

CORPORATE NETWORK DESIGN

PERSONAL PROJECT REPORT

by

ĐỖ KHẮC VĨ

Ho Chi Minh city
11/2024

Declaration by Author

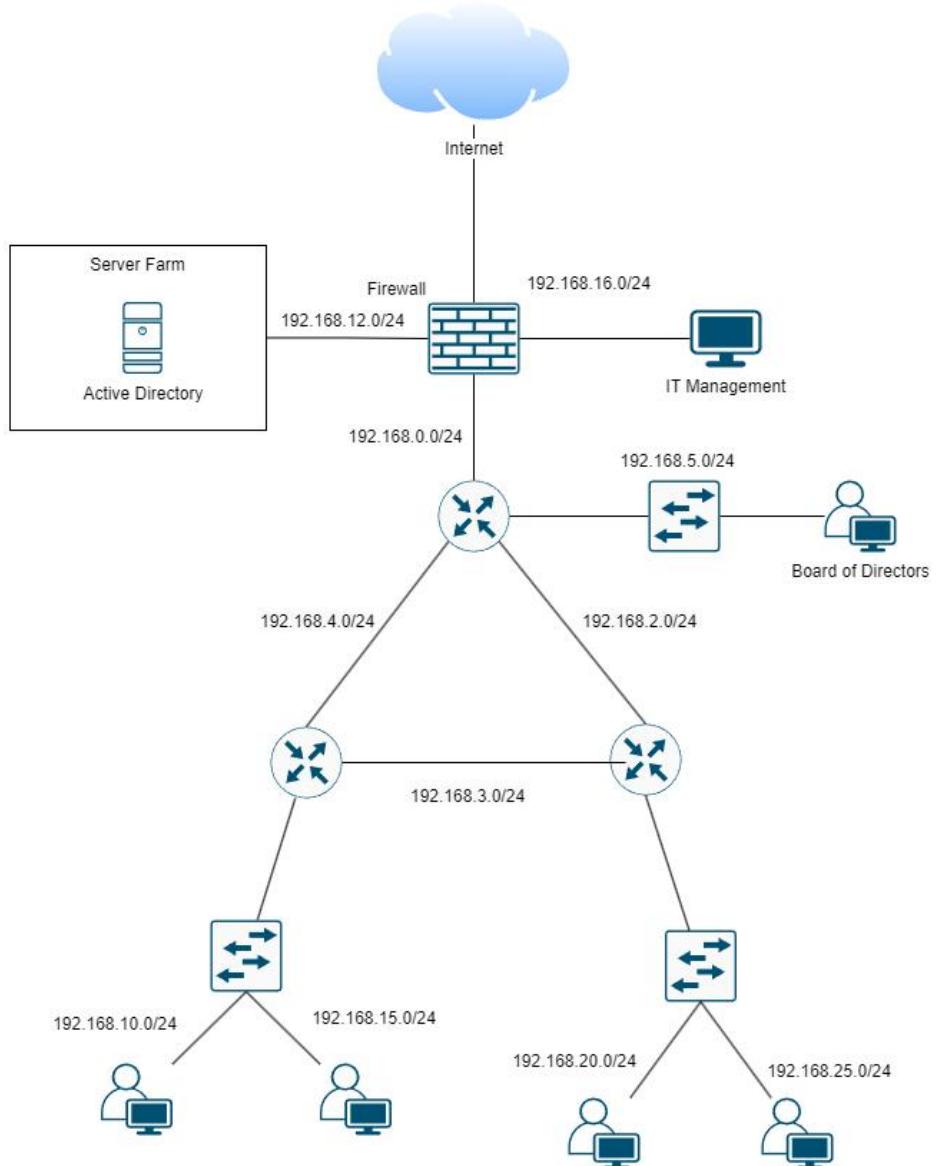
This is to declare that this report has been written by me. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I aver that if any part of the report is found to be plagiarized, I shall take full responsibility for it.

Đô Khắc Vĩ

Table of Contents

Table of Contents	- 3 -
1. Introduction	- 4 -
2. Establishing the network	- 6 -
2.1. LAN	- 6 -
2.1.1. Fundamental Configuration	- 6 -
2.1.2. Routing protocol	- 7 -
2.1.3. VLAN	- 10 -
2.1.4. NAT	- 13 -
2.1.5. Access Control List	- 14 -
2.2. Firewall	- 17 -
2.2.1. Firewall Configuration	- 17 -
2.2.2. Basic rules	- 23 -
2.2.3. Active Directory rules	- 27 -
2.3. Active Directory	- 28 -
2.3.1. Set up Active Directory	- 28 -
2.3.2. Configure DNS	- 35 -
2.3.3. Create OU, Groups and Users	- 38 -
2.3.4. Join Domain	- 44 -
3. Conclusion	- 49 -

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.

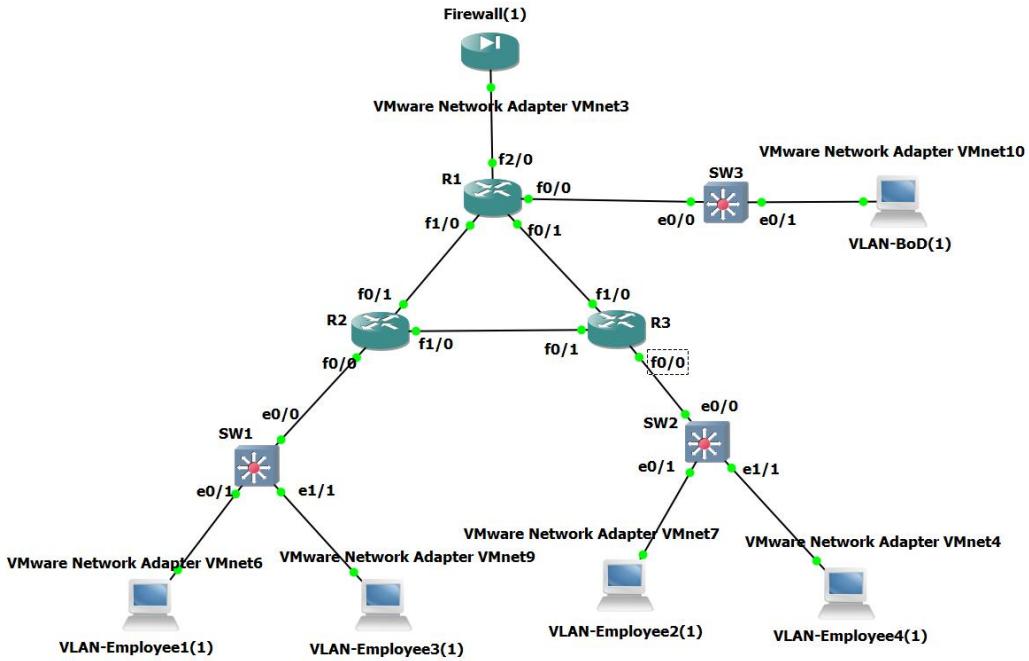
Router: Cisco IOS Software (C3725-AdvEnterpriseK9-M), Version 12.4(15)T14.

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 prevent 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 vrtle123
R2(config)#line vty 0 4
R2(config-line)#password vrtle123
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 vrtle123

R3(config)#line vty 0 4

R3(config-line)#password vrtle123

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 to 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 vrtle123
SW2(config-line)#login
SW2(config-line)#exit
SW2(config)#line vty 0 4
SW2(config-line)#password vrtle123
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.

```

1:root@ubuntu:/home/ubuntu ~
[sudo] password for ubuntu:
ubuntu@ubuntu:~$ sudo -s
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data.
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=14.4 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=7.18 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=4.08 ms
...
--> 192.168.10.254 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 4.075/8.555/14.415/4.332 ms
root@ubuntu:/home/ubuntu# telnet 192.168.10.254
Trying 192.168.10.254...
Connected to 192.168.10.254.
Escape character is '^J'.
User Access Verification

Password:
R2>ena
R2>enable
Password:
R2>show ip int br
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0     unassigned      YES NVRAM up           up
FastEthernet0/0.1   192.168.10.254 YES NVRAM up           up
FastEthernet0/0.2   192.168.15.254 YES NVRAM up           up
Serial0/0           unassigned      YES NVRAM administratively down down
FastEthernet0/1     192.168.1.1    YES NVRAM up           up
Serial0/1           unassigned      YES NVRAM administratively down down
Serial0/2           unassigned      YES NVRAM administratively down down
Serial0/3           unassigned      YES NVRAM administratively down down
FastEthernet1/0     192.168.3.2    YES NVRAM up           up
FastEthernet2/0     unassigned      YES NVRAM administratively down down
R2#
```

```

root@ubuntu:/home/ubuntu# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
              inet6 fe80::6b53:864b:cb07:7210  prefixlen 64  scopedid 0x20<link>
        ether 00:0c:29:73:f2:32  txqueuelen 1000  (Ethernet)
          RX packets 45656  bytes 68141708 (68.1 MB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 18496  bytes 1420245 (1.4 MB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
              inet6 ::1  prefixlen 128  scopedid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 1336  bytes 11270 (11.2 KB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 1336  bytes 11270 (11.2 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@ubuntu:/home/ubuntu#
```

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

```

1:root@ubuntu:/home/ubuntu ~
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
Connection closed by foreign host.
root@ubuntu:/home/ubuntu# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^J'.
User Access Verification

Password:
R1>ena
R1>enable
Password:
R1>show ip int br
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0     unassigned      YES NVRAM administratively down down
Serial0/0           unassigned      YES NVRAM administratively down down
FastEthernet0/1     192.168.1.1    YES NVRAM up           up
Serial0/1           unassigned      YES NVRAM administratively down down
Serial0/2           unassigned      YES NVRAM administratively down down
FastEthernet1/0     192.168.1.1    YES NVRAM up           up
FastEthernet2/0     192.168.0.1    YES NVRAM up           up
R1#
```

```

root@ubuntu:/home/ubuntu# ifconfig
root@ubuntu:/home/ubuntu#
```

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
```

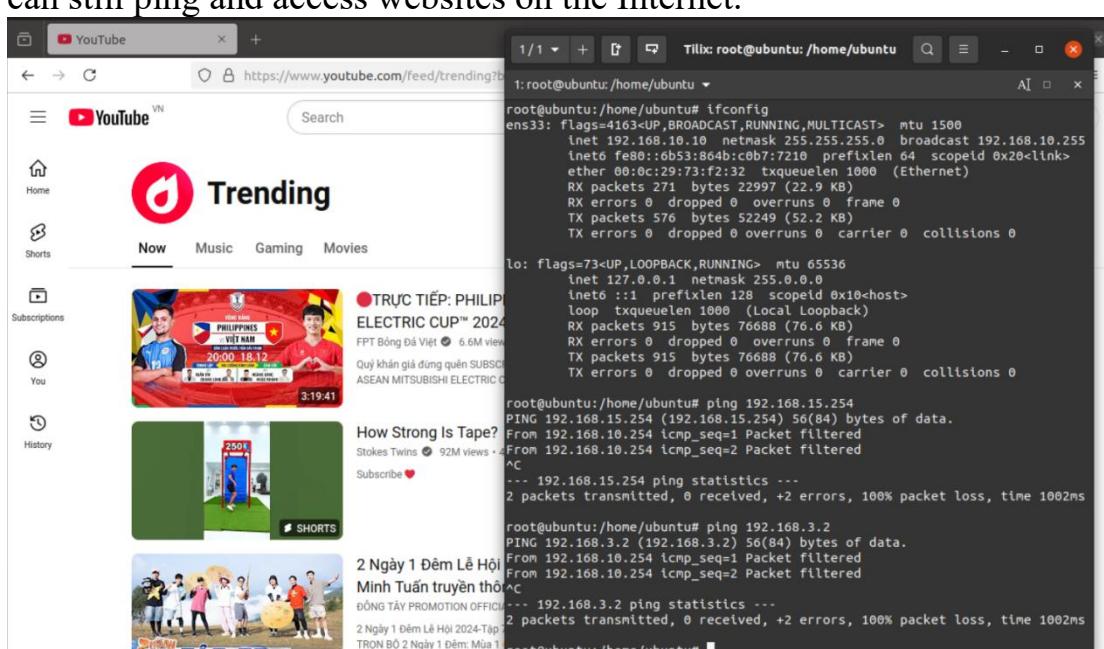
These rules will restrict devices in the 192.168.10.0 network from connecting to other networks within the LAN but will still allow them to access services from other networks and the Internet.

Now, apply them to the interface.

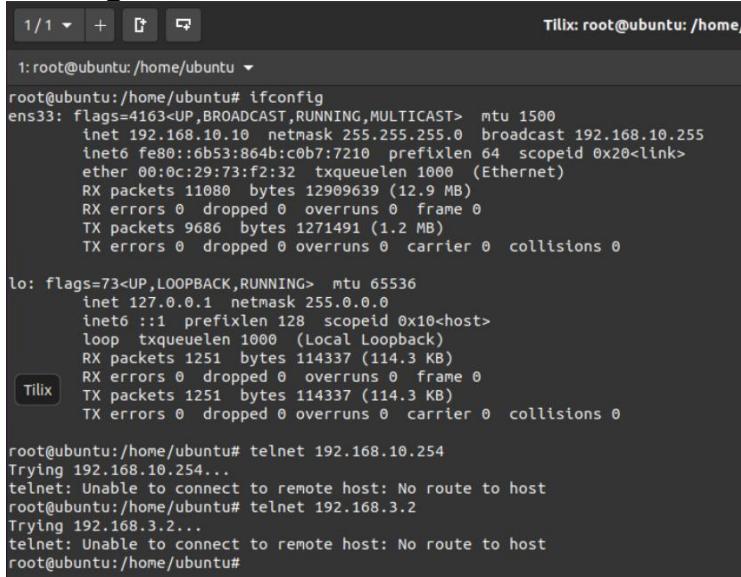
```
R2(config)#interface f0/0.1
```

```
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.



The screenshot shows a terminal window titled "Tilix: root@ubuntu: /home/" with the following content:

```
1/1 + ↻ Tilix: root@ubuntu: /home/
1:root@ubuntu:/home/ubuntu ~
root@ubuntu:/home/ubuntu# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.10 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::6b53:864b:c0b7:7210 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:73:f2:32 txqueuelen 1000 (Ethernet)
            RX packets 11080 bytes 12909639 (12.9 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 9686 bytes 1271491 (1.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 1251 bytes 114337 (114.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1251 bytes 114337 (114.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:/home/ubuntu# telnet 192.168.10.254...
Trying 192.168.10.254...
telnet: Unable to connect to remote host: No route to host
root@ubuntu:/home/ubuntu# telnet 192.168.3.2...
Trying 192.168.3.2...
telnet: Unable to connect to remote host: No route to host
root@ubuntu:/home/ubuntu#
```

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.

```

1:root@ubuntu:/home/ubuntu ~
root@ubuntu:/home/ubuntu# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.15.10 netmask 255.255.255.0 broadcast 192.168.15.255
        inet6 fe80::6b53:864b:cb07:7210 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:73:f2:32 txqueuelen 1000 (Ethernet)
                RX packets 11555 bytes 13105748 (13.1 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 10325 bytes 1341513 (1.3 MB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 1613 bytes 149862 (149.8 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1613 bytes 149862 (149.8 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:/home/ubuntu# telnet 192.168.3.2...
Trying 192.168.3.2...
Connected to 192.168.3.2.
Escape character is '^]'.

User Access Verification

Password:
Password:
R2>en
Password:
R2#show ip int br
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    unassigned     YES NVRAM up           up
FastEthernet0/0.1  192.168.10.254 YES NVRAM up           up
FastEthernet0/0.2  192.168.15.254 YES NVRAM up           up

```

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.

```
| Forums: https://forum.opnsense.org/ | @@@@// \\\@@@  
| Code: https://github.com/opnsense | @@@@ @@@@  
| Twitter: https://twitter.com/opnsense | @@@@@@@@@@@@  
  
*** OPNsense.localdomain: OPNsense 24.7 ***  
  
LAN (em0)      -> v4: 192.168.1.1/24  
WAN (em1)      ->  
  
HTTPS: sha256 94 F6 C0 2E DD E5 20 D6 FB 09 2E FD 41 57 6C 2F  
        37 54 8A 8A B1 51 10 81 41 4F 56 C3 A2 C0 47 9E  
SSH:   SHA256 WlKezIICZw4YvgvJ2bZ3k+kY6utHe6rYeT7gah2xW9A (ECDSA)  
SSH:   SHA256 sWgCrFarvL0PXTnow9XVz0ETBHbJbmA7MEXrtsmcjeo (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: █
```

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

WAN interface:

```
Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

em0          00:0c:29:78:70:59 Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1          00:0c:29:78:70:63 Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2          00:0c:29:78:70:6d Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3          00:0c:29:78:70:77 Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0
```

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.):

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished): em2

Enter the Optional interface 2 name or 'a' for auto-detection
(or nothing if finished): em3

Syncing OpenVPN settings...done.
Generating RRD graphs...done.

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

LAN (em1)      -> v4: 192.168.1.1/24
OPT1 (em2)     ->
OPT2 (em3)     ->
WAN (em0)      -> v4/DHCP4: 192.168.1.12/24

HTTPS: sha256 94 F6 C0 2E DD E5 20 D6 FB 09 2E FD 41 57 6C 2F
       37 54 8A B1 51 10 81 41 4F 56 C3 A2 C0 47 9E
SSH:  SHA256 W1KezIICZw4YugvJ2bZ3k+kY6utHe6rYeT7gah2x49A (ECDSA)
SSH:  SHA256 sWgCrFarvL0PXTnou9XUzOETBHbjbM7MEXrtsmcjeo (ED25519)
SSH:  SHA256 njziL5BcLe+Jow3JxUhcmsiJ6f0fcCsEBHBt+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: ■
```

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: 1

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.16.254

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

```

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 WlKezIIC2w4YvgvJ2bZ3k+KY6utHe6rYeT7gah2xW9A (ECDSA)
SSH:  SHA256 sWgCrFarvL0PXTnow9XUz0ETBHbJbMA7MEXrtsmc.jeo (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.

The image displays three separate browser windows showing the OPNsense web interface:

- Login Screen:** The first window shows the OPNsense logo at the top. Below it is a form with "Username:" set to "root" and "Password:" set to a masked value. A "Login" button is at the bottom right. The URL in the address bar is 192.168.16.254.
- General Setup Wizard:** The second window shows the "System: Wizard: General Setup" page. It contains a message: "This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen." A "Next" button is at the bottom right. The URL is 192.168.16.254/wizard.php?xml=system.
- General Information Configuration:** The third window shows the "System: Wizard: General Information" page. It includes fields for Hostname (OPNsense), Domain (localdomain), Language (English), Primary DNS Server (8.8.8.8), Secondary DNS Server (8.8.4.4), and an "Override DNS" checkbox which is checked. Below this is the "Unbound DNS" section with options for Enable Resolver (checked), Enable DNSSEC Support (unchecked), and Harden DNSSEC data (unchecked). A "Next" button is at the bottom right. The URL is 192.168.16.254/wizard.php?xml=system.

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

System: Wizard: Configure WAN Interface

PPTP Remote IP Address: 32

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.

The image contains two side-by-side screenshots of a web browser displaying the OPNsense configuration interface. Both screenshots show the left sidebar with various system management options like Lobby, Reporting, System, and Firewall. The top screenshot shows the 'System: Wizard: Set Root Password' page, which asks for a new root password and its confirmation. The bottom screenshot shows the 'System: Wizard: Reload Configuration' page, which has a single button labeled 'Reload'.

Now choose “Check for update”.

This screenshot shows the OPNsense dashboard after the initial configuration is complete. The main message says "Finished initial configuration!" and features the OPNsense logo. Below the message, there is a note about donations and a link to "check for updates".

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

Package	Current Version	New Version	Action	Source
py311-service-identity	24.1.0	24.2.0	upgrade	OPNsense
py311-sqlite3	3.11.9_7	3.11.10_7	upgrade	OPNsense
py311-trio	0.26.0	0.27.0	upgrade	OPNsense
py311-truststore	N/A	0.10.0	new	OPNsense
py311-tzdata	2024.1	2024.2	upgrade	OPNsense
py311-urllib3	1.26.19_1	1.26.20_1	upgrade	OPNsense
python311	3.11.9_1	3.11.10	upgrade	OPNsense
readline	8.2.10	8.2.13_2	upgrade	OPNsense
rrdtool	1.8.0_4	1.9.0	upgrade	OPNsense
sqlite3	3.46.0.1	3.46.1_1	upgrade	OPNsense
sudo	1.9.15p5_4	1.9.16	upgrade	OPNsense
suricata	7.0.6	7.0.7_1	upgrade	OPNsense
syslog-nginx	4.7.1	4.8.1_1	upgrade	OPNsense
unbound	1.20.0_1	1.22.0_1	upgrade	OPNsense
wpa_supplicant	2.11	2.11_2	upgrade	OPNsense

There are 79 updates available, total download size is 299.8MB.
This update requires a reboot.

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

2.2.2. Basic rules

Choose “Firewall” -> “Rules” -> “LAN”

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule
IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

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 changes” and the rule will become active.

```
1/1 + T ⓘ  Tilix: root@ubuntu: /home/ubuntu
1:root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.10.15 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::6b53:864b:c0b7:7210 prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:73:f2:32 txqueuelen 1000 (Ethernet)
            RX packets 74499 bytes 90750215 (90.7 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 50808 bytes 5613451 (5.6 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 27516 bytes 2274187 (2.2 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 27516 bytes 2274187 (2.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:/home/ubuntu# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=70.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=83.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=69.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3033ms
rtt min/avg/max/mdev = 69.142/74.551/83.730/6.524 ms
```

The LAN can now ping to any IP address.
Now, create a rule to allow DNS traffic.

This screenshot shows the OPNsense firewall rules configuration interface. The left sidebar is a navigation menu with various options like Automation, Categories, Groups, NAT, Rules, Floating, LAN, Loopback, OPT1, OPT2, WAN, Shaper, Settings, Log Files, and Diagnostics. The 'Rules' option is currently selected. The main panel displays a form for creating a new rule. The fields are as follows:

- Interface: OPT1
- Direction: in
- TCP/IP Version: IPv4
- Protocol: UDP
- Source / Invert: Use this option to invert the sense of the match. (unchecked)
- Source: OPT1 net
- Source: Advanced
- Destination / Invert: Use this option to invert the sense of the match. (unchecked)
- Destination: any
- Destination port range: from: DNS to: DNS

At the bottom of the page, there is a footer note: "OPNsense (c) 2014-2024 Deciso B.V."

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.

This screenshot shows the OPNsense firewall rules configuration interface, similar to the previous one but with different settings. The left sidebar is the same. The main panel displays a form for creating a new rule. The fields are as follows:

- Interface: OPT1
- Direction: in
- TCP/IP Version: IPv4
- Protocol: TCP
- Source / Invert: Use this option to invert the sense of the match. (unchecked)
- Source: OPT1 net
- Source: Advanced
- Destination / Invert: Use this option to invert the sense of the match. (unchecked)
- Destination: any
- Destination port range: from: HTTP to: HTTP

At the bottom of the page, there is a footer note: "OPNsense (c) 2014-2024 Deciso B.V."

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”.

OPNsense Firewall Rules Edit Page for OPT1:

- Interface: OPT1
- Direction: in
- TCP/IP Version: IPv4
- Protocol: TCP
- Source: OPT1 net
- Destination: any
- Destination port range: from: HTTPS to: HTTPS

These will be the current rules.

OPNsense Firewall Rules List for OPT1:

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action
IPv4 ICMP	OPT1 net	*	*	*	*	*	*	Automatically generated rules	
IPv4 UDP	OPT1 net	*	*	53 (DNS)	*	*	*		
IPv4 TCP	OPT1 net	*	*	80 (HTTP)	*	*	*		
IPv4 TCP	OPT1 net	*	*	443 (HTTPS)	*	*	*		
pass	x block	reject	log	in				first match	
pass (disabled)	x block (disabled)	reject (disabled)	log (disabled)	out				last match	

The network can now access the Internet.

Terminal (Tilix) Output:

```

root@ubuntu:/home/ubuntu# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.10.15 netmask 255.255.255.0 broadcast 192.168.10.255
inet6 fe80::b53:864b:cb07:7210 prefixlen 64 scopeld 0x20<link>
ether 00:0c:29:73:f2:32 txqueuelen 1000 (Ethernet)
RX packets 74499 bytes 90750215 (90.7 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 50888 bytes 5613451 (5.6 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeld 0x10<host>
loop txqueuelen 1000 (local loopback)
RX packets 27516 bytes 2274187 (2.2 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 27516 bytes 2274187 (2.2 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:/home/ubuntu# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=76.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=83.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=69.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3033ms
rtt min/avg/max/mdev = 69.142/74.551/83.730/6.524 ms

```

Browser (Facebook Login Page):

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.

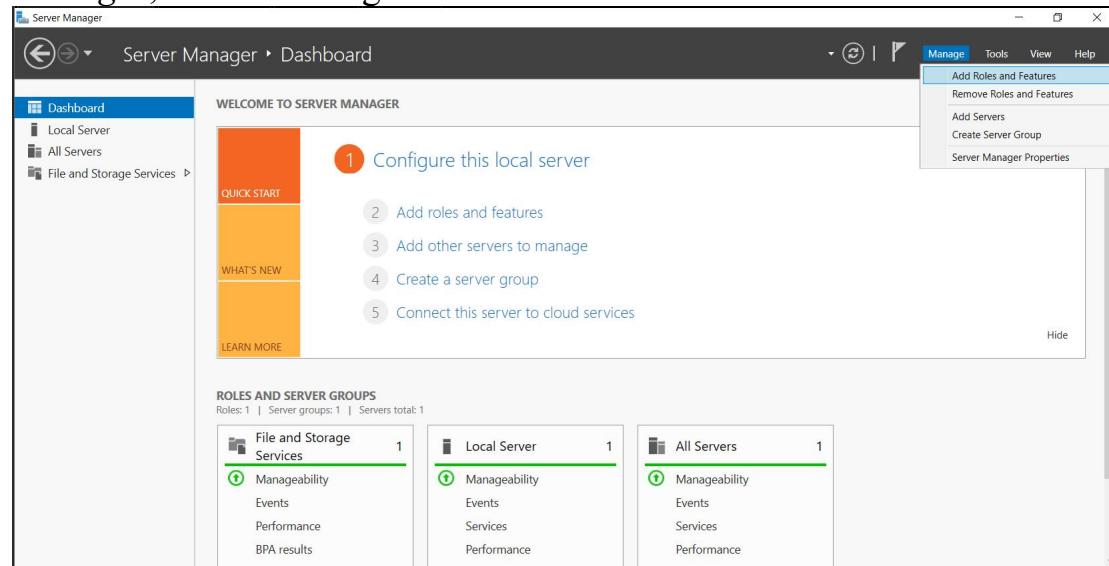
Client Port(s)	Server Port	Service
49152-65535/UDP	123/UDP	W32Time
49152-65535/TCP	135/TCP	RPC Endpoint Mapper
49152-65535/TCP	464/TCP/UDP	Kerberos password change
49152-65535/TCP	49152-65535/TCP	RPC for LSA, SAM, NetLogon (*)
49152-65535/TCP/UDP	389/TCP/UDP	LDAP
49152-65535/TCP	636/TCP	LDAP SSL
49152-65535/TCP	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 (*)

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

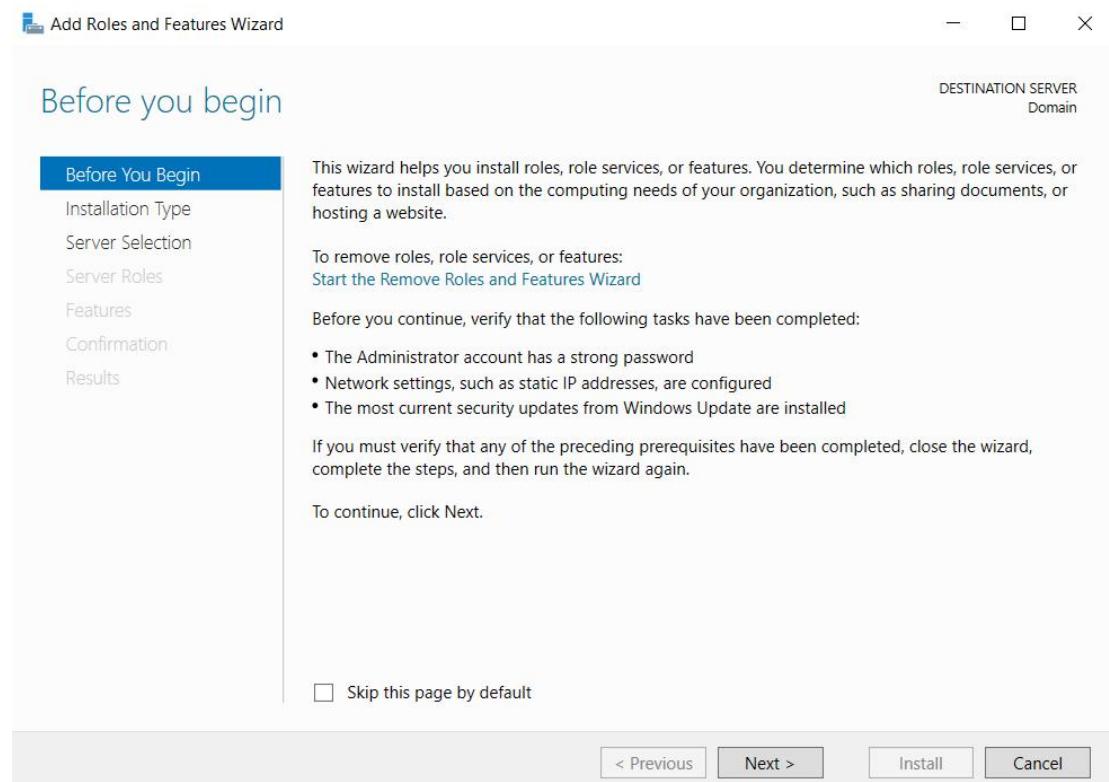
2.3. Active Directory

2.3.1. Set up Active Directory

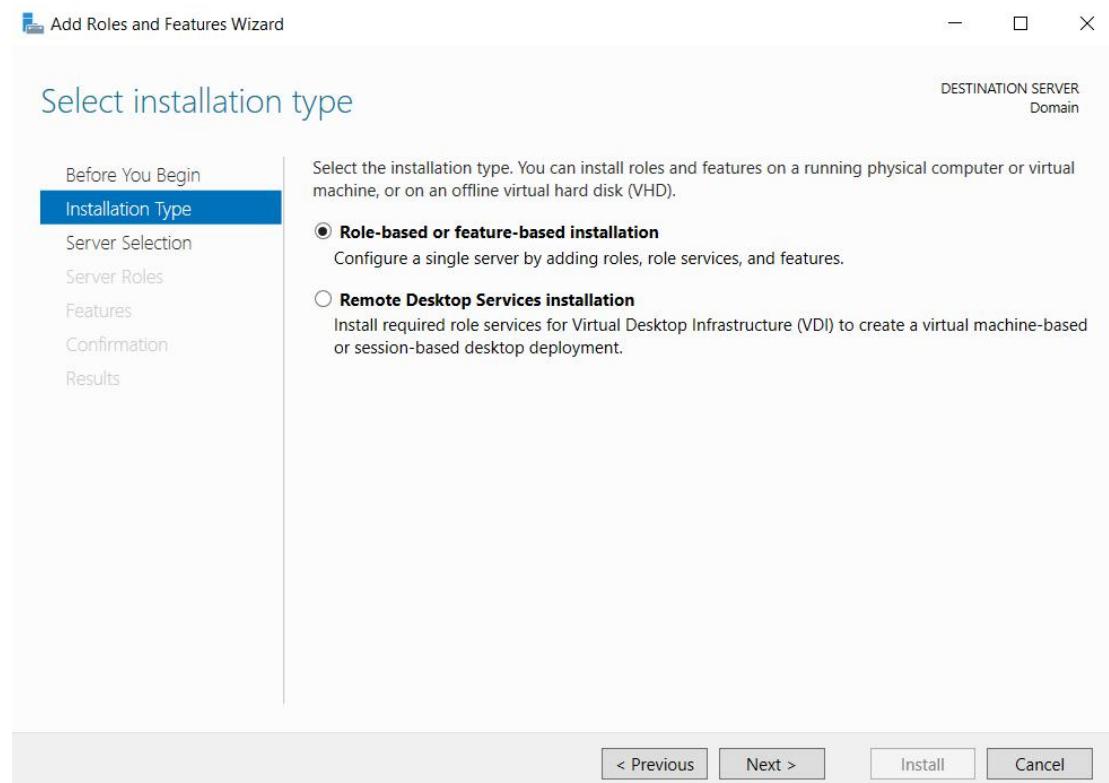
I will begin by creating a Active Directory (AD). In the *Server Manager*, select "Manage" -> "Add Roles and Features".



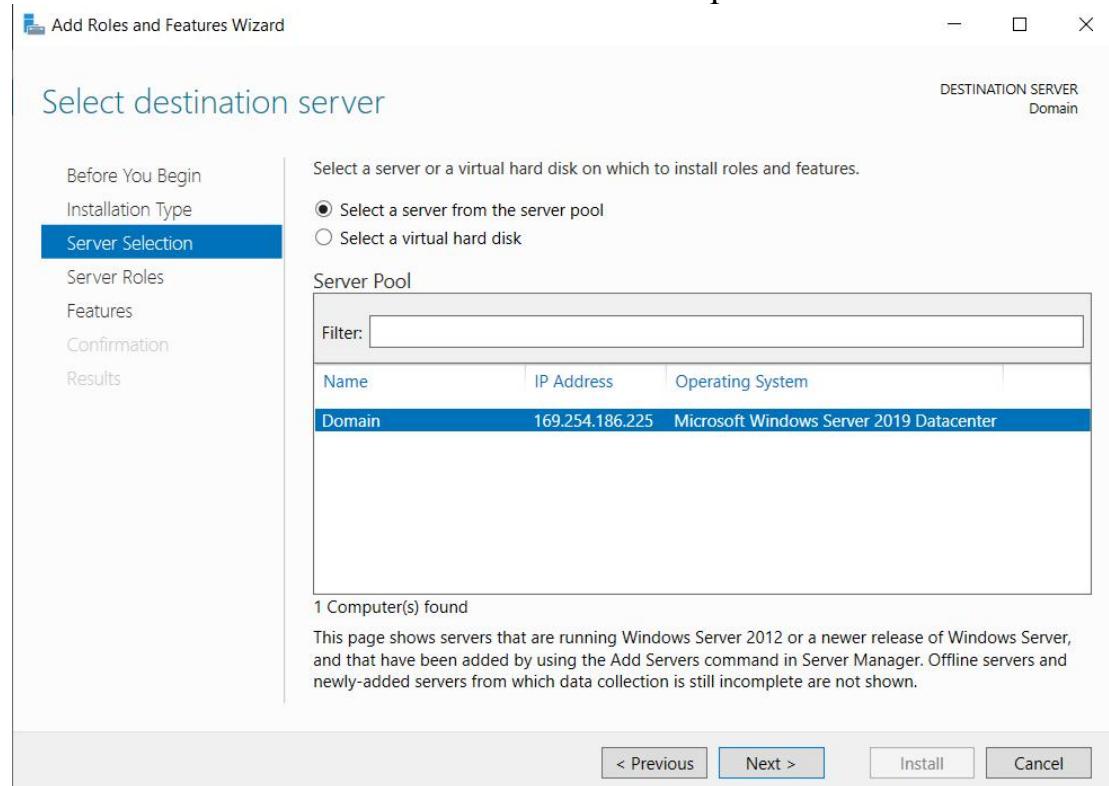
Click "Next".



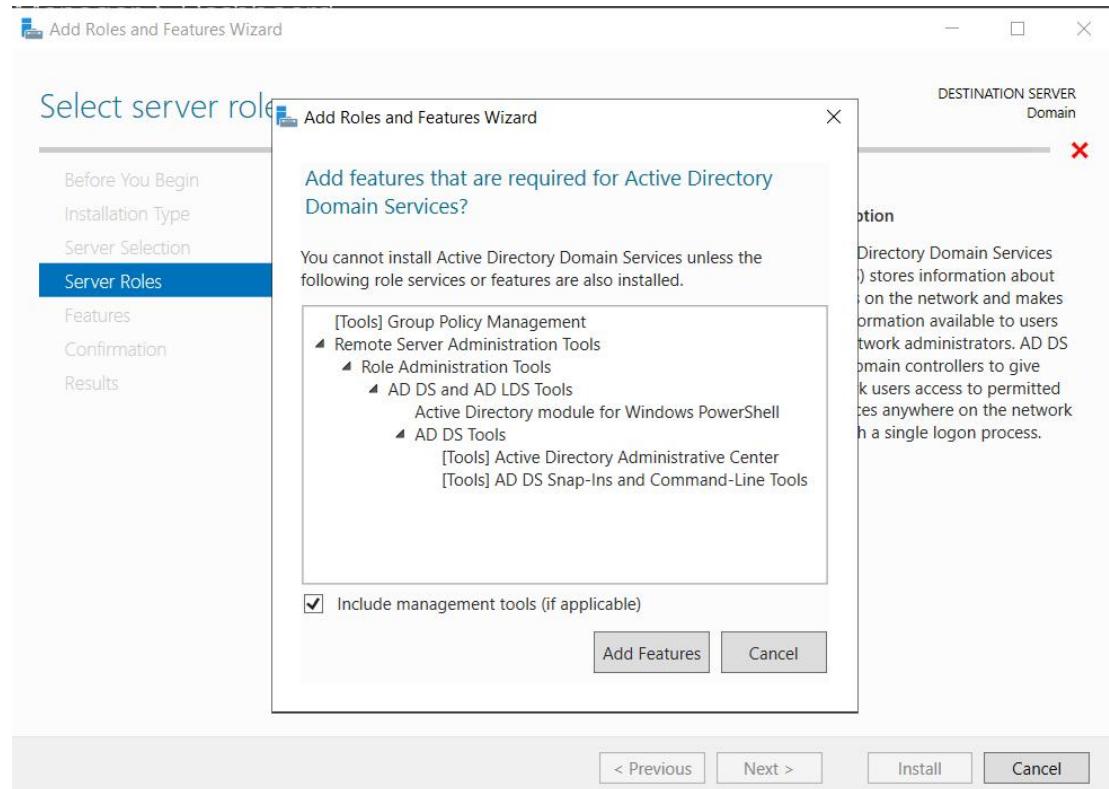
Choose “Role-based or Feature-based installation” and click “Next”.



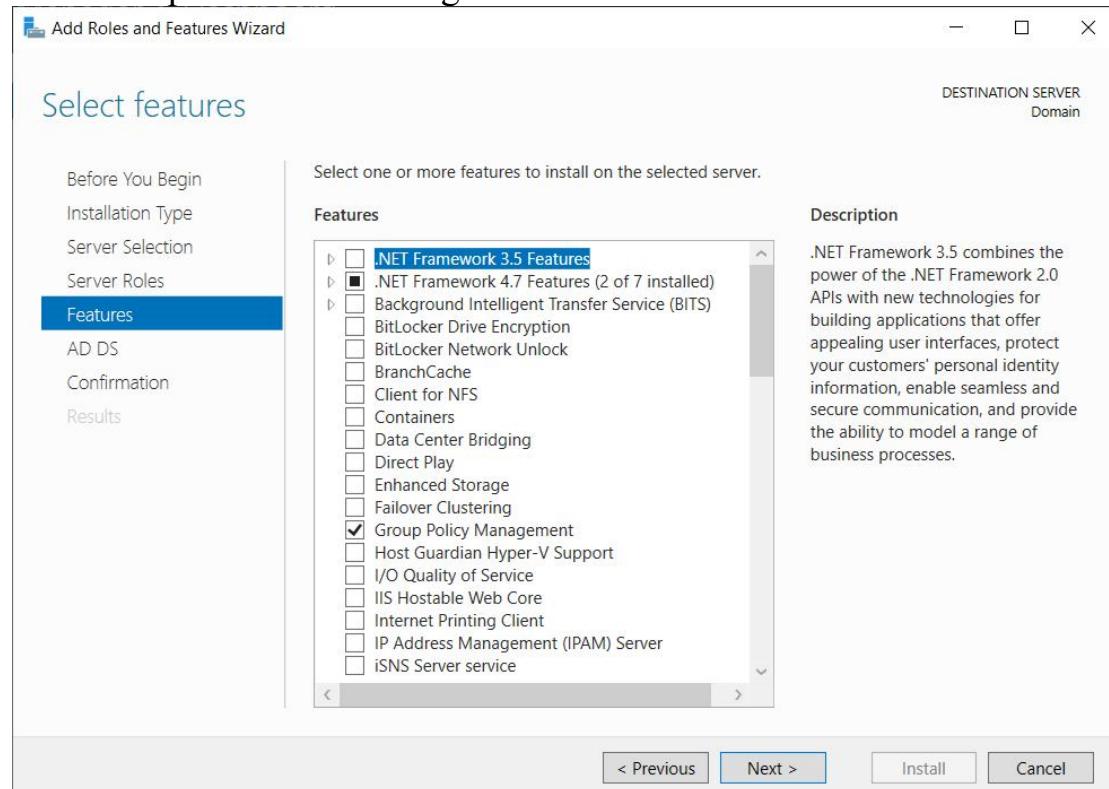
Choose “Select a server from the server pool” and click “Next”.



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



Keep the default configuration and click “Next”.



Continue to click “Next”.

Add Roles and Features Wizard

Active Directory Domain Services

DESTINATION SERVER
Domain

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous Next > Install Cancel

Now click the “Install” to start the installation.

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
Domain

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

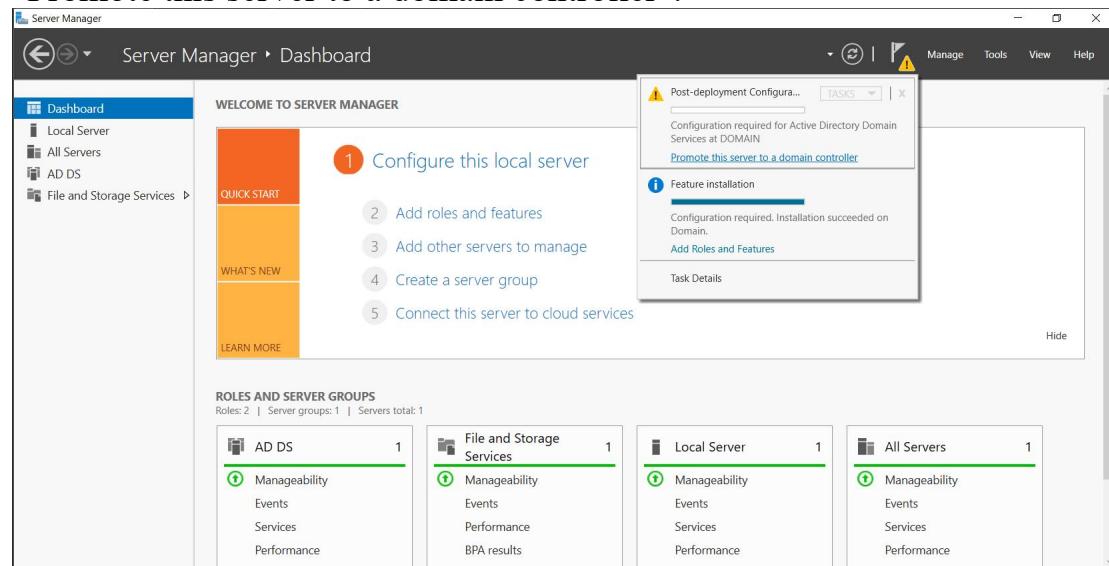
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

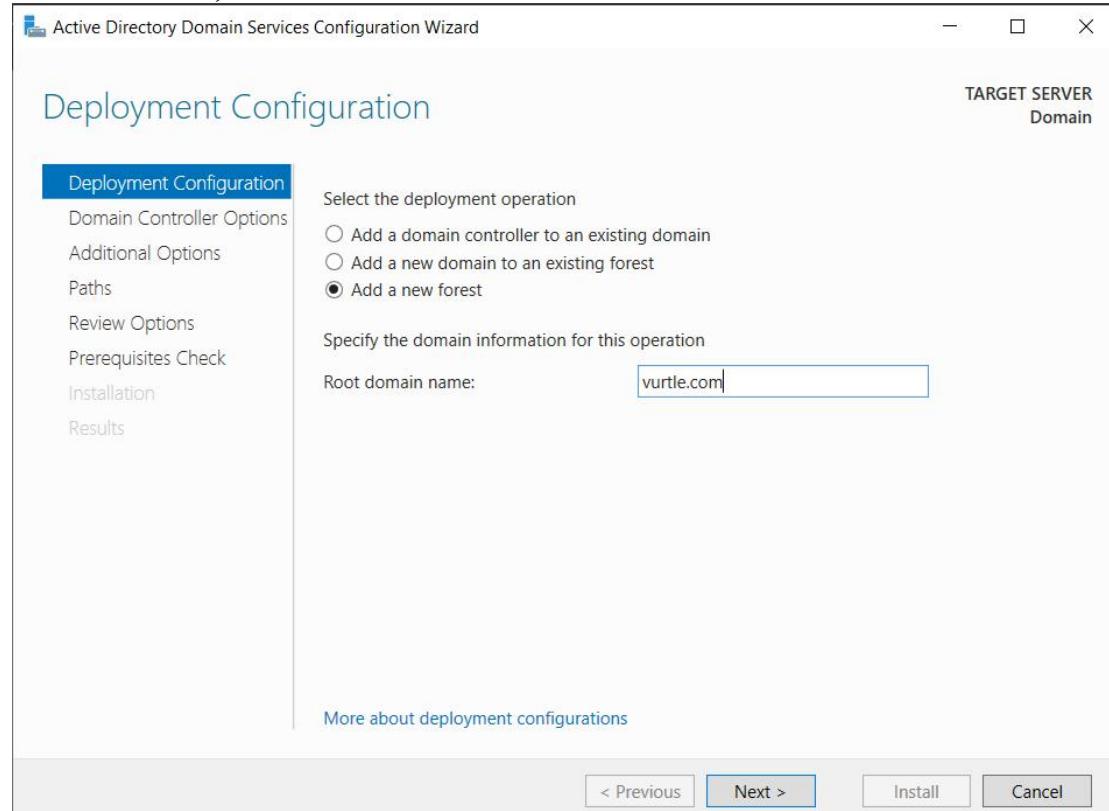
Export configuration settings
Specify an alternate source path

< Previous Next > Install Cancel

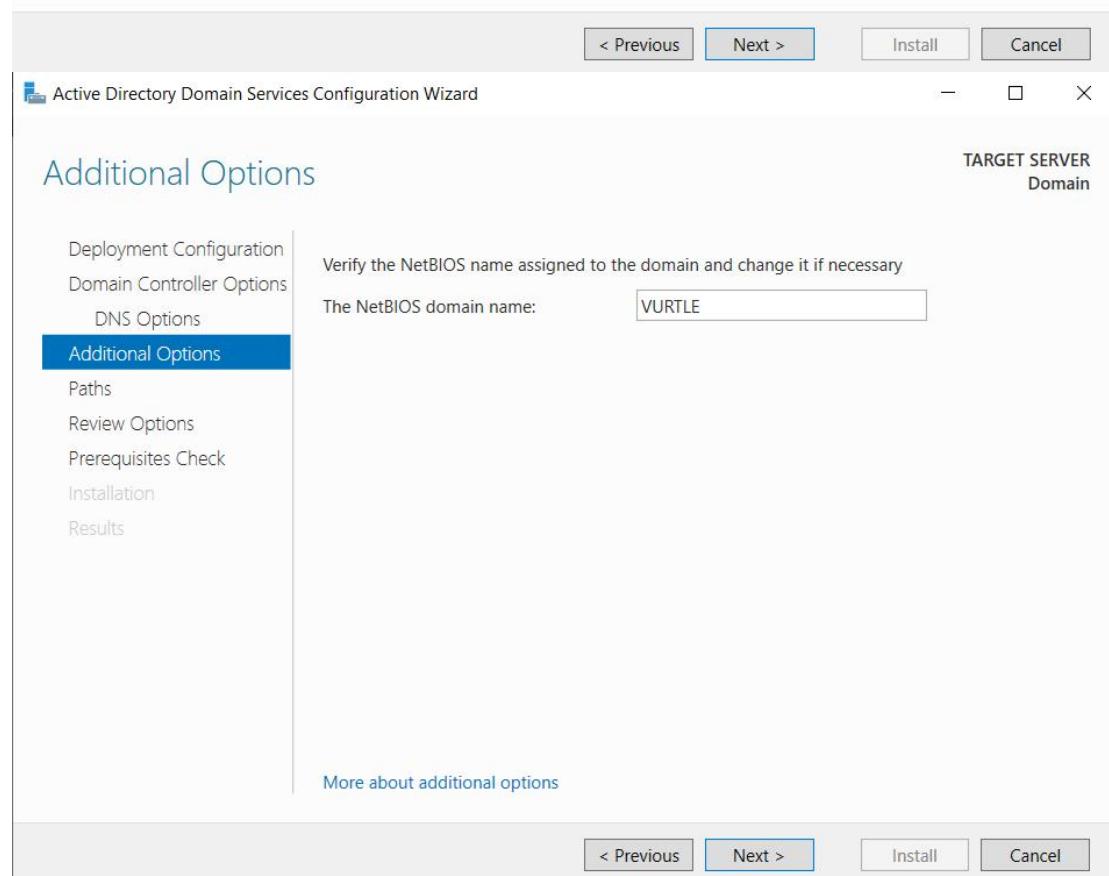
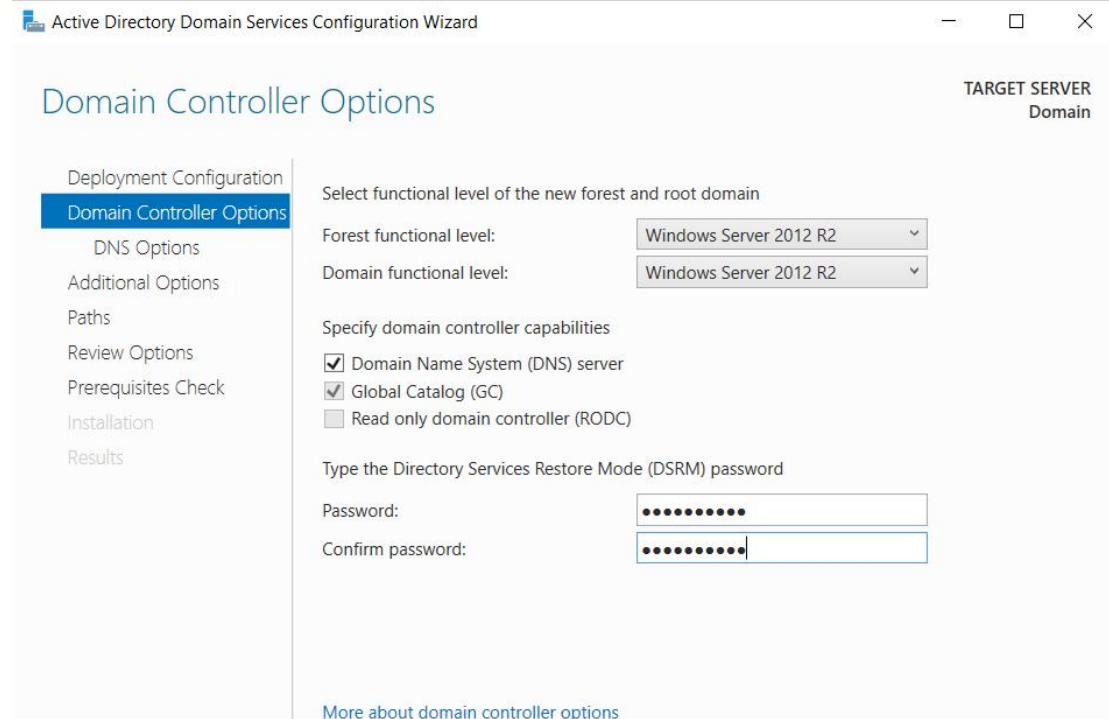
Once the installation is finished, click on the flag icon and select "Promote this server to a domain controller".



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.

Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
Domain

All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) [X](#)

Deployment Configuration
Domain Controller Options
 DNS Options
 Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
[Rerun prerequisites check](#)

[View results](#)

! Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

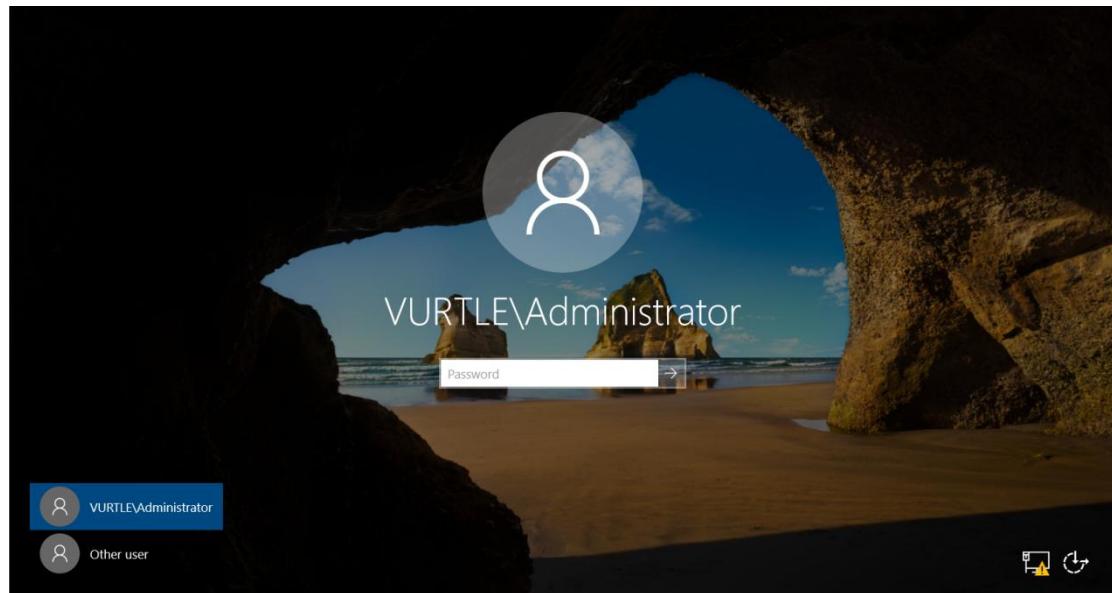
! This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System

! If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

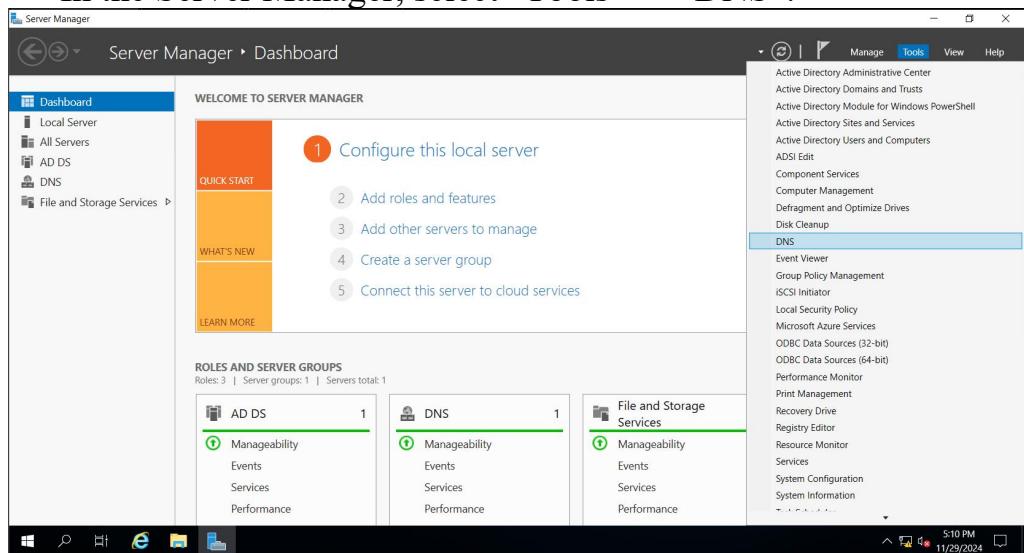
[< Previous](#) [Next >](#) [Install](#) [Cancel](#)

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

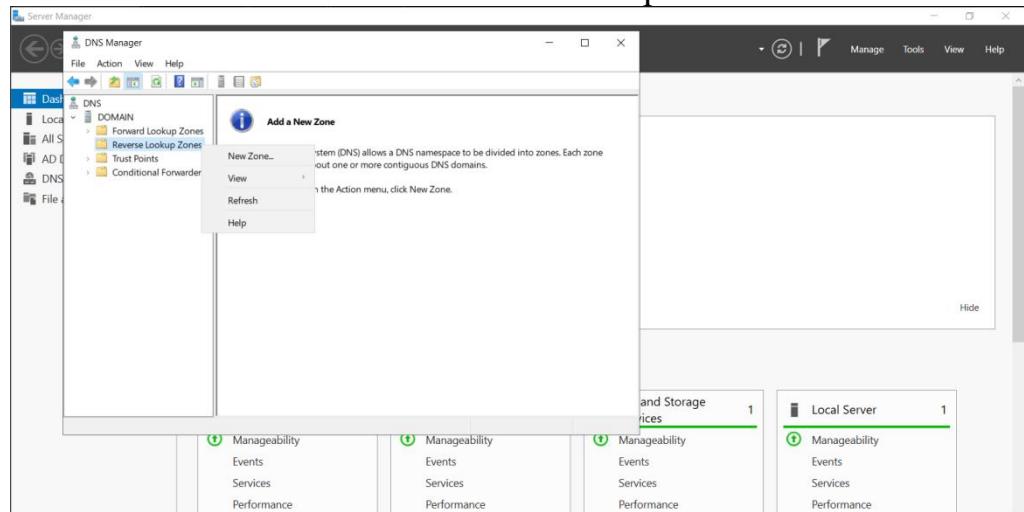


2.3.2. Configure DNS

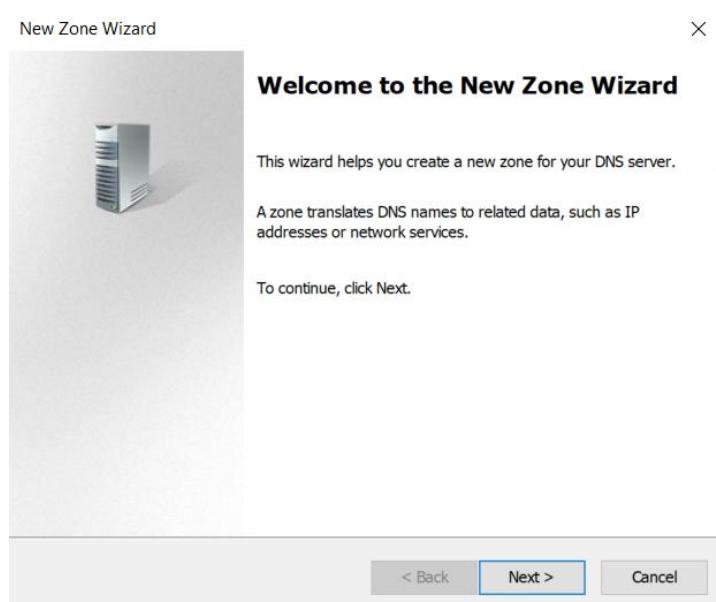
In the Server Manager, select “Tools” -> “DNS”.



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



Click “Next”.



Select “Primary Zone” and click “Next”.

New Zone Wizard X

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

Primary zone
Creates a copy of a zone that can be updated directly on this server.

Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

[< Back](#) [Next >](#) [Cancel](#)

New Zone Wizard X

Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

To all DNS servers running on domain controllers in this forest: vrtle.com

To all DNS servers running on domain controllers in this domain: vrtle.com

To all domain controllers in this domain (for Windows 2000 compatibility): vrtle.com

To all domain controllers specified in the scope of this directory partition:

[< Back](#) [Next >](#) [Cancel](#)

New Zone Wizard X

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

IPv4 Reverse Lookup Zone

IPv6 Reverse Lookup Zone

[< Back](#) [Next >](#) [Cancel](#)

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:

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:

< 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

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping vrtle.com

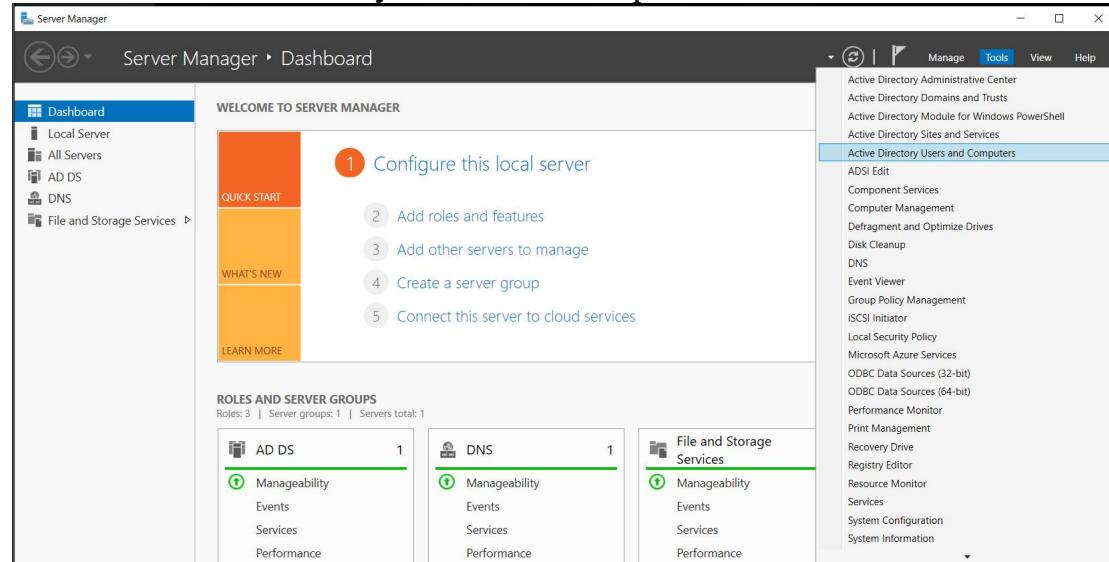
Pinging vrtle.com [192.168.12.10] with 32 bytes of data:
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

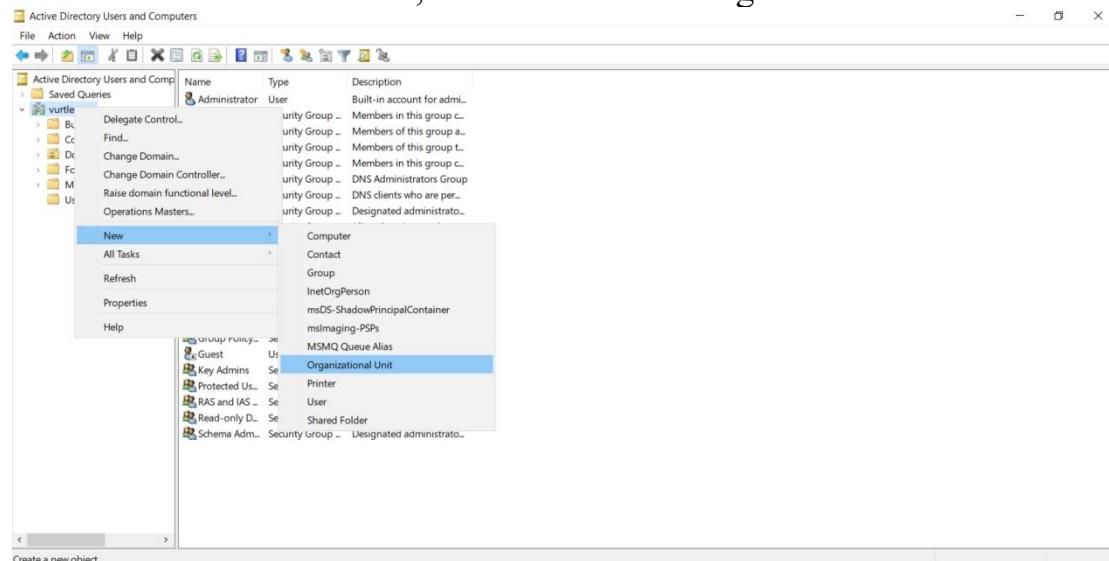
```

2.3.3. Create OU, Groups and Users

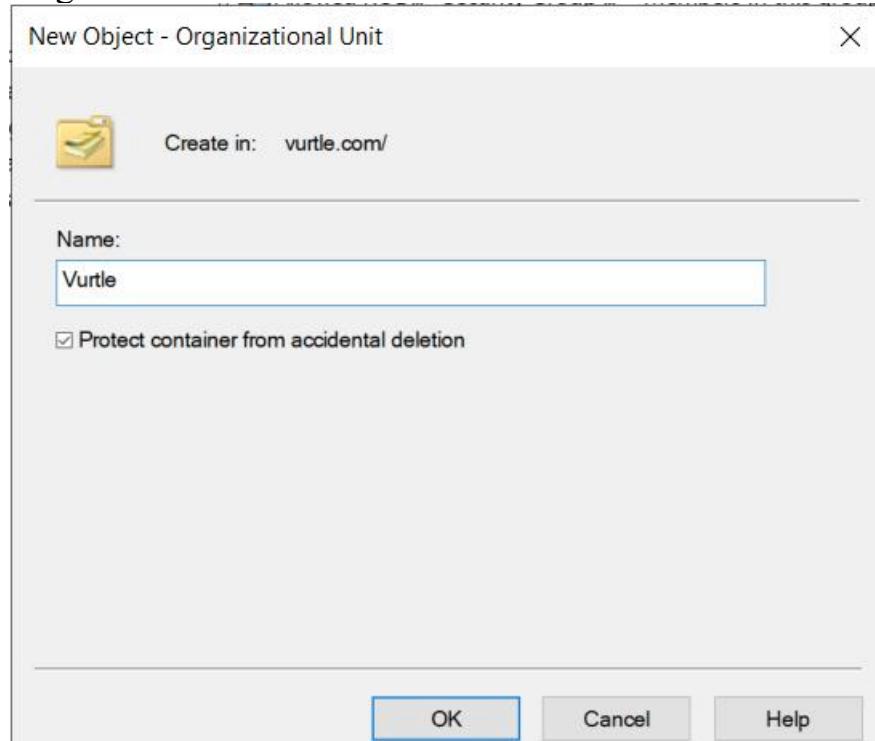
Now, create Organization Units (OU). Select “Tools” and then choose “Active Directory Users and Computers”.



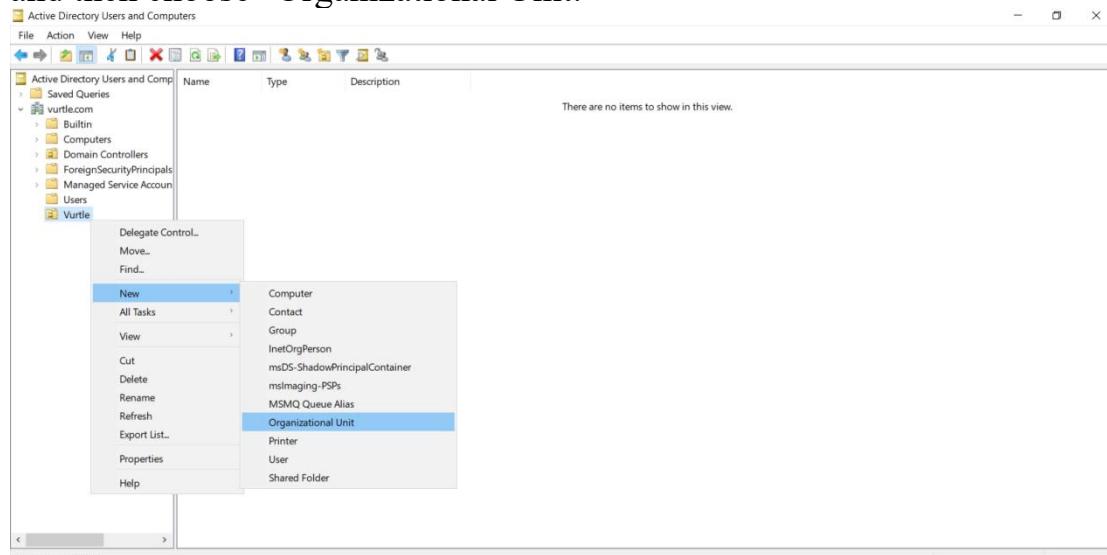
In "Active Directory Users and Computers", right-click on the domain name "vrtle.com", select "New" -> "Organizational Unit".



Assign a name to the OU.



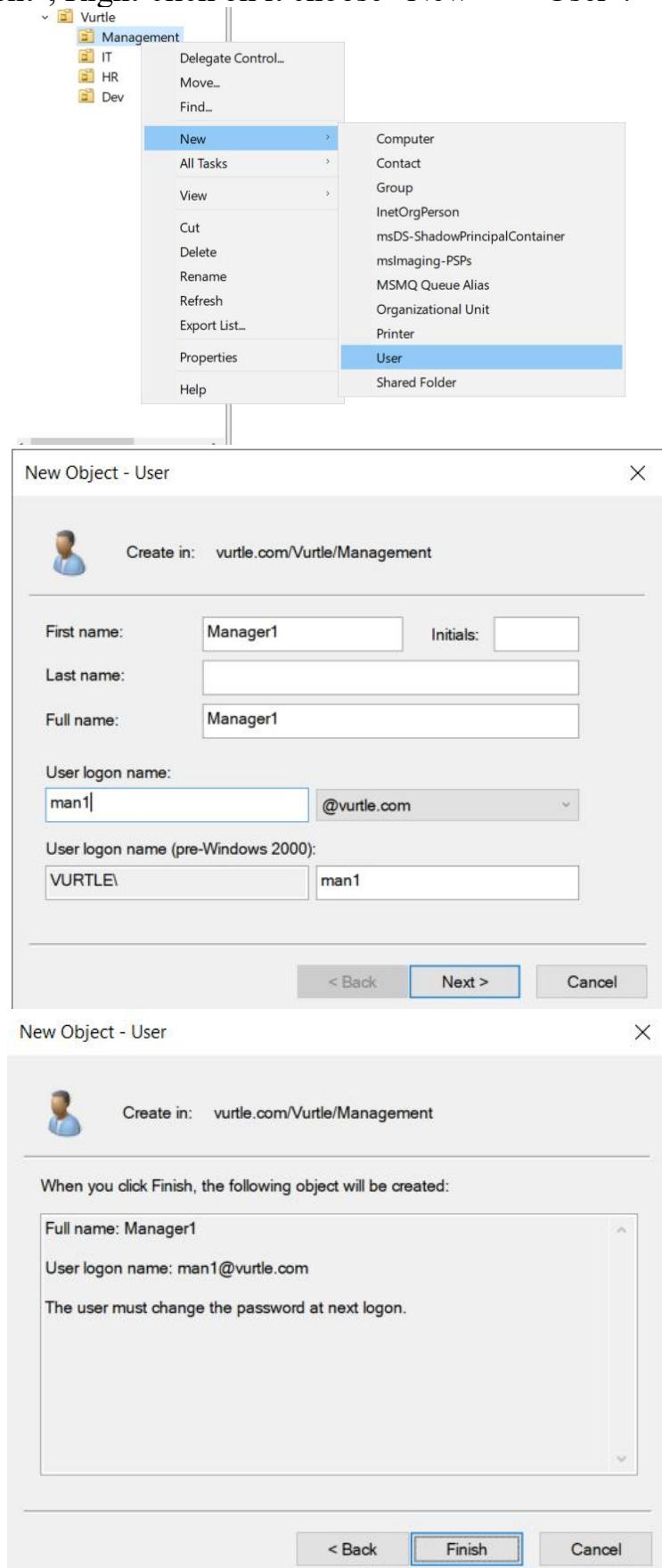
Next, I need to create additional OUs corresponding to the number of company teams. Right-click on the newly created OU, select "New", and then choose "Organizational Unit."

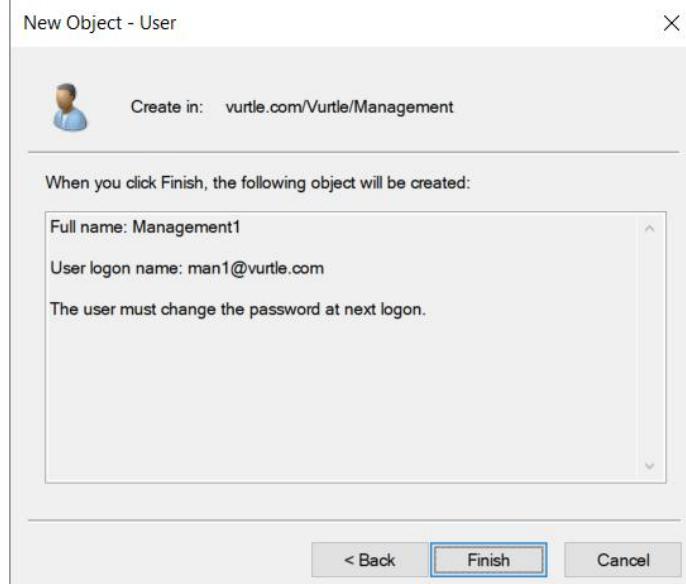


Create 4 teams: “Management”, “IT”, “HR” and “Dev”.



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





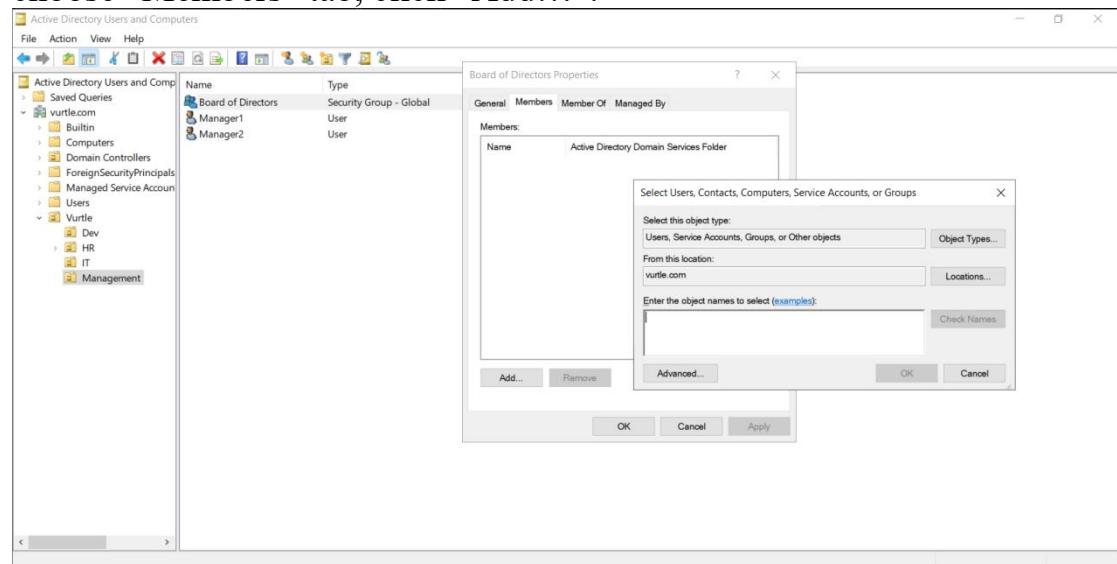
Now, I will create a group to manage the users. Right-click on “Management” -> “New” -> “Group”.

The screenshot shows a context menu for the 'Management' folder under 'Vrtle'. The 'New' option is selected, and a submenu is displayed with 'Group' highlighted. To the right, the 'New Object - Group' dialog box is open. It contains the following fields:

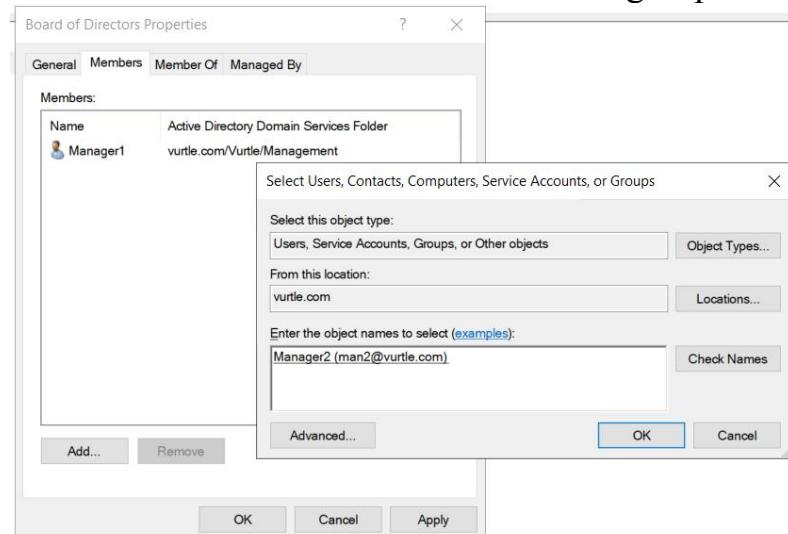
- Create in: vrtle.com/Vrtle/Management
- Group name: Board of Directors
- Group name (pre-Windows 2000): Board of Directors
- Group scope:
 - Domain local
 - Global
 - Universal
- Group type:
 - Security
 - Distribution

At the bottom, there are 'OK' and 'Cancel' buttons.

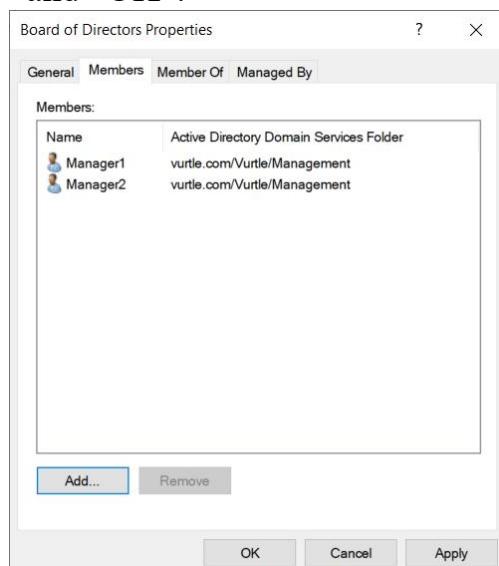
Next, add the users to the group. Select “Board of Directors” group, choose “Members” tab, click “Add...”.

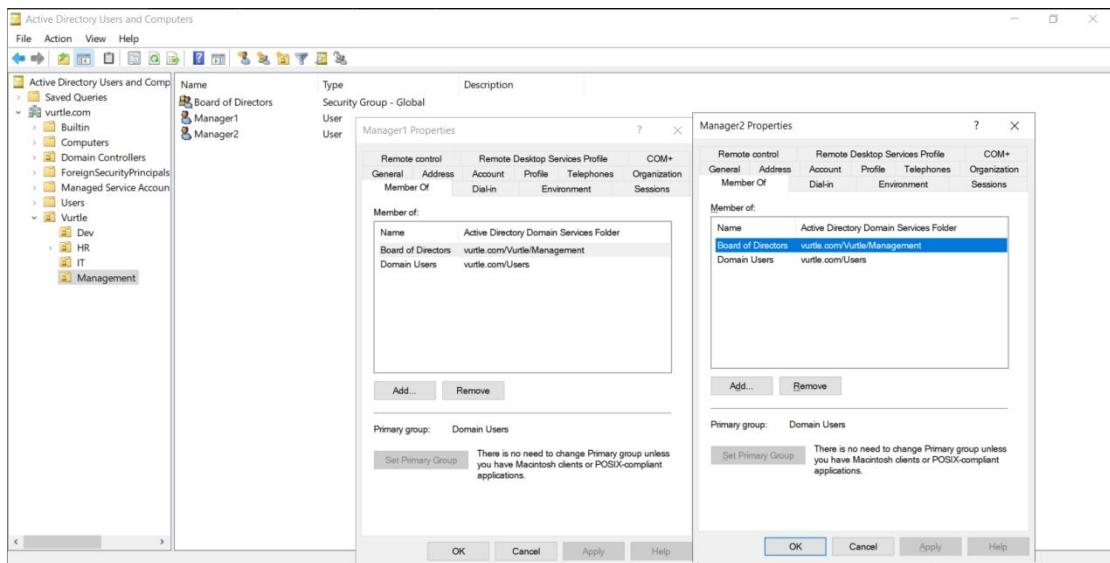


Enter the names of the users and add into the group.



Click “Apply” and “OK”.





Now, repeat the same process for the other OUs.

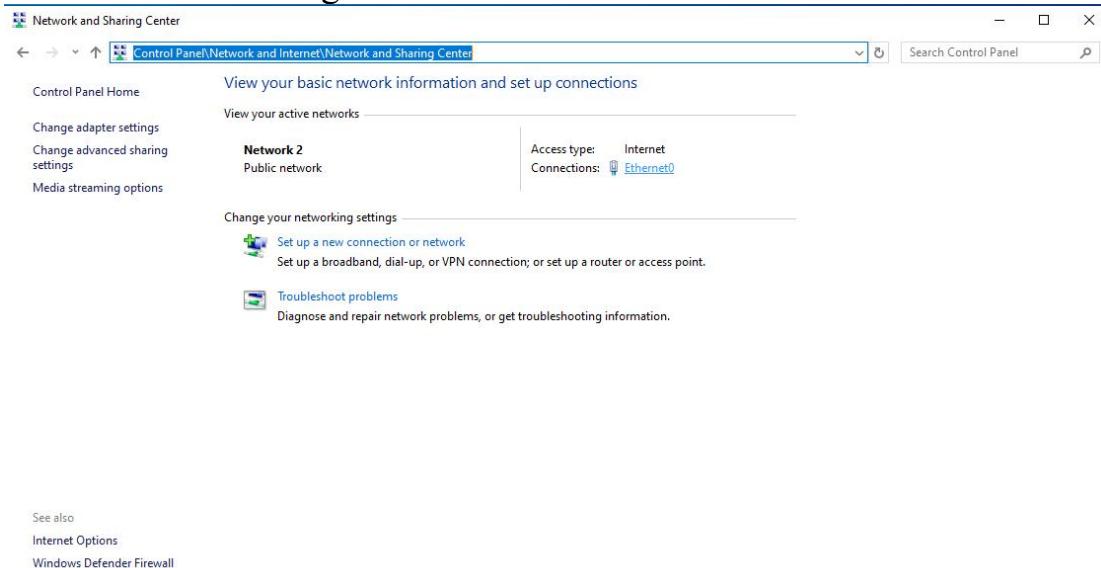
The image contains three separate screenshots of the Active Directory Users and Computers interface, each showing the properties of a different security group being added to its respective OU.

- Screenshot 1:** Shows the properties of 'Network Security' (Security Group - Global). It is being added to the 'IT' OU. The 'Primary group:' dropdown is set to 'Domain Users'.
- Screenshot 2:** Shows the properties of 'HR' (Security Group - Global). It is being added to the 'HR' OU. The 'Primary group:' dropdown is set to 'Domain Users'.
- Screenshot 3:** Shows the properties of 'Development' (Security Group - Global). It is being added to the 'Dev' OU. The 'Primary group:' dropdown is set to 'Domain Users'.

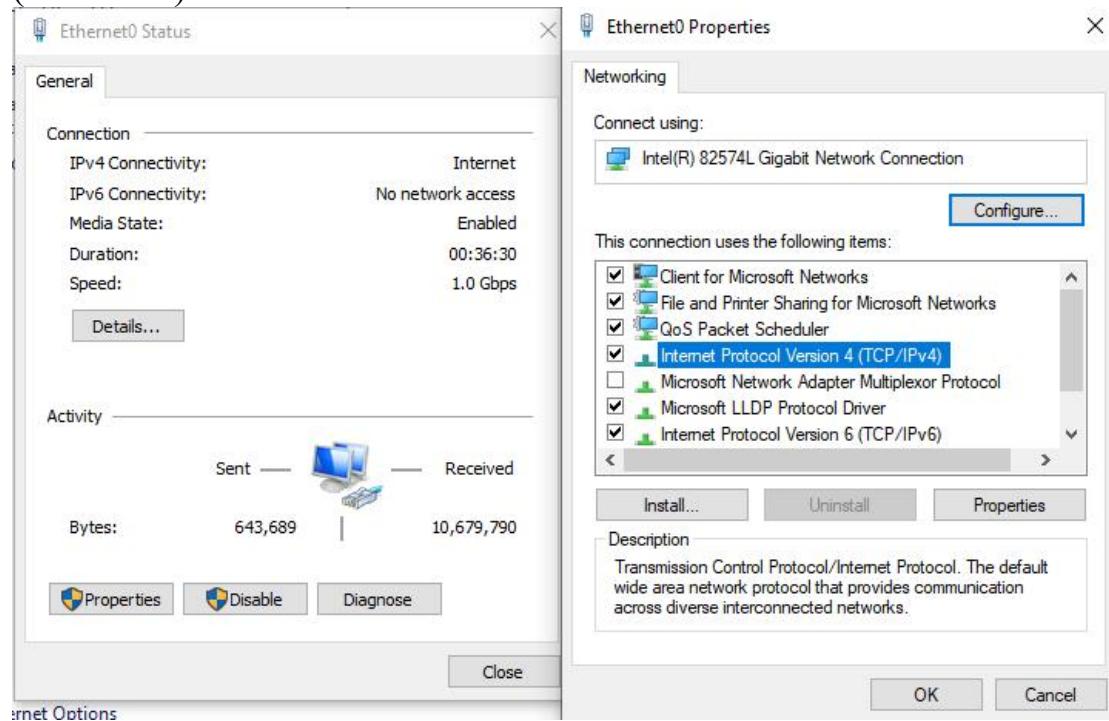
In all three cases, a note at the bottom of the properties window states: 'There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.'

2.3.4. Join Domain

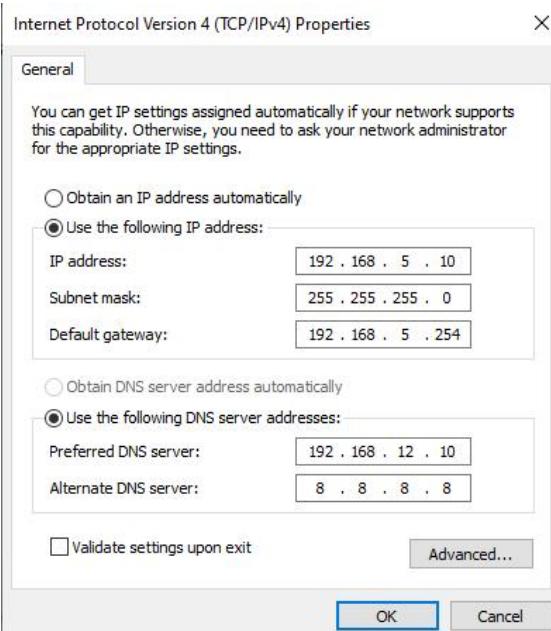
Now I need to have devices in the LAN to join the Domain. At the BoD device, open “Control Panel”, choose “Network and Internet” -> “Network and Sharing Center” then click “Ethernet0”.



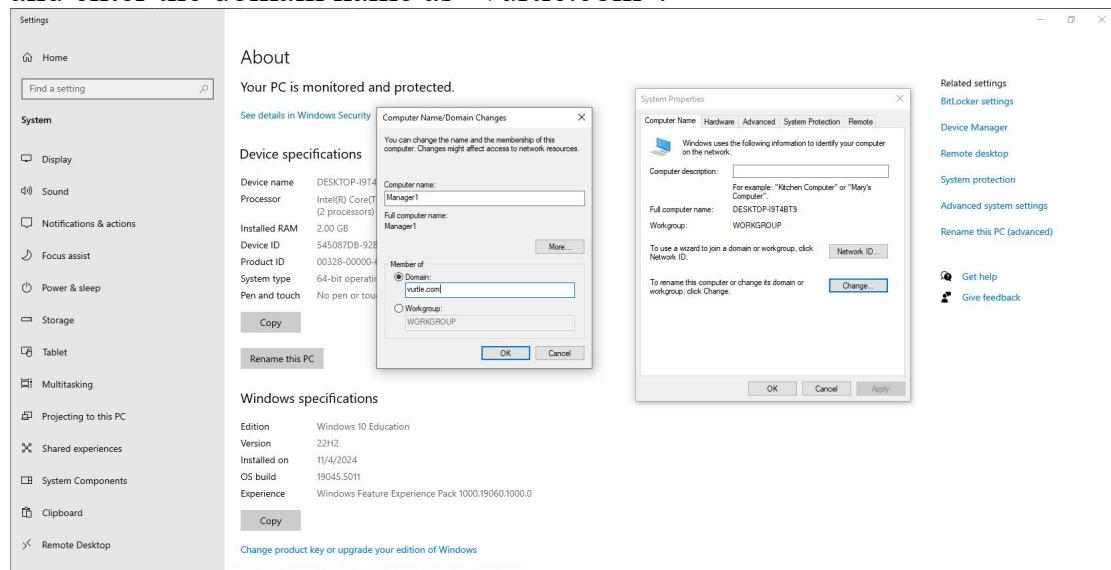
Click “Properties”, double-click “Internet Protocol Version 4 (TCP/IPv4)”.



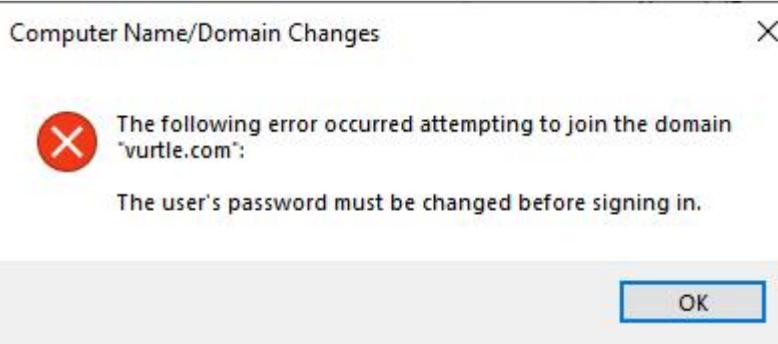
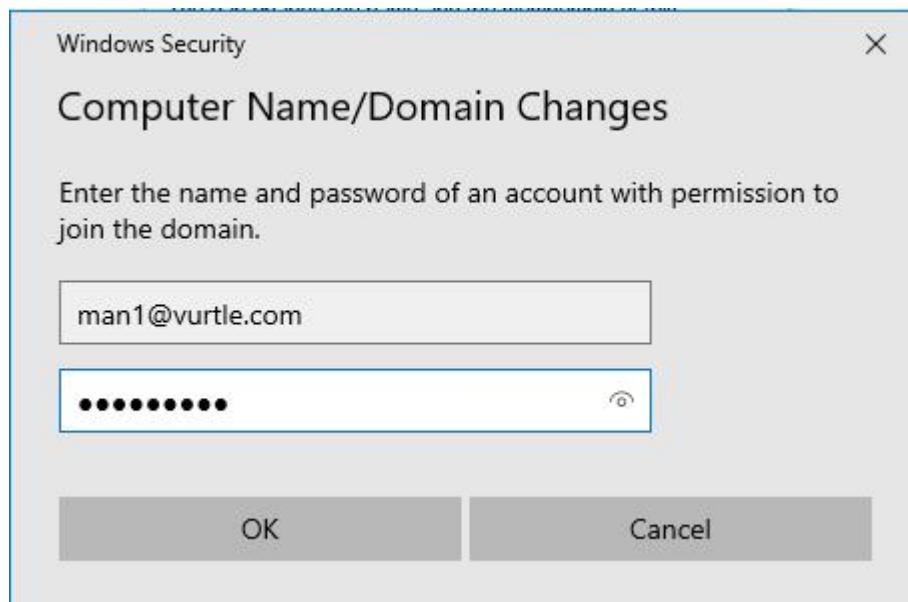
Assign IP address and DNS server addresses.



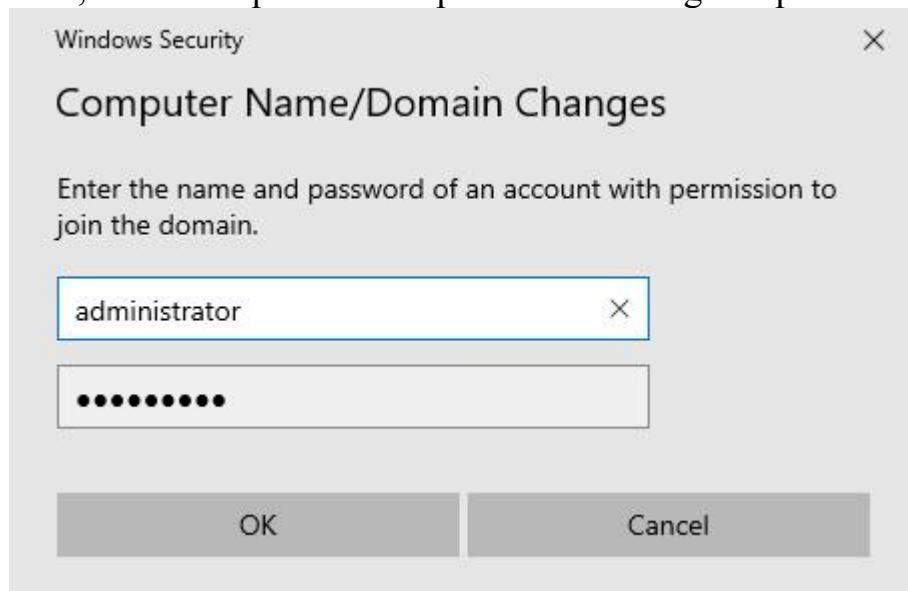
Open the “Settings” application, search for “About”, and under “Related settings”, click on “Advanced system settings”. Navigate to the “Computer Name” tab and click on “Change...”. Set the “Computer name” to “Manager1”. Under the “Member of” section, select “Domain” and enter the domain name as “vrtle.com”.

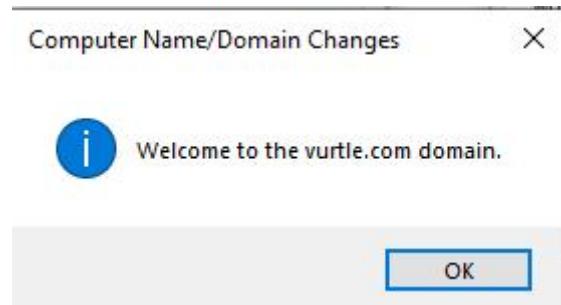


A window will appear prompting you to enter credentials, provide the “Manager1” credentials that were created on the domain server.

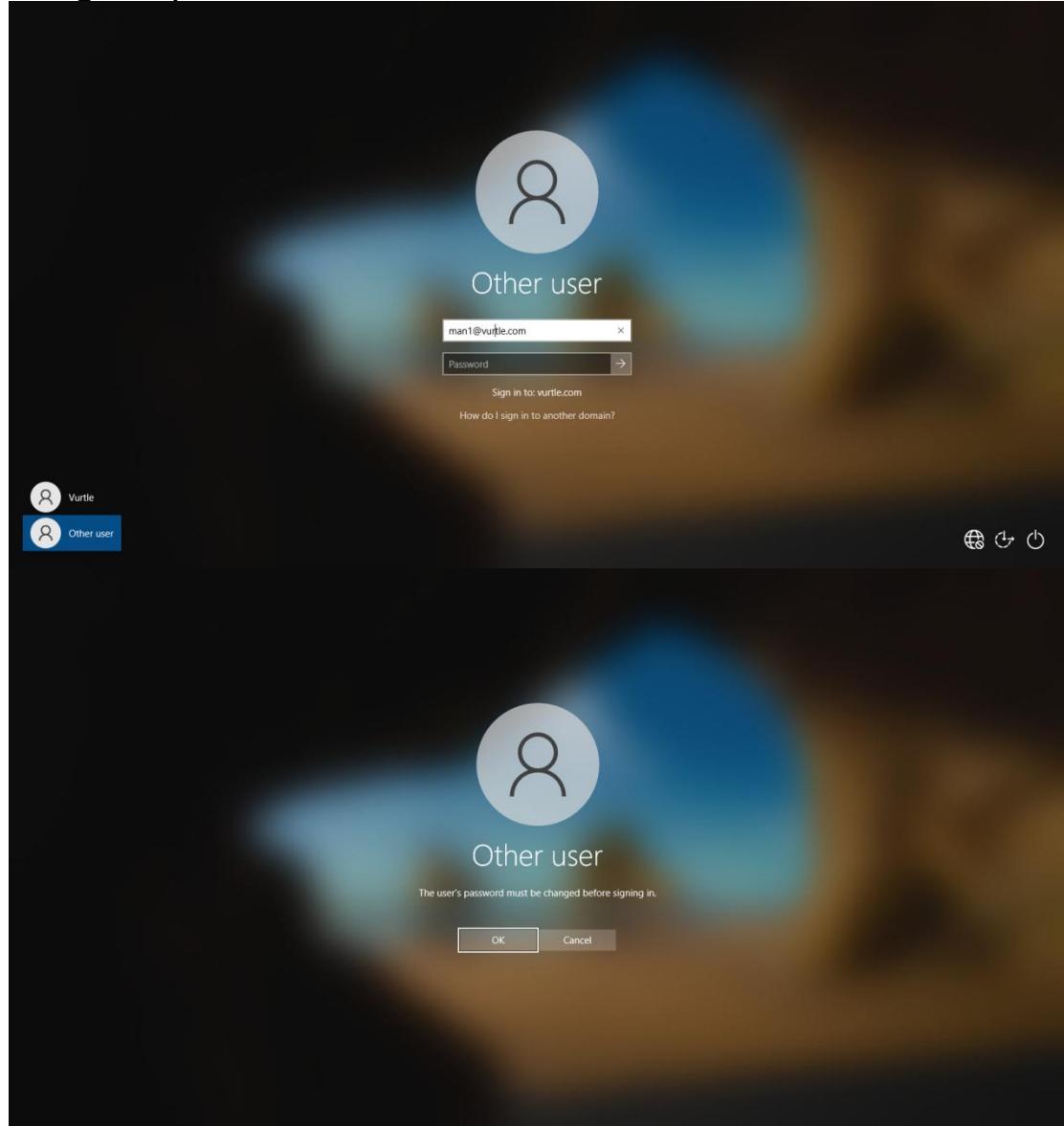


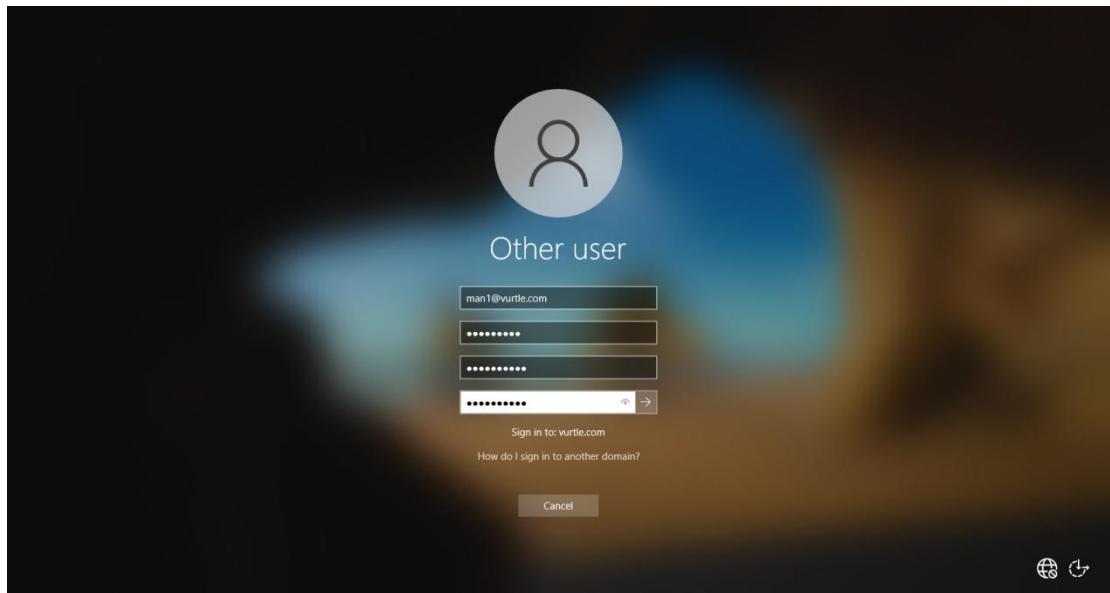
When creating the “Manager1” and other accounts, I enabled the option requiring users to change their passwords upon first login. Therefore, I must first enter the administrator credentials to gain access to the domain, then I can proceed to update the “Manager1” password.





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.

About

Your PC is monitored and protected.

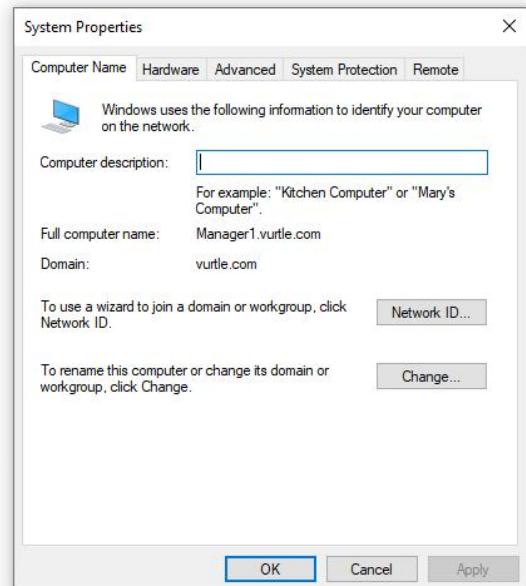
[See details in Windows Security](#)

Device specifications

Device name	Manager1
Full device name	Manager1.vrtle.com
Processor	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz (2 processors)
Installed RAM	2.00 GB
Device ID	545087DB-9280-43AB-9995-62EC6AAA8A72
Product ID	00328-00000-00000-AA759
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

[Copy](#)

[Rename this PC](#)



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.