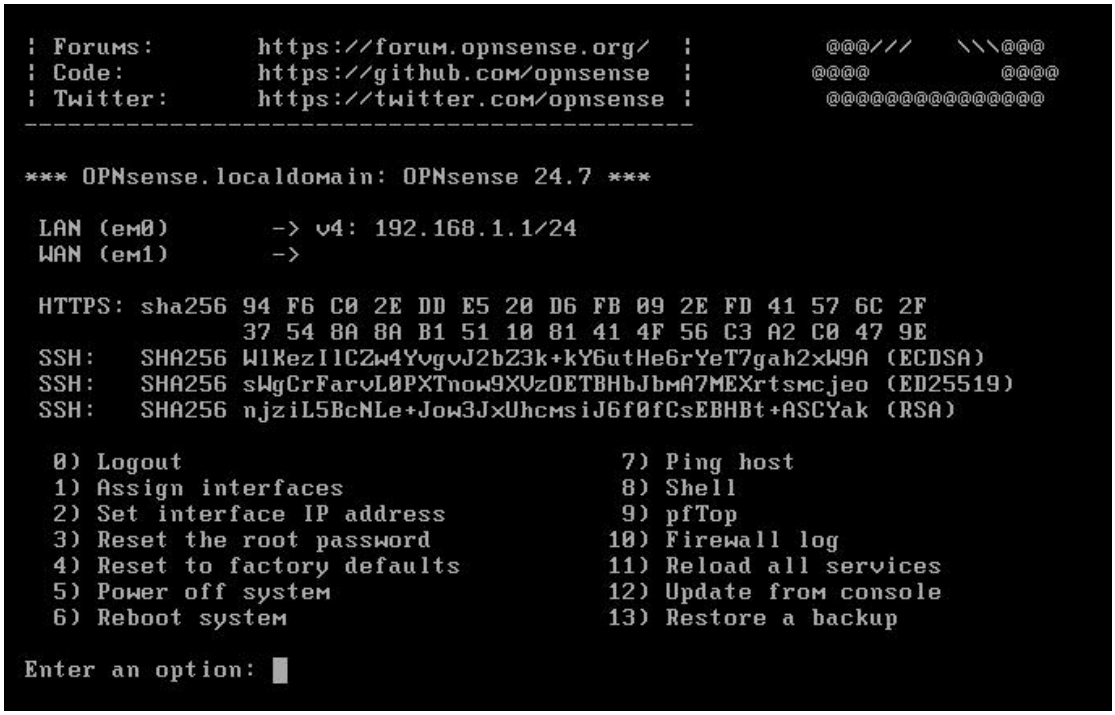
R1

R1(config)#ip access-list extended vlan5
R1(config-ext-nacl)#deny ip any 192.168.0.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.2.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.3.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.4.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.5.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.10.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.15.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.20.0 0.0.0.255
R1(config-ext-nacl)#deny ip any 192.168.25.0 0.0.0.255
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#interface f0/0.1
R1(config-if)#ip access-group vlan5 in

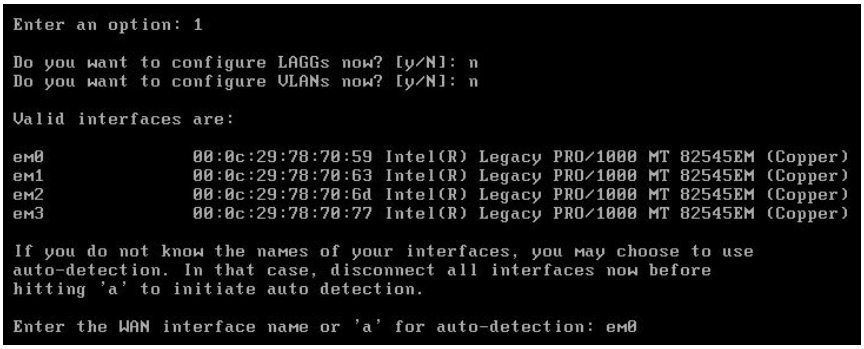
2.2. Firewall

2.2.1. Firewall Configuration

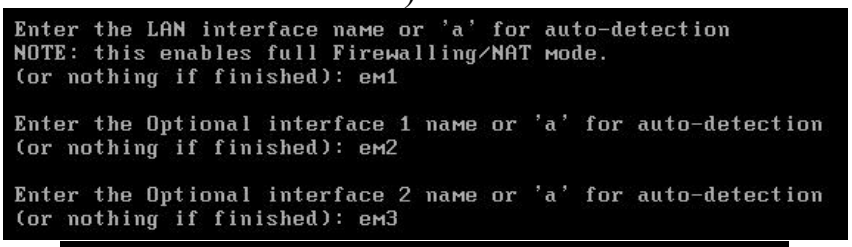
This is how the firewall look like after its installation.

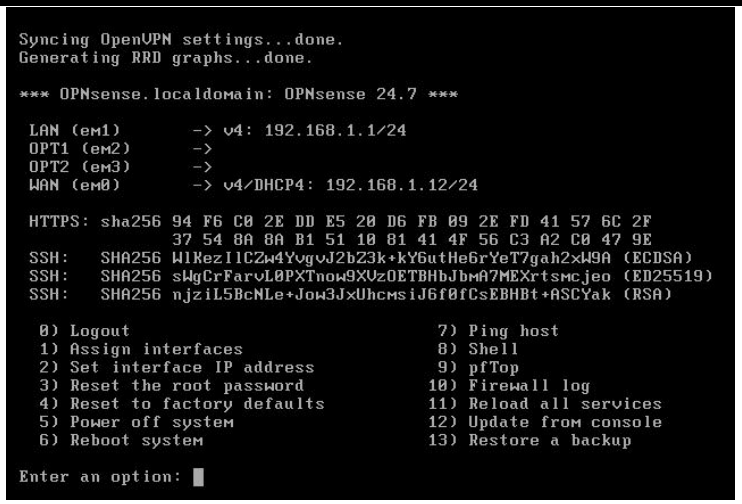


First, I need to assign the interfaces. Choose the first option.
WAN interface:

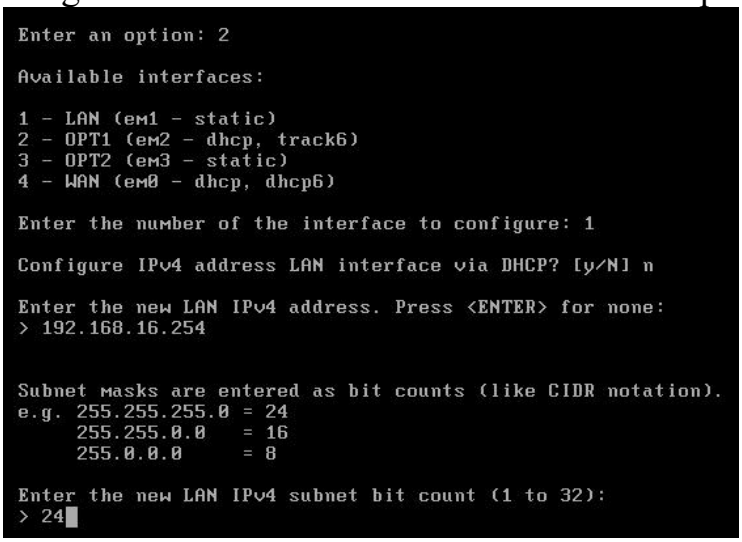


Web GUI, LAN, and Server farm network by order (since this firewall will be configured through the LAN interface, I have designated the LAN interface as the Web GUI.):





Next, assign IP addresses to the interfaces. Choose option 2.

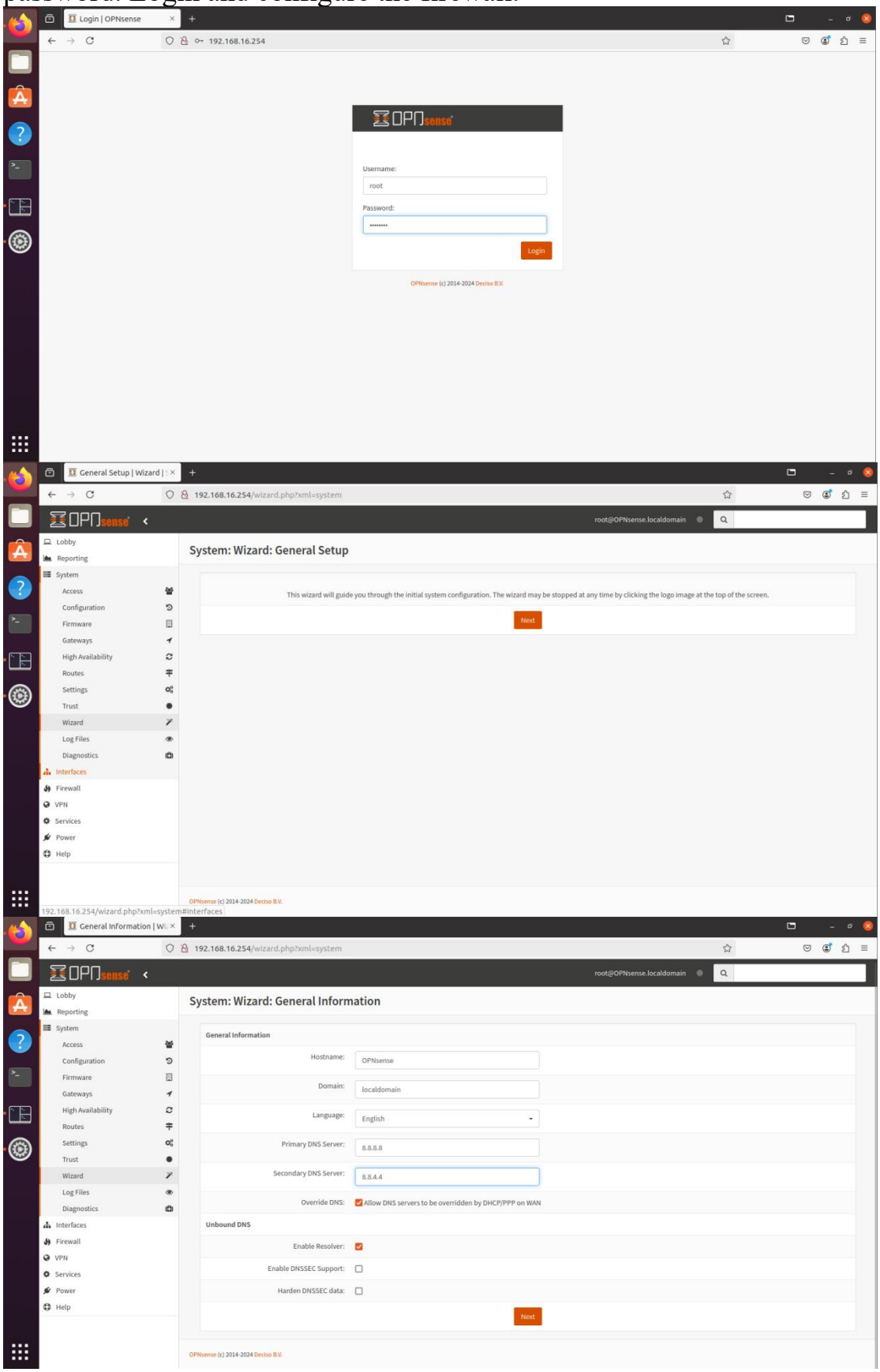


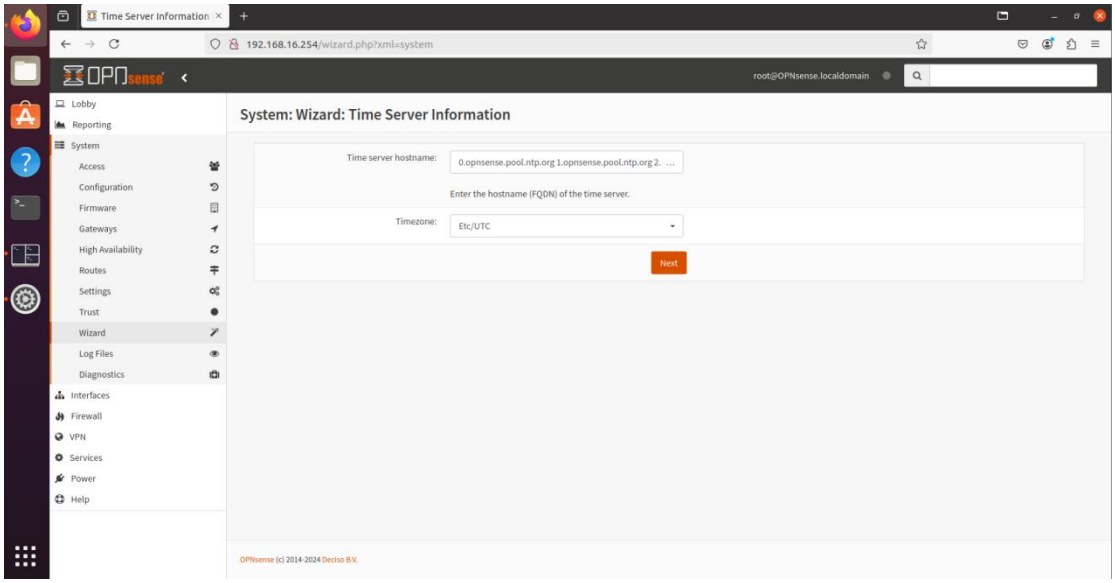
```
Enter an option: 2

Available interfaces:

1 - LAN (em1 - static)
2 - OPT1 (em2 - dhcp, track6)
3 - OPT2 (em3 - static)
4 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 2

Configure IPv4 address OPT1 interface via DHCP? [y/N] n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.0.254


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 OPT1 IPv4 subnet bit count (1 to 32):
> 24
```

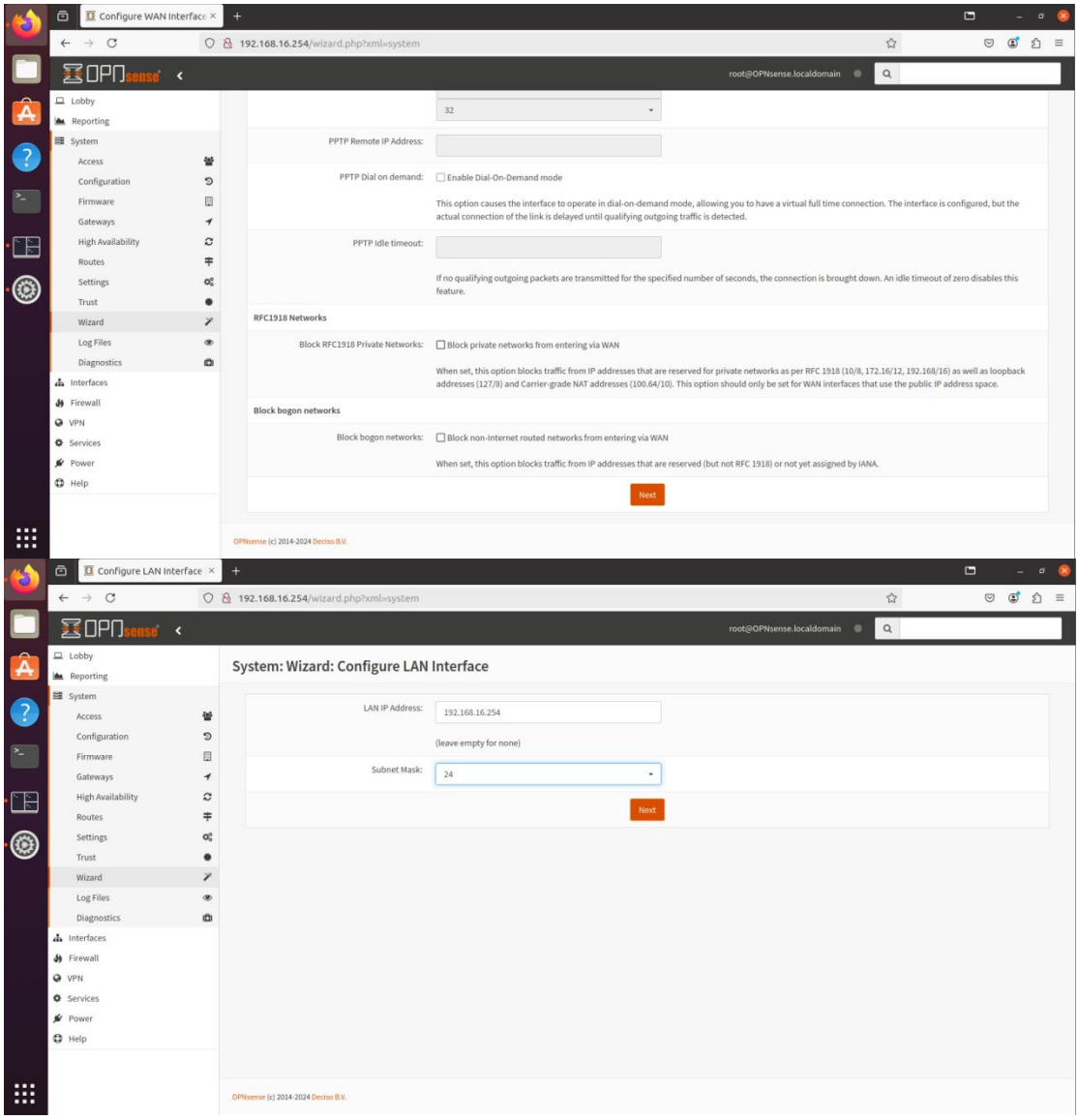
```
Enter an option: 2

Available interfaces:

1 - LAN (em1 - static)
2 - OPT1 (em2 - static, track6)
3 - OPT2 (em3)
4 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 3

Configure IPv4 address OPT2 interface via DHCP? [y/N] n

Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 192.168.12.254


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 OPT2 IPv4 subnet bit count (1 to 32):
> 24
```

```
Configuring firewall.......done.
Starting DHCPv6 service...done.
Starting router advertisement service...done.


*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (em1)       -> v4: 192.168.16.254/24
 OPT1 (em2)      -> v4: 192.168.0.254/24
 OPT2 (em3)      -> v4: 192.168.12.254/24
 WAN (em0)       -> v4/DHCP4: 192.168.1.12/24

 SSH:   SHA256 WlKezIlCZw4YvgvJ2bZ3k+kY6utHe6rYeT7gah2xW9A (ECDSA)
 SSH:   SHA256 sWgCrFarvL0PXTnow9XVzOETBHbJbmA7MEXrtsmcjeo (ED25519)
 SSH:   SHA256 njziL5BcNLe+Jow3JxUhcmsiJ6f0fCsEBHBt+ASCYak (RSA)

  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:
```

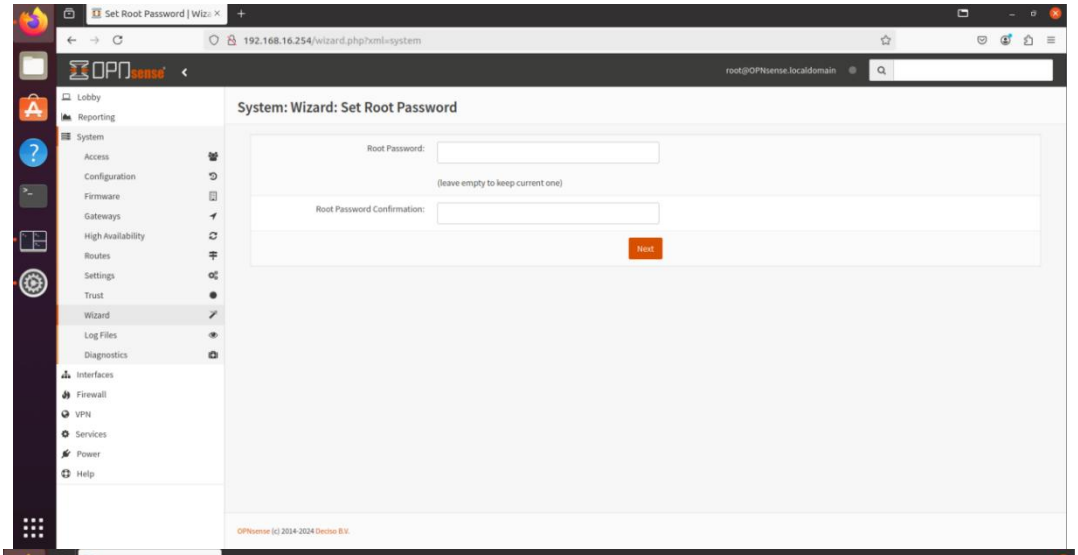
I can now access the web GUI of the firewall through LAN(em1). The login credentials are "root" as the username and "opnsense" as the password. Login and configure the firewall.

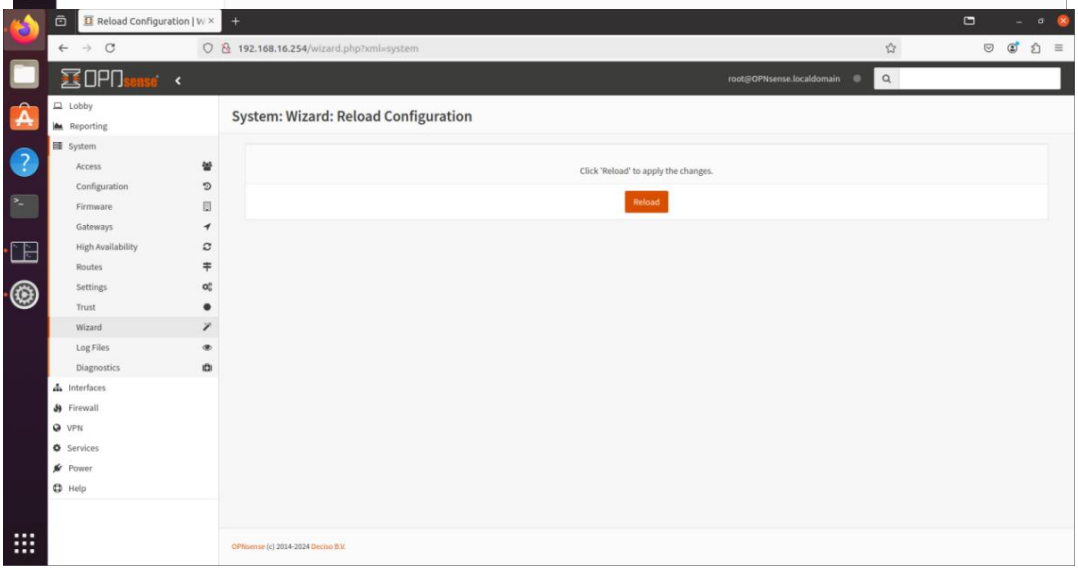



Time Server Information
192.168.16.254/wizard.php?xml=system
root@OPNsense.localdomain
System: Wizard: Time Server Information
Time server hostname:
0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2. ...
Enter the hostname (FQDN) of the time server.
Timezone:
Etc/UTC
Next
OPNsense (c) 2014-2024 Deciso B.V.

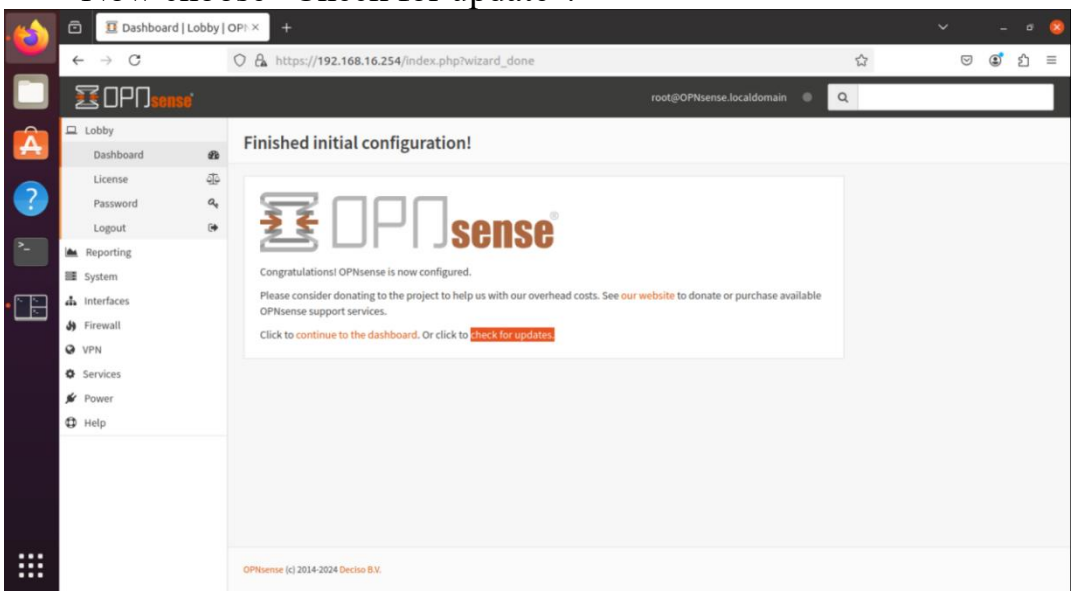

Configure WAN Interface
192.168.16.254/wizard.php?xml=system
root@OPNsense.localdomain
32
PPTP Remote IP Address:
PPTP Dial on demand:
Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing you to have a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout:
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.
RFC1918 Networks
Block RFC1918 Private Networks:
Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8) and Carrier-grade NAT addresses (100.64/10). This option should only be set for WAN interfaces that use the public IP address space.
Block bogon networks
Block bogon networks:
Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA.
Next
OPNsense (c) 2014-2024 Deciso B.V.
Configure LAN Interface
192.168.16.254/wizard.php?xml=system
root@OPNsense.localdomain
System: Wizard: Configure LAN Interface
LAN IP Address:
192.168.16.254
(leave empty for none)
Subnet Mask:
24
Next
OPNsense (c) 2014-2024 Deciso B.V.

Change the password if necessary, I will use the current password, so I will leave it blank.

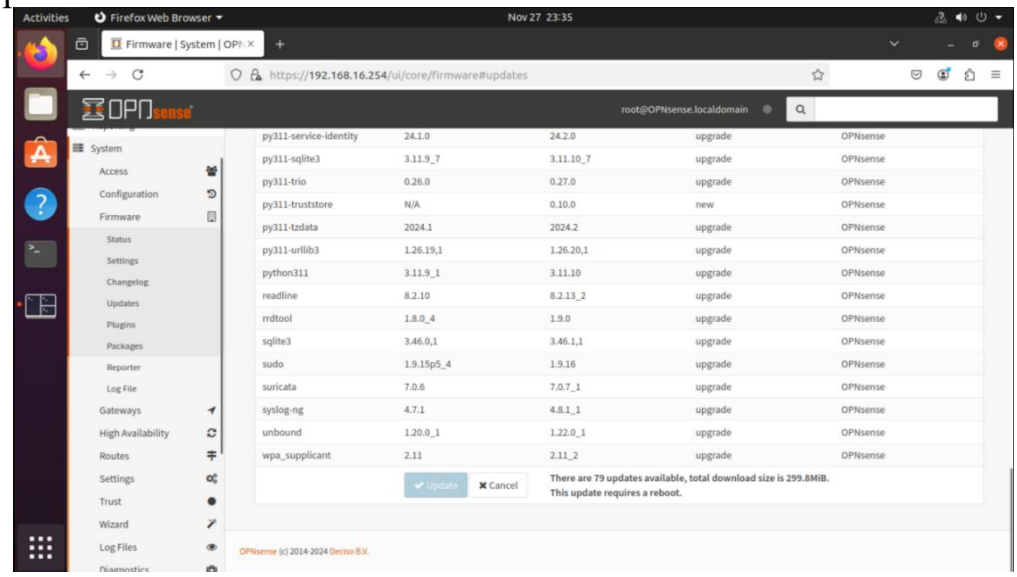




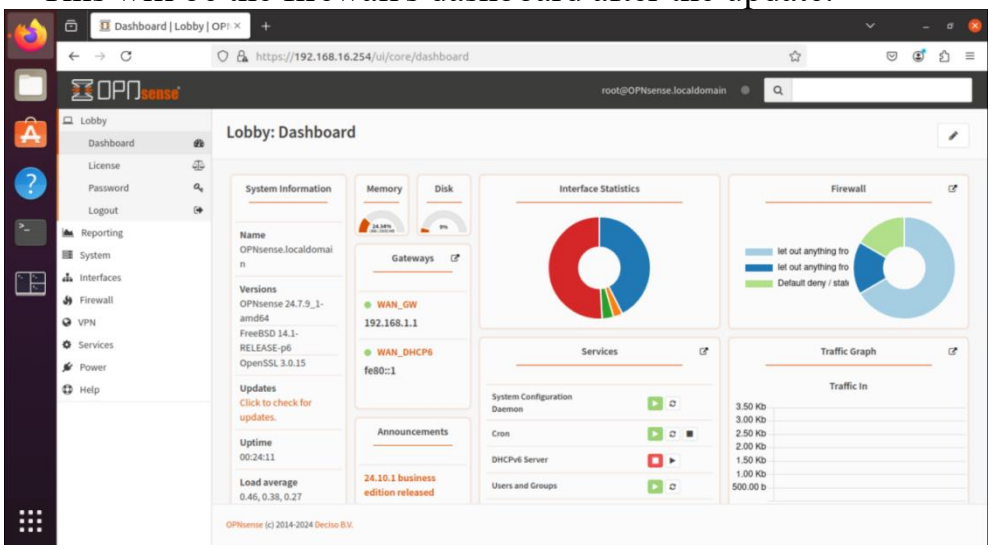
Now choose “Check for update”.



Once the verification process is complete, scroll down and select "Update."

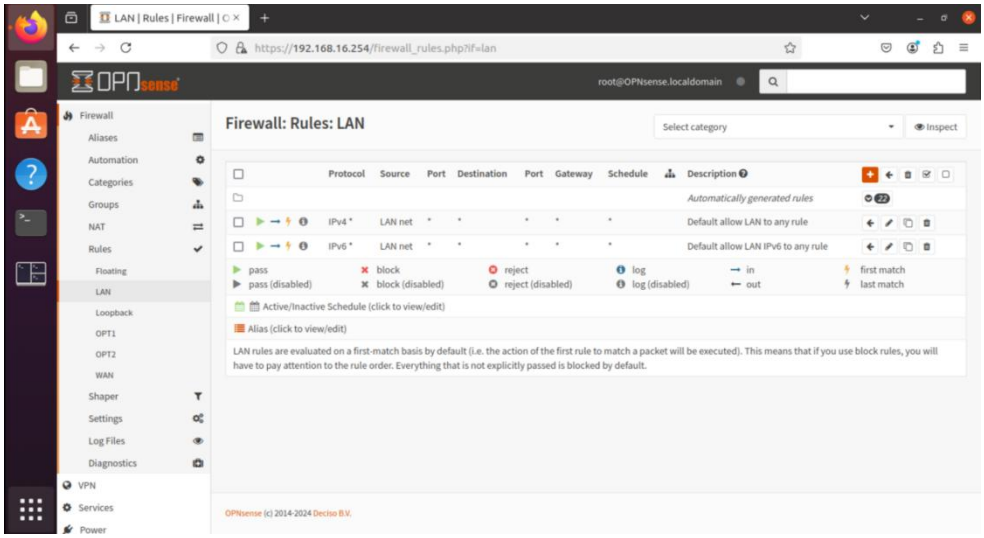


This will be the firewall's dashboard after the update.

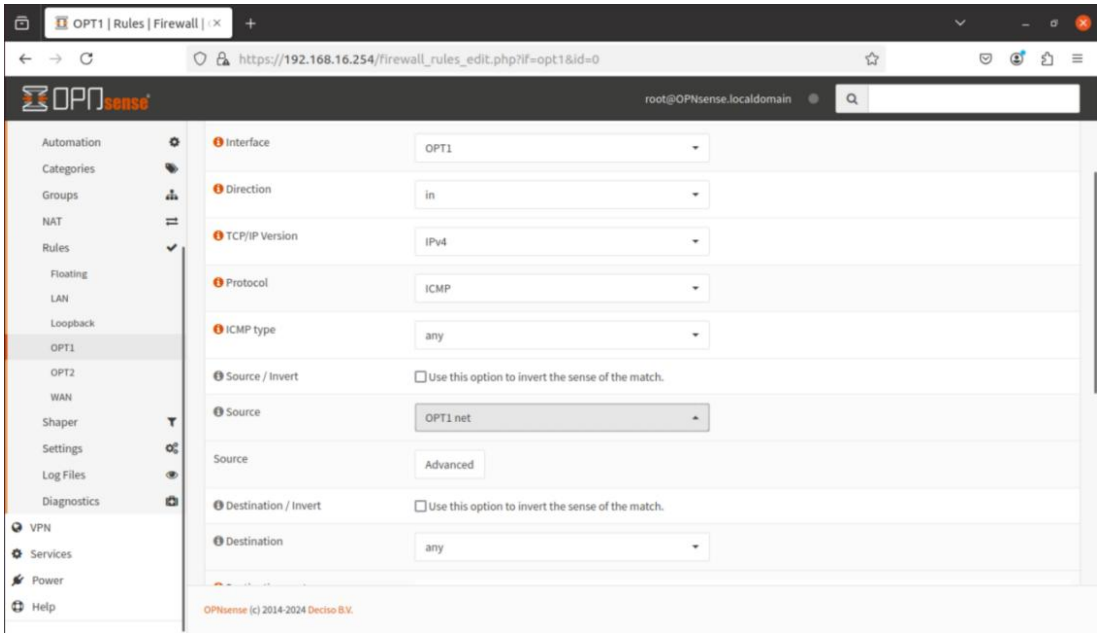


2.2.2. Basic rules

Choose “Firewall” -> “Rules” -> “LAN”

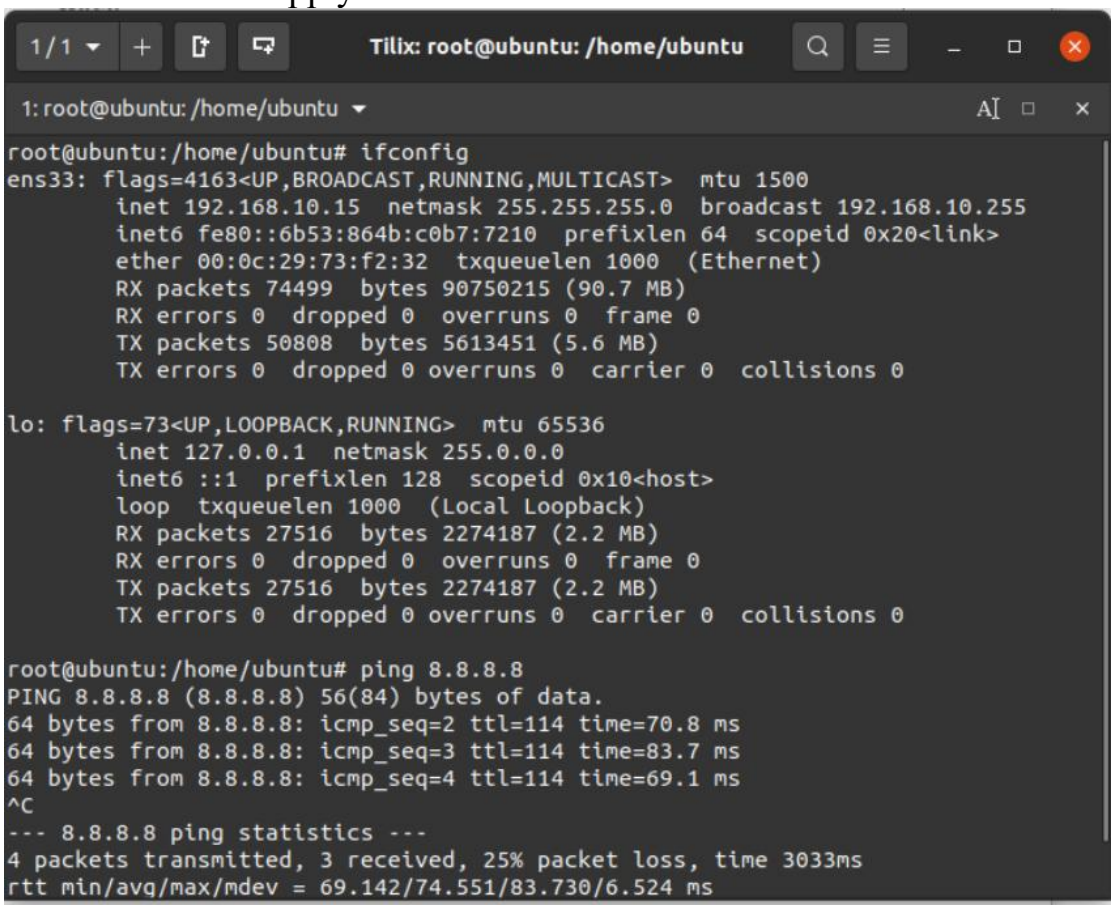


There are 2 default rules, I will delete both. Next, navigate to the “OPT1” and create a new rule.



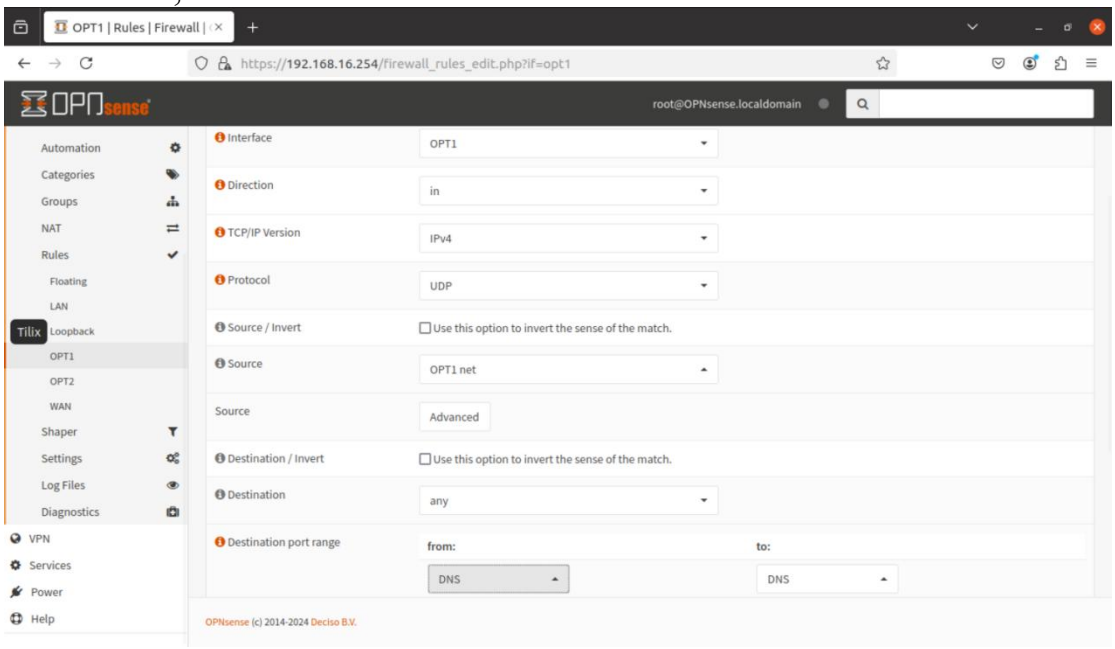
The first rule allows LAN to ping anywhere. The rule will be configured with interface is “OPT1”, direction “in”, protocol is “ICMP”, source is “OPT1” and destination is “any”.

Click the “Apply chanes” and the rule will become active.



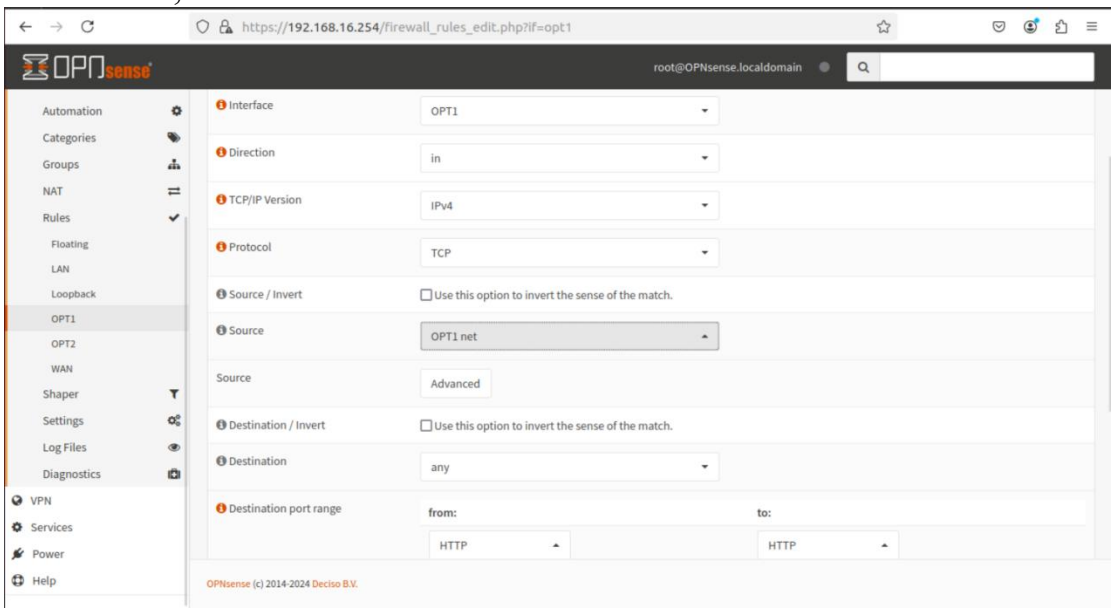
The LAN can now ping to any IP address.

Now, create a rule to allow DNS traffic.

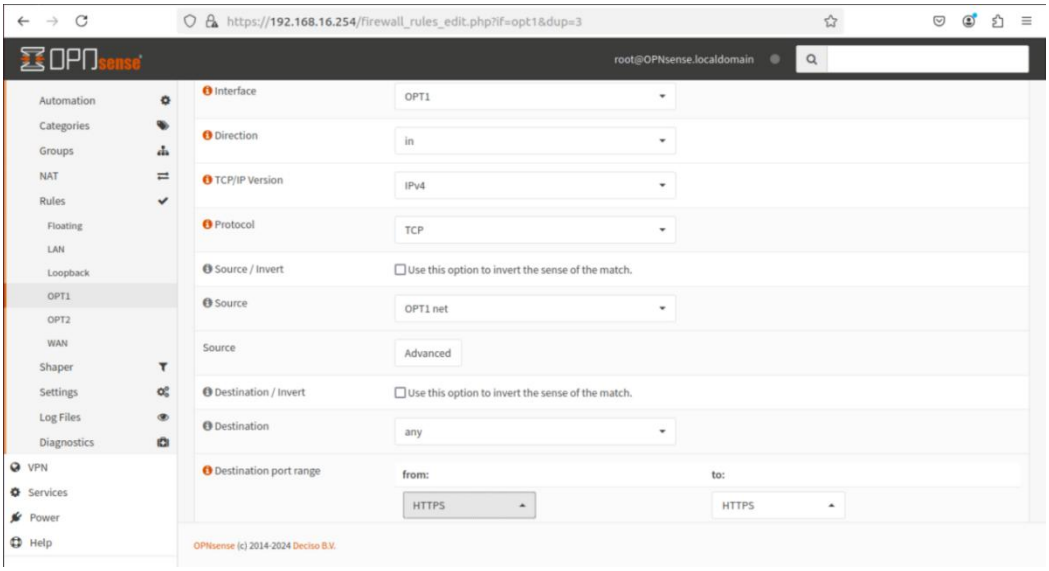


Interface is “OPT1”, direction “in”, protocol is “UDP” (since DNS use UDP protocol), source is “OPT1 net”, destination is “any” and destination port is “DNS”.

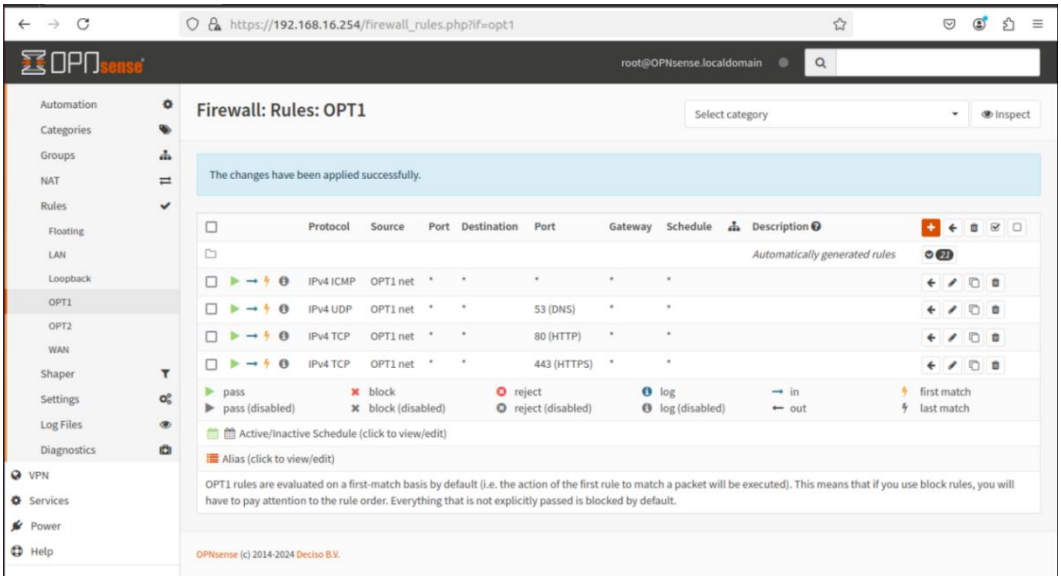
Next, create rules to allow HTTP and HTTPS traffic.



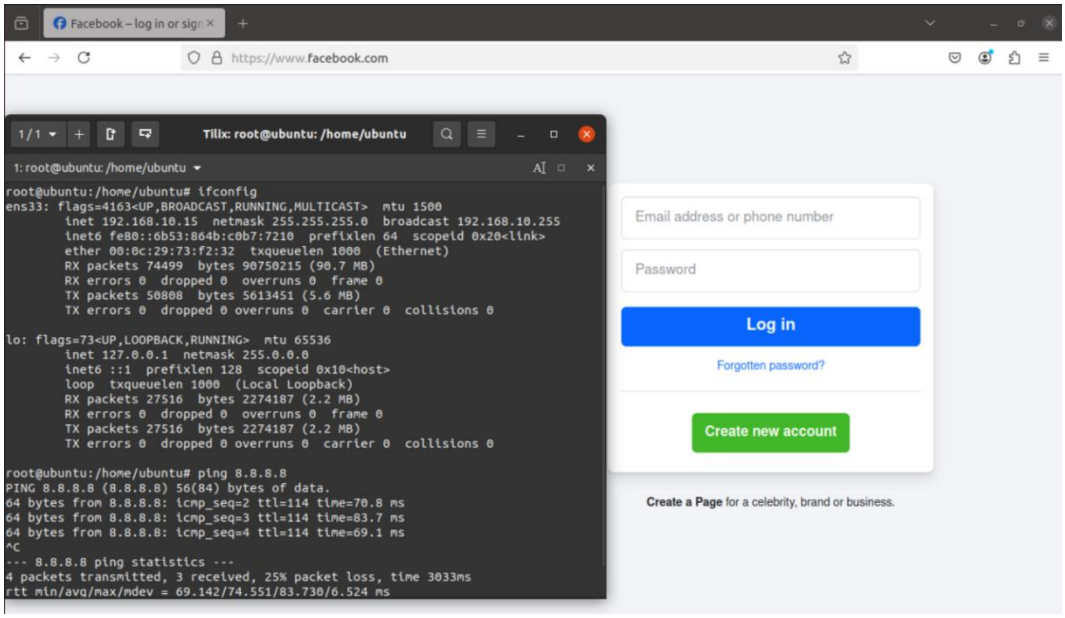
Interface is “OPT1”, direction “in”, protocol is “TCP”, source is “OPT1 net”, destination is “any” and destination port is “HTTP”. Do the same with the HTTPS rule but change the destination port to “HTTPS”.



These will be the current rules.



The network can now access the Internet.



2.2.3. Active Directory rules

Now, I need to configure rules to enable devices from the LAN to join the Domain. Based on the list of required ports for Active Directory services, I must establish rules that correspond to these ports.

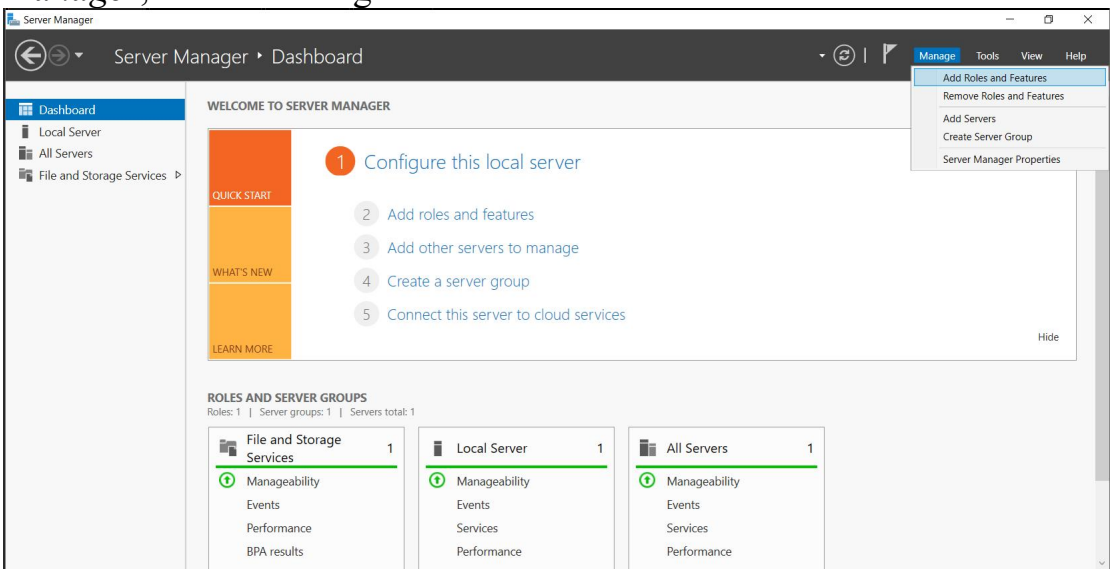
Client Port(s)	Server Port	Service
49152-65535/UDP	123/UDP	W32Time
49152-65535/TCP	135/TCP	RPC Endpoint Mapper
49152-65535/TCP	464/TCP/UDP	Kerberos password change
49152-65535/TCP	49152-65535/TCP	RPC for LSA, SAM, NetLogon (*)
49152-65535/TCP/UDP	389/TCP/UDP	LDAP
49152-65535/TCP	636/TCP	LDAP SSL
49152-65535/TCP	3268/TCP	LDAP GC
49152-65535/TCP	3269/TCP	LDAP GC SSL
53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
49152-65535/TCP	49152-65535/TCP	FRS RPC (*)
49152-65535/TCP/UDP	88/TCP/UDP	Kerberos
49152-65535/TCP/UDP	445/TCP	SMB (**)
49152-65535/TCP	49152-65535/TCP	DFSR RPC (*)

IPv4 UDP	OPT1 net	*	OPT2 net	123 (NTP)	*	*	AD rule		
IPv4 TCP	OPT1 net	*	OPT2 net	49152 - 65535	*	*	AD rule (DFSR RPC)		
IPv4 TCP	OPT1 net	*	OPT2 net	135	*	*	AD rule (RPC Endpoint Mapper)		
IPv4 TCP	OPT1 net	*	OPT2 net	636	*	*	AD rule (LDAP SSL)		
IPv4 TCP	OPT1 net	*	OPT2 net	3268	*	*	AD rule (LDAP GC)		
IPv4 TCP	OPT1 net	*	OPT2 net	3269	*	*	AD rule (LDAP GC SSL)		
IPv4 TCP	OPT1 net	*	OPT2 net	445 (MS DS)	*	*	AD rule (SMB)		
IPv4 TCP/UDP	OPT1 net	*	OPT2 net	389 (LDAP)	*	*	AD rule		
IPv4 TCP/UDP	OPT1 net	*	OPT2 net	464	*	*	AD rule (Kerberos password change)		
IPv4 TCP/UDP	OPT1 net	*	OPT2 net	53 (DNS)	*	*	AD rule (DNS - TCP/UDP)		
IPv4 TCP/UDP	OPT1 net	*	OPT2 net	88	*	*	AD rule (Kerberos)		

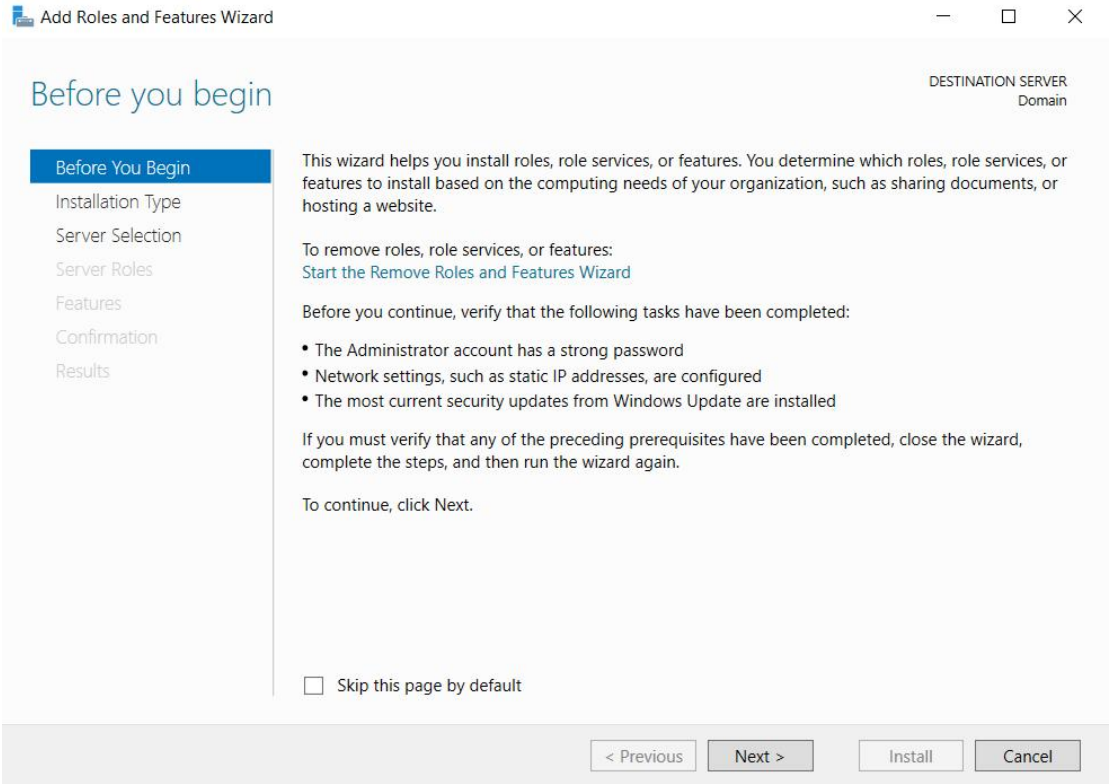
2.3. Active Directory

2.3.1. Set up Active Directory

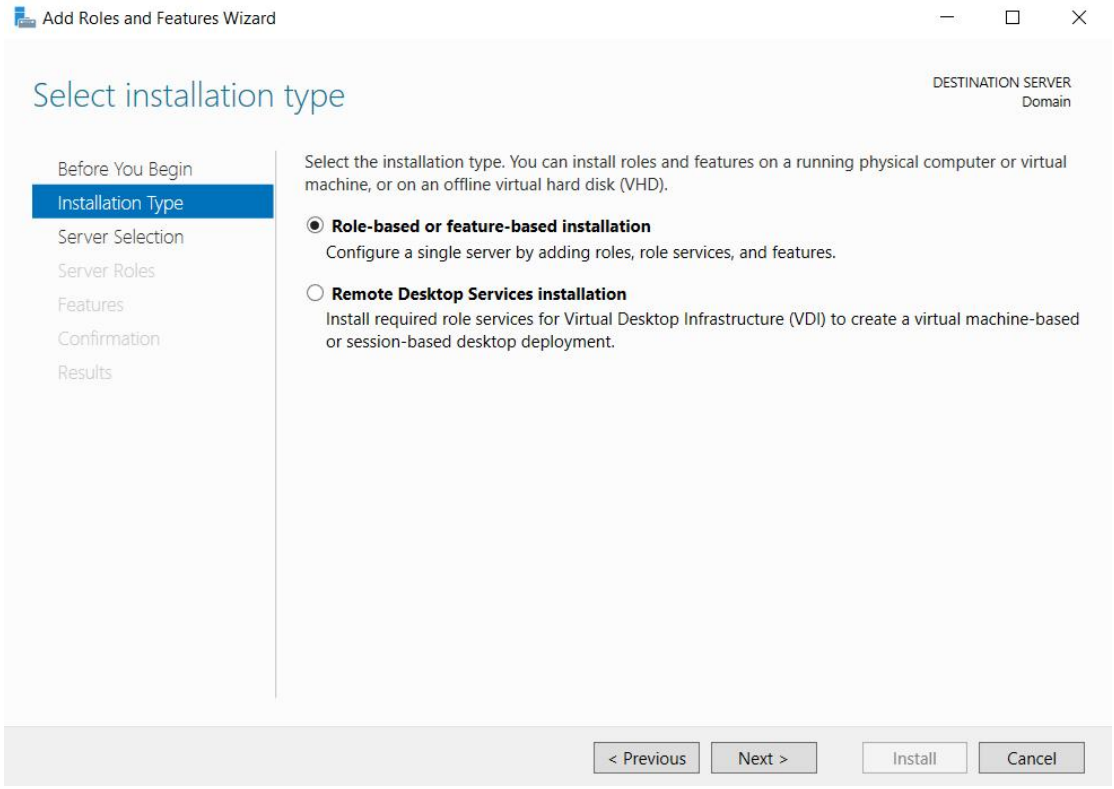
I will begin by creating a Active Directory (AD). In the *Server Manager*, select "Manage" -> "Add Roles and Features".



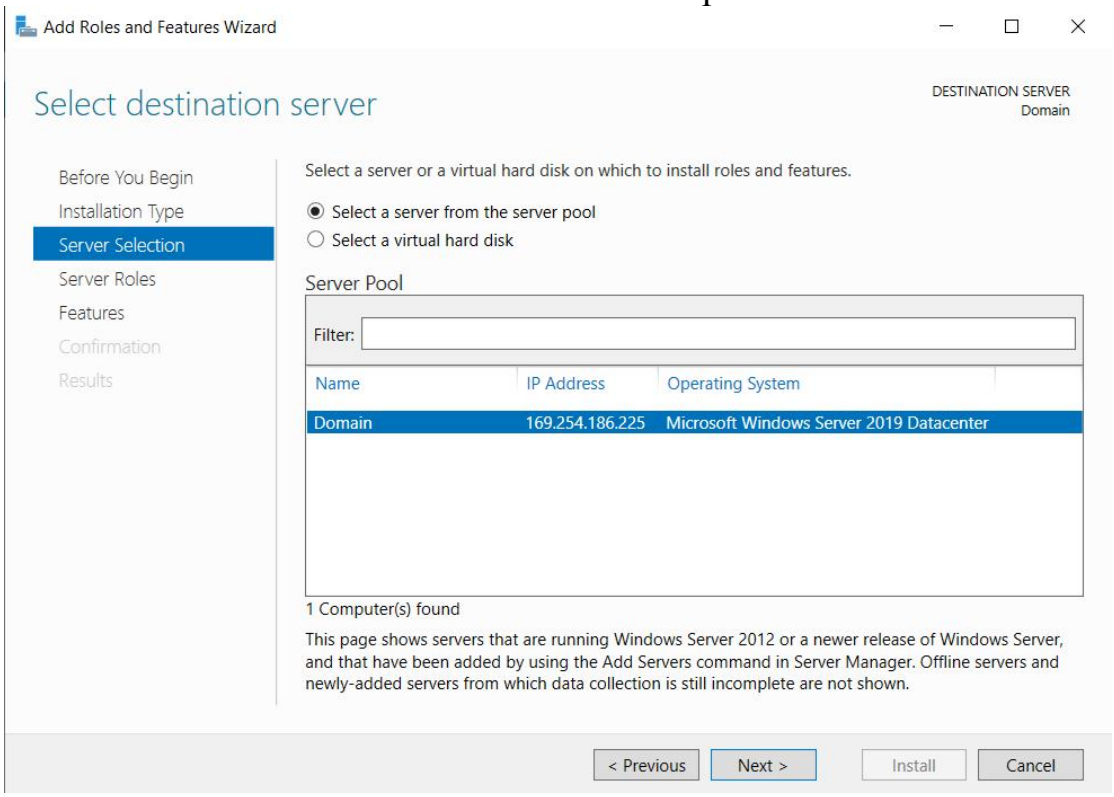
Click “Next”.



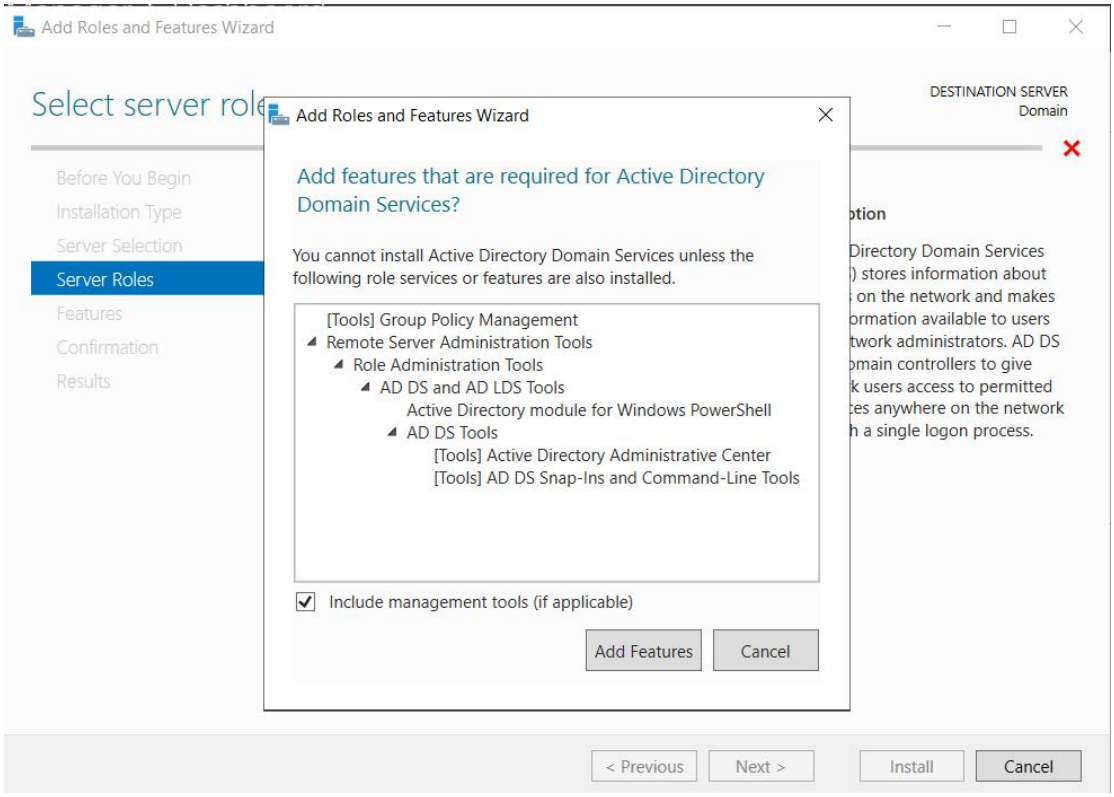
Choose “Role-based or Feature-based installation” and click “Next”.



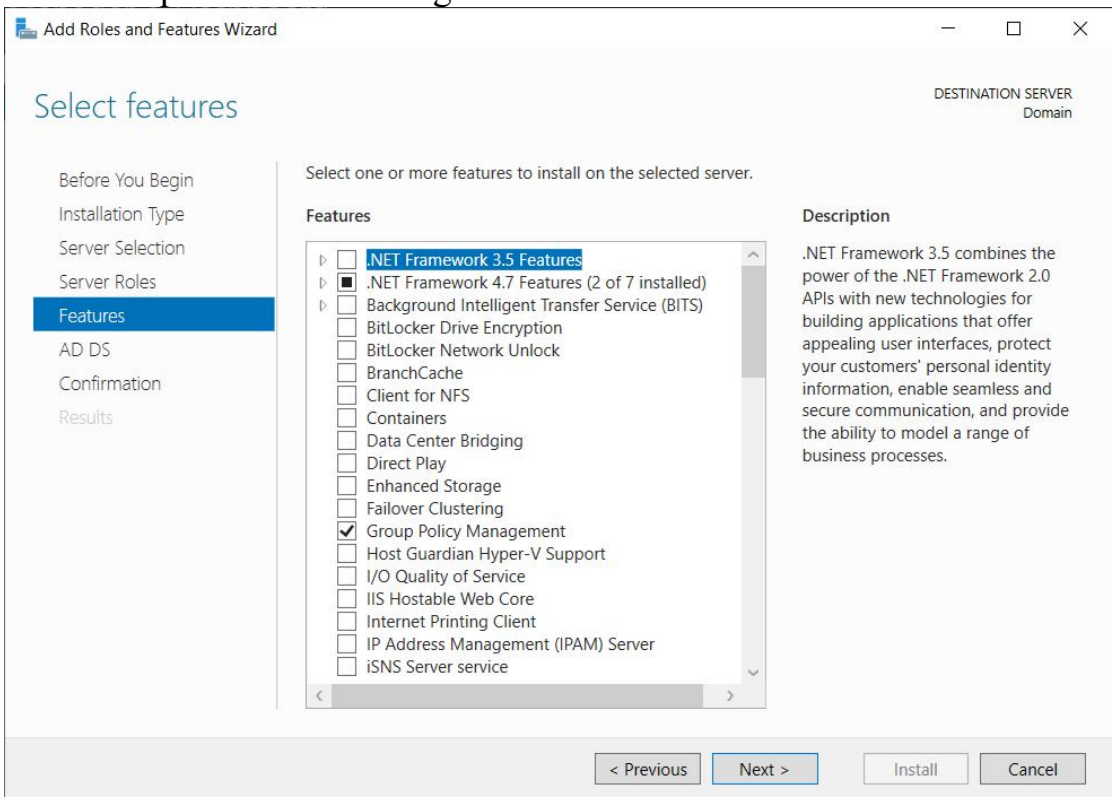
Choose “Select a server from the server pool” and click “Next”.



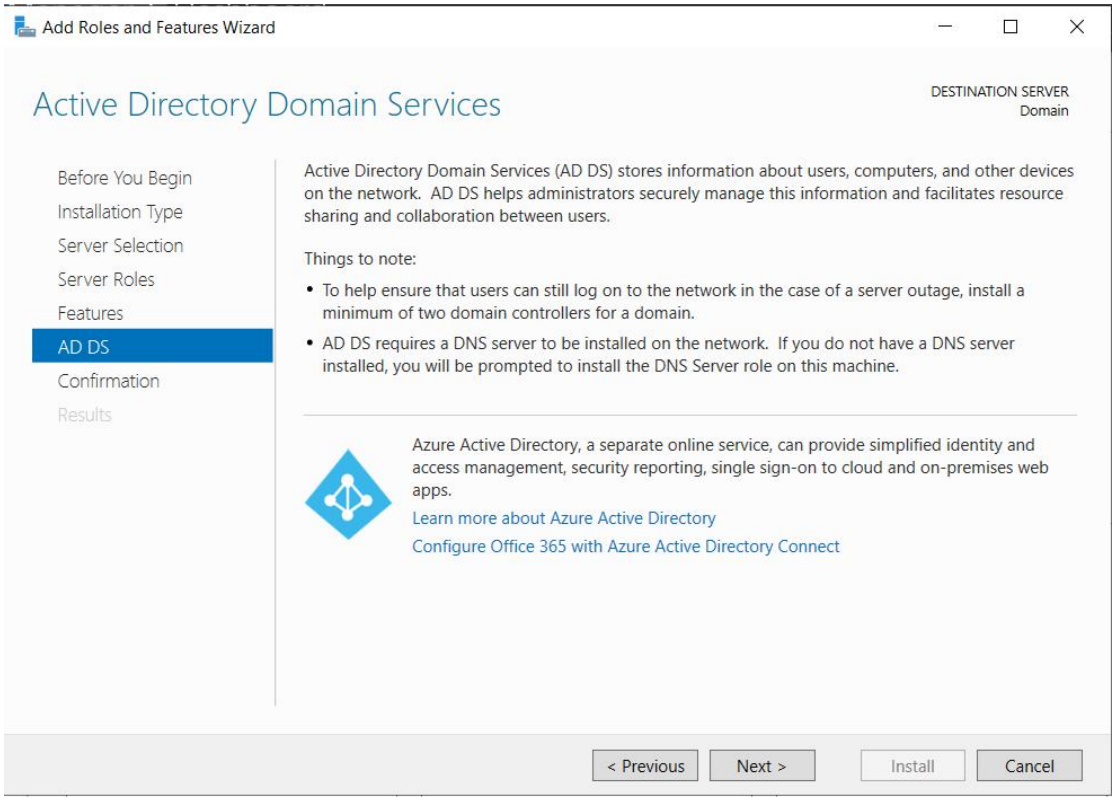
Choose “Active Directory Domain Services” and click “Add Features”.



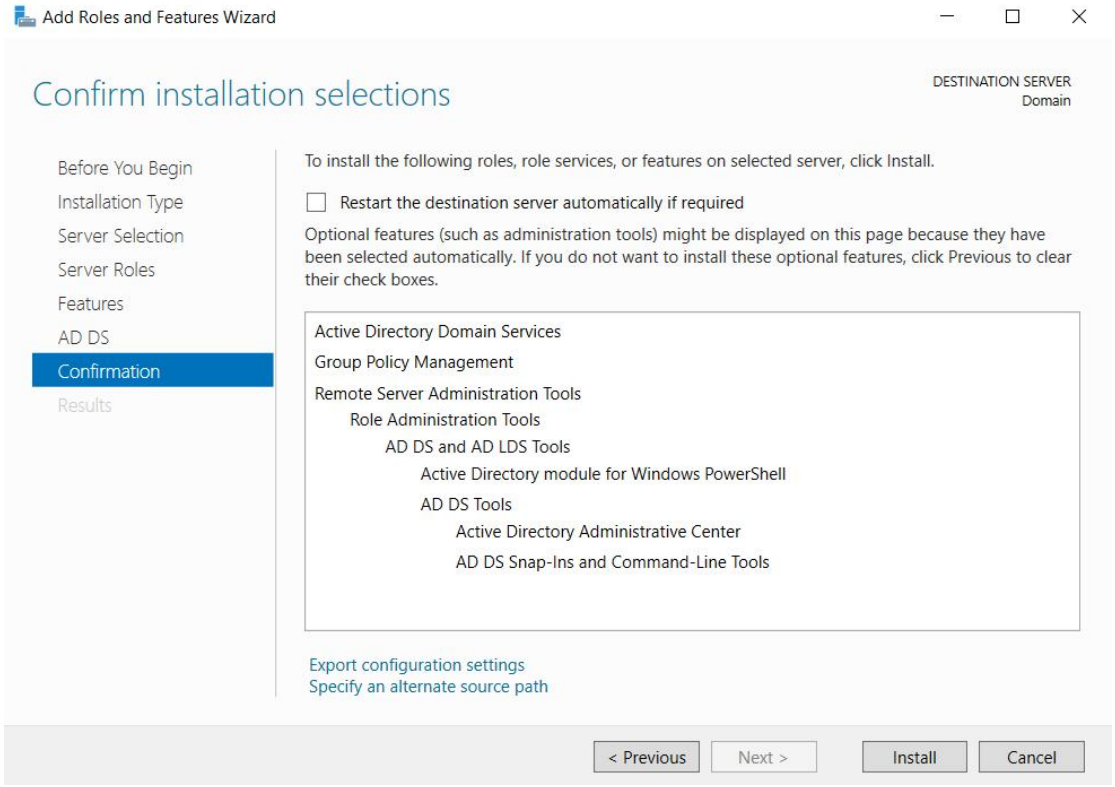
Keep the default configuration and click “Next”.



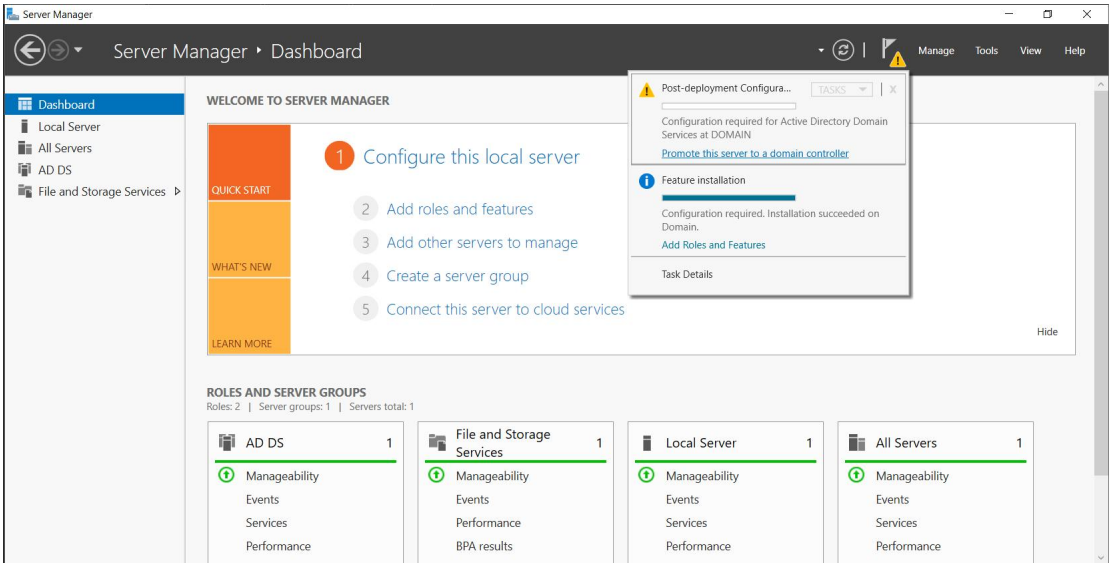
Continue to click “Next”.



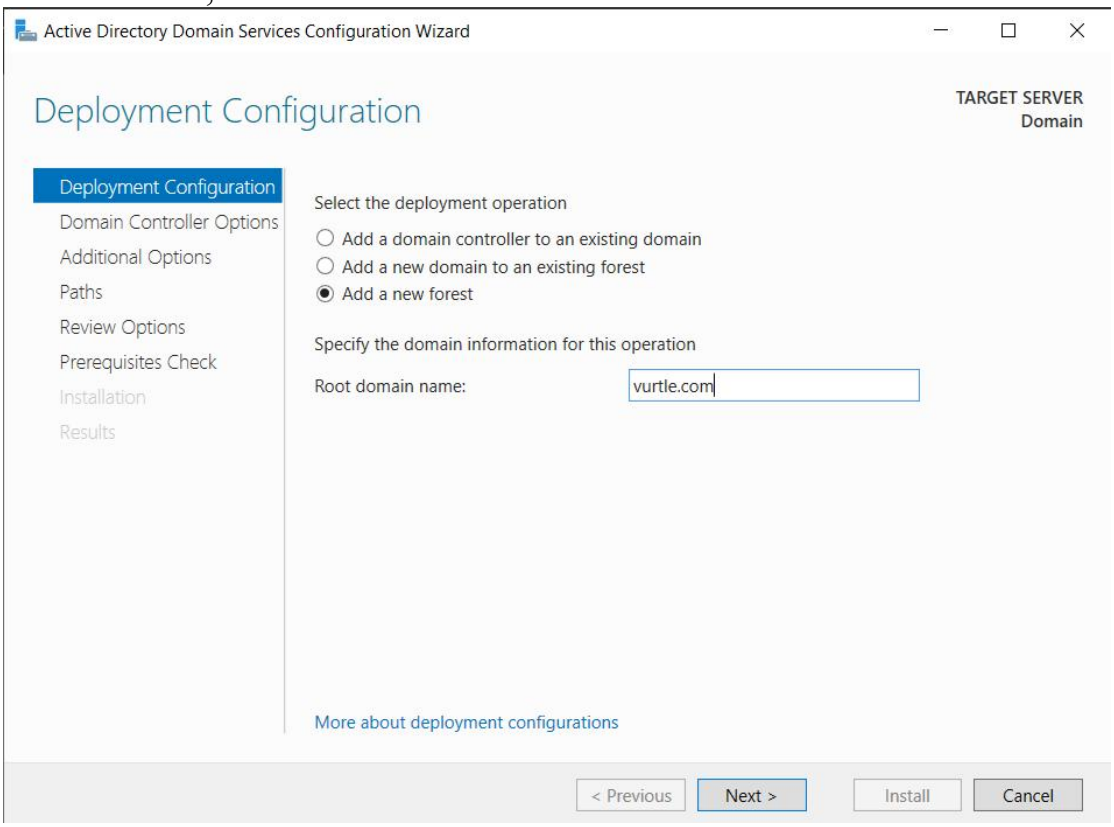
Now click the “Install” to start the installation.



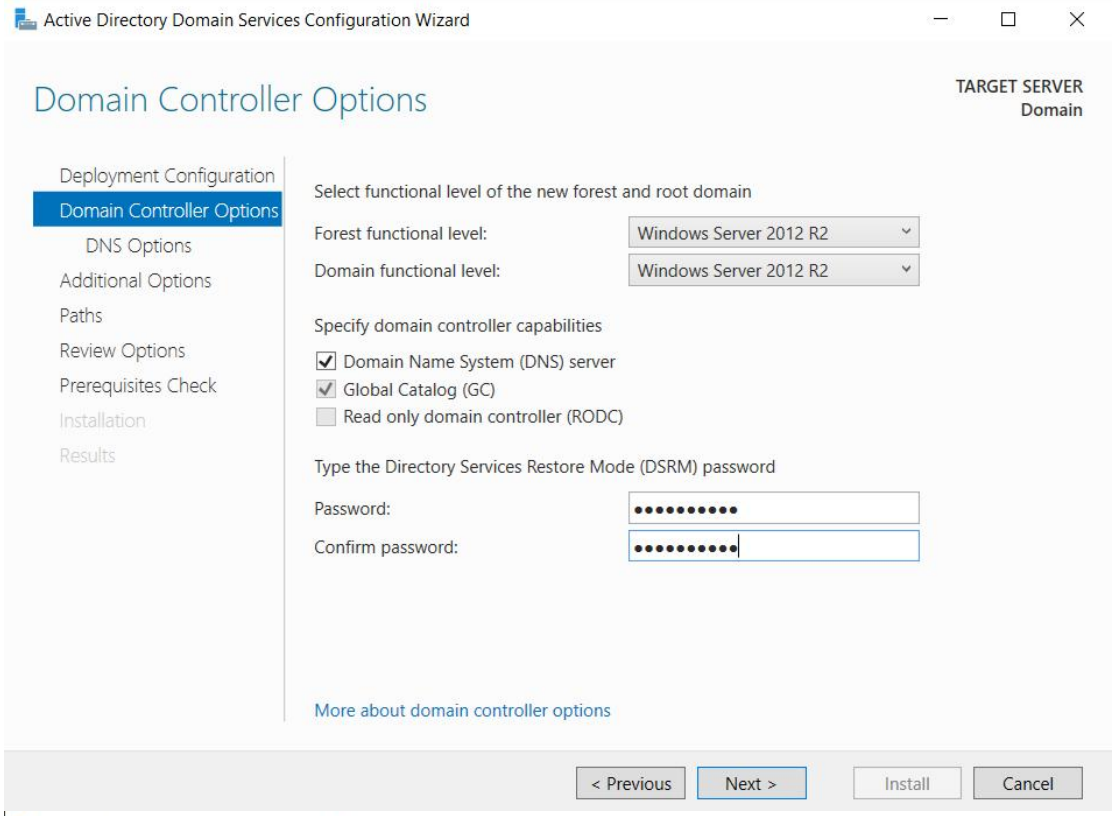
Once the installation is finished, click on the flag icon and select "Promote this server to a domain controller".

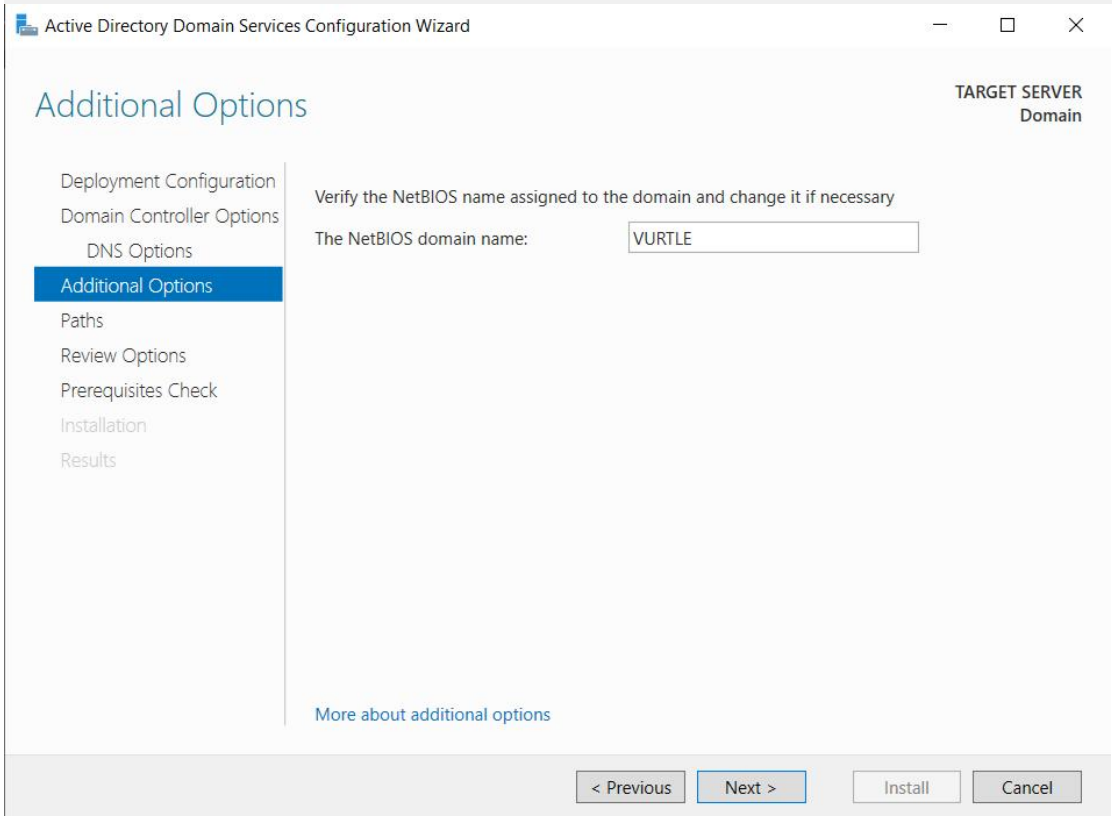


A new window will pop up. Select "Add a new forest", enter the domain name, and click "Next".

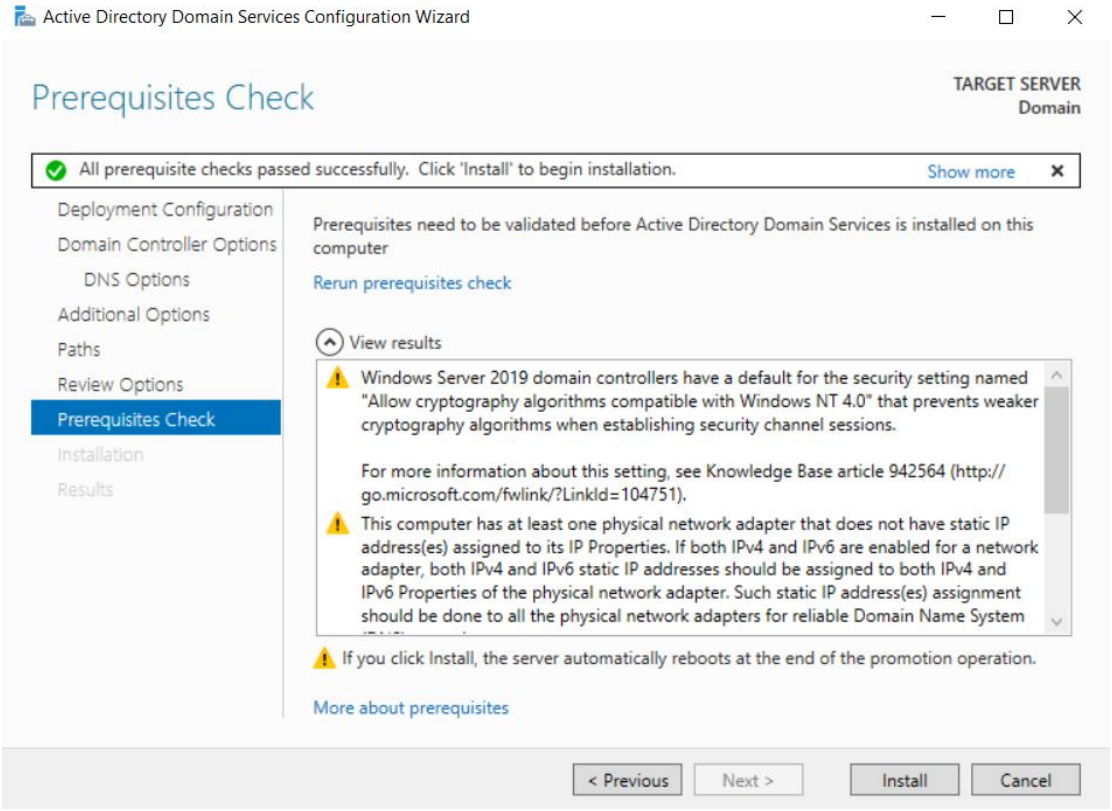


Select *Forest functional level* and *Domain function level* as "Windows Server 2012 R2", enter the password and click "Next".

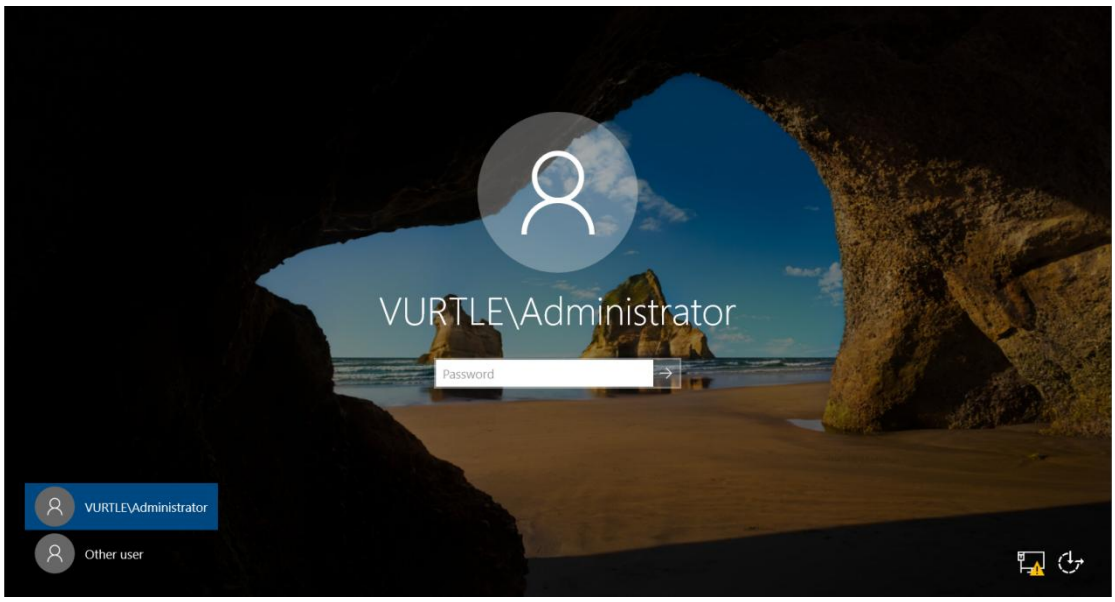




Click “Install” to start the installation.

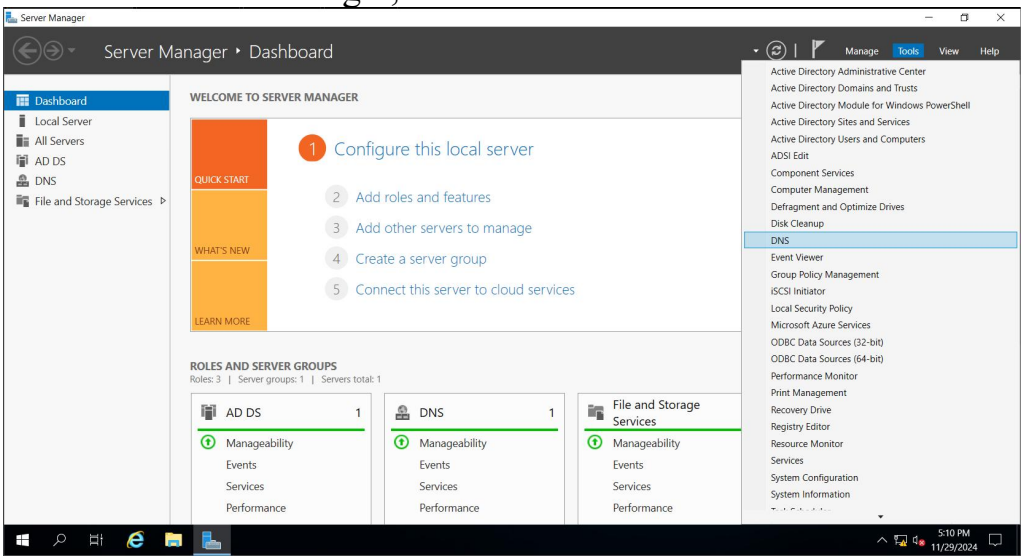


After the installation is finished, I have my device to become the DC.

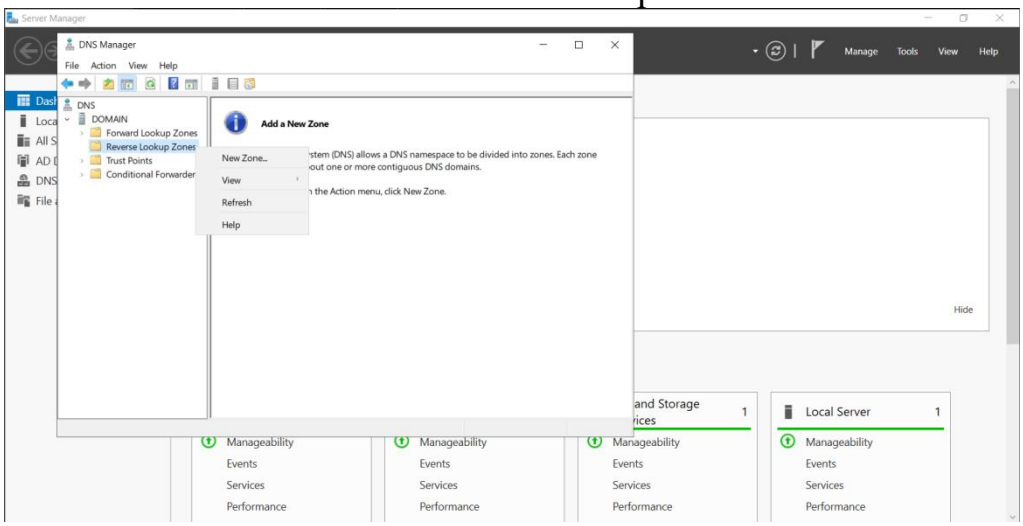


2.3.2. Configure DNS

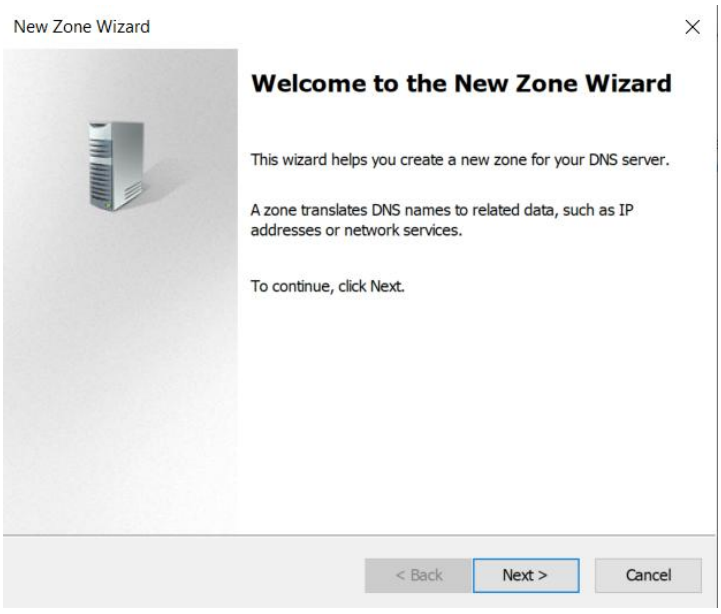
In the Server Manager, select “Tools” -> “DNS”.



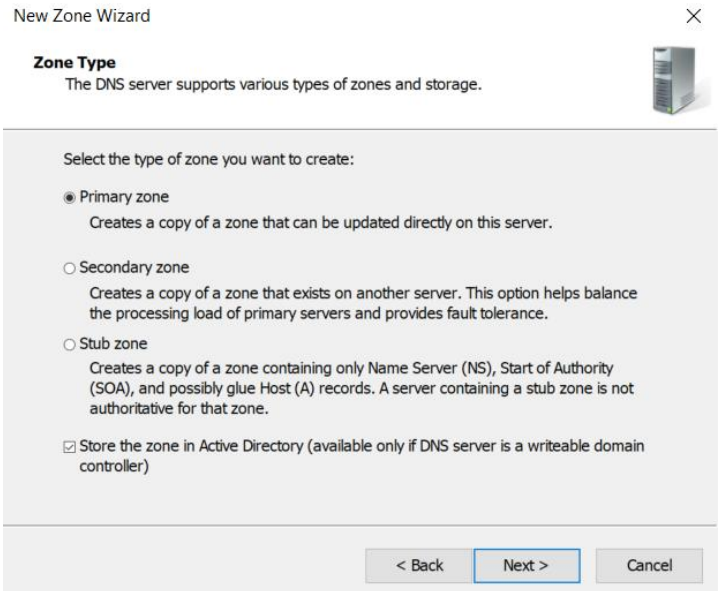
Select “DOMAIN” -> “Reverse Lookup Zones” -> “New Zones..”.

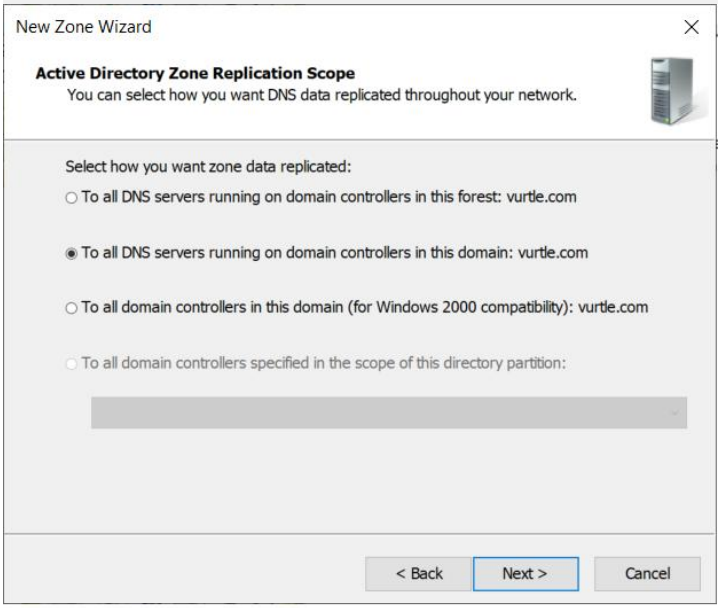


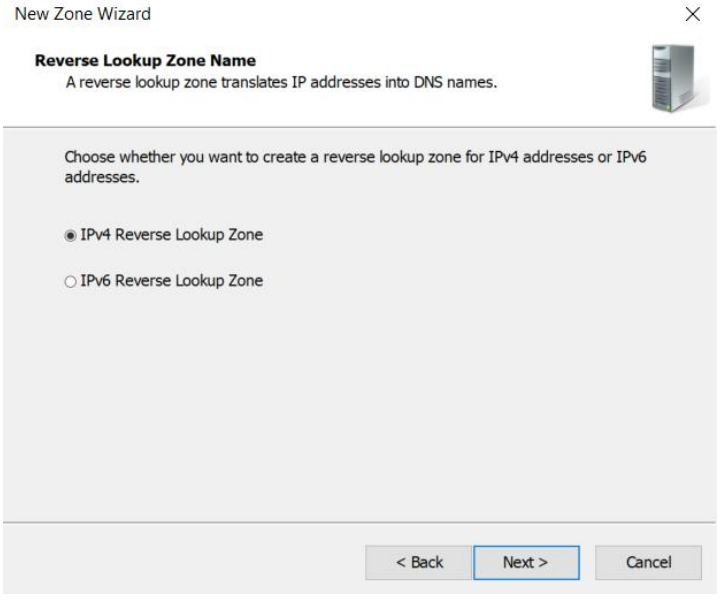
Click “Next”.

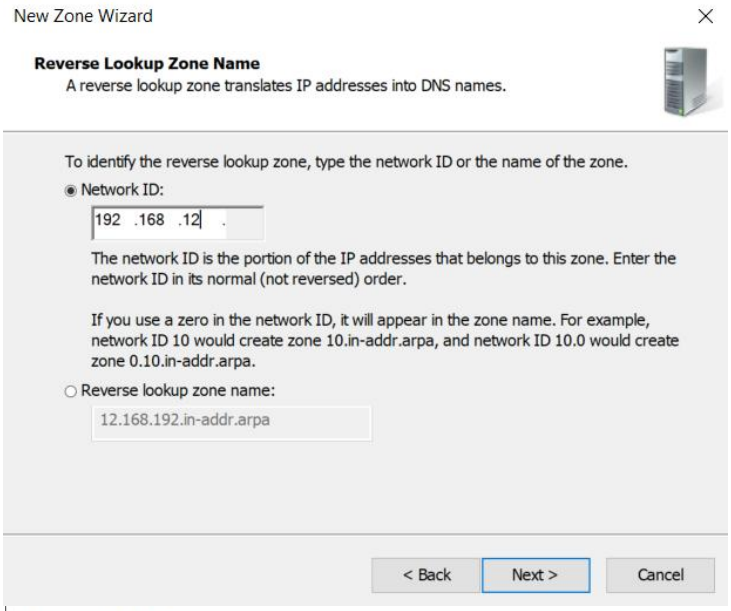


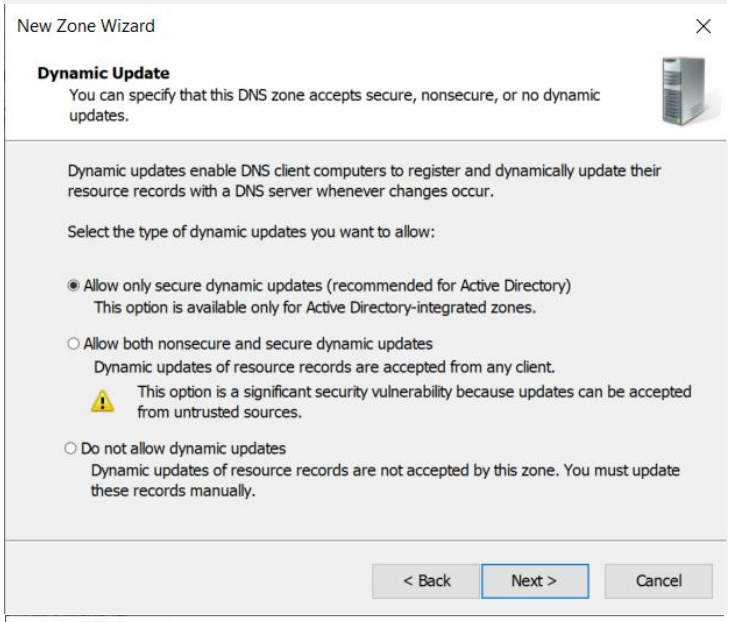
Select “Primary Zone” and click “Next”.

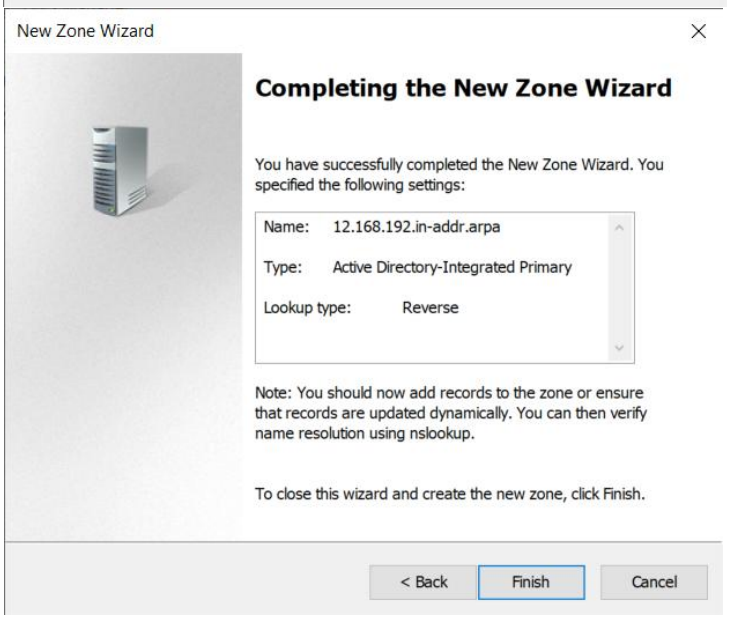


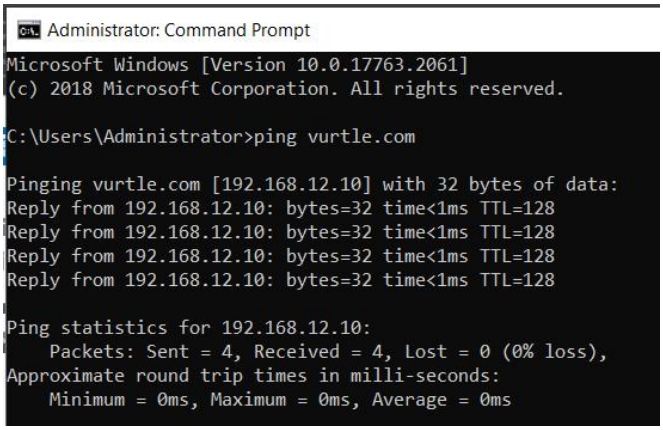





New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone.
Network ID:
192 .168 .12 .
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.
Reverse lookup zone name:
12.168.192.in-addr.arpa
< Back
Next >
Cancel

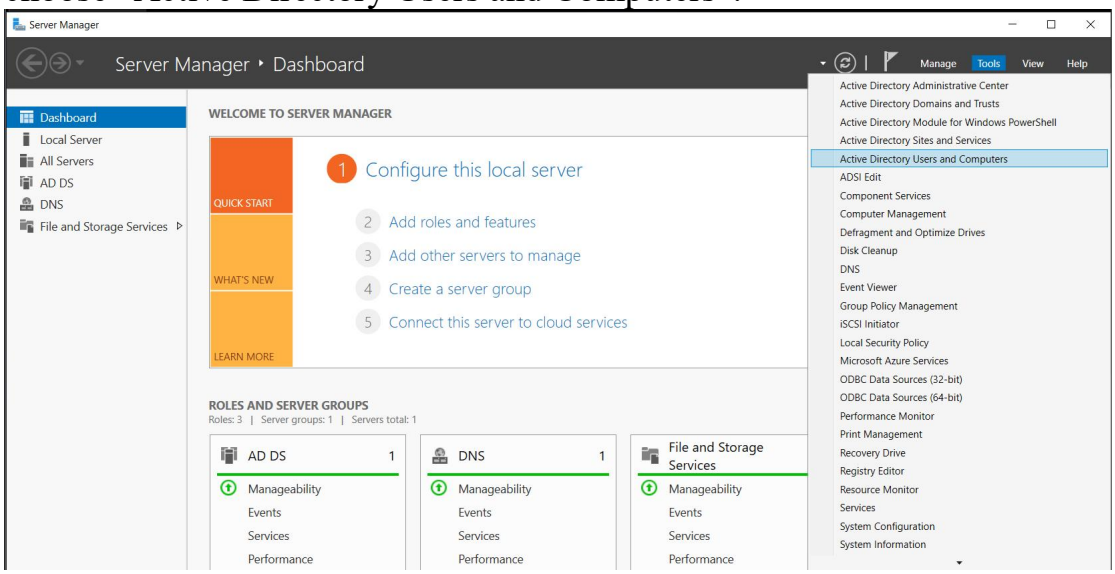

New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel


New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: 12.168.192.in-addr.arpa
Type: Active Directory-Integrated Primary
Lookup type: Reverse
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel

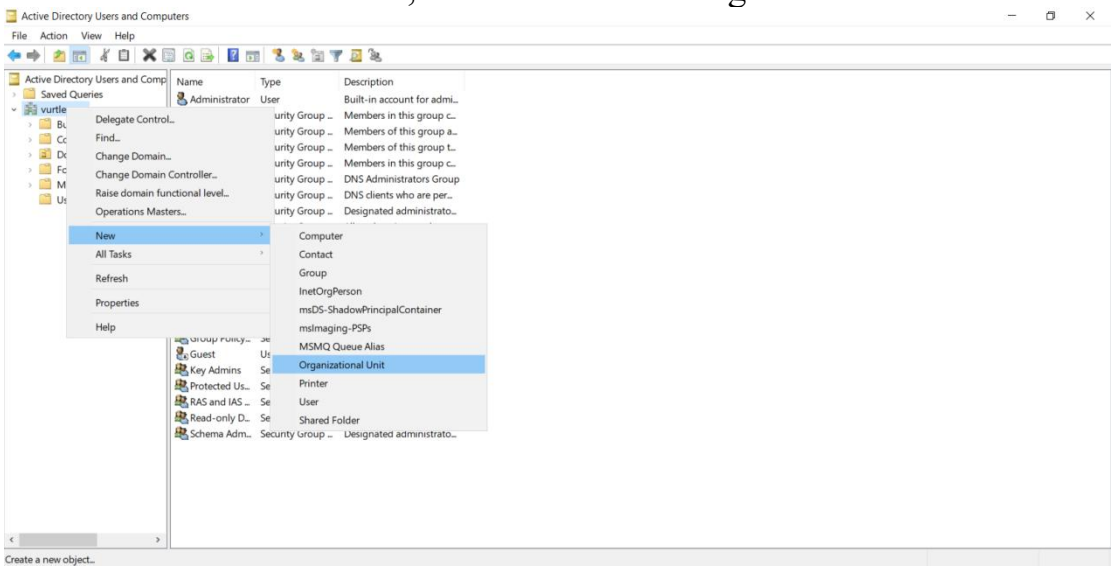


2.3.3. Create OU, Groups and Users

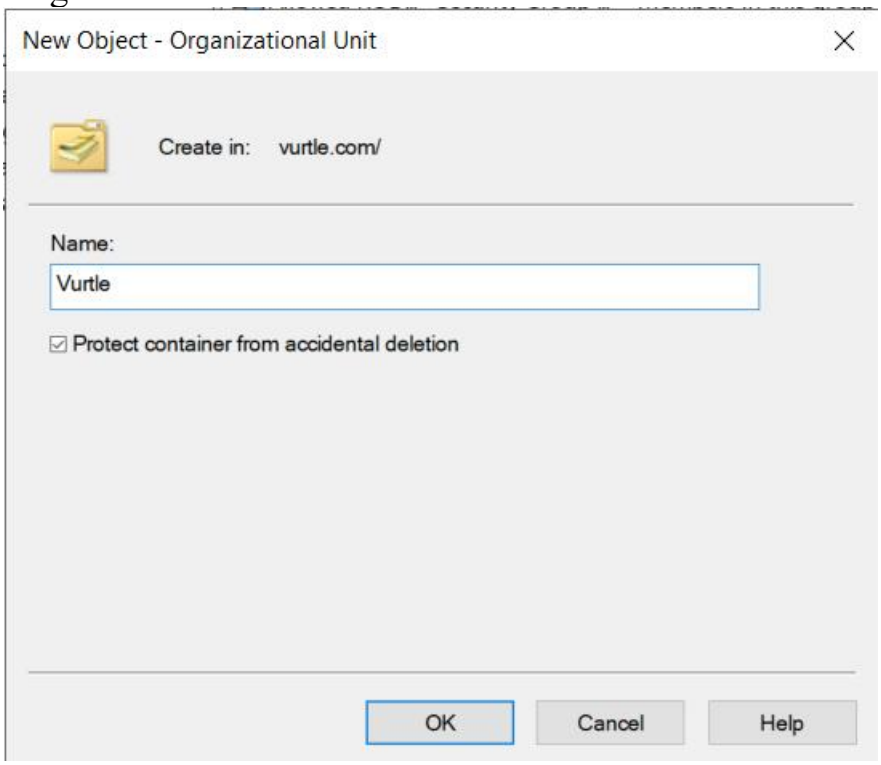
Now, create Organization Units (OU). Select “Tools” and then choose “Active Directory Users and Computers”.



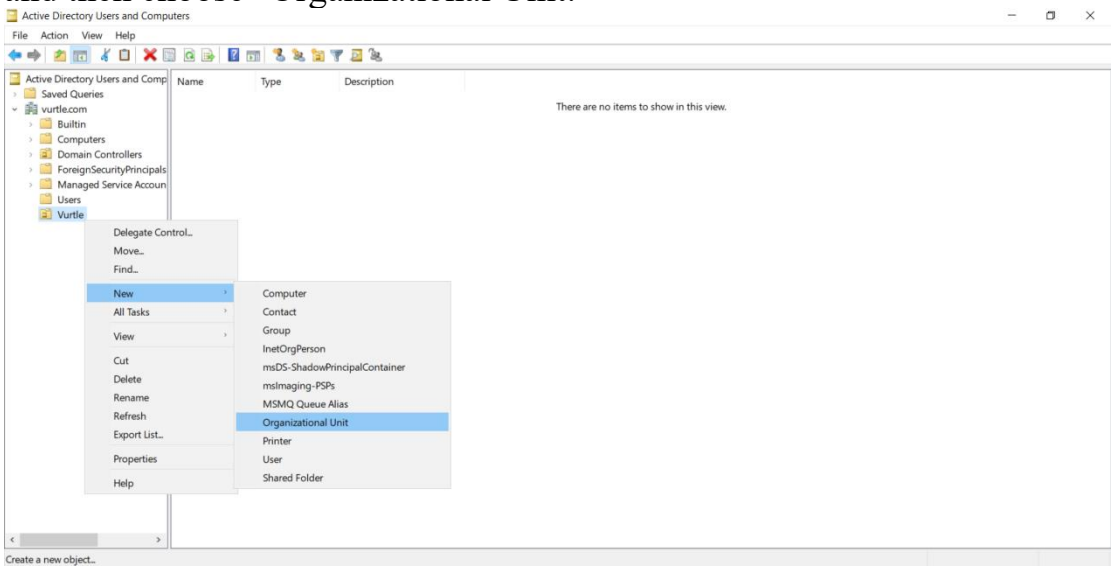
In "Active Directory Users and Computers", right-click on the domain name "vurtle.com", select "New" -> "Organizational Unit".



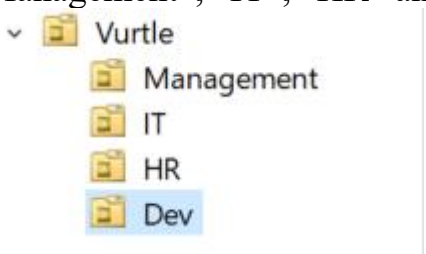
Assign a name to the OU.



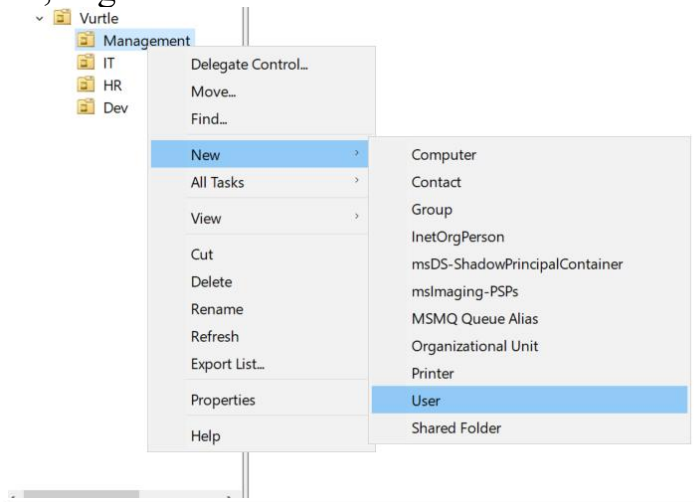
Next, I need to create additional OUs corresponding to the number of company teams. Right-click on the newly created OU, select "New", and then choose "Organizational Unit."

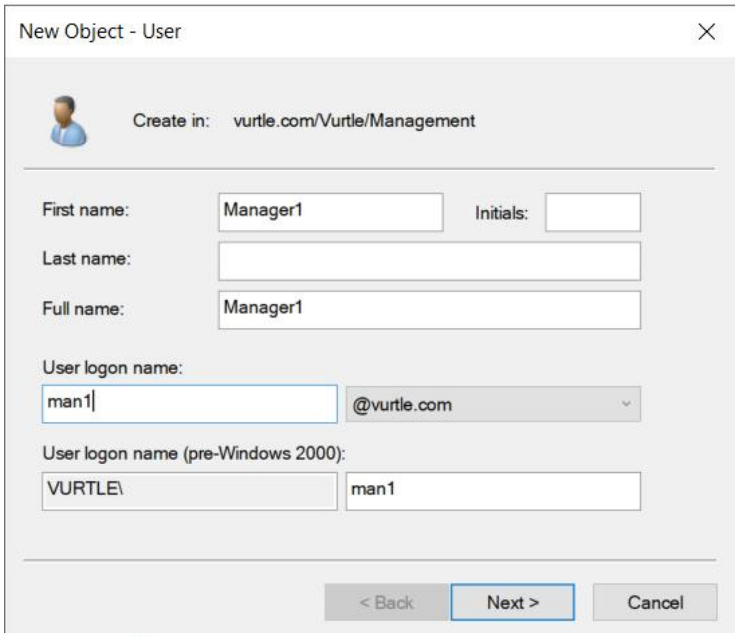


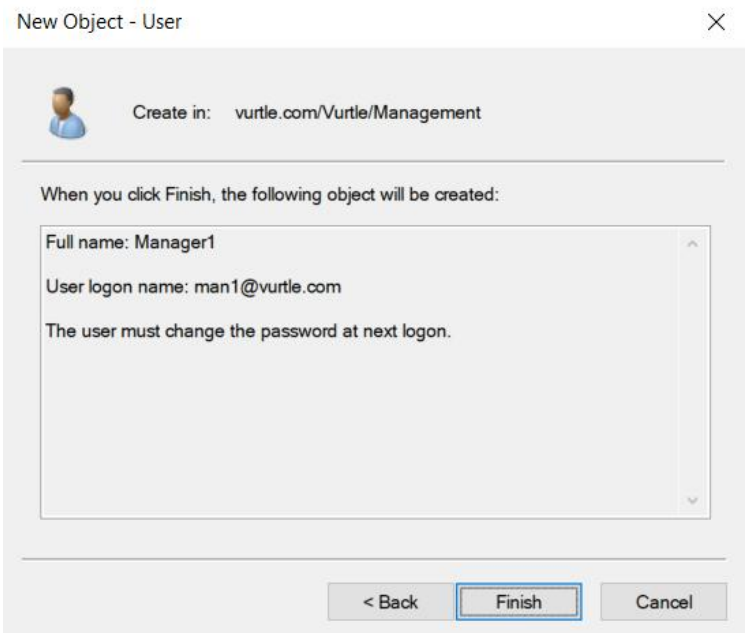
Create 4 teams: “Management”, “IT”, “HR” and “Dev”.

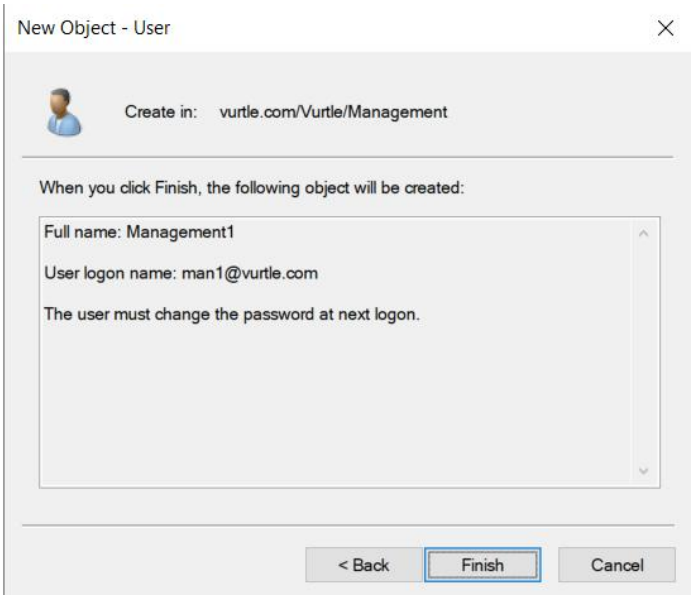


In each OU, I will create users and groups. Start with “Management”, Right-click on it choose “New” -> “User”.

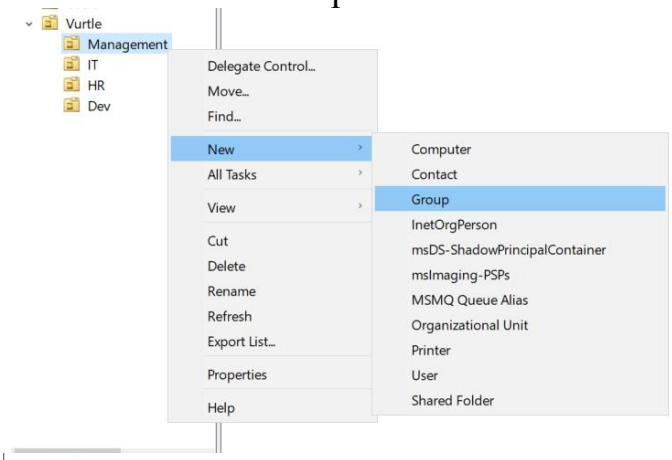


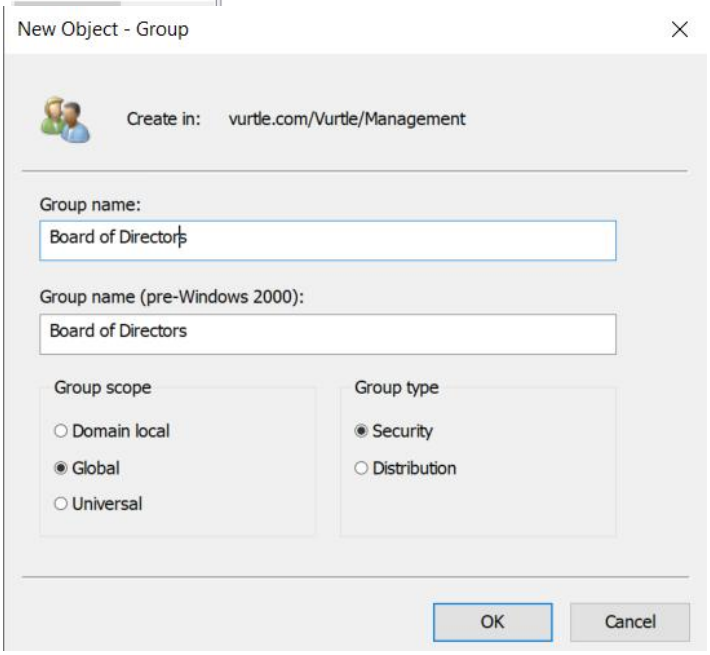




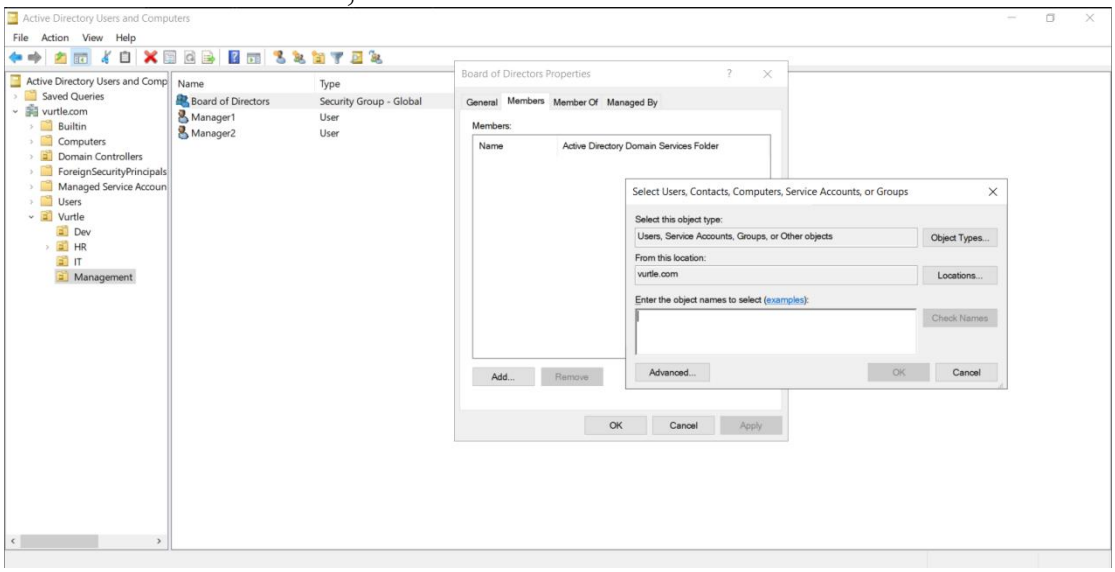


Now, I will create a group to manage the users. Right-click on "Management" -> "New" -> "Group".

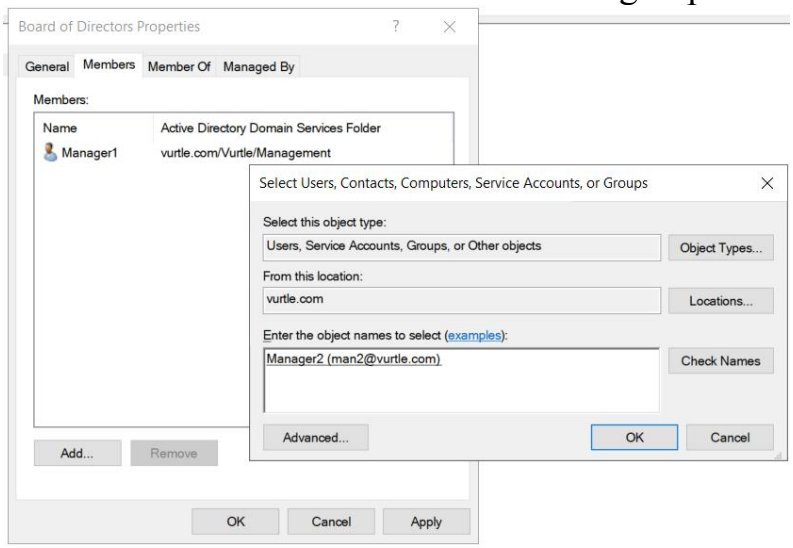




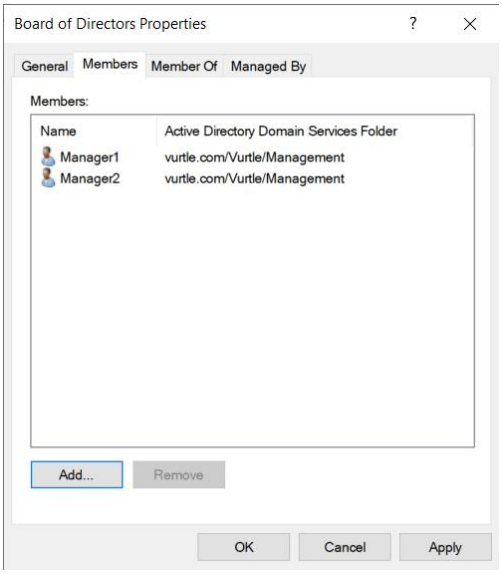
Next, add the users to the group. Select “Board of Directors” group, choose “Members” tab, click “Add…”.

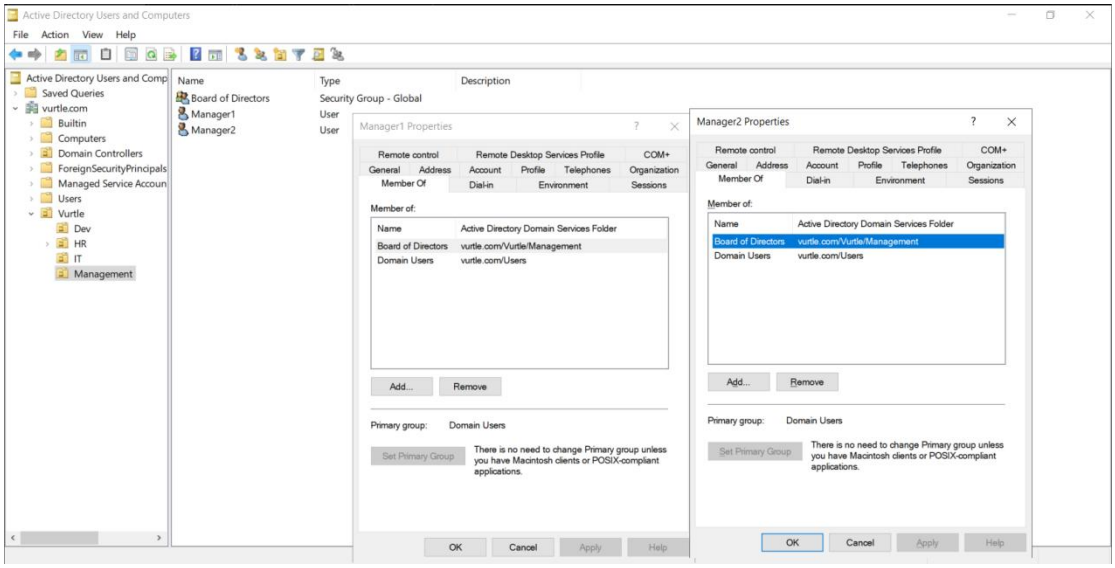


Enter the names of the users and add into the group.

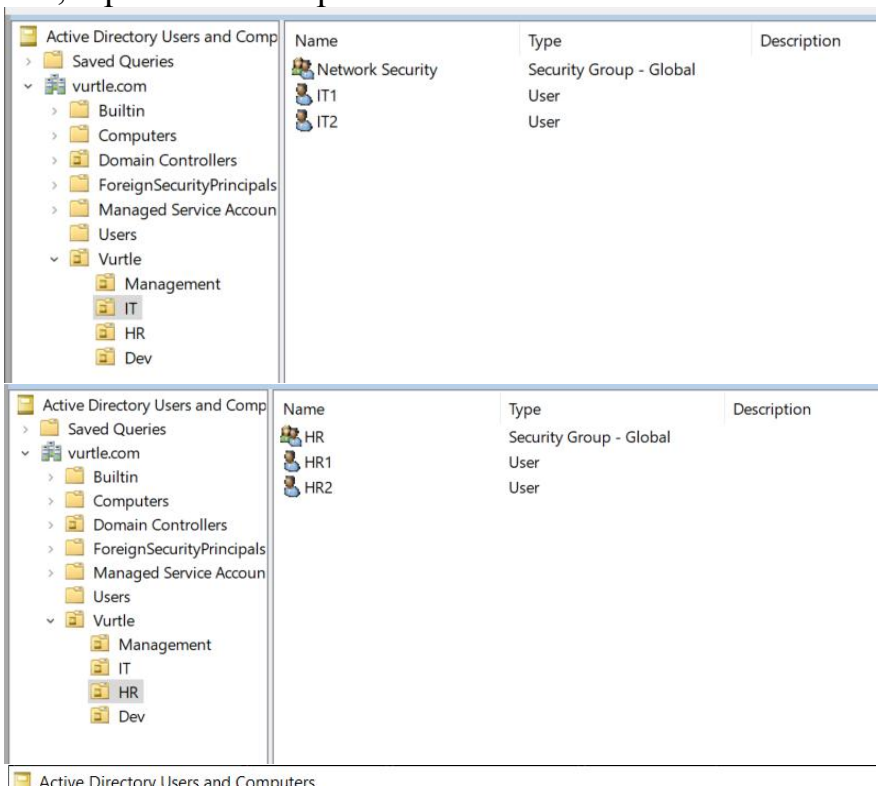


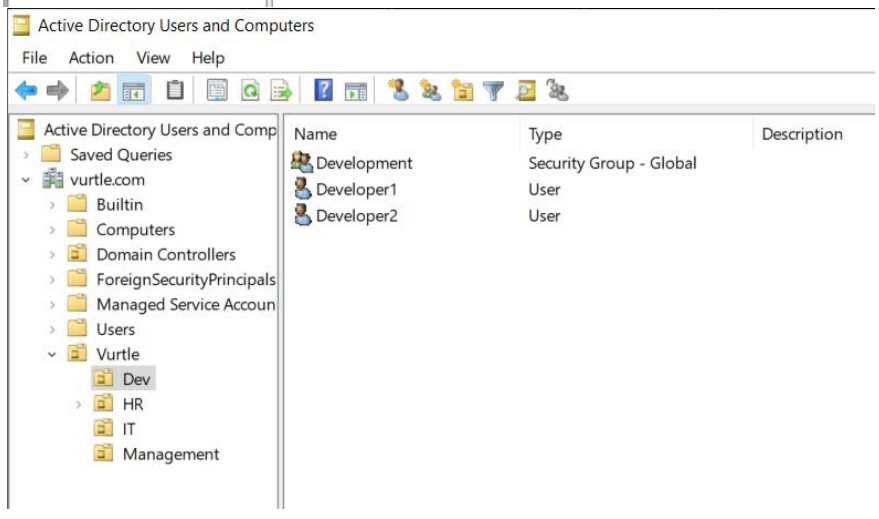
Click “Apply” and “OK”.





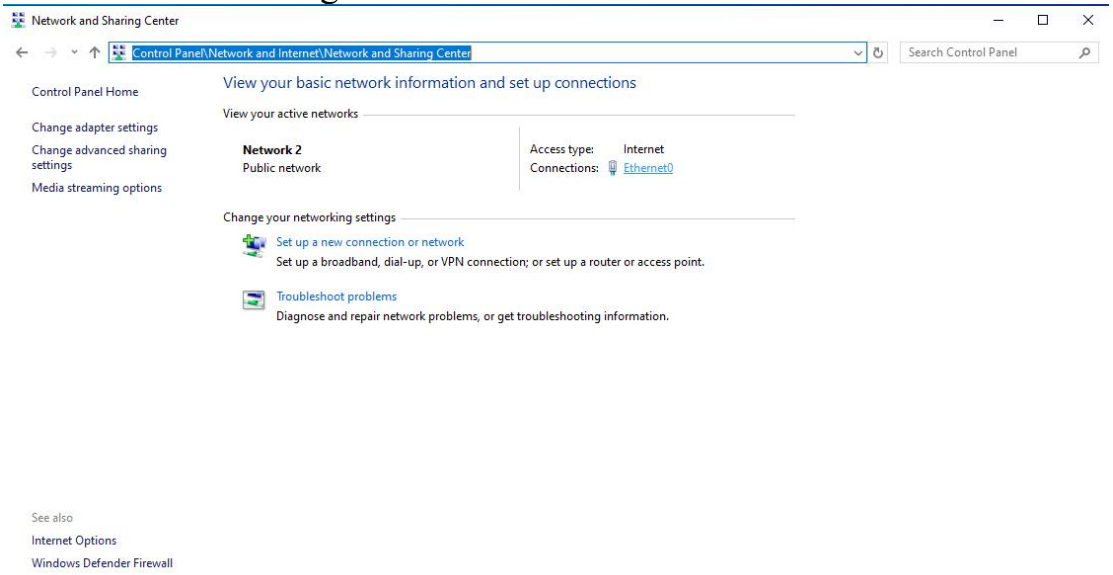
Now, repeat the same process for the other OUs.



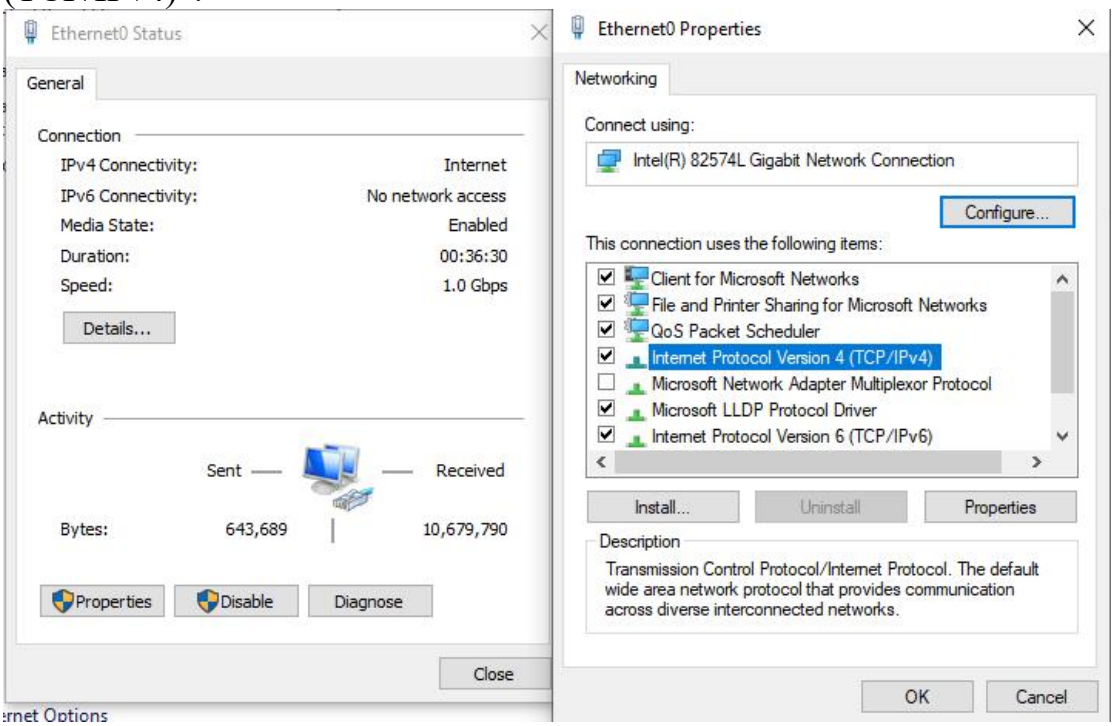


2.3.4. Join Domain

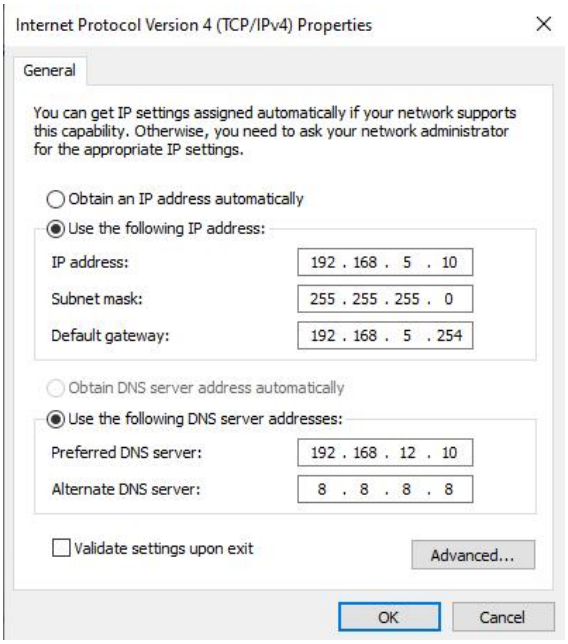
Now I need to have devices in the LAN to join the Domain. At the BoD device, open "Control Panel", choose "Network and Internet" -> "Network and Sharing Center" then click "Ethernet0".



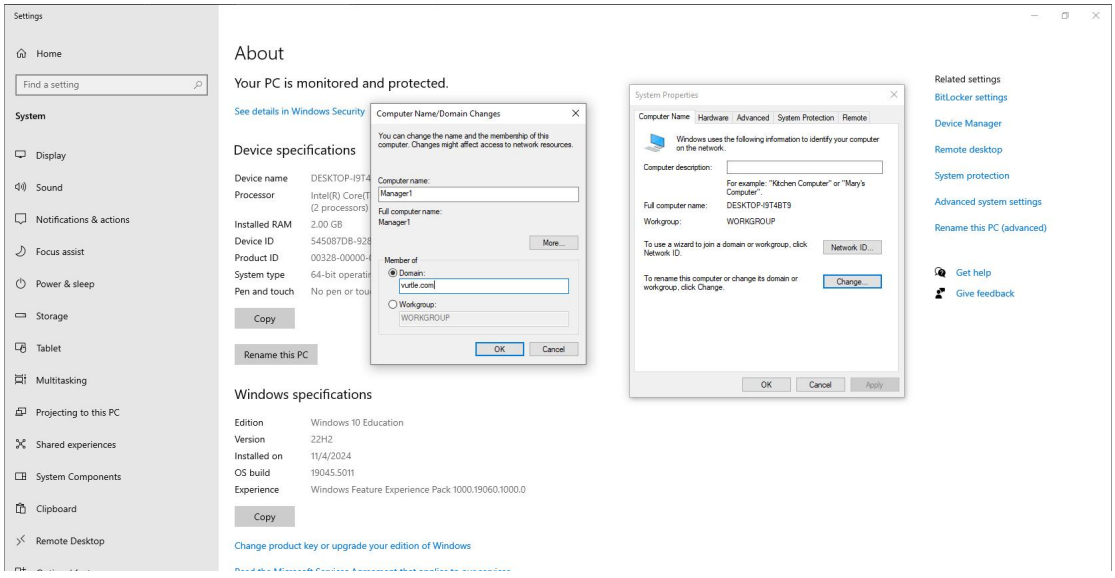
Click "Properties", double-click "Internet Protocol Version 4 (TCP/IPv4)".



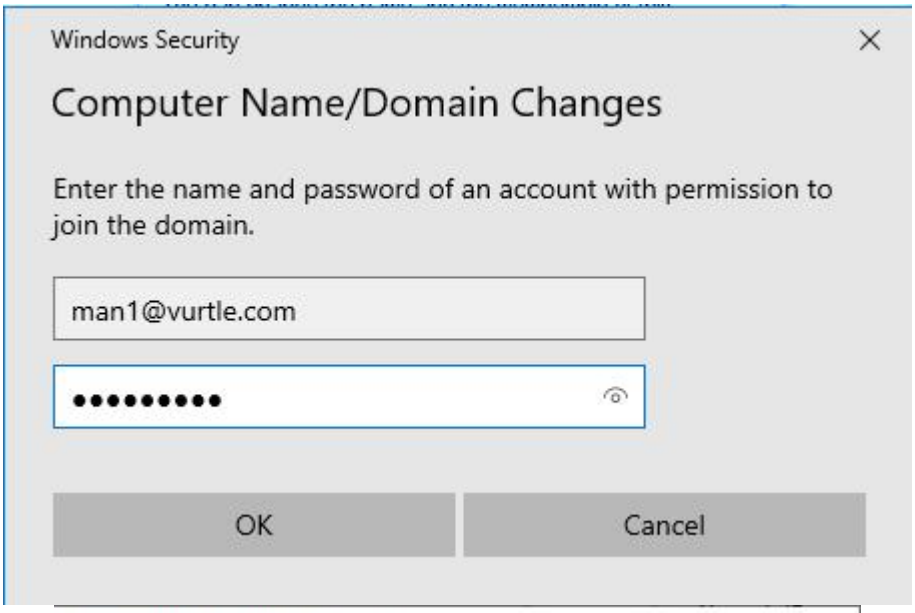
Assign IP address and DNS server addresses.

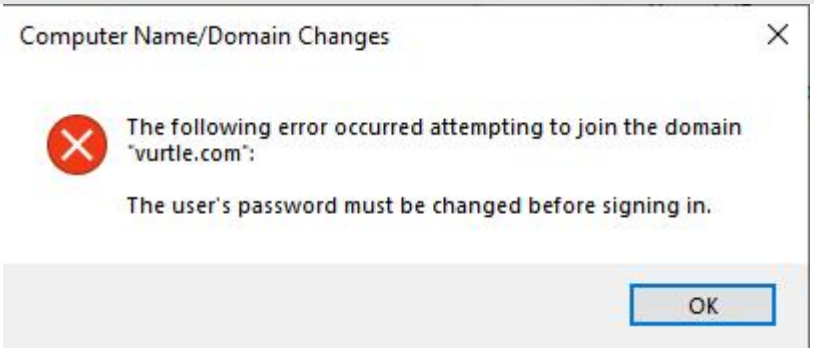


Open the “Settings” application, search for “About”, and under “Related settings”, click on “Advanced system settings”. Navigate to the “Computer Name” tab and click on “Change…”. Set the “Computer name” to “Manager1”. Under the “Member of” section, select “Domain” and enter the domain name as “vurtle.com”.

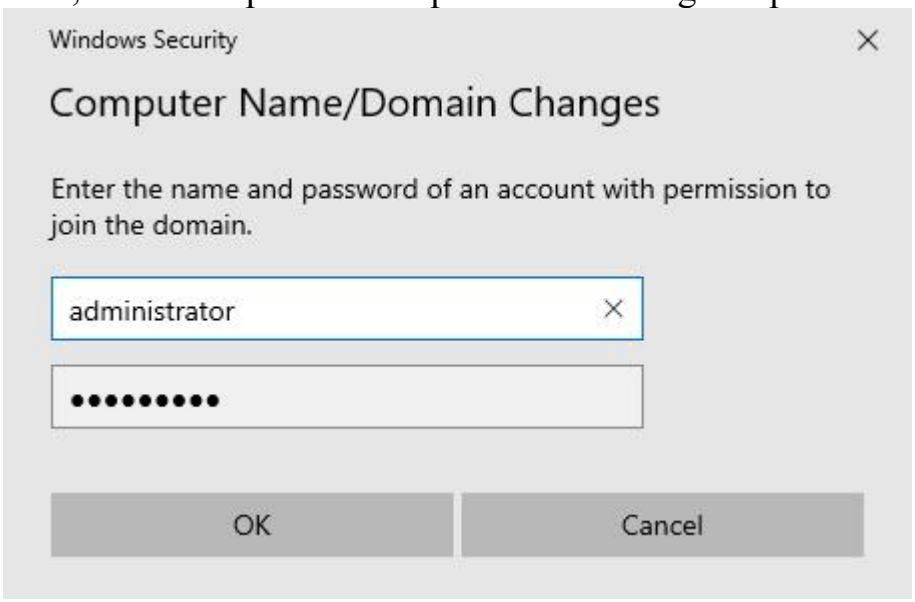


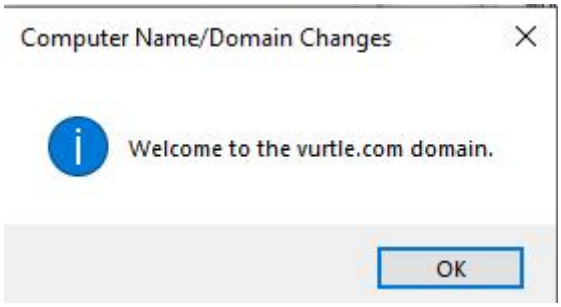
A window will appear prompting you to enter credentials, provide the “Manager1” credentials that were created on the domain server.



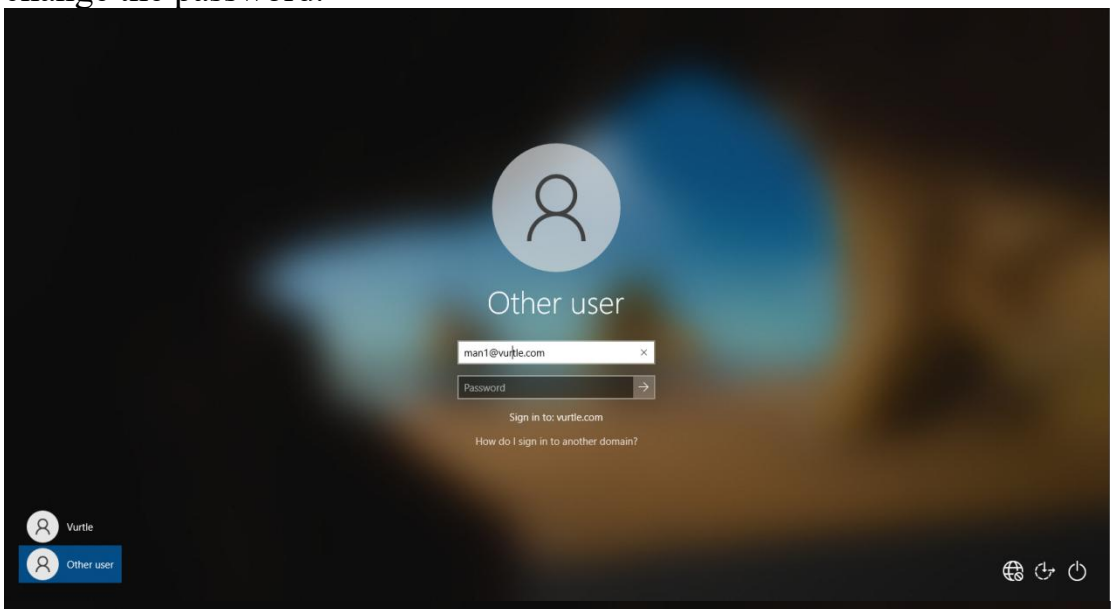


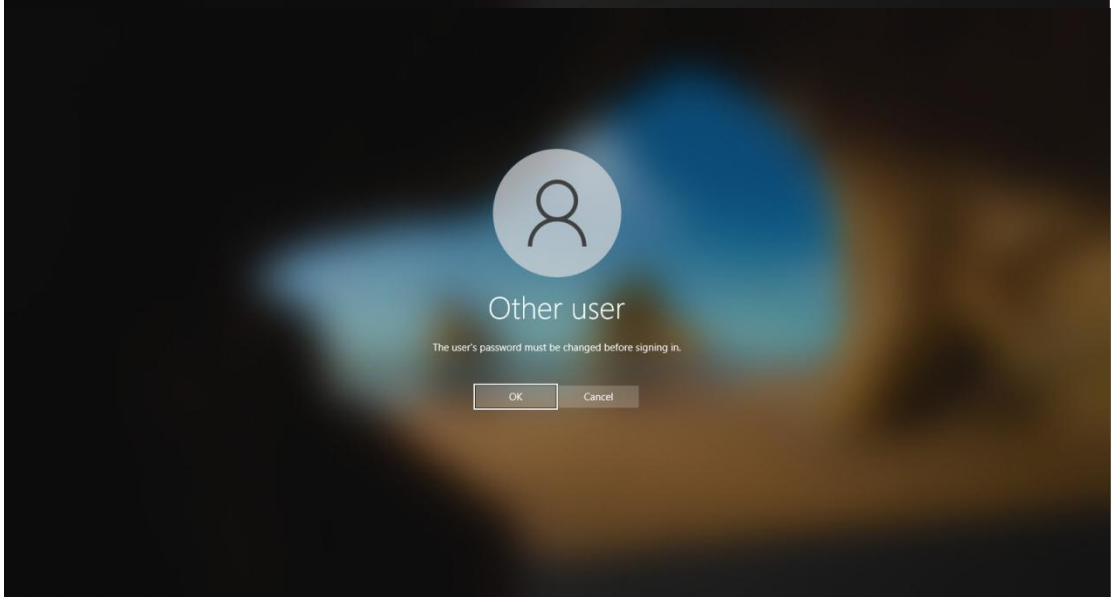
When creating the “Manager1” and other accounts, I enabled the option requiring users to change their passwords upon first login. Therefore, I must first enter the administrator credentials to gain access to the domain, then I can proceed to update the “Manager1” password.

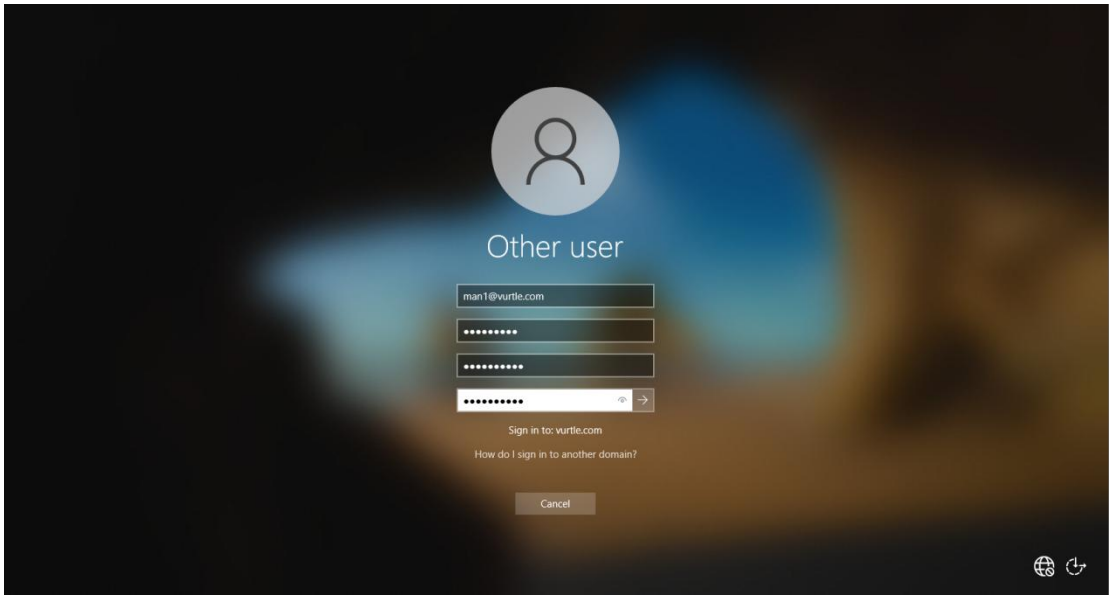




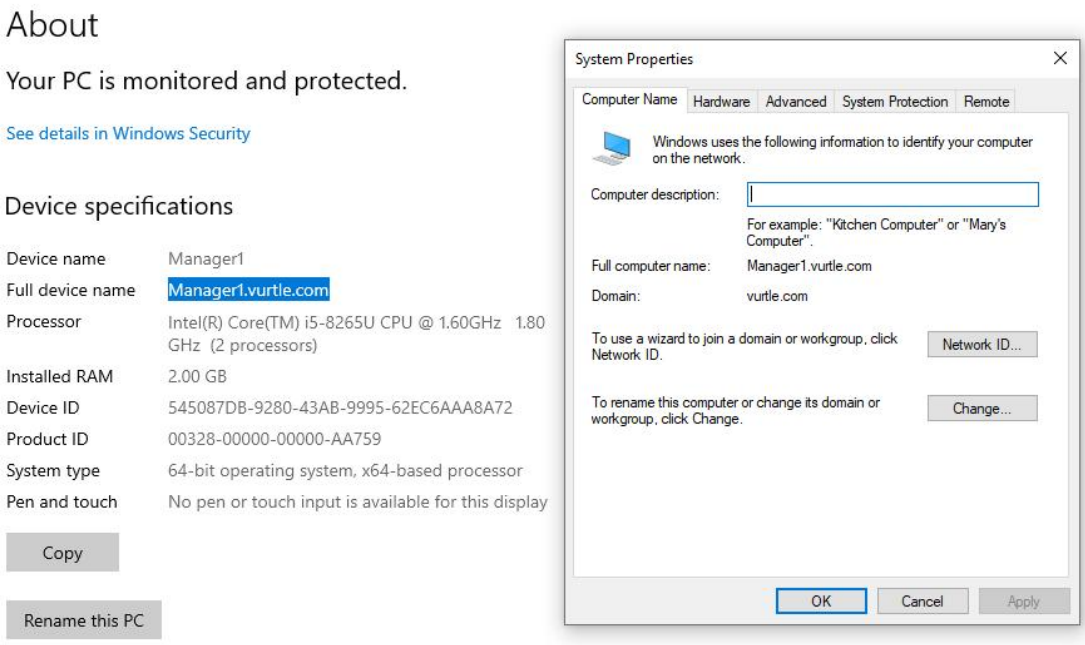
Now, I can log in using the “Manager1” account and proceed to change the password.







The device has successfully joined the domain. By repeating the same process on other devices across different networks, I can have all users join the domain and begin managing them effectively.



3. Conclusion

The successful implementation of this project will establish a robust, secure, and scalable network infrastructure, specifically tailored to meet the organization's needs. By segmenting the network into dedicated subnets, deploying centralized security measures, and configuring efficient routing and switching protocols, the design ensures optimized performance, enhanced security, and seamless communication across departments.

This infrastructure will support essential services such as Active Directory, facilitate future scalability, and ensure high availability for business continuity. The project will provide a solid foundation for the organization’s IT operations, enabling efficient resource management, fostering improved collaboration, and safeguarding against cybersecurity threats.

Through thorough testing, comprehensive documentation, and a focus on reliability, this network design will empower the organization to achieve its operational objectives while adapting seamlessly to future growth.