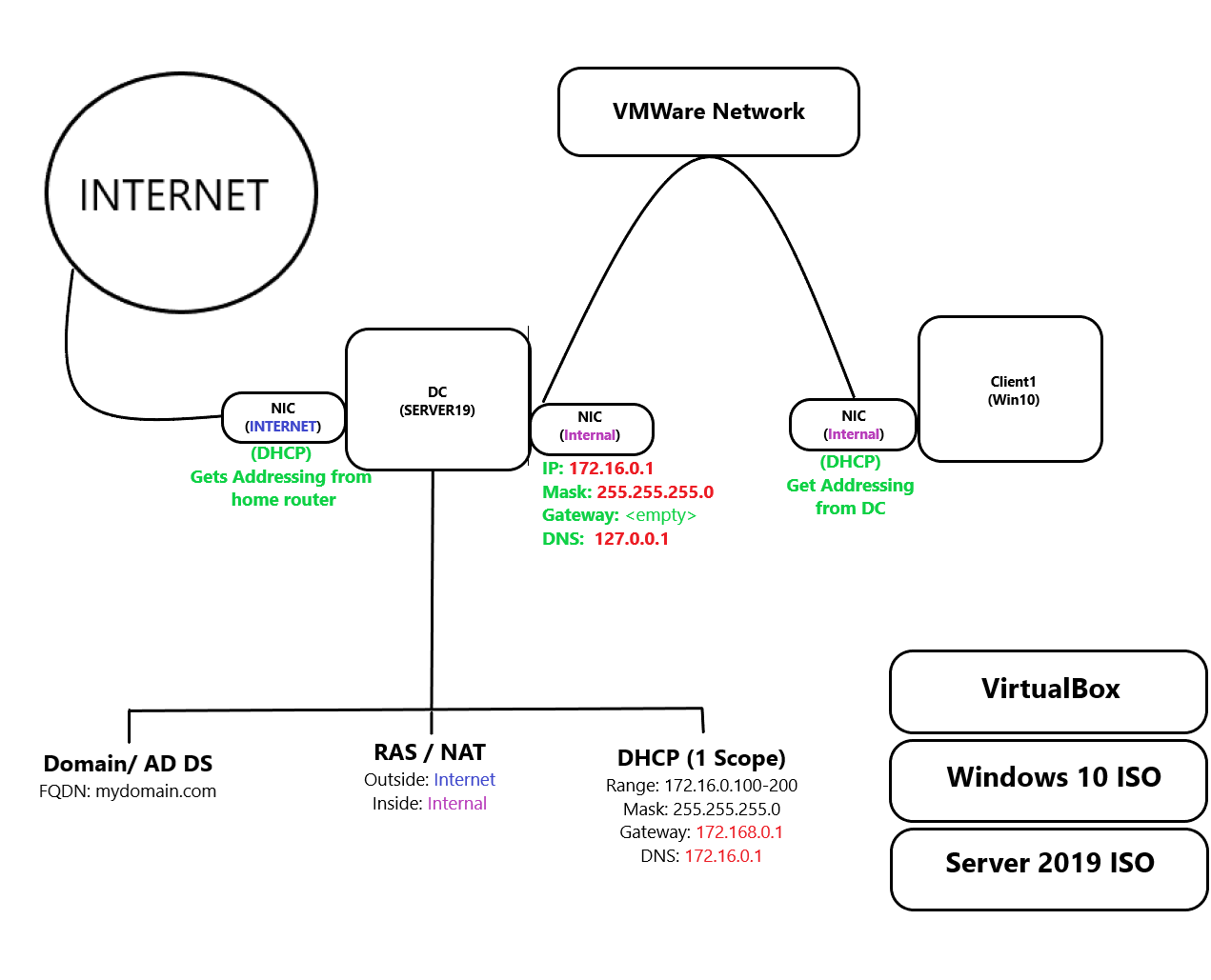
**Active Directory Project**

**Objective:** The goal of this project is to better understand how Active Directory can be set up in a “production” environment by setting up a basic home lab using Oracle VirtualBox, Windows 10 ISO, and Server 2019 ISO, also PowerShell will be used to automate the creation of a 1k+ users to add into active directory users organization unit.



**Domain Controller**

As mentioned in the objective, VirtualBox will be used to create virtual machines to run the “production” environment. Two separate virtual machines will be created; The first will be used to host the Domain Controller, using windows server 2019 ISO to install window server operating system. The second will be used as a client computer with windows 10 operating system. This section focuses on the creation of the Domain Controller (DC VM), which is going to house Active Directory. DC VM will contain a total of two Network interface cards (NIC); one facing the outside internet, the other will be used by client for internal (private) network. After the creation of the first virtual machine, Windows server 2019 will be mounted to install the operating system, then correct identification/labelling of the two network adapter; the external network adapter will automatically get IP addressing from the home network, while the internal adapter will be manually assigned an **IP:172.16.0.1 Mask: 255.255.255.0 Gateway: will not be used because the domain controller itself will act as the default gateway due to the fact it has two NICs DNS: 127.0.0.1 (after installing active directory, it will automatically install DNS, making the server use itself as the DNS server. Hence the loopback address)**

A screenshot of a computer

Description automatically generatedA computer screen shot of a network connection

Description automatically generated

**Domain / Active Directory Domain Services**

Next will be to install Active Directory Domain Services on the DC server, then creating **mydomain.com** being the fully qualified domain name A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

After the creation of mydomain.com, an organization unit called ADMINS will be created to store the very first domain admin account **a-sfajuyi**, the domain admin account will be used from this point on to manage the server and active directory. A screenshot of a computer

Description automatically generated

**RAS / NAT**

Next will be to install RAS/NAT, which is a remote access server network address translation which’s purpose is to allow the windows 10 client to exist on a private virtual network, but still be able to access the internet through the domain controller, to accomplish this; using server manager the **Remote Access** role will be installed with **routing**. A screenshot of a computer

Description automatically generated

After installing the Remote Access role, the **routing and remote access tool** will be used to configure/install NAT, which allows internal clients to connect to the internet using one address which will be the internet NIC created at the Domain Controller section.

A screenshot of a computer

Description automatically generated

**DHCP**

Next will be to set up a DHCP server on the Domain Controller with a scope, which allows windows 10 clients to obtain an IP address enabling them to access the internet while being on a virtual private network. Using the Domain Controller server manager, the DHCP role will be installed, then the DHCP tool will be used to set up the scope. The range for the scope will be **172.16.0.100 – 172.16.0.200** Mask: **255.255.255.0** with a lease of 8 days (which is not ideal, but for the basic home lab this will be the lease period). A screenshot of a computer

Description automatically generated

Next is to configure the DHCP Options which enables the specification of an address as the default gateway; Taking a step back to RAS/NAT section, NAT was configured on the domain controller with routing configured as well, its job is to forward traffic from clients to the internet, because of this, clients are going to use the internal NIC of the domain controller as a default gateway/router. Going back to DHCP configuration, the domain controller’s IP address **172.16.0.1** which has NAT configured on it will be used. After we activate the scope.

**USER Creation**

Using PowerShell ISE and a PowerShell script that uses a text file with 1k+ first and last name to create and add the user to the USER organizational unit which is also created by the same script. Reference the picture below for more explanation of what each line of code does.

A screenshot of a computer program

Description automatically generated

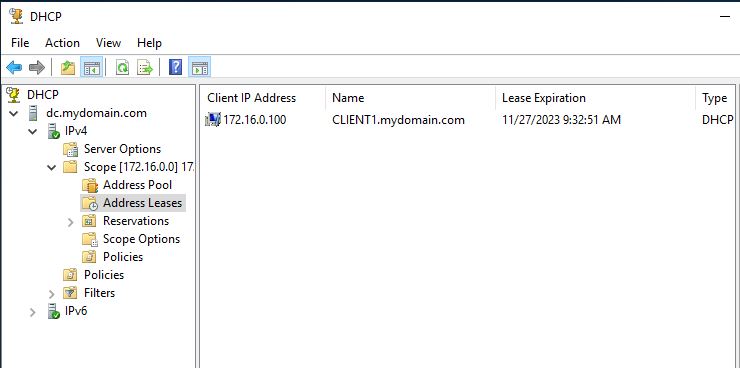
A screenshot of a computer

Description automatically generated

**Client Creation**

Creating a new virtual machine and mount it with windows 10 ISO as well as configuring its network adapter to use the internal network adapter. After the creation of Client1, to confirm IP addressing created in the latter sections are working, using the command prompt and executing the ipconfig command to display the ethernet adapter, we can see the correct domain, IPv4 address, subnet mask, and Default gateway. To test, google.com will be pinged.A screenshot of a computer

Description automatically generated

We then add the Client to the domain using our domain admin account, going back to the Domain Controller DHCP tool we can see a lease was created for Client1 computer. 

**Conclusion**

The sole purpose of this project was to better understand the creation and implementation of active directory using a basic home lab setup. Due to hardware resources, they were limitations on the amount of VMs and tools that can be implemented on the project, but with the resources provided, a mini corporate network was created with a 1k+ users which the addition was automated into Active Directory using PowerShell script. In theory, with the account creation process, when a new user is hired, their name goes into a batch file somewhere on the network, the next day the file runs, which creates the user account on Active Directory. The Client1virtual machine acts as the corporate laptop that gets added to the domain enabling the new user to login into their account with their corporate credentials which is stored on the domain as well.