

# **System Administration**

## Final Documentation

Created By: Hoo Won

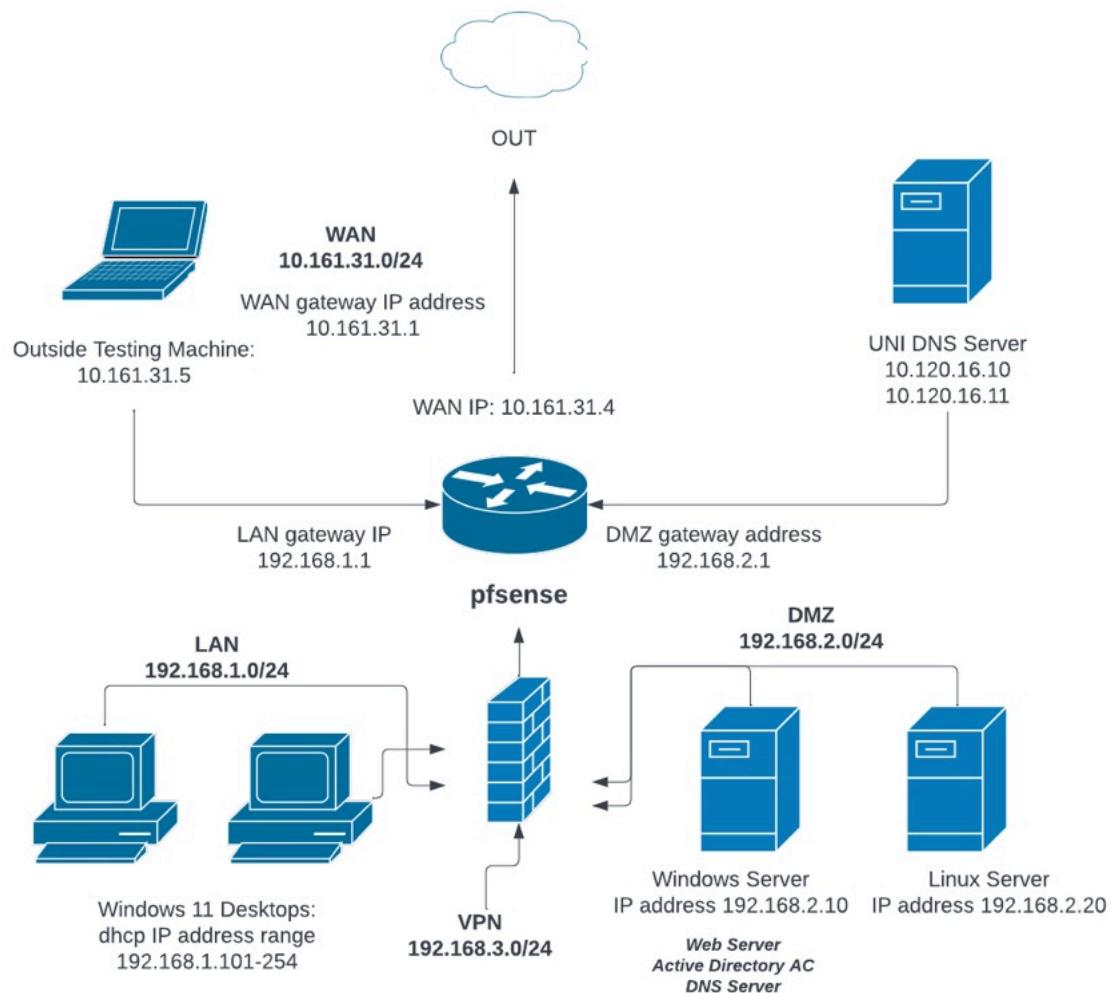
5/2/2025



# Table of Contents

<b>Network Diagram</b>	<b>3</b>
<b>pfSense Port Forwarding Rules</b>	<b>4</b>
<b>pfSense WAN Rules</b>	<b>5</b>
<b>pfSense LAN Rules</b>	<b>6</b>
<b>pfSense VPN Rules</b>	<b>7</b>
<b>Project: Linux Server Setup</b>	<b>8</b>
<b>Project: Windows Server Setup</b>	<b>9</b>
<b>Project: pfSense Setup</b>	<b>10</b>
<b>Project: Internal Caching DNS Server</b>	<b>11</b>
<b>Project: Bind DNS Server Setup</b>	<b>12</b>
<b>Project: Apache Server Setup</b>	<b>13</b>
<b>Project: Active Directory Setup Part A/B</b>	<b>14</b>
<b>Project: Remote Desktop Setup</b>	<b>15</b>
<b>Appendix</b>	<b>16</b>

# Network Diagram



# pfSense Port Forwarding Rules

Firewall / NAT / Port Forward

Port Forward    1:1    Outbound    NPt

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> WAN	TCP	*	*		WAN address	443 (HTTPS)	192.168.2.10	443 (HTTPS)	HTTP webserver	
<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> WAN	UDP	*	*		WAN address	53 (DNS)	192.168.2.10	53 (DNS)		

# pfSense WAN Rules

Firewall / Rules / WAN

Floating    WireGuard    WAN    LAN    DMZ    VPN

Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	*	*		VPN address	*	*	*	none		
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/14.18 MiB	IPv4 UDP	*	*		192.168.2.10	53 (DNS)	*	none	NAT		
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/2.11 MiB	IPv4 TCP	*	*		192.168.2.10	443 (HTTPS)	*	none	NAT HTTP webserver		
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/2 KiB	IPv4 TCP	*	*		DMZ subnets	*	*	none	Block inbound WAN to DMZ traffic		
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/624 B	IPv4 *	*	*		LAN subnets	*	*	*	Do not allow traffic from WAN to LAN		

# pfSense LAN Rules

Firewall / Rules / LAN

Floating    WireGuard    WAN    LAN    DMZ    VPN

Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/4.93 MiB	*	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/106.35 MiB	IPv4 *		LAN subnets	*	DMZ subnets	*	*	none		Allow all traffic from LAN to DMZ	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/437 KiB	IPv4 ICMP any		LAN subnets	*	*	*	*	none		Allow LAN to WAN (Ping)	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/10.04 MiB	IPv4 TCP/UDP		LAN subnets	*	53 (DNS)	*	none			Allow LAN to WAN (DNS)	
<input type="checkbox"/> <input checked="" type="checkbox"/> 3/3.31 GiB	IPv4 TCP/UDP		LAN subnets	*	80 - 443	*	none			Allow LAN to WAN (HTTP & HTTPS)	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/135.32 MiB	IPv4 *		LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv6 *		LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

# pfSense DMZ Rules

The screenshot shows the pfSense Firewall Rules interface. The top navigation bar includes links for Firewall, Rules, and DMZ. Below the navigation is a horizontal menu with tabs: Floating, WireGuard, WAN, LAN, DMZ (which is highlighted in red), and VPN. A table titled "Rules (Drag to Change Order)" lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/> <span style="color:red">X</span>	0/153 KiB	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none	Block all traffic from DMZ to LAN		
<input type="checkbox"/> <span style="color:green">✓</span>	15/3.91 GiB	IPv4 *	DMZ subnets	*	*	*	*	none	Allow all outbound traffic from DMZ to WAN		
<input type="checkbox"/> <span style="color:green">✓</span>	0/1.02 MiB	IPv4 *	*	*	*	*	*	none	ALLOW ALL		

# pfSense VPN Rules

The screenshot shows the pfSense Firewall Rules interface. The top navigation bar includes links for Firewall, Rules, and VPN. Below the navigation is a horizontal menu with tabs: Floating, WireGuard, WAN, LAN, DMZ, and VPN (which is highlighted in red). A table titled "Rules (Drag to Change Order)" lists two rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/> <span style="color:green">✓</span>	0/0 B	IPv4 TCP	192.168.3.0/24	*	DMZ subnets	*	*	none			
<input type="checkbox"/> <span style="color:red">X</span>	0/0 B	IPv4 TCP	192.168.3.0/24	*	LAN subnets	*	*	none			

# Project 1: Linux Server Setup

---

**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

In this project, I will install a Linux OS based Ubuntu server in my virtual folder on Vsphere and configure it to have access to the internet. Below I will document all the steps I took to create my Ubuntu Linux server and answer project related questions provided by my instructor. I have worked with Ubuntu, Linux, and Vsphere before from previous classes such as Operating Systems, so I am expecting this process to be quite simple and maybe even a bit familiar.

---

**Project Answers:** This is where questions should be answered in the project directly. Else Delete this section.

1. What are the /home, /var/www, /var/log, and /etc directories used for in Linux distributions? Please list and describe each directory separately.
  - /home: Stores user files and personal settings.
  - /var/www: Holds website files for web servers.
  - /var/log: Contains system and application logs.
  - /etc: Stores system configuration files.
2. Open a terminal, go to your home directory, and use the list "ls -a" command on the command line to show all files. (What does that flag -a mean?) Hidden files are files that begin with a "." Please list your hidden files and give me an in-depth description of why they are there and what they do.
  - The -a flag in ls -a stands for "all", meaning it lists all files, including hidden ones.
    - .bash\_logout: Runs commands when a user logs out of a Bash session. Often used for cleanup tasks like clearing the terminal screen.
    - .bashrc: A configuration file for Bash that runs when a new terminal session starts. It contains custom aliases, functions, environment variables, and prompt settings.
    - .profile: A script that runs at login for setting environment variables and executing startup commands. It is mainly used for login shells.
    - .ssh: A directory that stores SSH-related files, such as private/public keys, known hosts, and configuration settings for remote connections.

3. Linux is very proactive about implementing the security policy of “least-privilege”. This means that you often start off as a regular user with a limited set of permissions to do things. To make system administration changes, you often have to use permissions of a super user, with commands ‘su’ and ‘sudo’. Please answer the following questions:
- What is the ‘sudo’ command and how would you use it?
    - sudo lets a regular user run commands as a superuser. It is used for administrative tasks like installing software, modifying system files, or managing services.
  - What is the output of running the command: ls /root
    - wonh@hoolinuxserver:~\$ ls /root
    - ls: cannot open directory '/root': Permission denied
  - What is the output of running the command: sudo ls /root
    - wonh@hoolinuxserver:~\$ sudo ls /root
    - [sudo] password for wonh:
    - wonh@hoolinuxserver:~\$ \_
4. Linux package managers are important. Ubuntu is a Debian-based distribution, so it uses the "apt" repository system with the "dpkg" package manager. (Yes, it also uses snap, but please ignore that for now.) Please answer the following questions:
- How do you look for packages to install?
    - With the apt search command (apt search “package\_name”)
  - How do you install a package?
    - With command (sudo apt install “package\_name”)
  - How do you see what packages are already installed?
    - With command (dpkg --list)
  - How do you remove a package?
    - With command (sudo apt remove “package\_name”)
5. Linux servers will host “services”, which are large apps that typically begin on startup. Often times, a system administrator will have to stop/start/restart these services after making configuration changes. Please answer the following questions (you can use systemctl or service):
- List what services are running?
    - Use command (systemctl “list-units” --type=service --state=running)
  - Stop/start/restart a service?
    - Stop command: sudo systemctl stop “service\_name”
    - Start command: sudo systemctl start “service\_name”
    - Restart command: sudo systemctl restart “service\_name”
  - Get information about a service by looking at its status?
    - Use command (systemctl status “service\_name”)

6. Linux uses a service called cron to run needed scripts over certain time intervals. Please describe the cron jobs your server is running and when those jobs occur. How would you add a new cron job?
- There are cron jobs that periodically clean up temporary files to free up space. One that runs system security updates and runs at 5 AM everyday to install security updates. Another one that periodically checks for system updates.
  - You can add a new cron job by opening the cron editor with command (crontab -e) and adding a new job using the format (minute hour day month day-of-week command)
7. How do you add users to a Linux system through the command line? How do you remove users through the command line?
- Add users command: sudo useradd username
  - Remove users command: sudo userdel username
8. File permissions are important. If you run the command “ls –la” in any directory on the command line, you will see a string of permissions for files and directories like this (here are 5 random ones from my system):
- ```
drwxr-xr-x
drwxr-xr-x
-rw-----
-rw-r--r--
-rw-r--r--
```

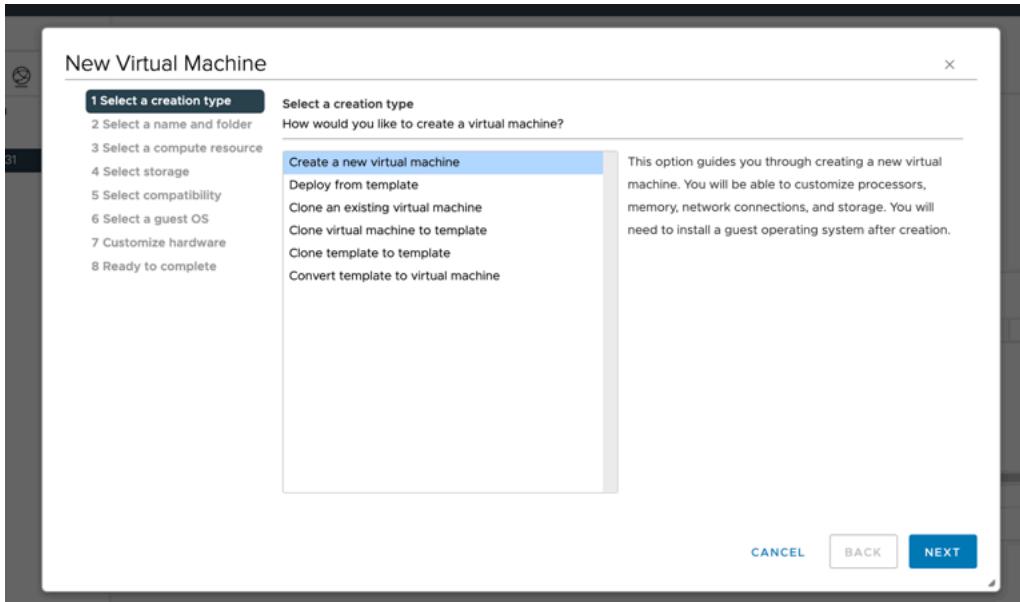
Please tell me (1) what the permissions mean, (2) how you change them, and (3) what this permission string means: “drwxr-xr-x”.

1. First 3 characters are for “owner”, the second batch of 3 characters is for “group”, the third group of 3 characters is for “others”. “r” is read permission, “w” is write permission, “x” is execute permission. “-” means permission is not granted.
2. You can change them with command “chmod”
3. The string “drwxr-xr-x” means that it is a directory (“d”), the owner has read, write and execute permissions (“rwx”), the group has read and execute permissions (“r-x”), the others have read and execute permission (“r-x”).

---

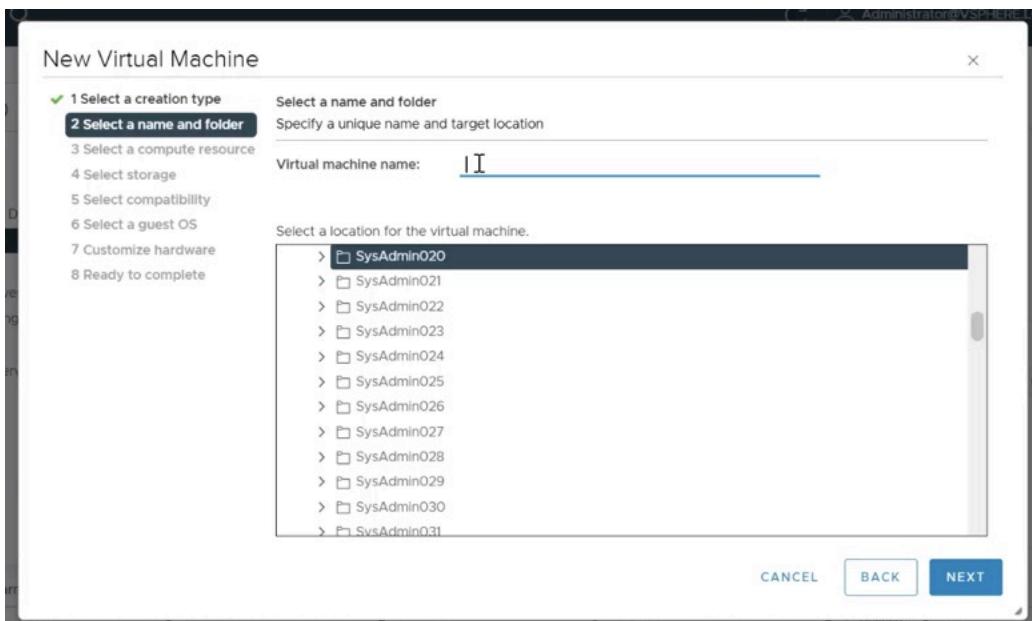
**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.

1. Log in to Vsphere and find your assigned virtual folder
2. Right click on the folder and click “New Virtual Machine...”



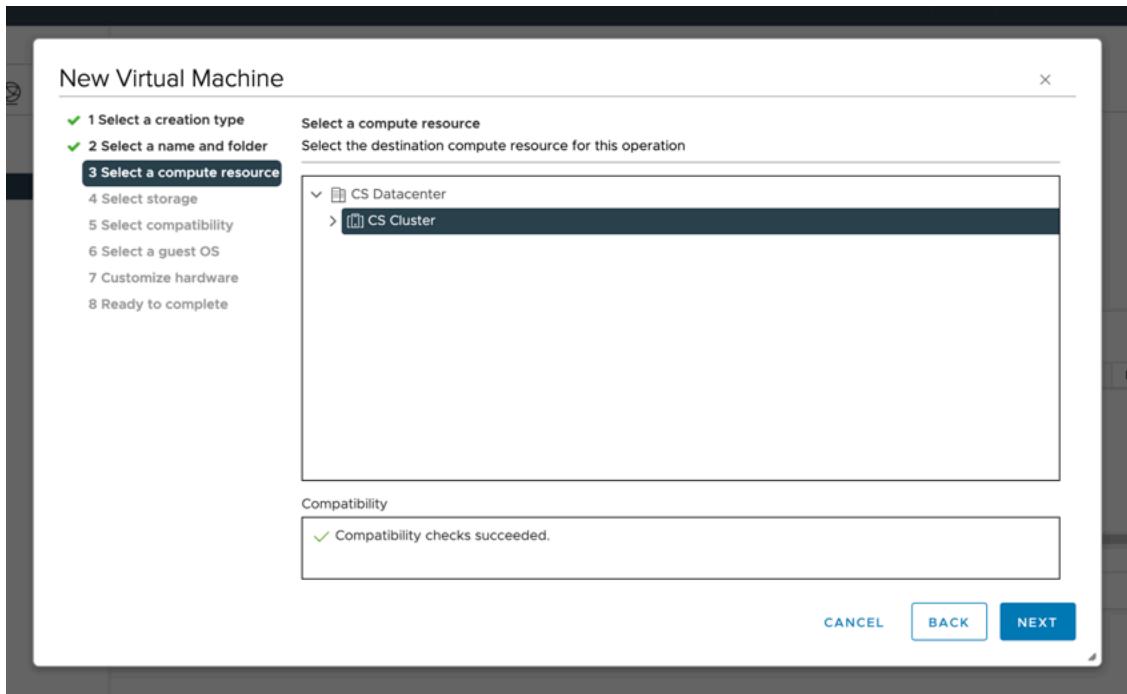
3.

- Select "Create a new virtual machine"
- Hit "NEXT"



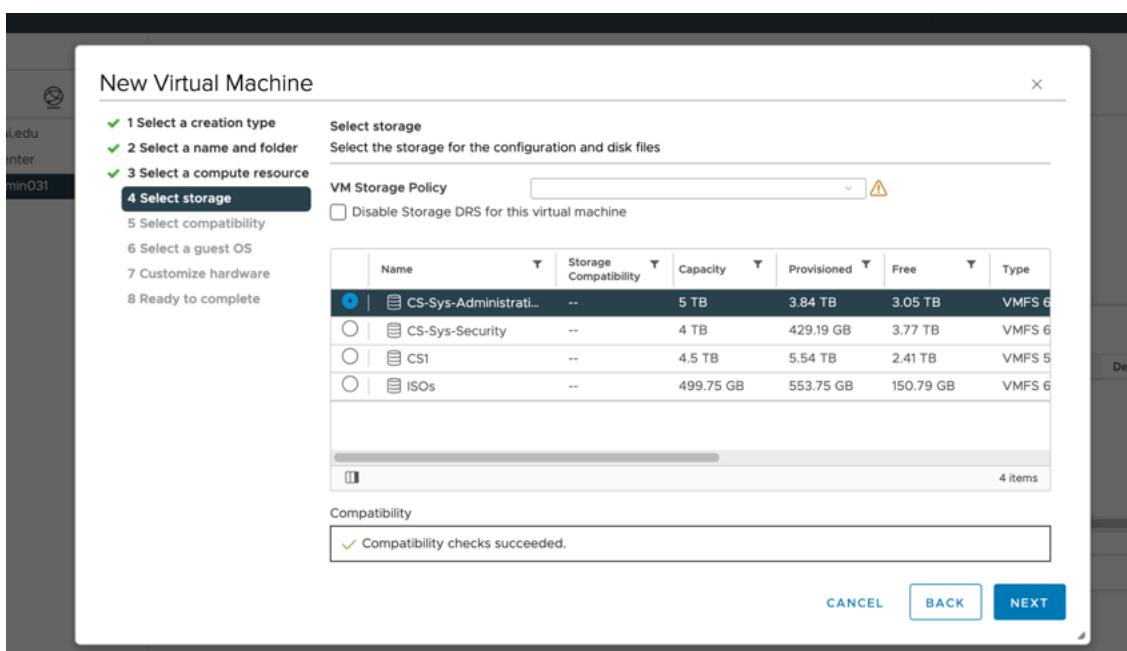
4.

- Name your virtual machine!
- Hit "NEXT"



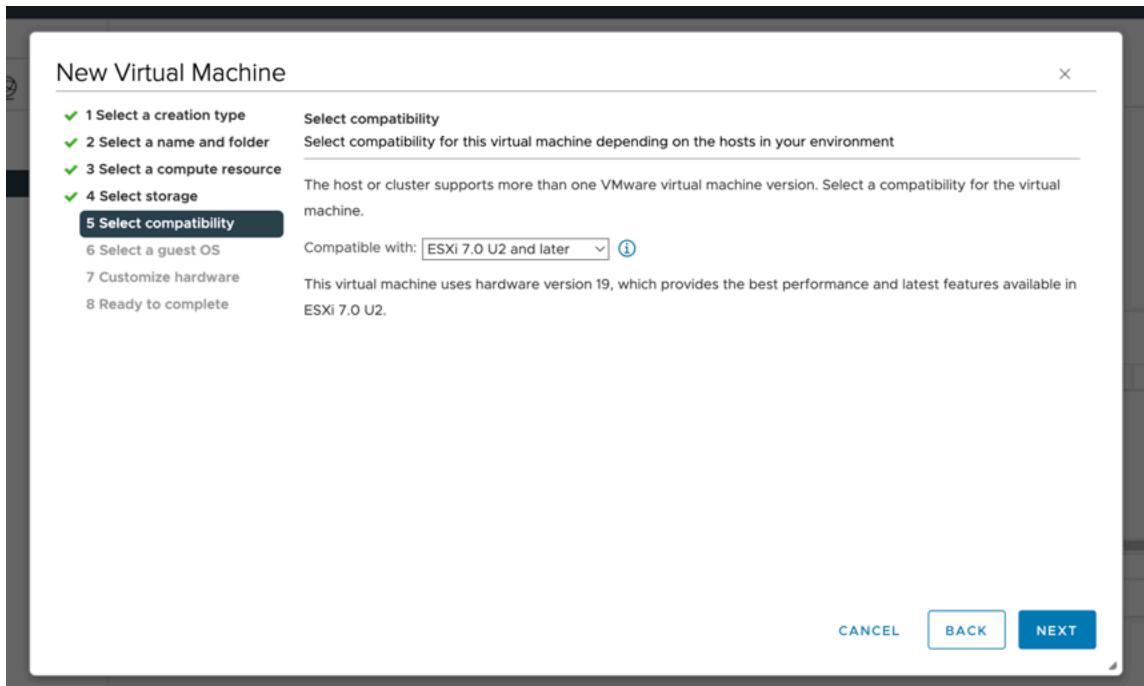
5.

- Select "CS Cluster" for compute resource
- Hit "NEXT"



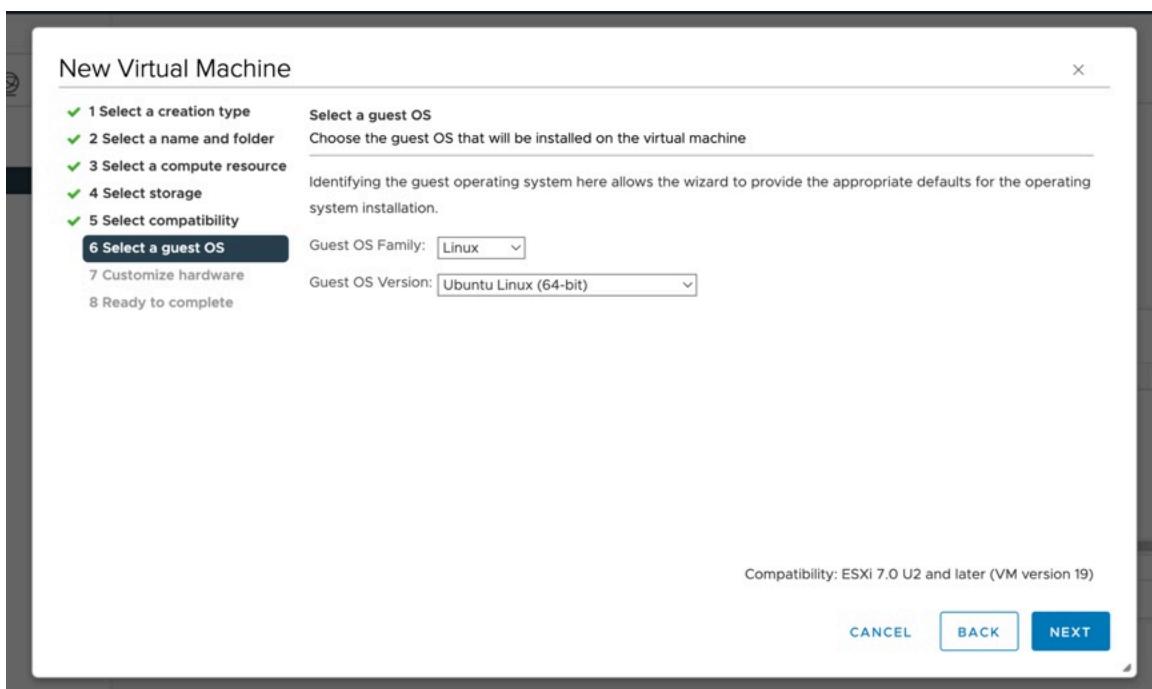
6.

- Select "CS-Sys-Administration" for storage
- Hit "NEXT"



7.

- Select compatibility with "ESXi 7.0 U2 and later"
- Hit "NEXT"



8.

- Select Guest OS Family "Linux"
- Select OS Version "Ubuntu Linux (64-bit)"
- Hit "NEXT"

New Virtual Machine

✓ 1 Select a creation type  
 ✓ 2 Select a name and folder  
 ✓ 3 Select a compute resource  
 ✓ 4 Select storage  
 ✓ 5 Select compatibility  
 ✓ 6 Select a guest OS  
**7 Customize hardware**  
 8 Ready to complete

| CPU                 |                                             |
|---------------------|---------------------------------------------|
| > Memory *          | 8 GB                                        |
| ✓ New Hard disk *   | 60 GB                                       |
| Maximum Size        | 3.05 TB                                     |
| VM storage policy   |                                             |
| Location            | Store with the virtual machine              |
| Disk Provisioning   | Thin Provision                              |
| Sharing             | Unspecified                                 |
| Shares              | Normal 1000                                 |
| Limit - IOPs        | Unlimited                                   |
| Disk Mode           | Dependent                                   |
| Virtual Device Node | New SCSI controller SCSI(0:0) New Hard disk |

CANCEL BACK NEXT

9.

- Set Memory to 8 GB
- Set New Hard disk to 60 GB
- Set Disk Provisioning to "Thin Provision"

New Virtual Machine

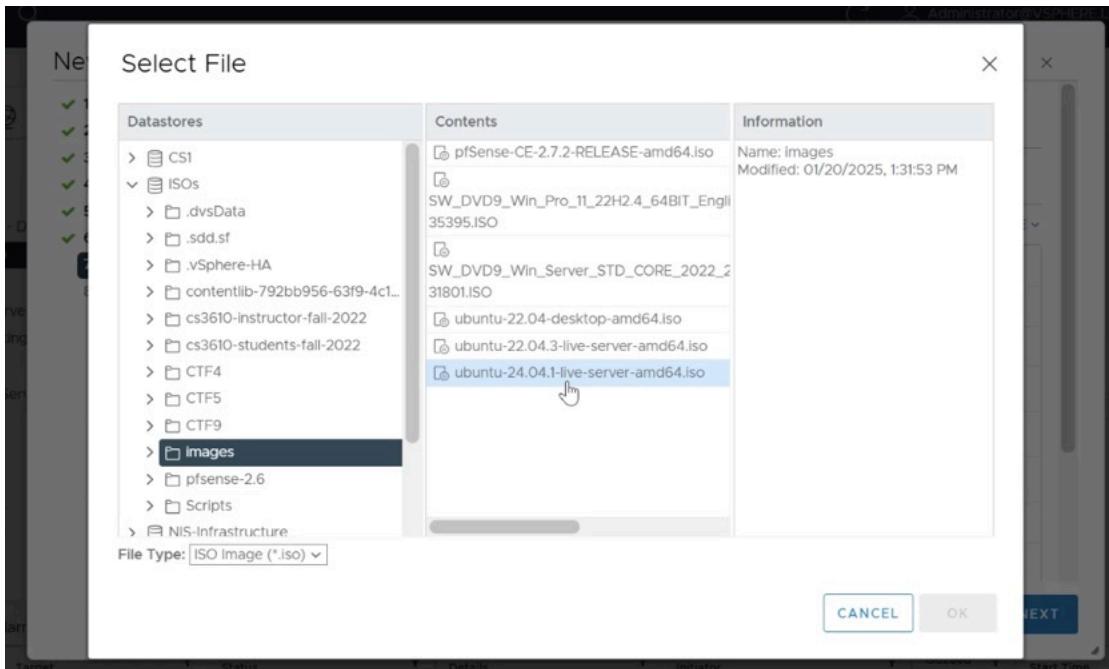
✓ 1 Select a creation type  
 ✓ 2 Select a name and folder  
 ✓ 3 Select a compute resource  
 ✓ 4 Select storage  
 ✓ 5 Select compatibility  
 ✓ 6 Select a guest OS  
**7 Customize hardware**  
 8 Ready to complete

|                         |                         |
|-------------------------|-------------------------|
| > CPU                   | 2                       |
| > Memory *              | 8 GB                    |
| > New Hard disk *       | 60 GB                   |
| > New SCSI controller * | VMware Paravirtual      |
| > New Network *         | SysAdmin031             |
| > New CD/DVD Drive *    | Datastore ISO File      |
| > Video card *          | Specify custom settings |
| > Security Devices      | Not Configured          |
| VMCI device             |                         |
| New SATA Controller     | New SATA Controller     |
| > Other                 | Additional Hardware     |

CANCEL BACK NEXT

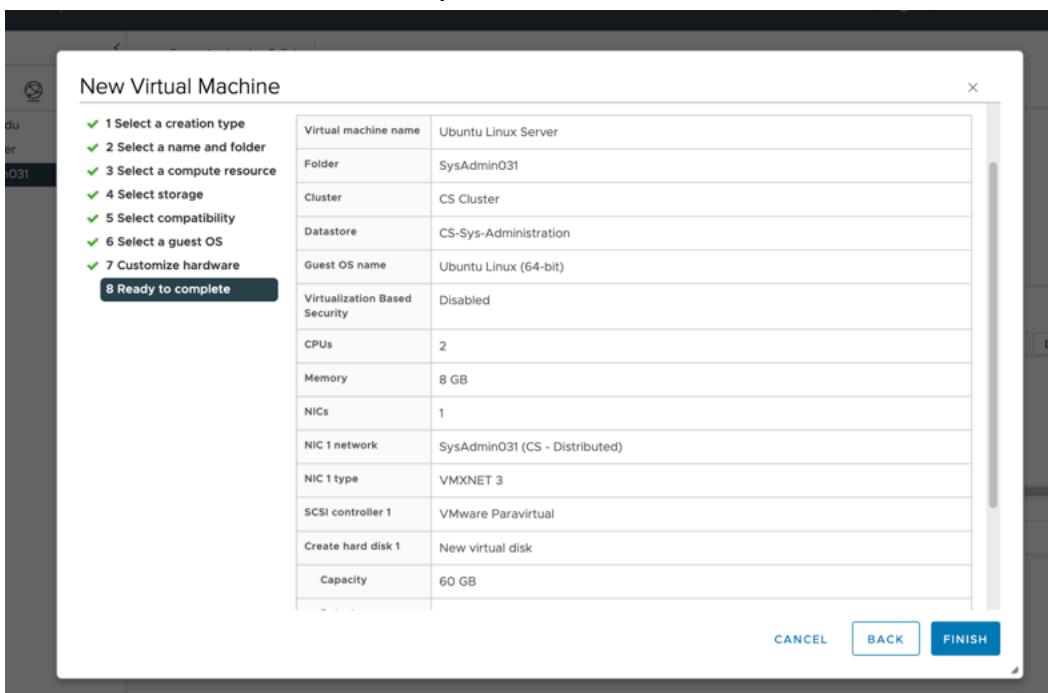
10.

- Set New Network to your Folder (SysAdmin031)



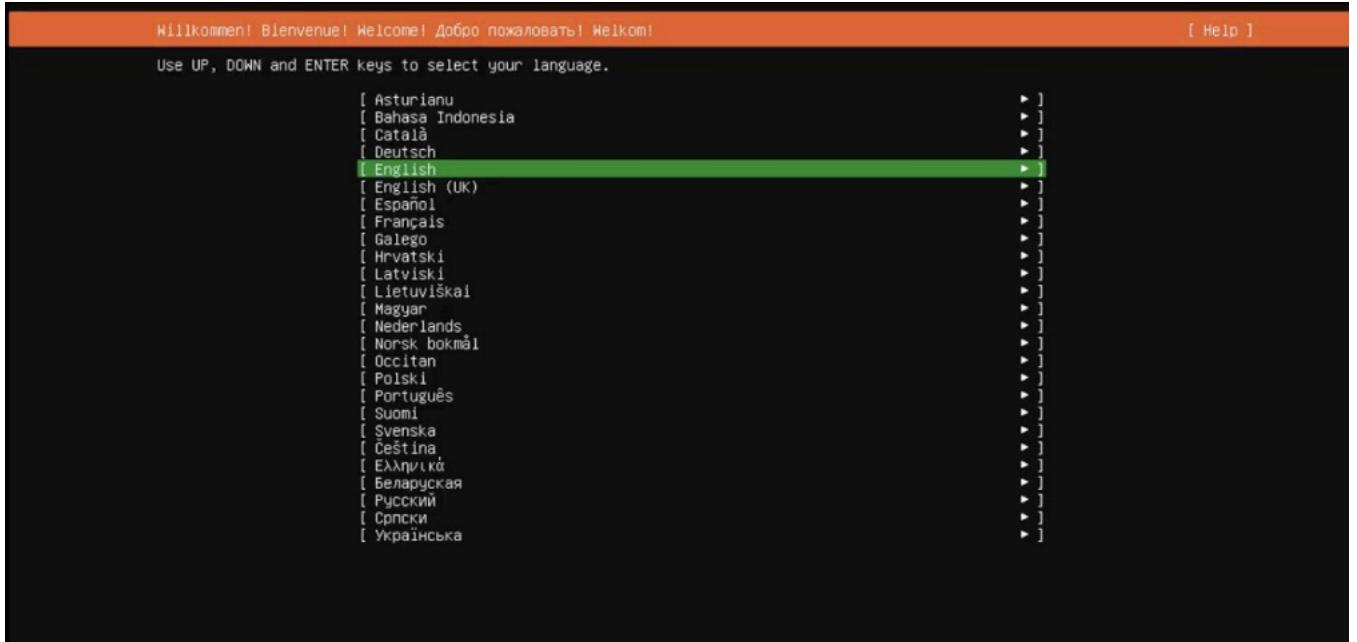
11.

- Select “Datastore ISO File” for New CD/DVD Drive
- Go to ISOs -> images -> “ubuntu-24.04.1-live-server-amd64.iso”
- Hit “OK”
- Hit Connect for New CD/DVD Drive



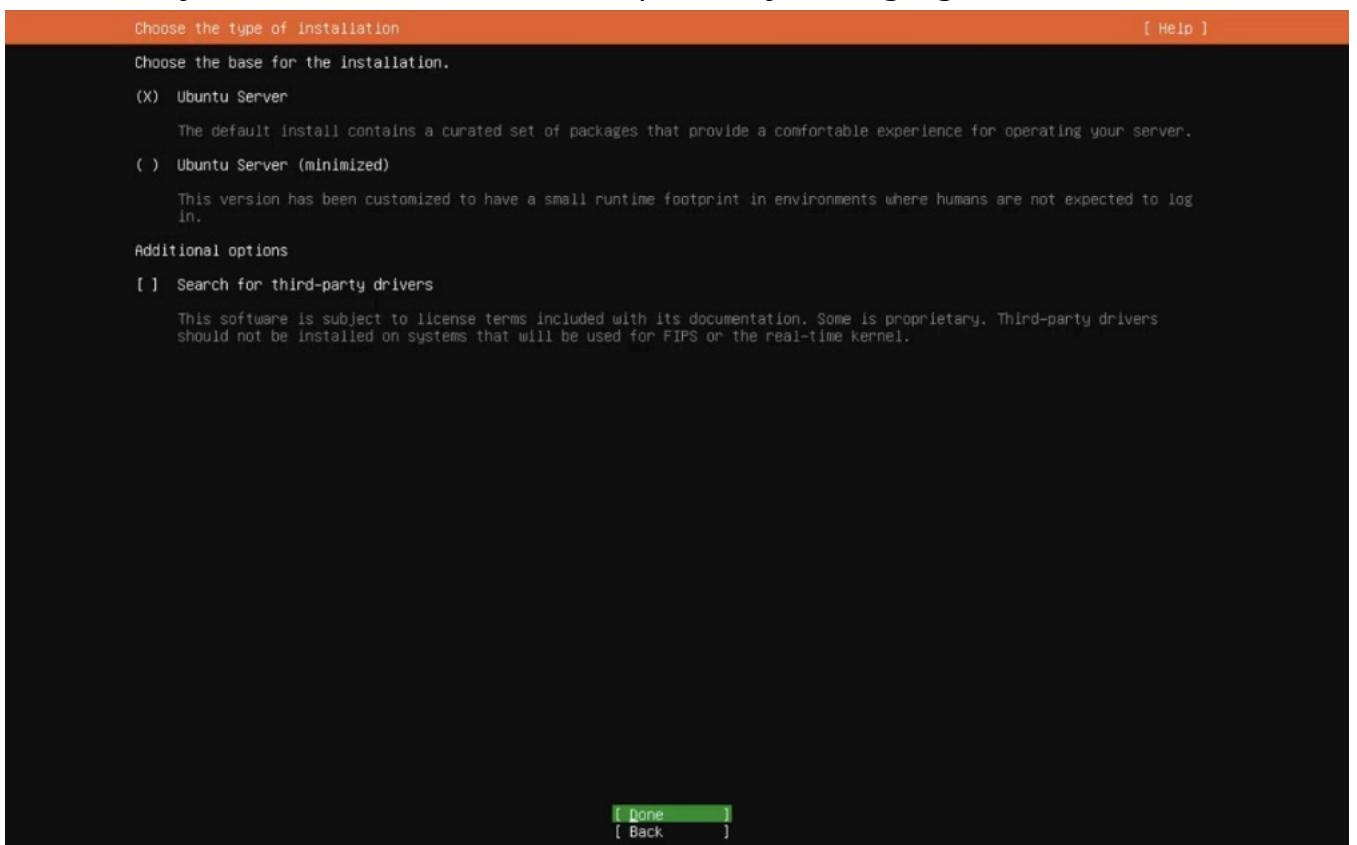
12.

- Go over configurations and make sure they match the requirements!
- Hit “FINISH”
- Power ON your virtual machine!



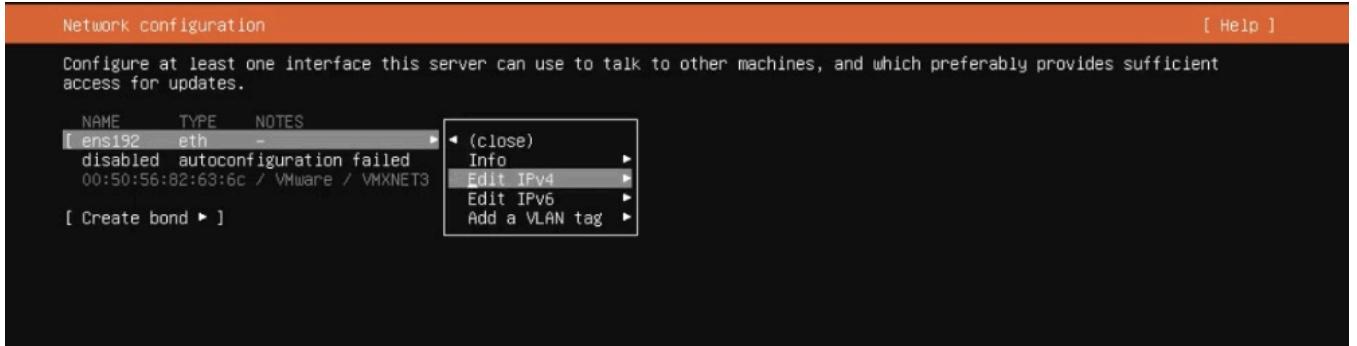
13.

- Once your virtual machine is loaded up, select your language!



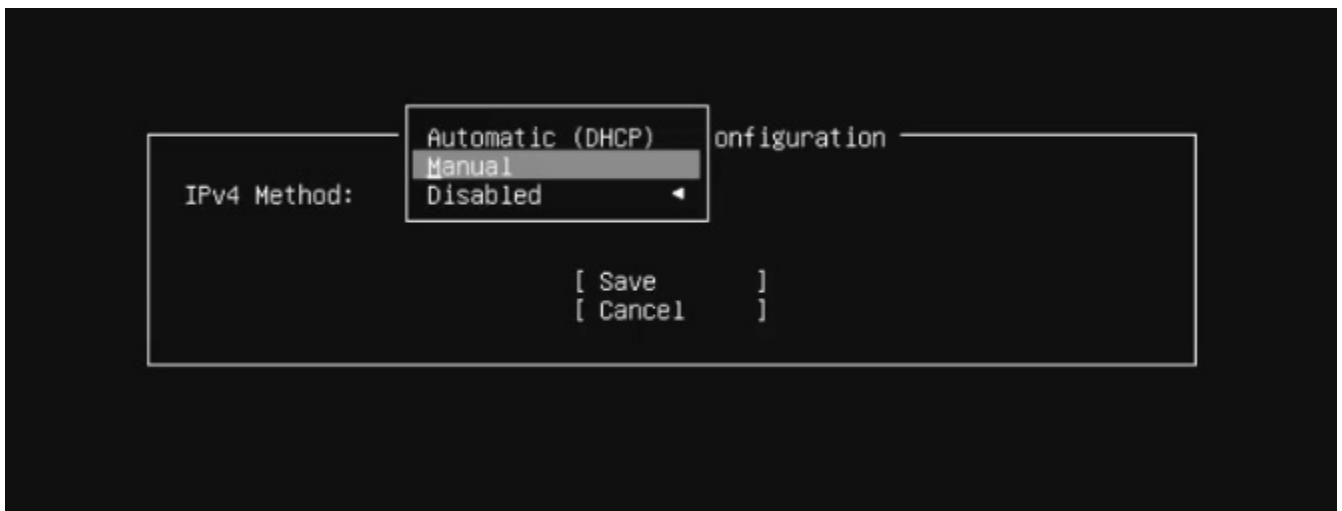
14.

- Select "Ubuntu Server" and hit "Done" until the next checkpoint



15.

- Select your network -> select "Edit IPv4"



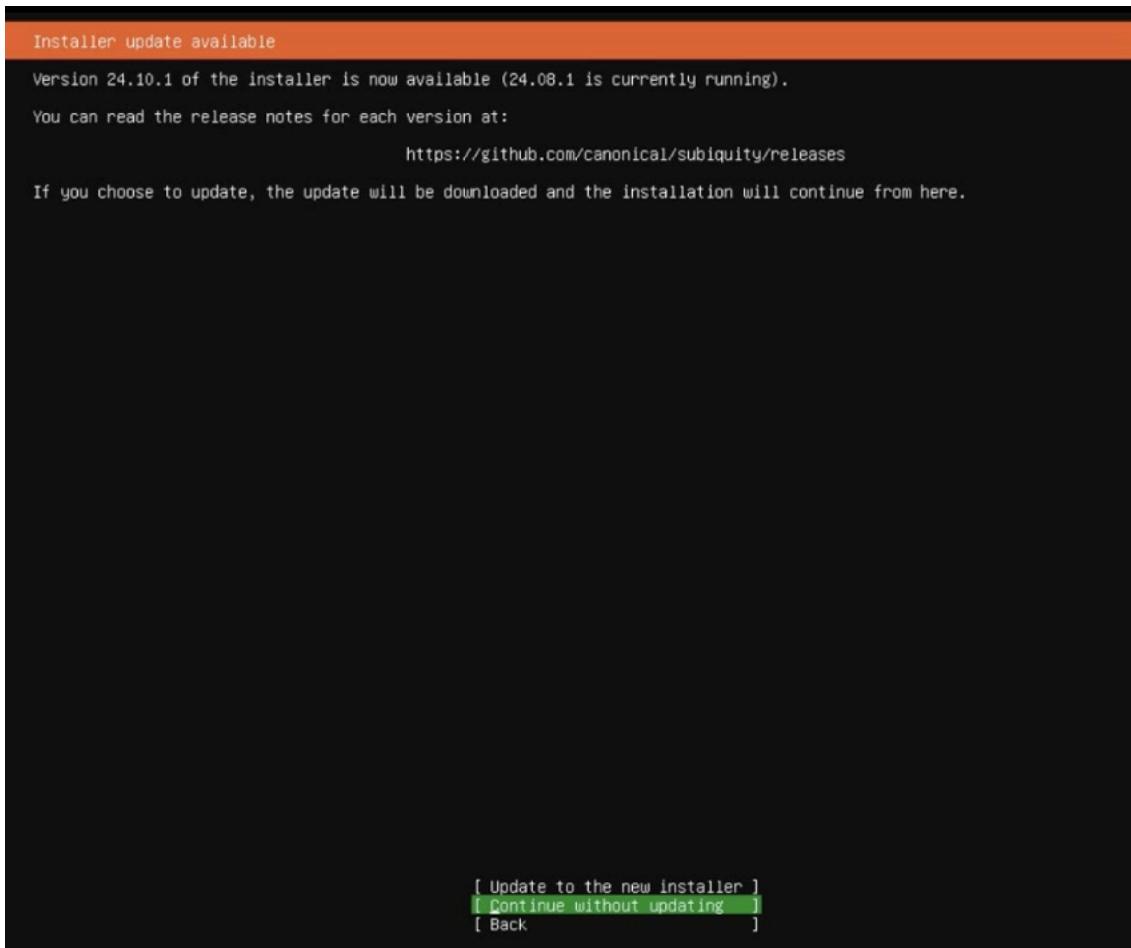
16.

- Select "Manual" and hit "Save"



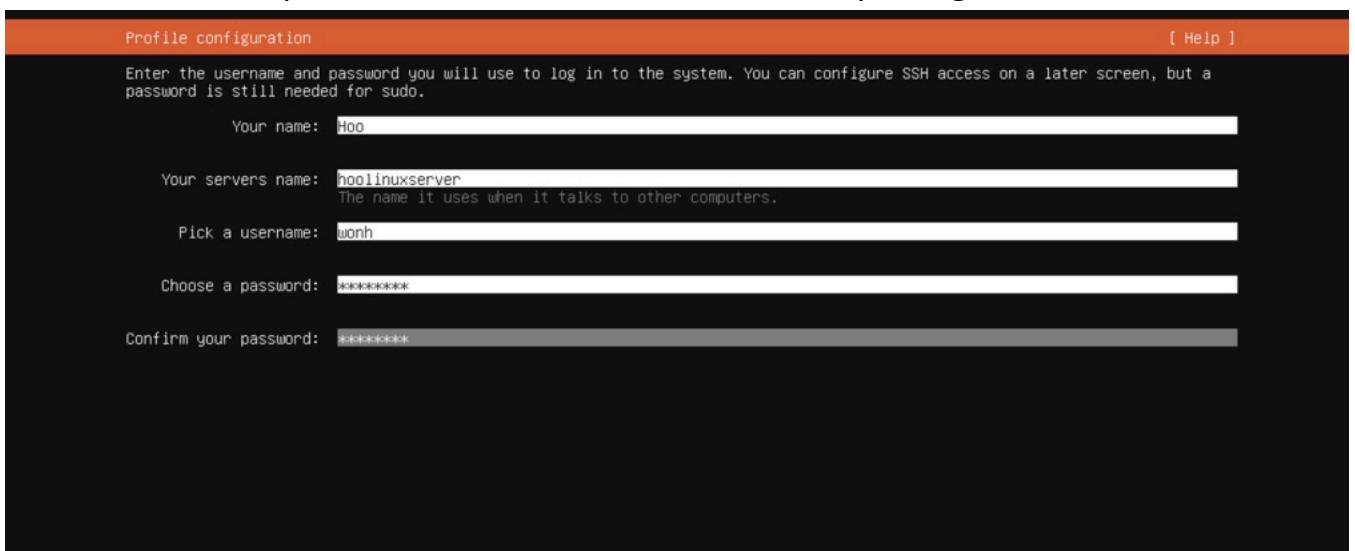
17.

- Enter correct Subnet, Address, Gateway, and Name servers based on your network
- Hit "Done" until next checkpoint



18.

- At Installer update available, hit “Continue without updating”



19.

- Fill in information for Profile configuration and hit “Done” until next checkpoint
- \*\*\*\*\*
- Juspen6h

```
Updating system [ Help ]  
configuring format: format-0  
configuring partition: partition-2  
configuring lvm_vggroup: lvm_vggroup-0  
configuring lvm_partition: lvm_partition-0  
configuring format: format-1  
configuring mount: mount-1  
configuring mount: mount-0  
executing curtin install extract step  
curtin command install  
writing install sources to disk  
running 'curtin extract'  
curtin command extract  
acquiring and extracting image from cp:///tmp/tmp_bvyudu3/mount  
configuring keyboard  
curtin command in-target  
executing curtin install curthooks step  
curtin command install  
configuring installed system  
running 'curtin curthooks'  
curtin command curthooks  
configuring apt configuring apt  
installing missing packages  
Installing packages on target system: ['grub-pc']  
configuring isc-dhcp service  
configuring raid (mdadm) service  
configuring NME over TCP  
installing kernel  
setting up swap  
apply networking config  
writing etc/fstab  
configuring multipath  
updating packages on target system  
configuring pollinate user-agent on target  
updating initramfs configuration  
configuring target system bootloader  
installing grub to target devices  
copying metadata from /cdrom  
final system configuration  
calculating extra packages to install  
configuring cloud-init  
downloading and installing security updates  
curtin command in-target /
```

20.

- Your virtual machine should be starting!

```
Ubuntu 24.04.1 LTS ubuntu tty1  
ubuntu login: sarahm  
Password:  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/pro  
  
System information as of Mon Jan 27 06:46:47 PM UTC 2025  
  
System load: 0.25 Processes: 243  
Usage of /: 22.0% of 28.37GB Users logged in: 0  
Memory usage: 3% IPv4 address for ens192: 10.161.20.2  
Swap usage: 0%  
  
Expanded Security Maintenance for Applications is not enabled.  
93 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
sarahm@ubuntu:~$ _
```

21.

- This is what it should look like when you're all done!

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

I learned how to install a Linux OS based Ubuntu server in my virtual folder on Vsphere and configure it to have access to the internet. I learned it by following the steps provided in the project specification and the demonstration shown by Prof. Diesburg. I also learned about cron jobs and how they manage and keep my systems running. Nothing broke my initial expectations and the project was what I expected.

---

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

<https://support.cs.wm.edu/index.php/tips-and-tricks/basic-linux-commands>

<https://ubuntu.com/server/docs/package-management>

<https://www.geeksforgeeks.org/crontab-in-linux-with-examples/>

<https://www.codementor.io/@akul08/the-ultimate-crontab-cheatsheet-5op0f>

# Project 2: Windows Server Setup

---

**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

For this project, I will install a Windows server in my virtual folder on vSphere and configure it so it has access to the internet. After doing the last project, I do not expect to face many difficulties as this project is similar. I also use Windows OS at home and it is very familiar to me, so I expect this project to go smoothly.

---

## Project Answers:

1. Where can you find installed programs? (I'm not asking about the start menu, but instead where you can see a list of installed programs with options to modify or uninstall them.)

- You can view a list of installed programs in the Control Panel under Programs and Features (Control Panel -> Programs -> Programs and Features).

2. How do you modify Explorer to show hidden files and directories?

- Open File Explorer -> Click on View tab.
- Select Options -> Change folder and search options.
- In Folder Options, go to the View tab.
- Check Show hidden files, folders, and drives and click Apply.

3. Where can you find the system logs? What are they?

- System logs are found in the Event Viewer
  - Application logs (program related events)
  - Security logs (login attempts, access permissions)
  - System logs (OS level events like driver failures)

4. What does the Windows Services Manager do? How can you start/stop/restart a service? How can you get a service to start automatically on bootup?

- Windows Services Manager allows you to view, manage, and configure background services.
- Right-click a service and choose start, stop, or restart.
- Right-click the service, select Properties and Under Startup type, choose Automatic.

5. How do you add users to a Windows system? How do you remove users?

- Open Settings -> Accounts -> Users.
  - Click Add a user and follow the prompts.
  - To remove, select the user, and click Remove.

6. Suppose you need a custom Windows powershell or batch script to run once a day every day. How would you set this up? (In other words, does Windows have a cron equivalent)?

- Use Task Scheduler (type “taskschd.msc” in cmd to bring up)
- Click Create Basic Task.
- Set a trigger to run Daily.
- Select powershell or batch script and save the task

7. Go to the Server Manager (this generally pops up when you boot into your server).

1. How would you assign a new role to your Server, like a webserver? (Don’t actually do this, but instead tell me what menus/buttons you would click on to start the process.

- Open Server Manager
- Click Manage -> Add Roles and Features.
- Use the Role-based option and select the server.
- Choose Web Server and install

2. In your local server, where can you see if Remote Desktop is turned on or off?

- In Server Manager, click Local Server.
- Find Remote Desktop and check if it is Enabled or Disabled.

3. In your local server, find an event with an error or warning message. Explain what that message means.

| WIN-KHV7TRSMBOA                                                                                                                                               | 10149 | Warning | Microsoft-Windows-Windows Remote Management | System      | 2/17/2025 7:36:12 PM |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|---------------------------------------------|-------------|----------------------|
| WIN-KHV7TRSMBOA                                                                                                                                               | 8198  | Error   | Microsoft-Windows-Security-SPP              | Application | 2/17/2025 7:33:08 PM |
| The WinRM service is not listening for WS-Management requests.                                                                                                |       |         |                                             |             |                      |
| User Action<br>If you did not intentionally stop the service, use the following command to start the WinRM service:<br>C:\Windows\system32\sc.exe start WinRM |       |         |                                             |             |                      |

- This warning indicates that the Windows Remote Management service is not set up to accept remote management connections.

4. On your dashboard, if there are any areas in red, please describe what you did to resolve it. (You may or may not have these.)

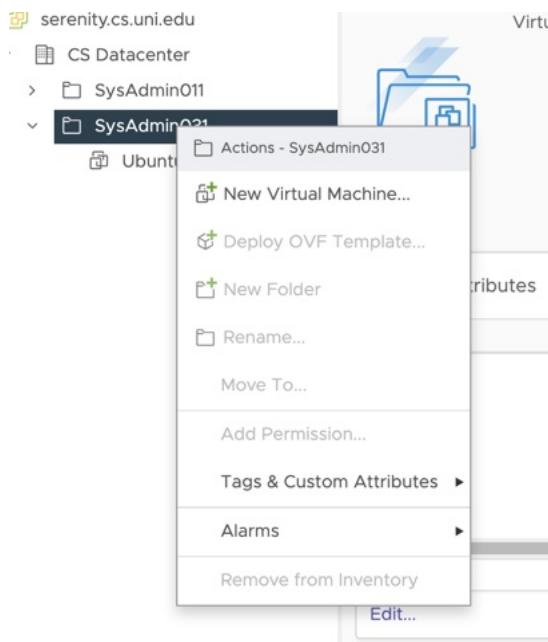
**ROLES AND SERVER GROUPS**  
Roles: 1 | Server groups: 1 | Servers total: 1

| File and Storage Services                             | Local Server                                                      | All Servers                                                       |
|-------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------|
| Manageability<br>Events<br>Performance<br>BPA results | Manageability<br>Events<br>Services<br>Performance<br>BPA results | Manageability<br>Events<br>Services<br>Performance<br>BPA results |

2/17/2025 8:10 PM

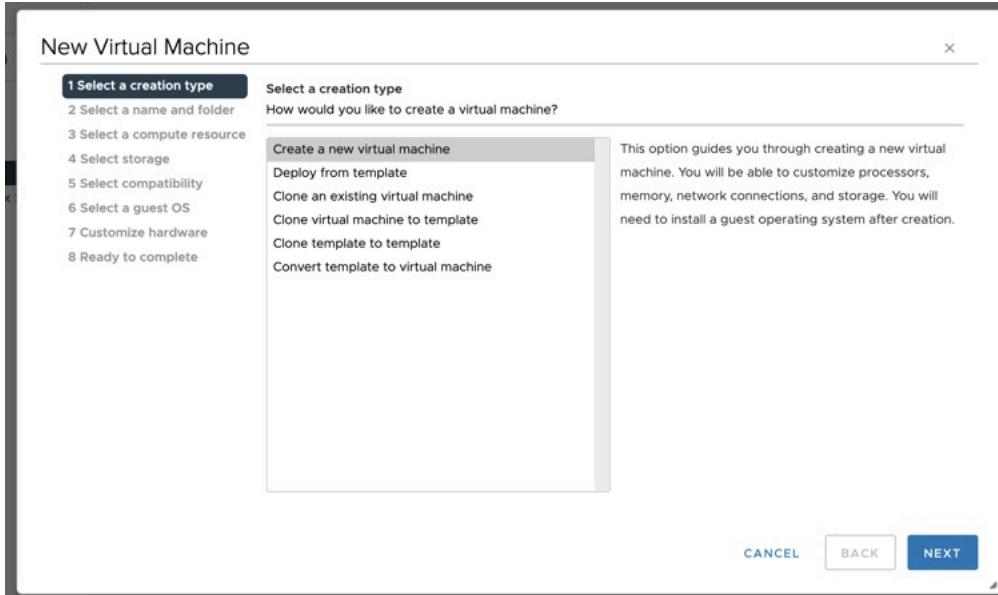
- I connected my virtual server to the internet and downloaded VMware. I do not know if that specifically resolved the issues but after restarting my machine, the areas in red were gone.

**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



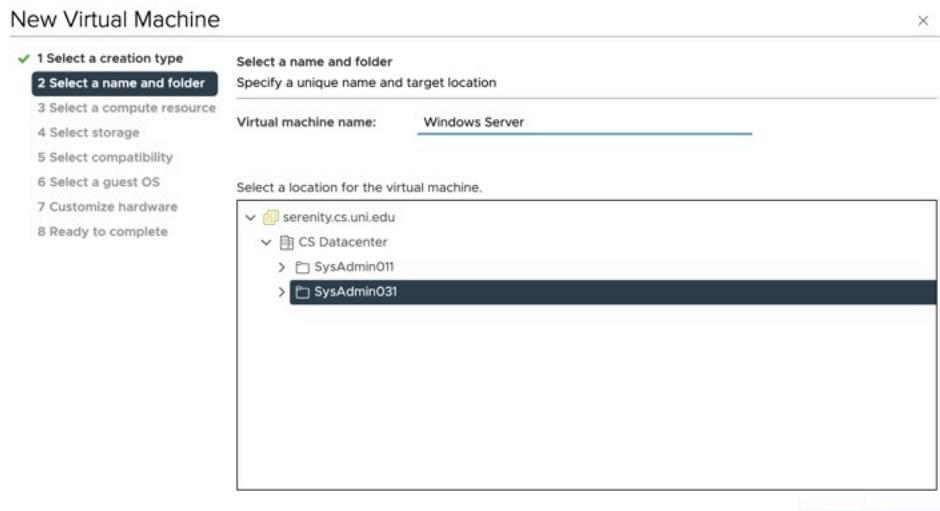
1.

- Right click your Virtual Folder and click "New Virtual Machine..."



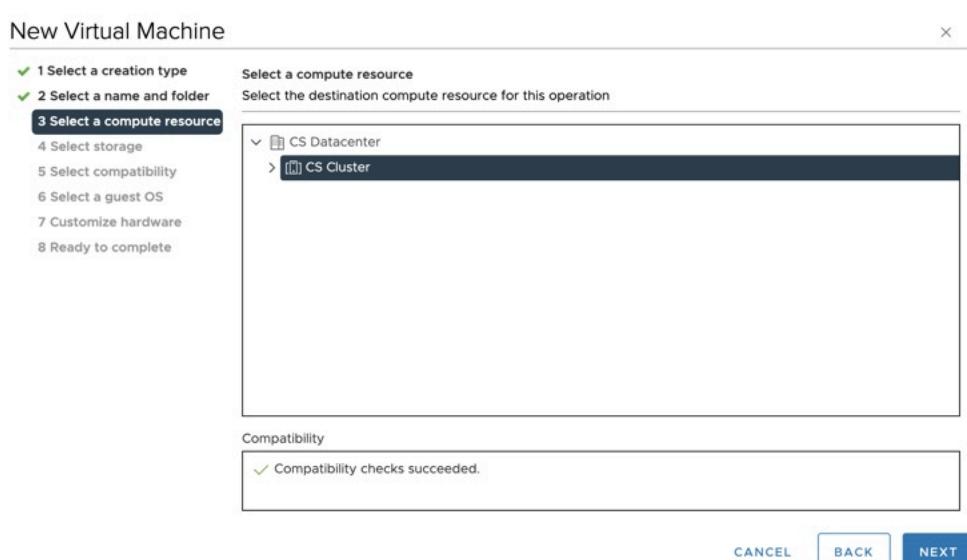
2.

- Select "Create a new virtual machine" and hit "NEXT"

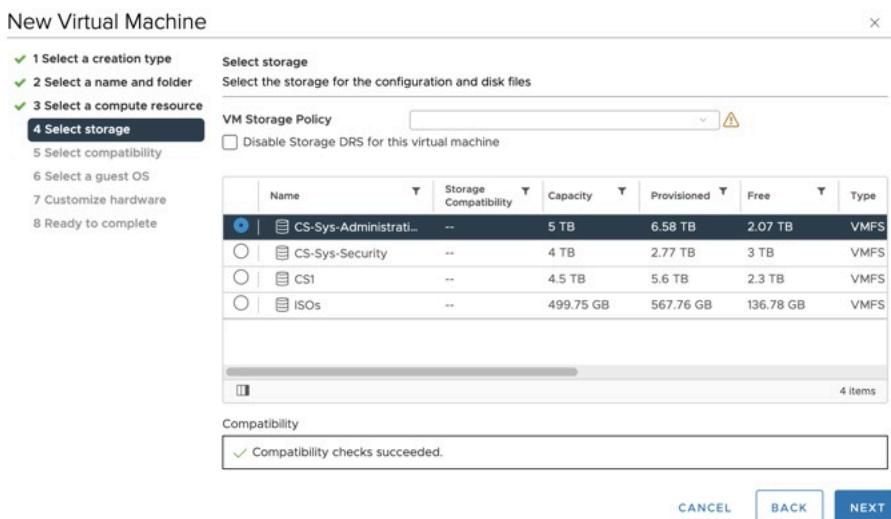


3.

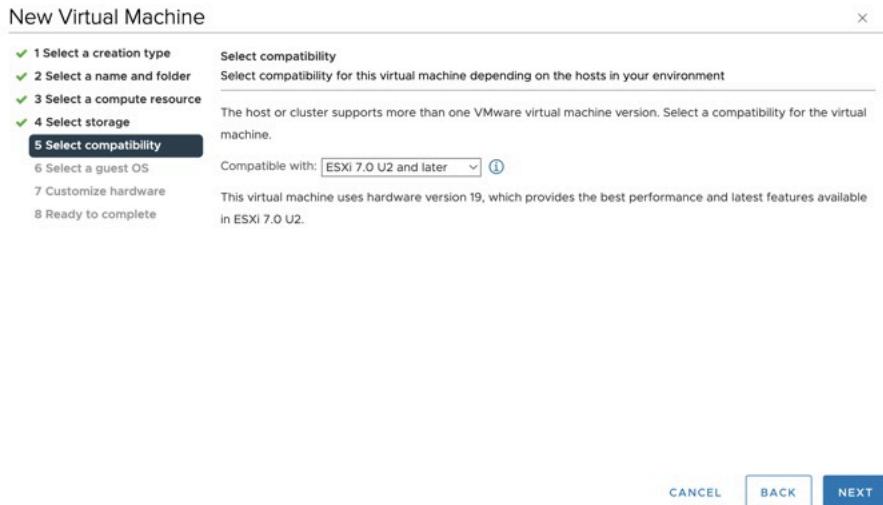
- Select your Virtual Folder, name your virtual machine, and hit "NEXT"



- 4.
- Select "CS Cluster" and hit "NEXT"

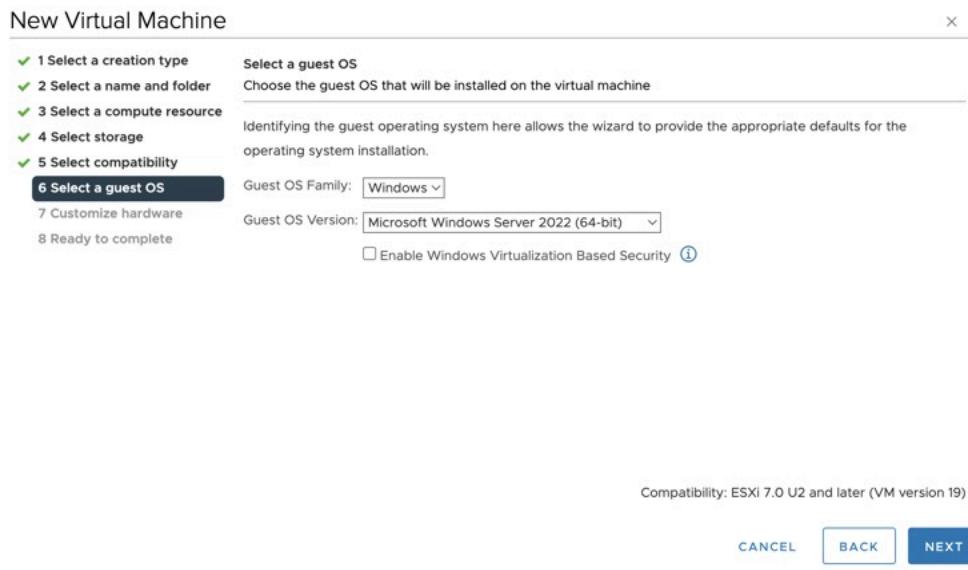


- 5.
- Select "CS-Sys-Administration" for storage and hit "NEXT"



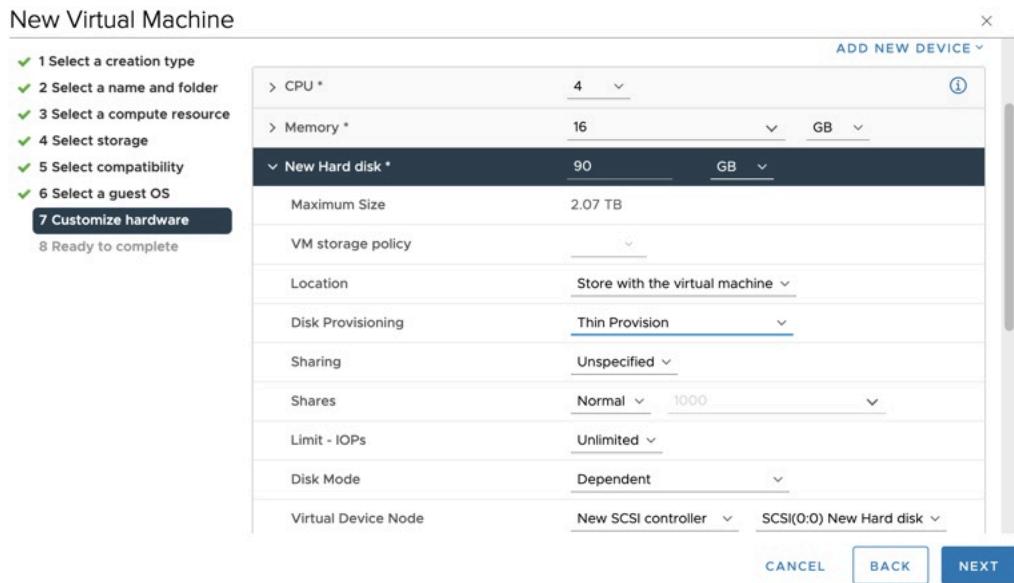
6.

- Leave as is and hit “NEXT”



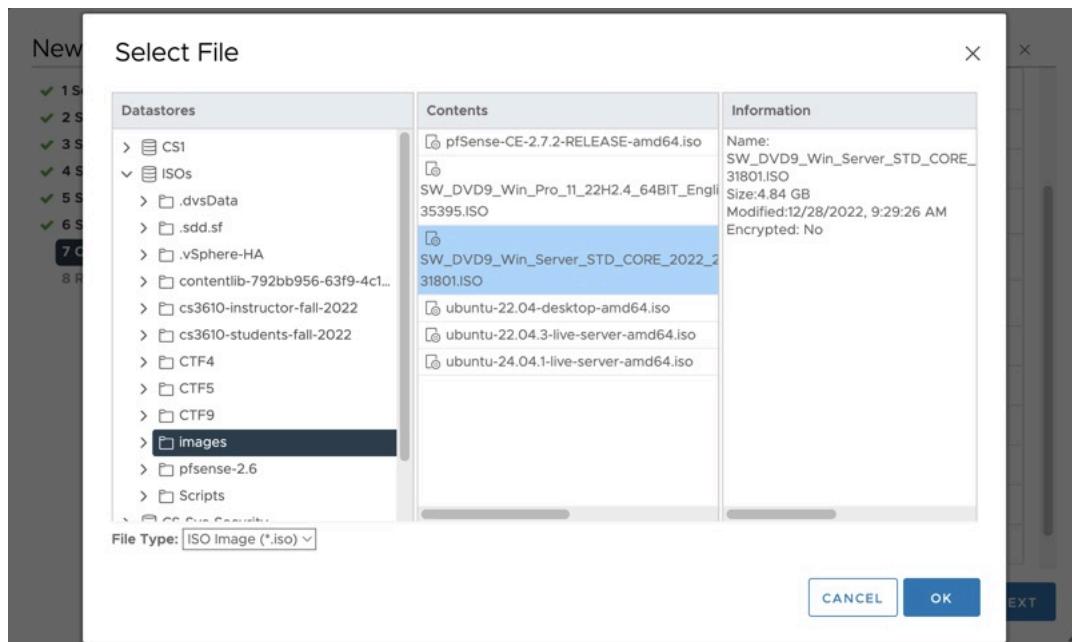
7.

- Select “Microsoft Windows Server 2022 (64-bit)” for Guest OS Version and hit “NEXT”



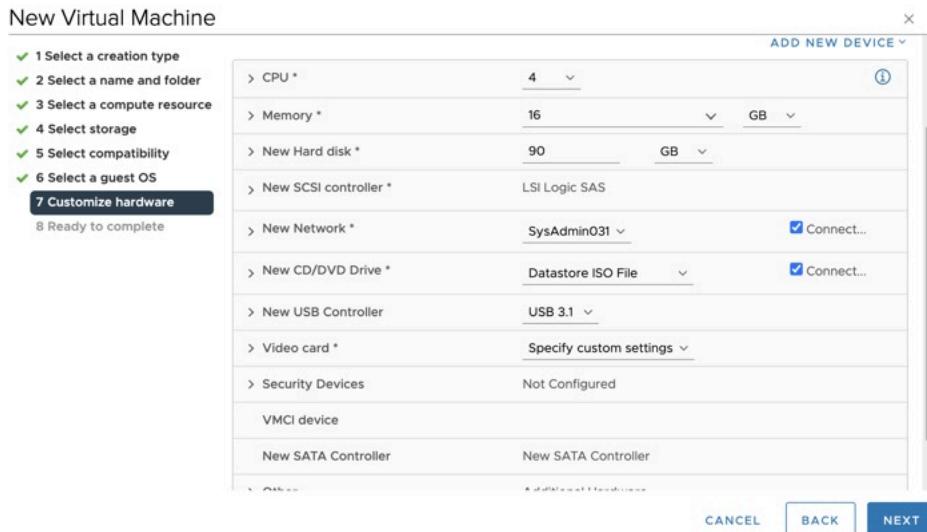
8.

- Set CPU to "4"
- Set Memory to "16 GB"
- Set Disk Provisioning to "Thin Provision"



9.

- Select "Datastore ISO File" for New CD/DVD Drive
- Select ISOs -> images -> "SW\_DVD9\_Win\_Server..." then hit "OK"



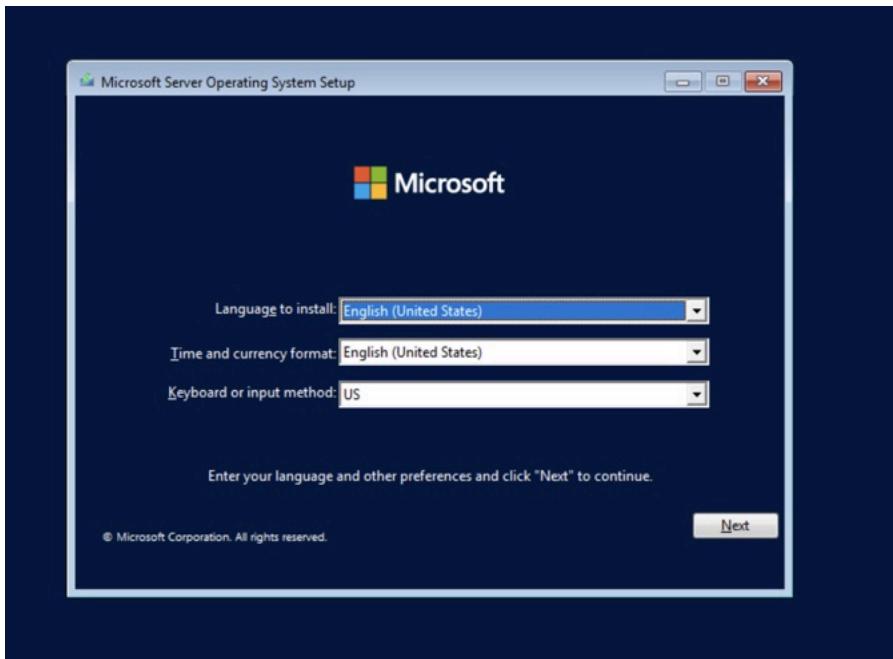
10.

- Make sure to Connect the new Datastore ISO File and hit “NEXT”

| New Virtual Machine           |                                        |
|-------------------------------|----------------------------------------|
| <b>8 Ready to complete</b>    |                                        |
| Virtual machine name          | Windows Server                         |
| Folder                        | SysAdmin031                            |
| Cluster                       | CS Cluster                             |
| Datastore                     | CS-Sys-Administration                  |
| Guest OS name                 | Microsoft Windows Server 2022 (64-bit) |
| Virtualization Based Security | Disabled                               |
| CPUs                          | 4                                      |
| Memory                        | 16 GB                                  |
| NICs                          | 1                                      |
| NIC 1 network                 | SysAdmin031 (CS - Distributed)         |
| NIC 1 type                    | E1000E                                 |
| SCSI controller 1             | LSI Logic SAS                          |

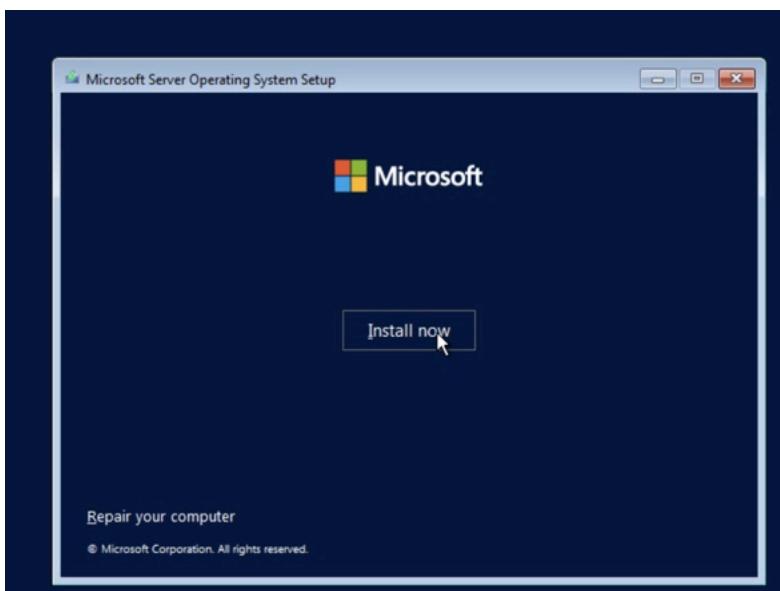
11.

- Review, make sure everything looks right, and hit “FINISH”
- Start your virtual machine
- Let your system boot up and restart. After some patience, the Windows OS setup will show up.



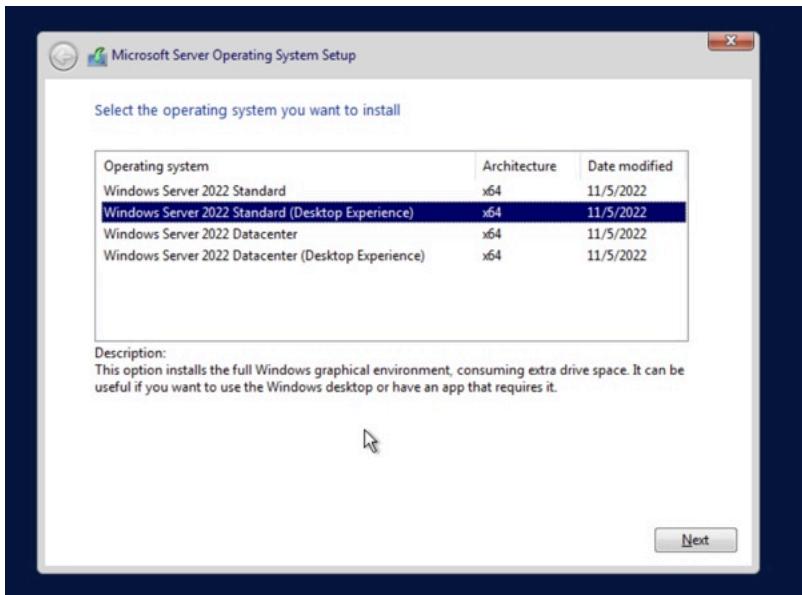
12.

- Select your language



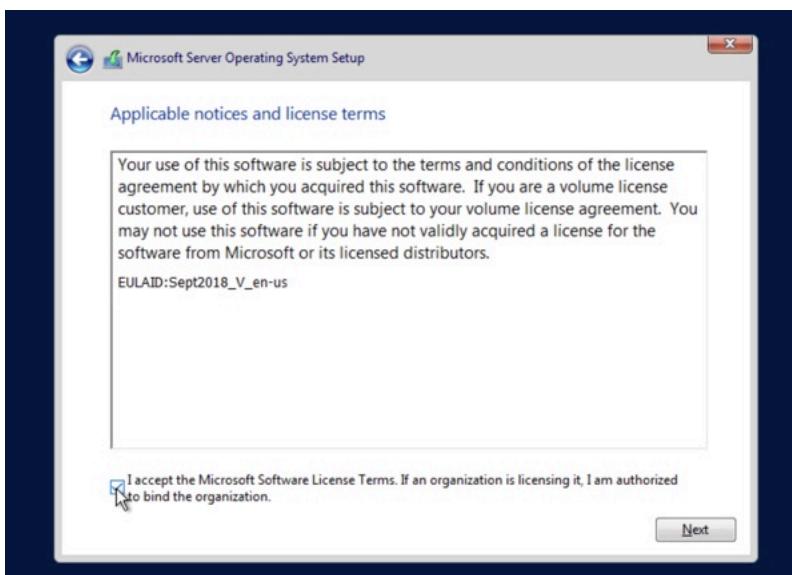
13.

- Click "Install now"



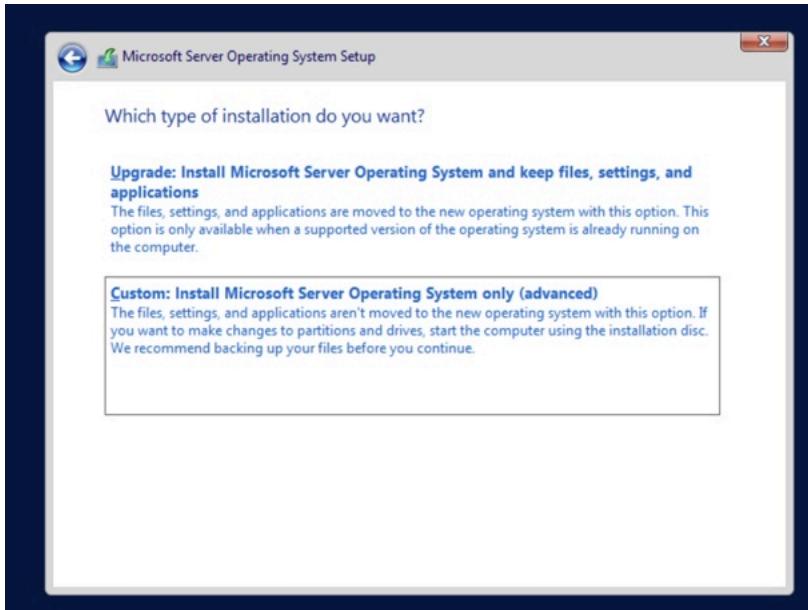
14.

- Select "Windows Server 2022 Standard (Desktop Experience)"



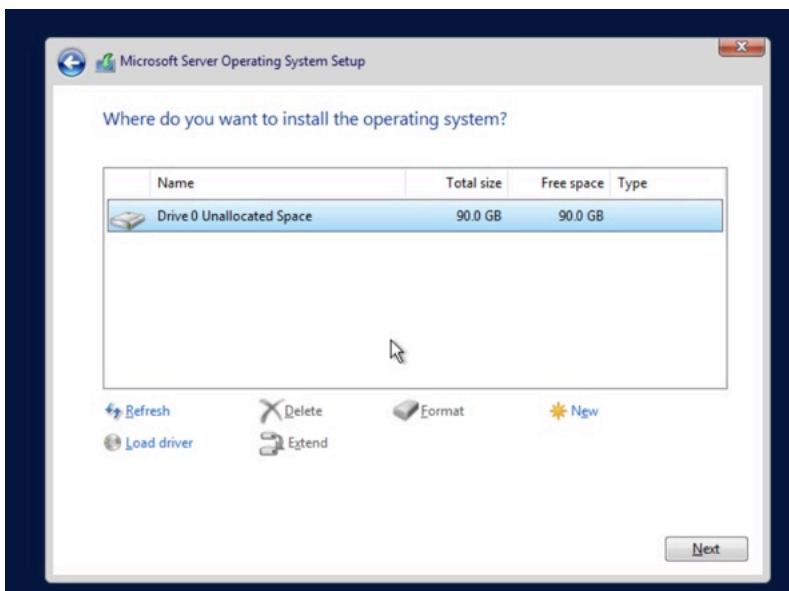
15.

- Accept Terms and Conditions



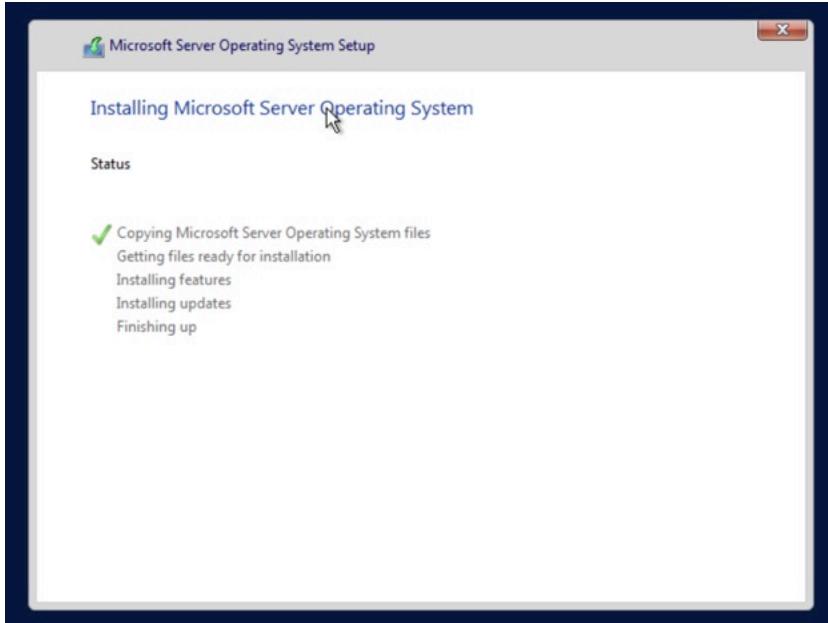
16.

- Select Custom install



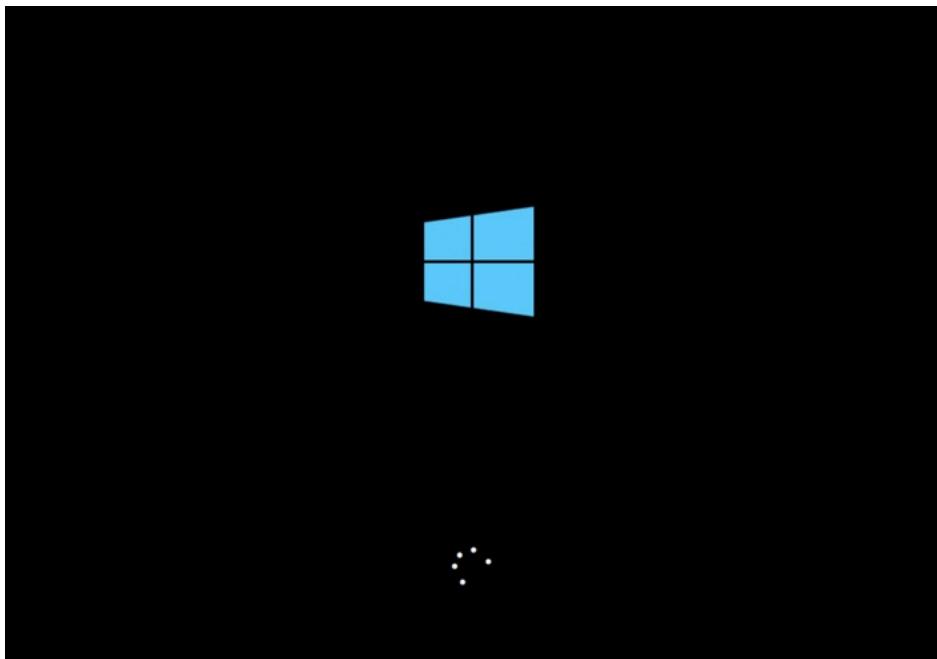
17.

- Select your drive and install



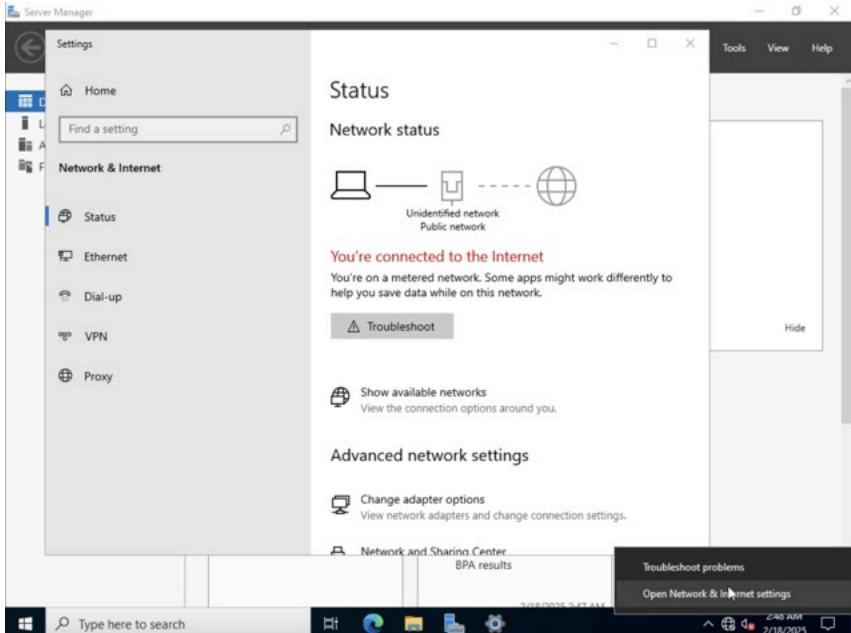
18.

- This is how it should look while installing



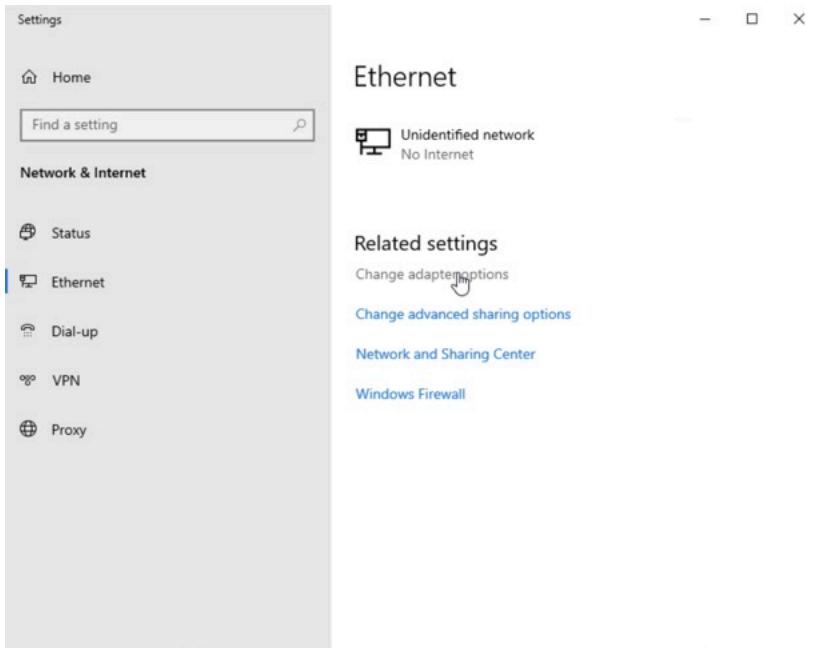
19.

- After installing, wait for Windows the boot up
- Set your Administrator password (Gummibear020128) and log in



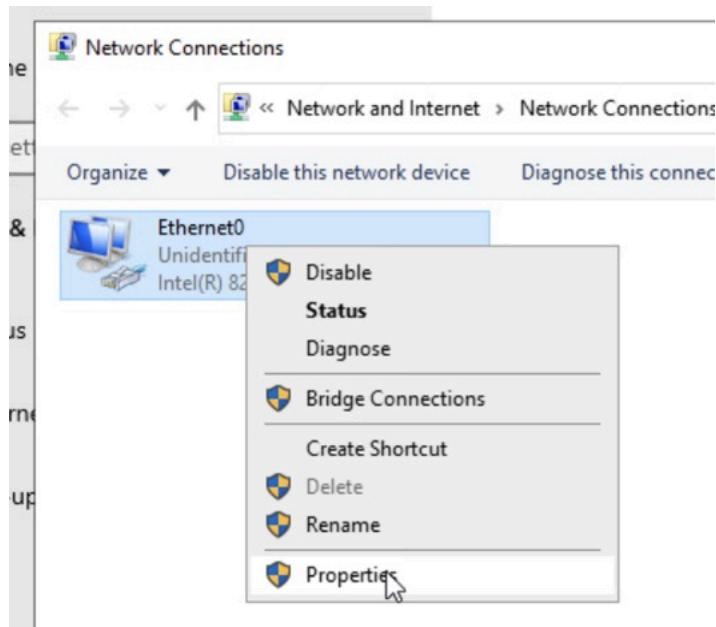
20.

- After logging in, right click on the network icon and select “Open Network & Internet settings”



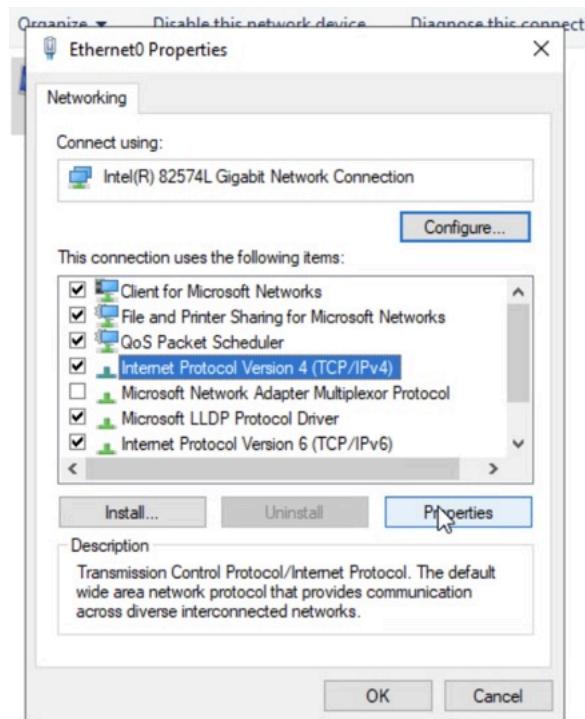
21.

- Select “Ethernet” on the side and click on “Change adapter options”



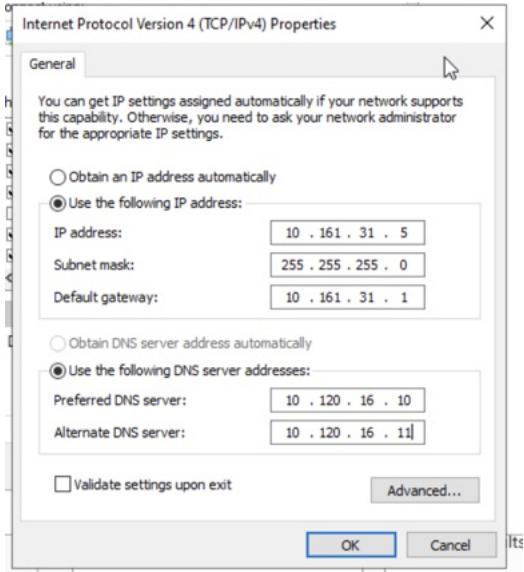
22.

- Right click on "Ethernet0" and select "Properties"



23.

- Select "Internet Protocol Version 4 (TCP/IPv4)" and hit "Properties"



24.

- Select “Use the following IP address” and fill in correct information for IP address, subnet mask, and default gateway according to your virtual folder number
- Select “Use the following DNS server addresses” and fill in with UNI DNS server address.

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

I learned how to download a Windows OS without being initially connected to the internet. I also learned how to connect to the internet manually in virtual machines by configuring the ethernet properties. Although the project went smoothly, I was surprised to learn about ethernet properties and how to manually connect a virtual machine to the internet through them.

---

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

- Windows Task Scheduler - [https://en.wikipedia.org/wiki/Windows\\_Task\\_Scheduler](https://en.wikipedia.org/wiki/Windows_Task_Scheduler)
- Installed Programs - <https://www.makeuseof.com/tag/list-installed-programs-windows/>
- Event Viewer - [https://en.wikipedia.org/wiki/Event\\_Viewer](https://en.wikipedia.org/wiki/Event_Viewer)
- Windows Services - <https://www.thewindowsclub.com/open-windows-services>
- Windows Server 2022 Server Manager Documentation: <https://learn.microsoft.com/en-us/windows-server/administration/server-manager/server-manager#tasks-that-you-can-perform-in-server-manager>

# Project 3: Network Setup

---

**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

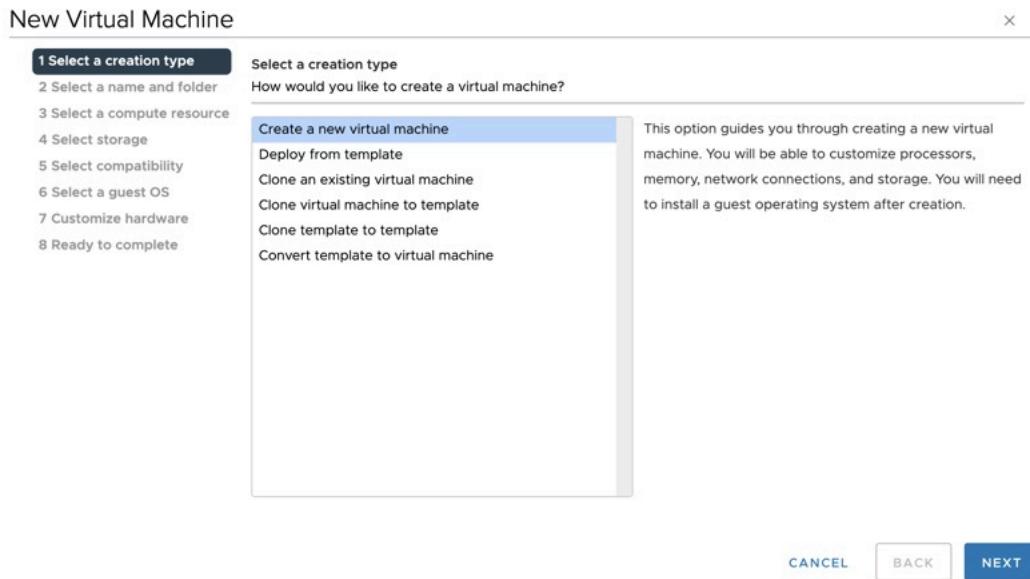
In this project, I will configure a secure network using pfSense with WAN, LAN, and DMZ segmentation, ensuring proper firewall rules and DHCP settings. LAN devices will use DHCP, while DMZ servers will have static IPs, and proper DNS settings must be configured. Testing with ping will help confirm connectivity between the network zones. I expect setting up pfSense and assigning network interfaces to be straightforward, but I feel like I might run into some unexpected network behavior that will require some troubleshooting.

---

**Project Answers:** This is where questions should be answered in the project directly asks a question. Else Delete this section.

---

**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



- Create a new virtual machine and hit "NEXT"

## New Virtual Machine

X

✓ 1 Select a creation type

**2 Select a name and folder**

3 Select a compute resource

4 Select storage

5 Select compatibility

6 Select a guest OS

7 Customize hardware

8 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

pfSense

Select a location for the virtual machine.

✓  serenity.cs.uni.edu  
  ▼  CS Datacenter  
    >  SysAdmin011  
    >  SysAdmin031

CANCEL

BACK

NEXT

- Name your virtual machine and select the correct location "SysAdmin31"

## New Virtual Machine

X

✓ 1 Select a creation type

✓ 2 Select a name and folder

**3 Select a compute resource**

4 Select storage

5 Select compatibility

6 Select a guest OS

7 Customize hardware

8 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

✓  CS Datacenter  
  >  CS Cluster

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

- Select "CS Cluster" for compute resource and hit "NEXT"

## New Virtual Machine

X

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Select storage

Select the storage for the configuration and disk files

#### VM Storage Policy



Disable Storage DRS for this virtual machine

| Name                     | Storage Compatibility | Capacity  | Provisioned | Free      | Type   |
|--------------------------|-----------------------|-----------|-------------|-----------|--------|
| CS-Sys-Administration... | --                    | 5 TB      | 8.9 TB      | 837.02 GB | VMFS 6 |
| CS-Sys-Security          | --                    | 4 TB      | 4.89 TB     | 2.09 TB   | VMFS 6 |
| CS1                      | --                    | 4.5 TB    | 5.57 TB     | 2.08 TB   | VMFS 5 |
| ISOs                     | --                    | 499.75 GB | 567.76 GB   | 136.78 GB | VMFS 6 |
| 4 items                  |                       |           |             |           |        |

#### Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

- Select “CS-Sys-Administration” for the storage and hit “NEXT”

## New Virtual Machine

X

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- 5 Select compatibility**
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Select compatibility

Select compatibility for this virtual machine depending on the hosts in your environment

The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with:  ⓘ

This virtual machine uses hardware version 19, which provides the best performance and latest features available in ESXi 7.0 U2.

CANCEL

BACK

NEXT

- The default option “ESXi 7.0 U2 and later” is fine, hit “NEXT”

## New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- 6 Select a guest OS**

7 Customize hardware  
8 Ready to complete

Select a guest OS  
Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: Other

Guest OS Version: FreeBSD 13 or later versions (64-bit)

Compatibility: ESXi 7.0 U2 and later (VM version 19)

CANCEL

BACK

NEXT

- Select “Other” for Guest OS Family and “FreeBSD 13 or later versions (64-bit)” for Guest OS Version.

|                     |                                  |                         |      |
|---------------------|----------------------------------|-------------------------|------|
| > CPU *             | 2                                | ▼                       | (i)  |
| > Memory *          | 8                                | ▼                       | GB ▼ |
| ▼ New Hard disk *   | 30                               | GB                      | ▼    |
| Maximum Size        | 837.02 GB                        |                         |      |
| VM storage policy   | ▼                                |                         |      |
| Location            | Store with the virtual machine ▼ |                         |      |
| Disk Provisioning   | Thin Provision ▼                 |                         |      |
| Sharing             | Unspecified ▼                    |                         |      |
| Shares              | Normal                           | 1000                    | ▼    |
| Limit - IOPs        | Unlimited ▼                      |                         |      |
| Disk Mode           | Dependent ▼                      |                         |      |
| Virtual Device Node | New SCSI controller              | SCSI(0:0) New Hard disk | ▼    |

CANCEL

BACK

NEXT

- Set CPU to “2”, set Memory to “8 GB”, set Hard disk to “30 GB”, set Disk Provisioning to “Thin Provision”

## New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- 7 Customize hardware**

8 Ready to complete

| ADD NEW DEVICE ▾        |                         |                                                  |
|-------------------------|-------------------------|--------------------------------------------------|
| > CPU *                 | 2                       | ⓘ                                                |
| > Memory *              | 8                       | GB                                               |
| > New Hard disk *       | 30                      | GB                                               |
| > New SCSI controller * | VMware Paravirtual      |                                                  |
| > New Network *         | SysAdmin031             | ⓘ <input checked="" type="checkbox"/> Connect... |
| > New CD/DVD Drive *    | Client Device           | ⓘ <input type="checkbox"/> Connect...            |
| > Video card *          | Specify custom settings |                                                  |
| > Security Devices      | Not Configured          |                                                  |
| VMCI device             |                         |                                                  |
| > Other                 | Additional Hardware     |                                                  |

CANCEL

BACK

NEXT

- Make sure your network is set to your folder (SysAdmin031)

## New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- 7 Customize hardware**

8 Ready to complete

|                         |                         |                                                  |
|-------------------------|-------------------------|--------------------------------------------------|
| > Memory *              | 8                       | GB                                               |
| > New Hard disk *       | 30                      | GB                                               |
| > New SCSI controller * | VMware Paravirtual      |                                                  |
| > New Network *         | SysAdmin031             | ⓘ <input checked="" type="checkbox"/> Connect... |
| > New Network *         | SysAdmin031             | ⓘ <input checked="" type="checkbox"/> Connect... |
| > New Network *         | SysAdmin031             | ⓘ <input checked="" type="checkbox"/> Connect... |
| > New CD/DVD Drive *    | Client Device           | ⓘ <input type="checkbox"/> Connect...            |
| > Video card *          | Specify custom settings |                                                  |
| > Security Devices      | Not Configured          |                                                  |
| VMCI device             |                         |                                                  |
| > Other                 | Additional Hardware     |                                                  |

CANCEL

BACK

NEXT

- Add 2 more networks by clicking "Add New Device" on the top right

## Select File

X

The screenshot shows a 'Select File' dialog box with three main sections: Datastores, Contents, and Information.

- Datastores:** A tree view showing various datastores including CS1, ISOs, and images.
- Contents:** A list of ISO files available in the selected datastore:
  - pfSense-CE-2.7.2-RELEASE-amd64.iso
  - SW\_DVD9\_Win\_Pro\_11\_22H2.4\_64BIT\_English35395.ISO
  - SW\_DVD9\_Win\_Server\_STD\_CORE\_2022\_231801.ISO
  - ubuntu-22.04-desktop-amd64.iso
  - ubuntu-22.04.3-live-server-amd64.iso
  - ubuntu-24.04.1-live-server-amd64.iso
- Information:** Details about the selected file (pfSense-CE-2.7.2-RELEASE-amd64.iso):
  - Name: pfSense-CE-2.7.2-RELEASE-amd64.iso
  - Size: 834.15 MB
  - Modified: 01/12/2024, 3:22:32 PM
  - Encrypted: No

File Type: ISO Image (\*.iso) ▾

CANCEL OK

- For CD/DVD Drive, select “Datastore ISO File” and follow this file path: ISOs > images > pfSense-CE-2.7.2-RELEASE-amd64.iso

## New Virtual Machine

X

The screenshot shows the 'New Virtual Machine' configuration screen with the following steps completed:

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware** (highlighted)
- 8 Ready to complete

The 'Customize hardware' section contains the following settings:

| Setting               | Value                   | Options                                        |
|-----------------------|-------------------------|------------------------------------------------|
| CPU *                 | 2                       | ▼ ⓘ                                            |
| Memory *              | 8                       | GB ▼                                           |
| New Hard disk *       | 30                      | GB ▼                                           |
| New SCSI controller * | VMware Paravirtual      |                                                |
| New Network *         | SysAdmin031             | Connect... <input checked="" type="checkbox"/> |
| New Network *         | SysAdmin031             | Connect... <input checked="" type="checkbox"/> |
| New Network *         | SysAdmin031             | Connect... <input checked="" type="checkbox"/> |
| New CD/DVD Drive *    | Datastore ISO File      | Connect... <input checked="" type="checkbox"/> |
| Video card *          | Specify custom settings |                                                |
| Security Devices      | Not Configured          |                                                |
| VMCI device           |                         |                                                |
| Other                 | Additional Hardware     |                                                |

CANCEL BACK NEXT

- Make sure to connect the Datastore ISO File, hit “NEXT”

## New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- ✓ 7 Customize hardware
- 8 Ready to complete**

|                               |                                       |
|-------------------------------|---------------------------------------|
| Virtual machine name          | pfSense                               |
| Folder                        | SysAdmin031                           |
| Cluster                       | CS Cluster                            |
| Datastore                     | CS-Sys-Administration                 |
| Guest OS name                 | FreeBSD 13 or later versions (64-bit) |
| Virtualization Based Security | Disabled                              |
| CPUs                          | 2                                     |
| Memory                        | 8 GB                                  |
| NICs                          | 3                                     |
| NIC 1 network                 | SysAdmin031 (CS - Distributed)        |
| NIC 1 type                    | VMXNET 3                              |
| NIC 2 network                 | SysAdmin031 (CS - Distributed)        |

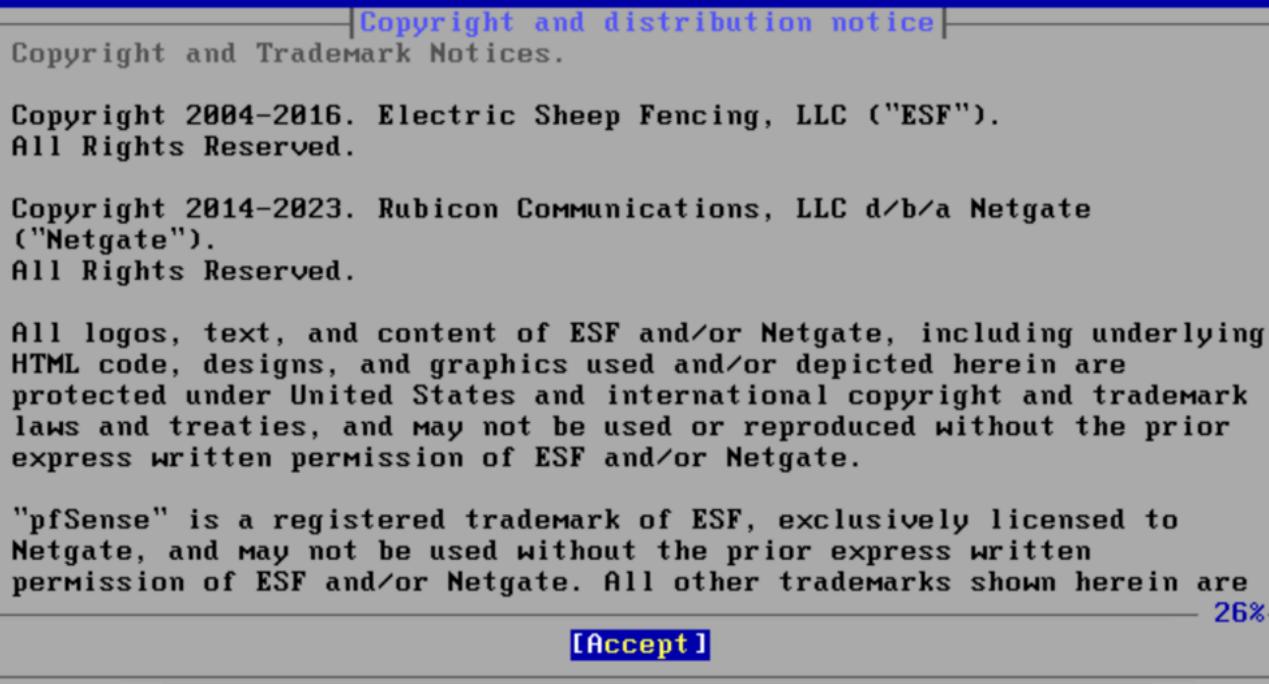
CANCEL

BACK

FINISH

- Make sure filled in information is correct and hit "FINISH"

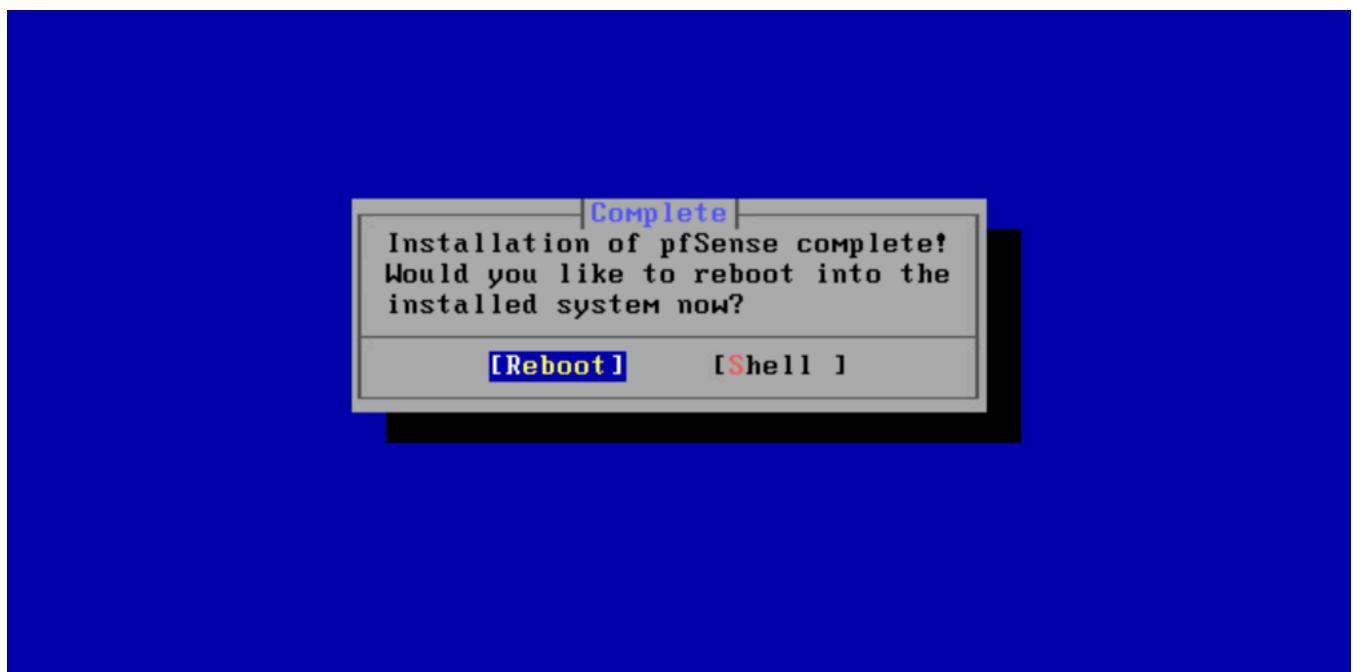
## pfSense Installer



- Once you boot up your virtual machine, this is what you will see.



- Hit the ENTER key until you get to this screen. Hit the SPACE to select VMware Virtual disk and hit ENTER to select "OK"



- Once all settings are selected, hit "Reboot"

```
Updating configuration....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
vmx0: link state changed to UP
vmx1: link state changed to UP
vmx2: link state changed to UP

Valid interfaces are:

vmx0      00:50:56:82:ce:2b (down) VMware VMXNET3 Ethernet Adapter
vmx1      00:50:56:82:7d:36 (down) VMware VMXNET3 Ethernet Adapter
vmx2      00:50:56:82:65:2d (down) VMware VMXNET3 Ethernet Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? 2025-03-24T01:31:35.996658+00:00 - php-fpm 394
-- /rc.linkup: Ignoring link event during boot sequence.
2025-03-24T01:31:36.000926+00:00 - php-fpm 393 -- /rc.linkup: Ignoring link eve
nt during boot sequence.
2025-03-24T01:31:36.001016+00:00 - php-fpm 394 -- /rc.linkup: Ignoring link eve
nt during boot sequence.
n
```

- Once you boot up, you will see a screen like this.

```
2025-03-24T01:31:36.001016+00:00 - php-fpm 394 -- /rc.linkup: Ignoring link eve
nt during boot sequence.
n
```

If the names of the interfaces are not known, auto-detection can  
be used instead. To use auto-detection, please disconnect all  
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection  
(vmx0 vmx1 vmx2 or a): vmx0

Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(vmx1 vmx2 a or nothing if finished): vmx1

Enter the Optional 1 interface name or 'a' for auto-detection  
(vmx2 a or nothing if finished): vmx2

The interfaces will be assigned as follows:

WAN -> vmx0  
LAN -> vmx1  
OPT1 -> vmx2

```
Do you want to proceed [y\?n]? ■
```

- It will ask you to enter WAN, LAN, and OPT1 interface names. Match vmx0 to WAN, vmx1 to LAN, and vmx2 to OPT1

```
The IPv4 OPT1 address has been set to 192.168.2.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.2.1/
```

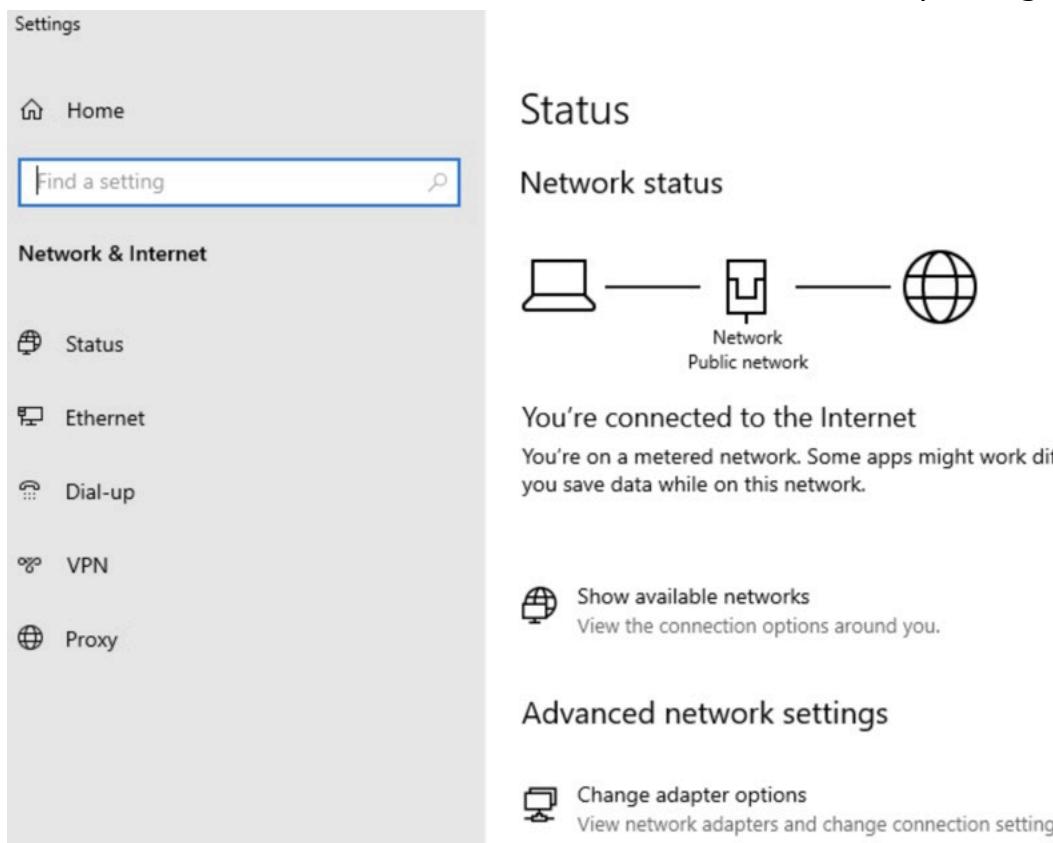
```
Press <ENTER> to continue. VMware Virtual Machine - Netgate Device ID: 790fabca3b
79e1232de8
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
```

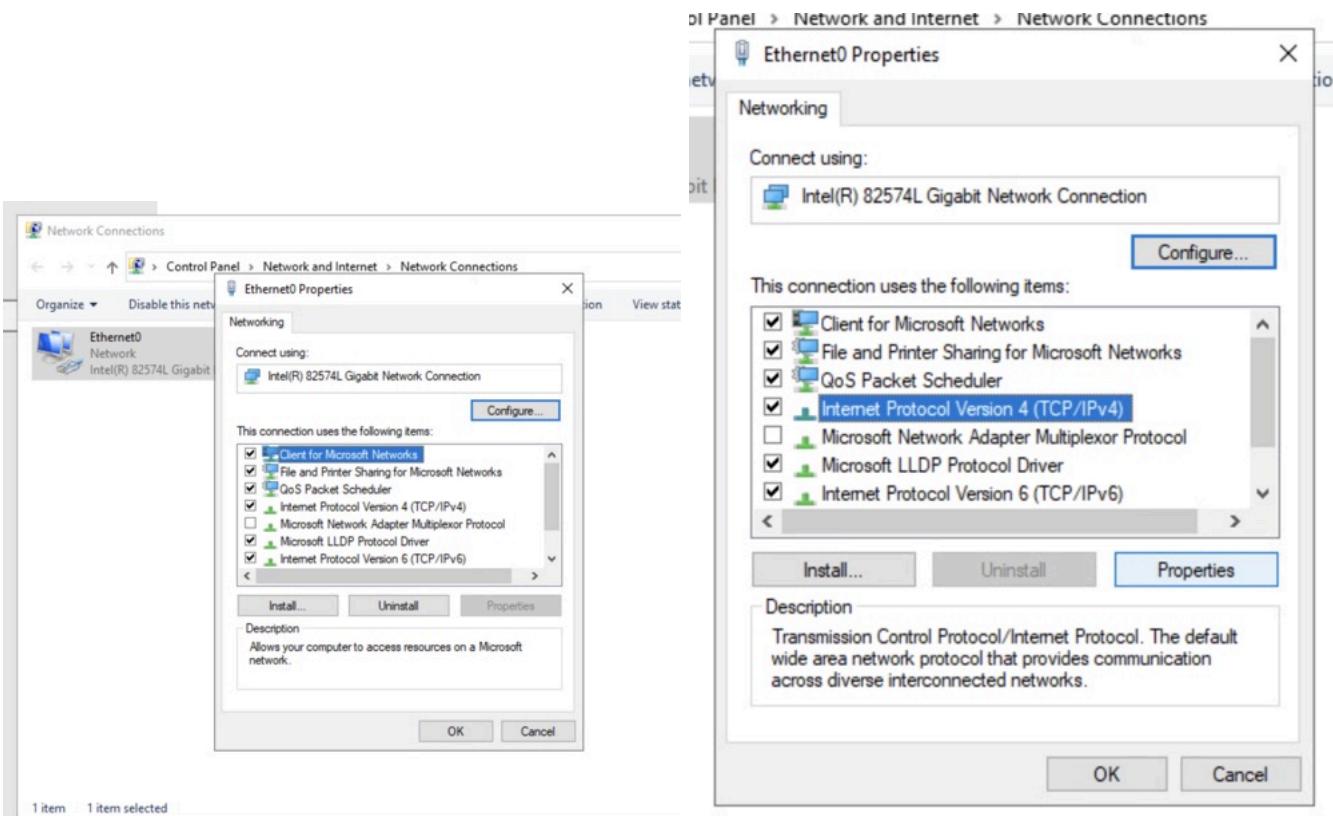
```
WAN (wan)      -> vmx0      -> v4: 10.161.31.4/24
LAN (lan)      -> vmx1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> vmx2      -> v4: 192.168.2.1/24
```

- |                                   |                                  |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only)              | 9) pfTop                         |
| 1) Assign Interfaces              | 10) Filter Logs                  |
| 2) Set interface(s) IP address    | 11) Restart webConfigurator      |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools    |
| 4) Reset to factory defaults      | 13) Update from console          |
| 5) Reboot system                  | 14) Enable Secure Shell (sshd)   |
| 6) Halt system                    | 15) Restore recent configuration |
| 7) Ping host                      | 16) Restart PHP-FPM              |
| 8) Shell                          |                                  |

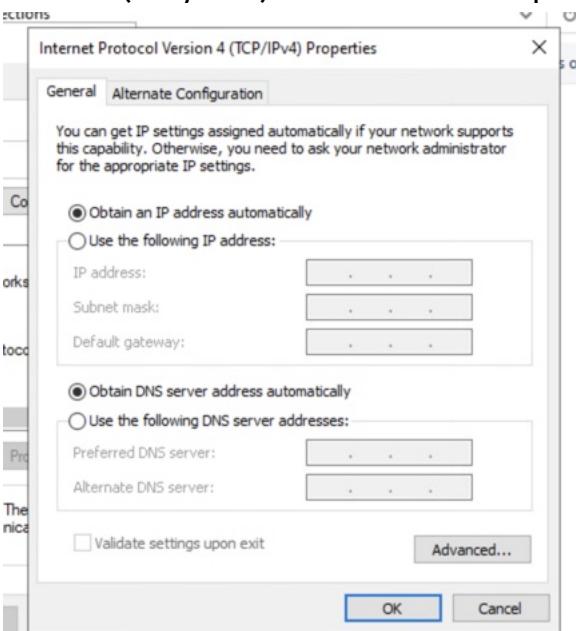
- You will be taken to a screen like this. Select “2) Set interfaces IP address” for WAN, LAN, and OPT1 and enter the correct IP addresses corresponding to project 3A.



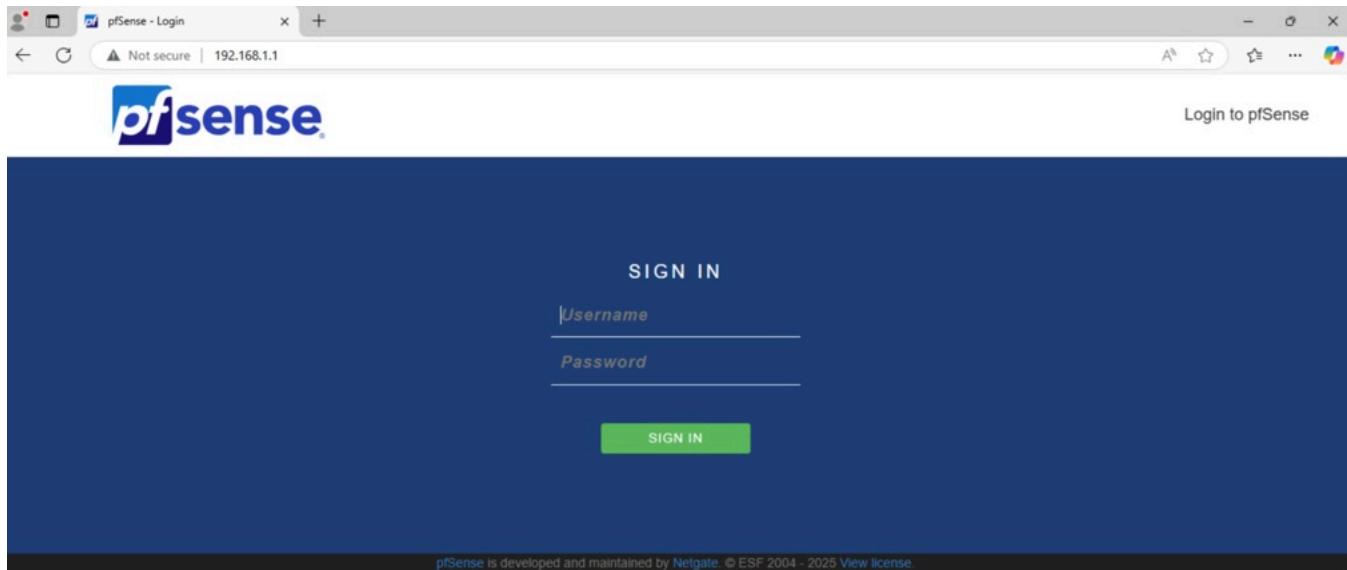
- Once that is done, open your Windows server, right click the network on the bottom right to open network settings. Select “Change adaptor options”.



- Right click on “Ethernet0” and click on “Properties”. Select “Internet Protocol Version 4 (TCP/IPv4)” and click on “Properties”.



- Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Hit “OK”.



- Type in your IP address into a browser to open pfSense. Sign in with username: admin and password: pfsense.

The default behavior of the DNS Resolver will ignore manually configured DNS servers manually configured DNS servers below for client queries, visit Services > DNS Resolv

**Primary DNS Server** 10.120.16.10

**Secondary DNS Server** 10.120.16.11

**Override DNS**

Allow DNS servers to be overridden by DHCP/PPP on WAN

- After signing in, hit "NEXT" until you see DNS Servers. Put 10.120.16.10 for Primary and 10.120.16.11 for secondary.

### Static IP Configuration

**IP Address** 10.161.31.4

**Subnet Mask** 24

**Upstream Gateway** 10.161.31.1

- Put in your WAN gateway IP address into Upstream Gateway.

**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). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

**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. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

- Make sure to uncheck the two boxes at the bottom. Hit “Next”.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: .....  
Admin Password AGAIN: .....

» Next

- Set a new Admin password: Gummybear020128

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

**Wizard completed.**

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.  
[Click here](#) to learn about Netgate 24/7/365 support services.

**User survey**  
Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)  
[Anonymous User Survey](#)

**Useful resources.**

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, visit our [store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

- Once you hit this page, hit “Finish”.

The screenshot shows the pfSense web interface with the "Services" menu selected. The menu items listed are:

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server**
- DHCPv6 Relay
- DHCPv6 Server
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy

- Click on the “Services” drop down menu at the top, click on “DHCP Server”.

**Primary Address Pool**

|                                                                                                                           |                               |
|---------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Subnet                                                                                                                    | 192.168.1.0/24                |
| Subnet Range                                                                                                              | 192.168.1.1 - 192.168.1.254   |
| Address Pool Range                                                                                                        | 192.168.1.101 - 192.168.1.254 |
| From To                                                                                                                   |                               |
| The specified range for this pool must not be within the range configured on any other address pool for this interface.   |                               |
| Additional Pools                                                                                                          | <b>+ Add Address Pool</b>     |
| If additional pools of addresses are needed inside of this subnet outside of the above range, they may be specified here. |                               |

- Make sure Address Pool Range is “192.168.1.101 - 192.168.1.254”

**Server Options**

|                     |               |
|---------------------|---------------|
| <b>WINS Servers</b> | WINS Server 1 |
|                     | WINS Server 2 |
| <b>DNS Servers</b>  | 10.120.16.10  |
|                     | 10.120.16.11  |

- Make sure DNS Servers have both primary and secondary addresses

|                     |  |
|---------------------|--|
| NTP                 |  |
| TFTP                |  |
| LDAP                |  |
| Network Booting     |  |
| Custom DHCP Options |  |
|                     |  |

Services / DHCP Server / LAN

The DHCP Server configuration has changed.  
The changes must be applied for them to take effect.

- Make sure to click on the "Save" button at the bottom and then click "Apply Changes"!

Control Panel > Network and Internet

Ethernet0  
Network 2  
Intel(R) 82574L Gigabit Network C...

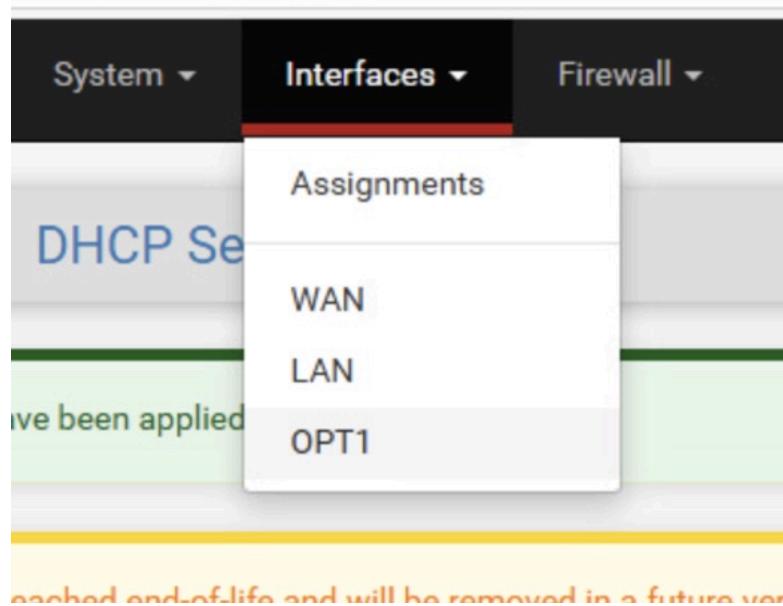
Organize ▾      Disable this network device      Diagnose this co

Organize ▾      Enable this network device      Diagnose thi

Ethernet0  
Disabled  
Intel(R) 82574L Gigabit Network C...

- Go back to Ethernet0, click on "Disable this network device" and click it again to enable it. Now you should be connected to the internet.

68.1.1/services\_dhcp.php



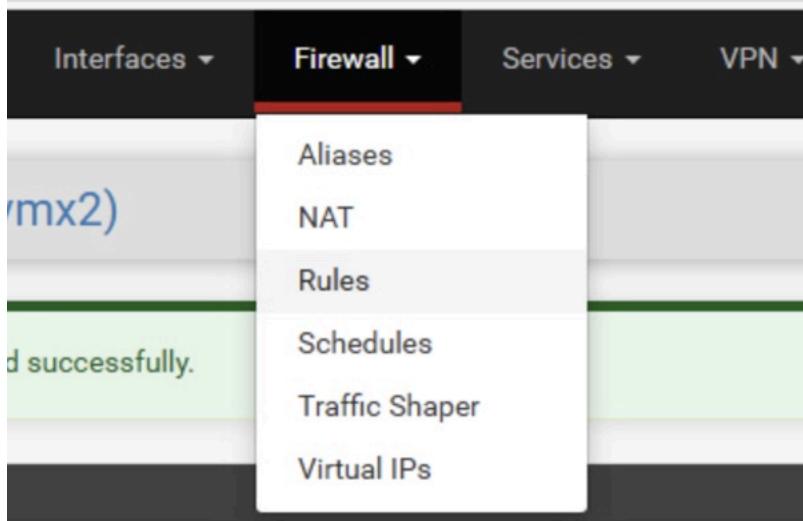
- Click on the "Interfaces" drop down menu and click on "OPT1".

A screenshot of the 'General Configuration' page for the 'OPT1' interface. The title bar says 'General Configuration'. There are two main sections: 'Enable' and 'Description'. Under 'Enable', there is a checkbox labeled 'Enable interface' which is checked. Under 'Description', there is a text input field containing the value 'DMZ'. Below the input field is a placeholder text: 'Enter a description (name) for the interface here.'

| General Configuration |                                                           |
|-----------------------|-----------------------------------------------------------|
| Enable                | <input checked="" type="checkbox"/> Enable interface      |
| Description           | DMZ<br>Enter a description (name) for the interface here. |

- Change the name to "DMZ" for clarity.

s.php?if=opt1



## 2 Enable interface

- Click on the “Firewall” drop down menu and select “Rules”.

A screenshot of the 'Rules' configuration page for the 'DMZ' interface. The top navigation bar shows tabs for Floating, WAN, LAN, and DMZ, with 'DMZ' selected. Below the tabs is a header row with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A message box states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom are several action buttons: Add (green), Add (blue), Delete (red), Toggle (grey), Copy (light blue), Save (blue), and Separator (orange).

- Go to the “DMZ” tab and click on “Add”.

A screenshot of the 'Protocol' configuration section. It shows a dropdown menu with 'Any' selected. Below the dropdown is a descriptive text: "Choose which IP protocol this rule should match." There is also a 'Source' section at the bottom.

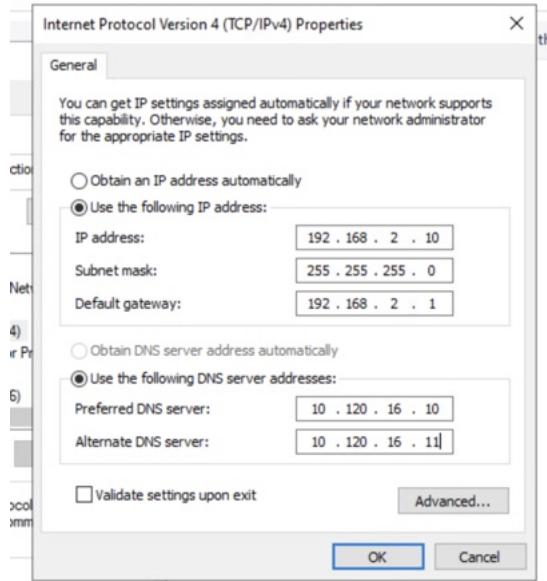
- Make sure Protocol is selected to “Any”.

(use Status, System Logs, Settings page).

|                                                                                                 |                                  |
|-------------------------------------------------------------------------------------------------|----------------------------------|
| Description                                                                                     | ALLOW ALL                        |
| A description may be entered here for administrative reference. A maximum of 52 characters log. |                                  |
| Advanced Options                                                                                | <a href="#">Display Advanced</a> |
| <a href="#">Save</a>                                                                            |                                  |

- Add a description that gives a simple explanation of the rule.

work and Internet > Network Connections



- Go back to ethernet0 > internet protocols > properties. Put in the correct IP addresses corresponding to your Lucid Chart created in Project 3A. This will connect you to the internet.

Firewall / Rules / WAN

Floating   WAN   LAN   DMZ

Rules (Drag to Change Order)

| #                        | States  | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description                          | Actions                                                                               |
|--------------------------|---------|----------|--------|------|-------------|------|---------|-------|----------|--------------------------------------|---------------------------------------------------------------------------------------|
| <input type="checkbox"/> | X 0/0 B | IPv4 TCP | *      | *    | DMZ subnets | *    | *       | none  |          | Block inbound WAN to DMZ traffic     | <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a> |
| <input type="checkbox"/> | X 0/0 B | IPv4 *   | *      | *    | LAN subnets | *    | *       | none  |          | Do not allow traffic from WAN to LAN | <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a> |

[Add](#) [Up](#) [Down](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Firewall / Rules / LAN

Floating WireGuard WAN **LAN** DMZ VPN

**Rules (Drag to Change Order)**

|                                     | States         | Protocol      | Source      | Port | Destination | Port        | Gateway | Queue | Schedule | Description                       | Actions |
|-------------------------------------|----------------|---------------|-------------|------|-------------|-------------|---------|-------|----------|-----------------------------------|---------|
| <input checked="" type="checkbox"/> | 0/4.93 MiB     | *             | *           | *    | LAN Address | 80          | *       | *     |          | Anti-Lockout Rule                 |         |
| <input type="checkbox"/>            | ✓ 0/106.39 MiB | IPv4 *        | LAN subnets | *    | DMZ subnets | *           | *       | none  |          | Allow all traffic from LAN to DMZ |         |
| <input type="checkbox"/>            | ✓ 0/437 KiB    | IPv4 ICMP any | LAN subnets | *    | *           | *           | *       | none  |          | Allow LAN to WAN (Ping)           |         |
| <input type="checkbox"/>            | ✓ 0/10.04 MiB  | IPv4 TCP/UDP  | LAN subnets | *    | *           | 53 (DNS)    | *       | none  |          | Allow LAN to WAN (DNS)            |         |
| <input type="checkbox"/>            | ✓ 0/0 B        | IPv4 TCP      | LAN subnets | *    | DMZ subnets | 80 (HTTP)   | *       | none  |          |                                   |         |
| <input type="checkbox"/>            | ✓ 0/0 B        | IPv4 TCP      | LAN subnets | *    | DMZ subnets | 443 (HTTPS) | *       | none  |          |                                   |         |

[Go to Settings to edit](#)

Firewall / Rules / DMZ

Floating WAN **LAN** DMZ

**Rules (Drag to Change Order)**

|                          | States      | Protocol | Source      | Port | Destination | Port | Gateway | Queue | Schedule | Description                                | Actions |
|--------------------------|-------------|----------|-------------|------|-------------|------|---------|-------|----------|--------------------------------------------|---------|
| <input type="checkbox"/> | ✗ 0/0 B     | IPv4 *   | DMZ subnets | *    | LAN subnets | *    | *       | none  |          | Block all traffic from DMZ to LAN          |         |
| <input type="checkbox"/> | ✓ 4/28 KiB  | IPv4 *   | DMZ subnets | *    | *           | *    | *       | none  |          | Allow all outbound traffic from DMZ to WAN |         |
| <input type="checkbox"/> | ✓ 0/849 KiB | IPv4 *   | *           | *    | *           | *    | *       | none  |          | ALLOW ALL                                  |         |

Add Add Delete Toggle Copy Save Separator

- Add all the rules provided in step #2 of Project 3B.

New Virtual Machine

1 Select a creation type  
2 Select a name and folder  
3 Select a compute resource  
4 Select storage  
5 Select compatibility  
6 Select a guest OS  
7 Customize hardware  
8 Ready to complete

Select a name and folder  
Specify a unique name and target location

Virtual machine name: Win 11 Desktop 01

Select a location for the virtual machine.

serenity.cs.uni.edu  
  CS Datacenter  
    SysAdmin011  
    SysAdmin031

CANCEL BACK NEXT

- Create a new virtual machine for Windows 11

## New Virtual Machine

X

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- 6 Select a guest OS**
- 7 Customize hardware
- 8 Ready to complete

### Select a guest OS

Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: **Windows** ▾

Guest OS Version: **Microsoft Windows 10 (64-bit)** ▾

Enable Windows Virtualization Based Security (i)

Compatibility: ESXi 7.0 U2 and later (VM version 19)

CANCEL

BACK

NEXT

- Select “Windows” for Guest OS Family and “Microsoft Windows 10 (64-bit) for Guest OS Version

## New Virtual Machine

X

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- 7 Customize hardware**
- 8 Ready to complete

| ADD NEW DEVICE         |                                  |                           |
|------------------------|----------------------------------|---------------------------|
| > CPU *                | 4                                | ⓘ                         |
| > Memory *             | 16                               | GB ▾                      |
| <b>New Hard disk *</b> |                                  |                           |
| Maximum Size           | 803.53 GB                        |                           |
| VM storage policy      | ▼                                |                           |
| Location               | Store with the virtual machine ▾ |                           |
| Disk Provisioning      | Thin Provision ▾                 |                           |
| Sharing                | Unspecified ▾                    |                           |
| Shares                 | Normal ▾                         | 1000 ▾                    |
| Limit - IOPs           | Unlimited ▾                      |                           |
| Disk Mode              | Dependent ▾                      |                           |
| Virtual Device Node    | New SCSI controller ▾            | SCSI(0:0) New Hard disk ▾ |

CANCEL

BACK

NEXT

- Set CPU to 4, set memory to 16 GB, set hard disk to 60GB, set disk provisioning to thin provision

## Select File

X

| Datastores                        | Contents                                         | Information                                     |
|-----------------------------------|--------------------------------------------------|-------------------------------------------------|
| > CS1                             | pfSense-CE-2.7.2-RELEASE-amd64.iso               | Name: SW_DVD9_Win_Pro_11_22H2.4_64Bit_35395.ISO |
| < ISOs                            | SW_DVD9_Win_Pro_11_22H2.4_64BIT_English35395.ISO | Size: 5.2 GB                                    |
| > .dvsData                        | SW_DVD9_Win_Server_STD_CORE_2022_231801.ISO      | Modified: 12/28/2022, 10:39:12 AM               |
| > .sdd.sf                         | ubuntu-22.04-desktop-amd64.iso                   | Encrypted: No                                   |
| > .vSphere-HA                     | ubuntu-22.04.3-live-server-amd64.iso             |                                                 |
| > contentlib-792bb956-63f9-4c1... | ubuntu-24.04.1-live-server-amd64.iso             |                                                 |
| > cs3610-instructor-fall-2022     |                                                  |                                                 |
| > cs3610-students-fall-2022       |                                                  |                                                 |
| > CTF4                            |                                                  |                                                 |
| > CTF5                            |                                                  |                                                 |
| > CTF9                            |                                                  |                                                 |
| > images                          |                                                  |                                                 |
| > pfSense-2.6                     |                                                  |                                                 |
| > Scripts                         |                                                  |                                                 |
| < CS_SVC_Security                 |                                                  |                                                 |

File Type: ISO Image (\*.iso) ▾

CANCEL OK

- For CD/DVD Drive, select Datastore ISO File > ISOs > images > Win\_Pro\_11

ADD NEW DEVICE ▾

- Disks, Drives and Storage
  - Hard Disk
  - Existing Hard Disk
  - RDM Disk
  - Host USB Device
  - NVDIMM
  - CD/DVD Drive
- Controllers
  - NVMe Controller
  - SATA Controller
  - SCSI Controller
  - USB Controller
- Other Devices
  - PCI Device
  - Trusted Platform Module
  - Watchdog Timer
  - Precision Clock

- Click ADD NEW DEVICE and select Trusted Platform Module

## New Virtual Machine

✓ 1 Select a creation type  
✓ 2 Select a name and folder  
✓ 3 Select a compute resource  
✓ 4 Select storage  
✓ 5 Select compatibility  
✓ 6 Select a guest OS

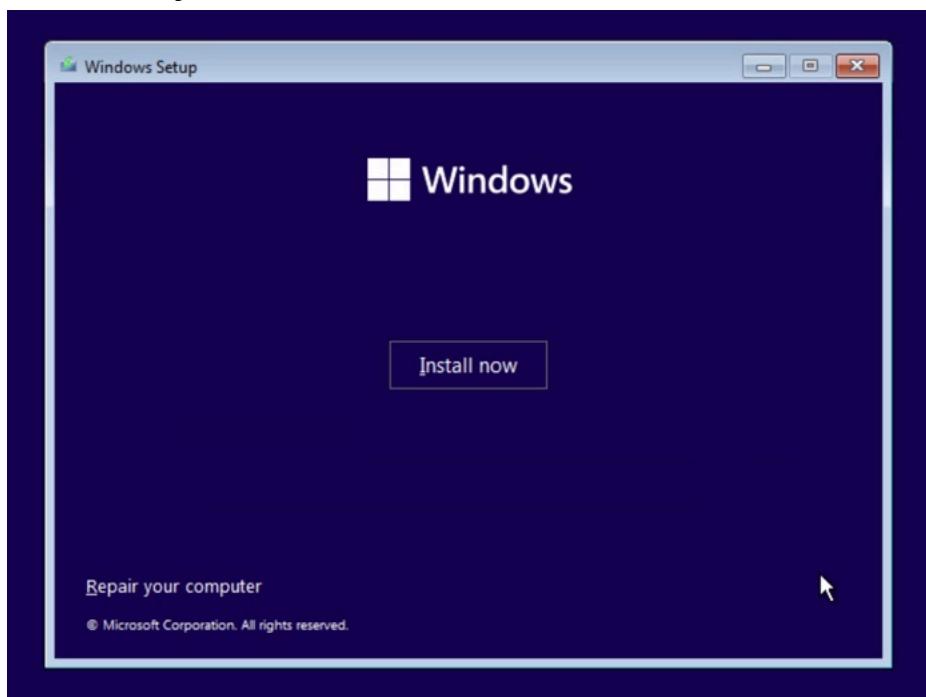
**7 Customize hardware**

8 Ready to complete

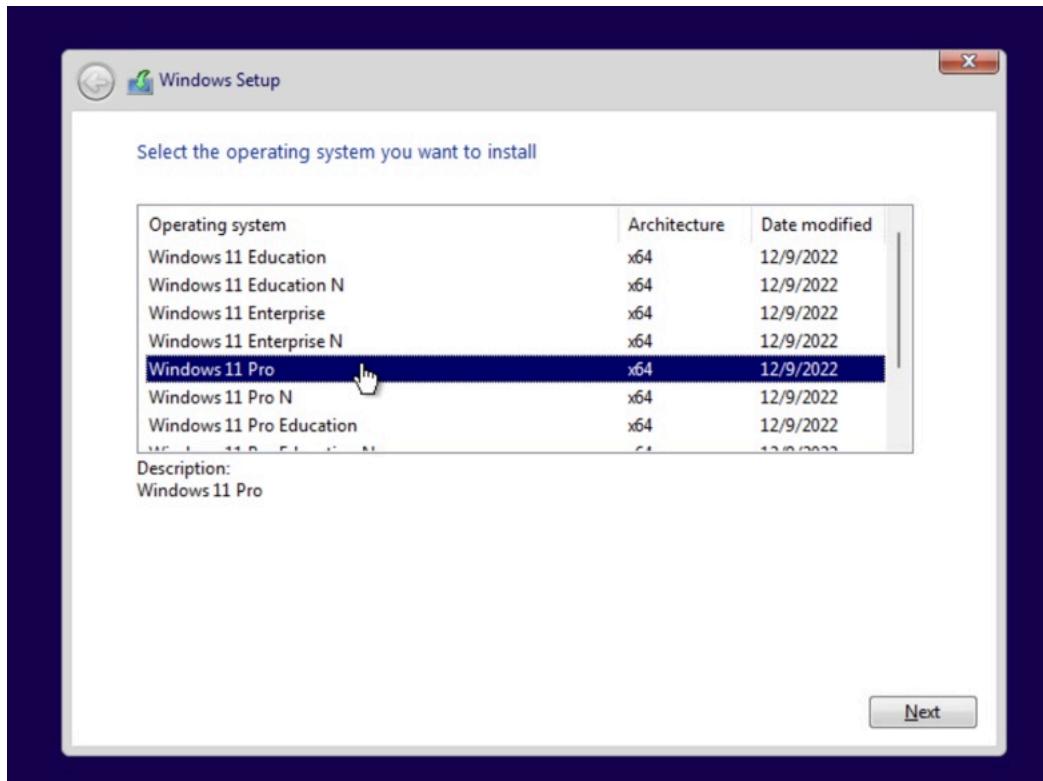
|                         |                               |   |                                                |
|-------------------------|-------------------------------|---|------------------------------------------------|
| > CPU *                 | 4                             | v | ⓘ                                              |
| > Memory *              | 16                            | v | GB v                                           |
| > New Hard disk *       | 60                            | v | GB v                                           |
| > New SCSI controller * | LSI Logic SAS                 |   |                                                |
| > New Network *         | SysAdmin031                   | v | <input checked="" type="checkbox"/> Connect... |
| > New CD/DVD Drive *    | Datastore ISO File            | v | <input checked="" type="checkbox"/> Connect... |
| > New USB Controller    | USB 3.1                       | v |                                                |
| > Video card *          | Specify custom settings v     |   |                                                |
| Security Devices        | TPM                           |   |                                                |
| > SGX                   | SGX not available on the host |   |                                                |
| Trusted Platform Module | Present                       | ⓘ |                                                |
| VMCI device             |                               |   |                                                |

**CANCEL** **BACK** **NEXT**

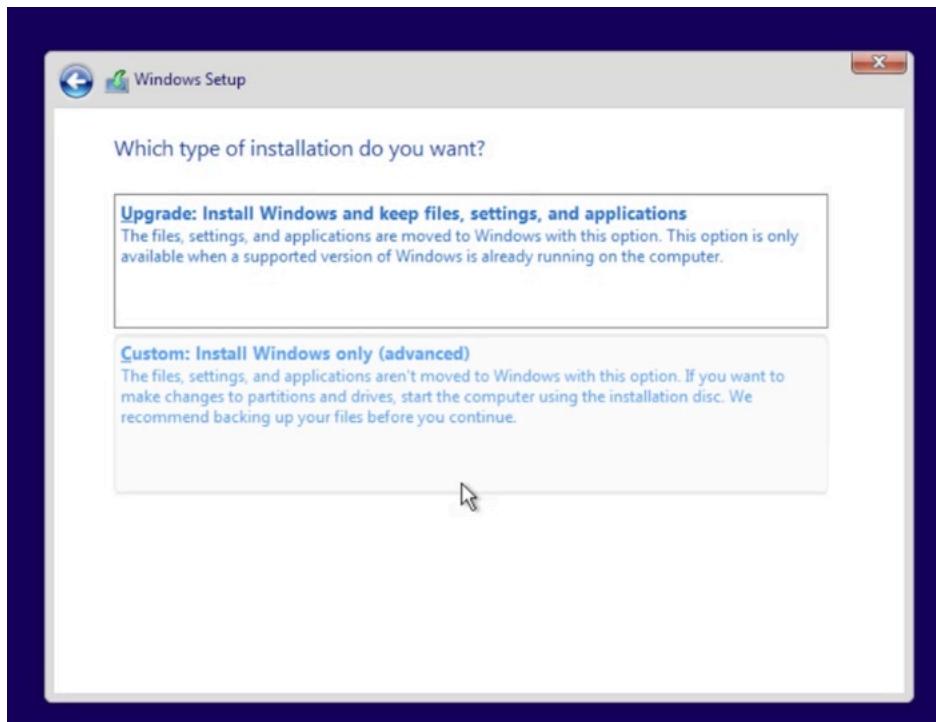
- Make sure Datastore ISO File is connected and hardware has these settings. Finish and start your virtual machine.



- Click Install now



- Select Windows 11 Pro

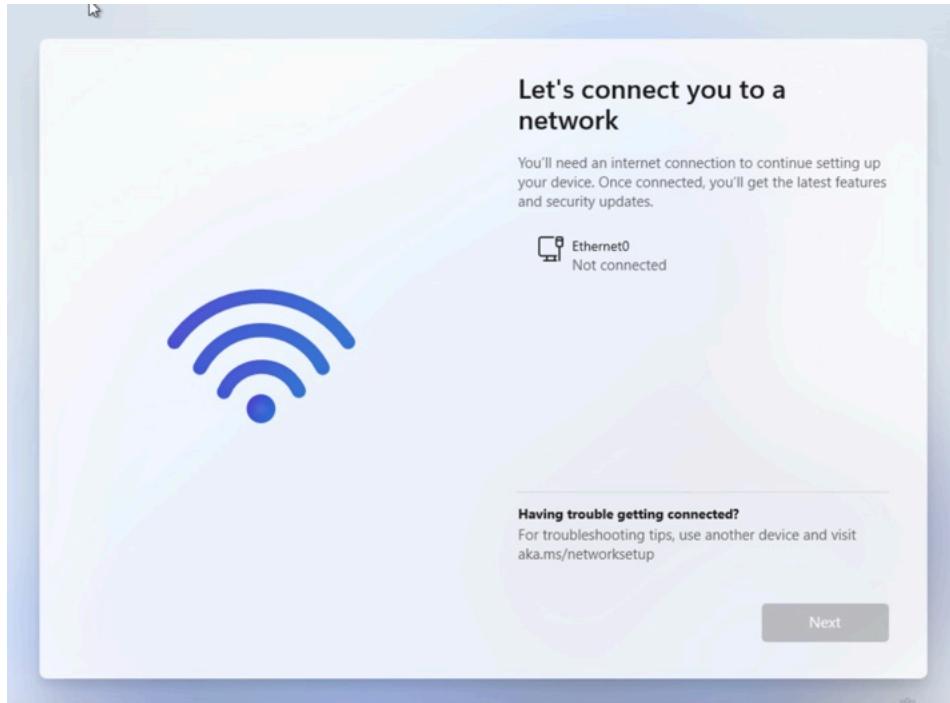


- Make sure to select custom installation

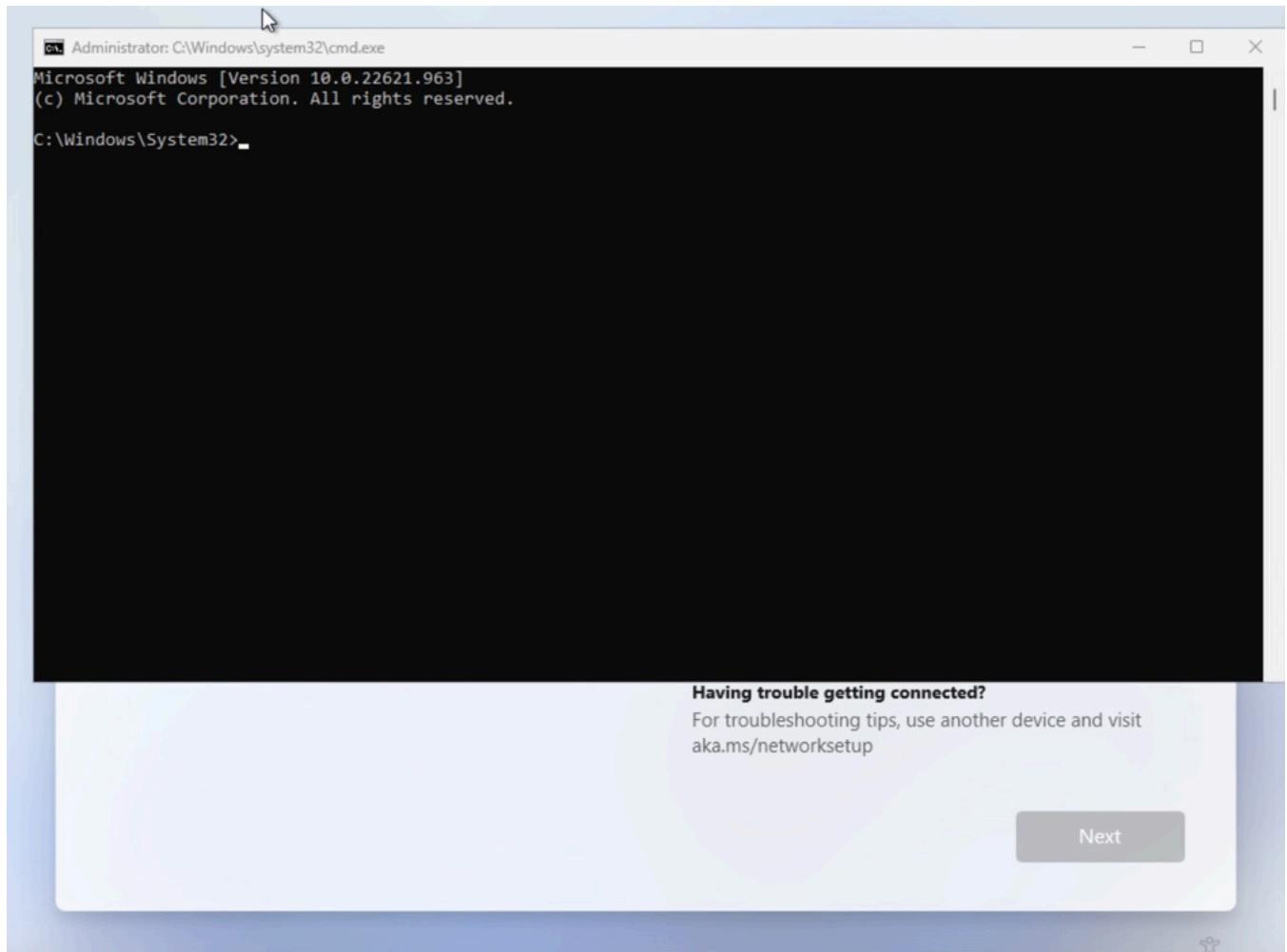
| VM Hardware                               |                                                                                                             |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Encryption                                | VM configuration files are encrypted.<br>No hard disks are encrypted.                                       |
| > CPU                                     | 4 CPU(s)                                                                                                    |
| > Memory                                  | 16 GB, 14.72 GB memory active                                                                               |
| > Hard disk 1                             | 60 GB                                                                                                       |
| > Network adapter 1                       | SysAdmin031 (disconnected)                                                                                  |
| > CD/DVD drive 1                          | Connected                                                                                                   |
| > Video card                              | 8 MB                                                                                                        |
| > Virtual Trusted Platform Module Present |                                                                                                             |
| VMCI device                               | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface |
| > Other                                   | Additional Hardware                                                                                         |
| Compatibility                             | ESXi 7.0 U2 and later (VM version 19)                                                                       |

[Edit Settings...](#)

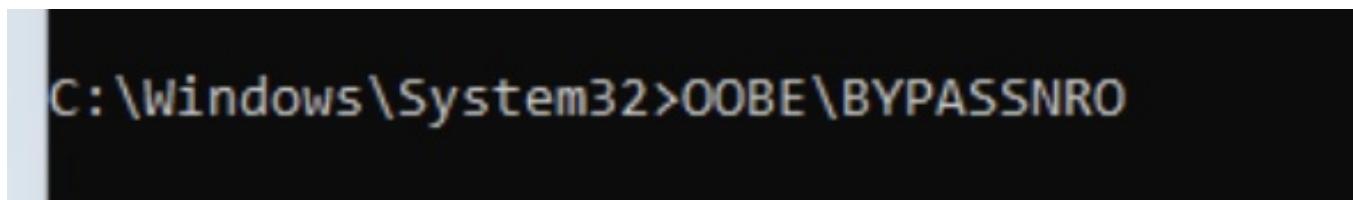
- Go to vSphere and disconnect the network adapter



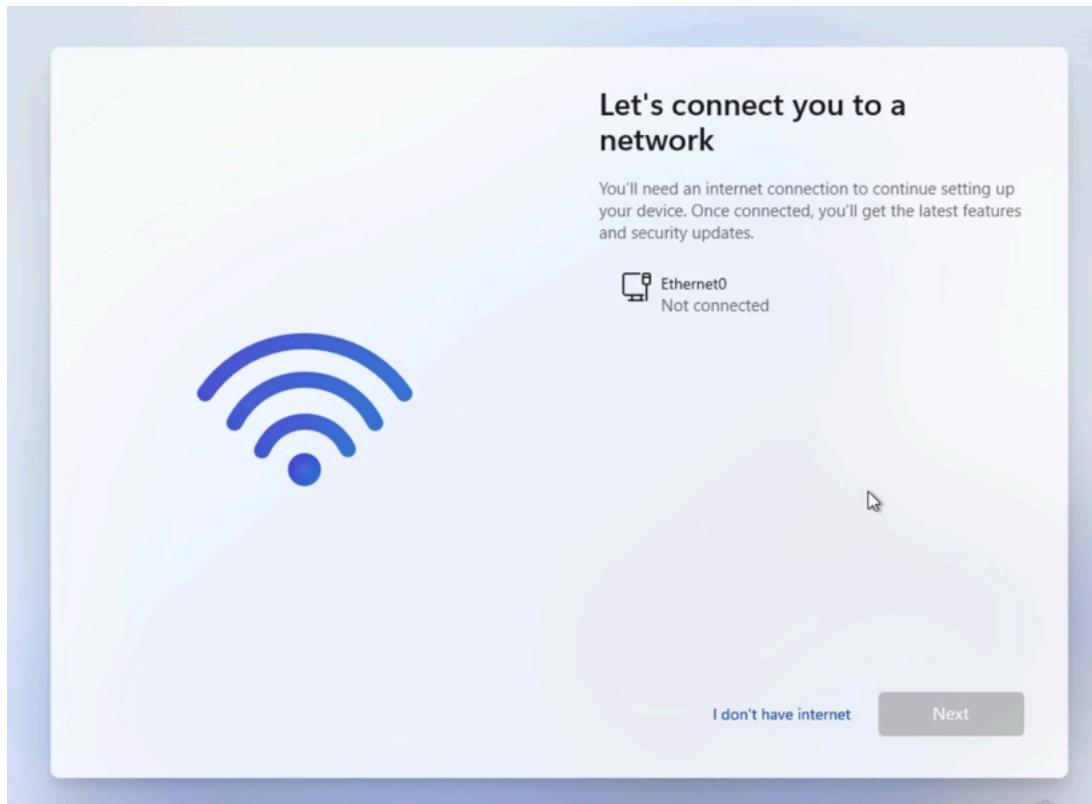
- Once that is done, you will see this screen as windows 11 loads up.



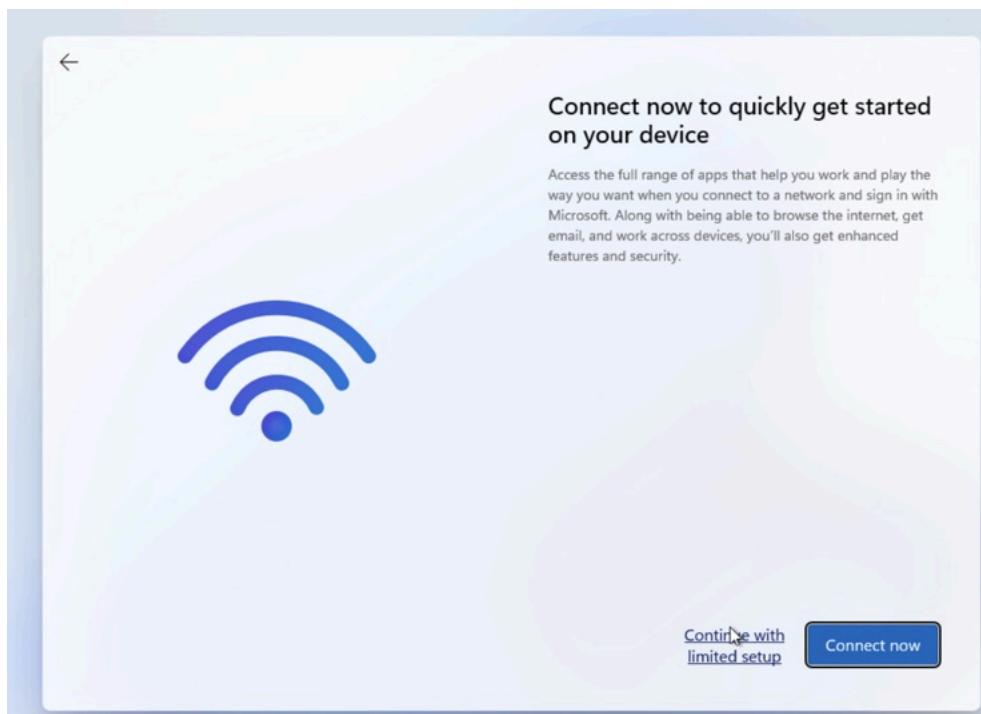
- Hit Shift + F10 to bring up the command prompt



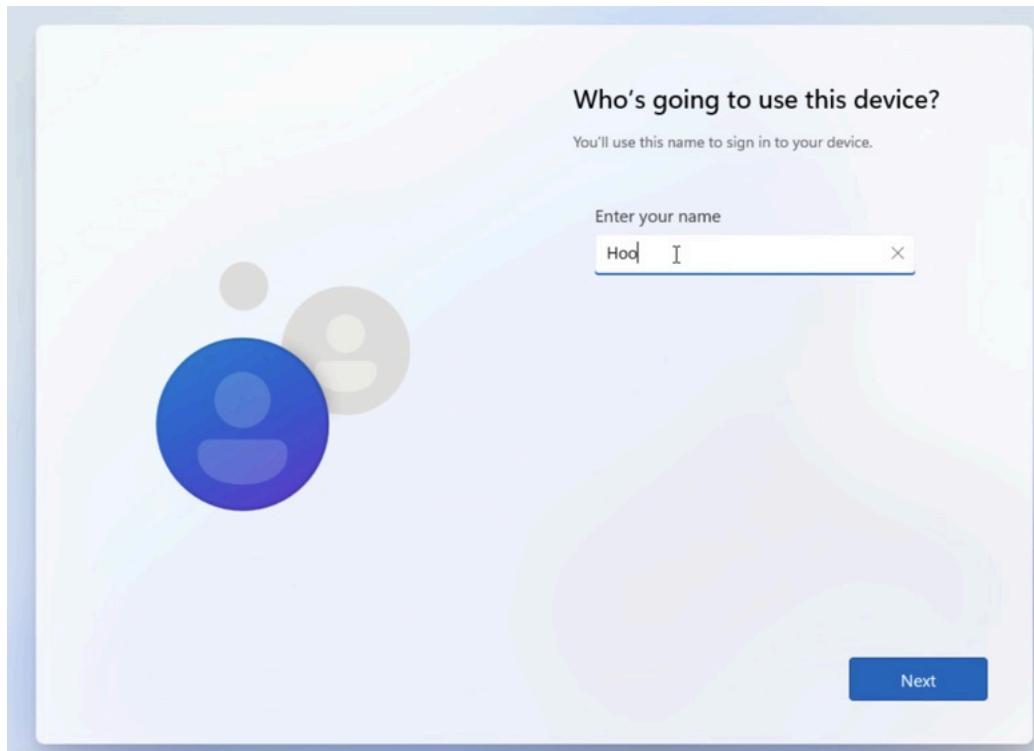
- Type in the command OOBE\BYPASSNRO



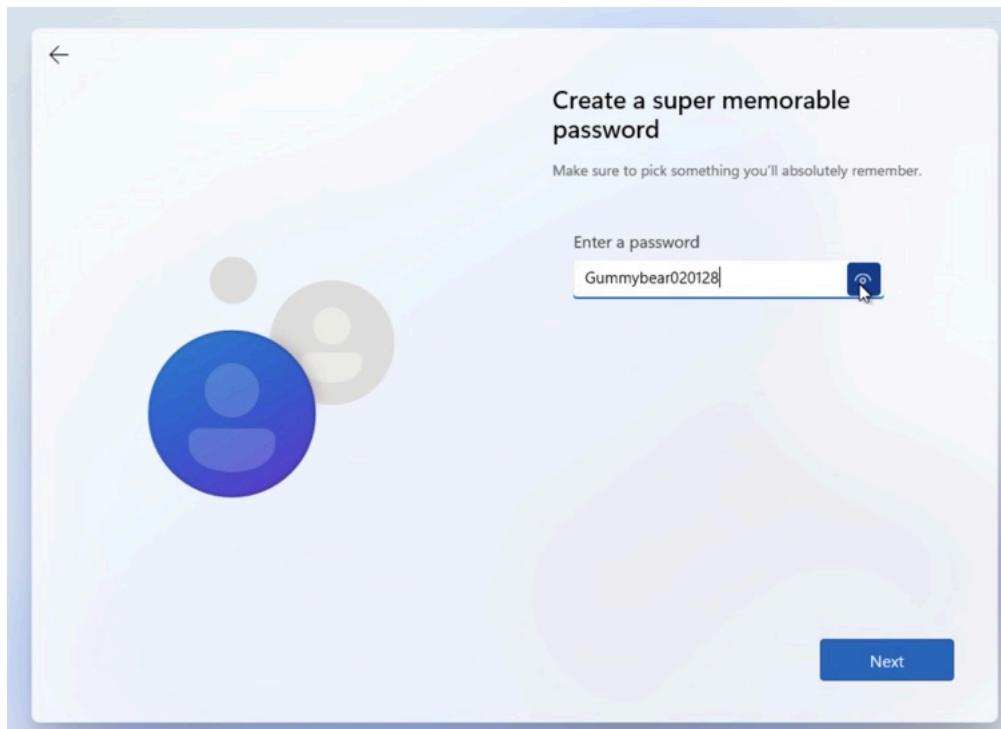
- Once it reboots, you will now have a "I don't have internet" option to select at the bottom.



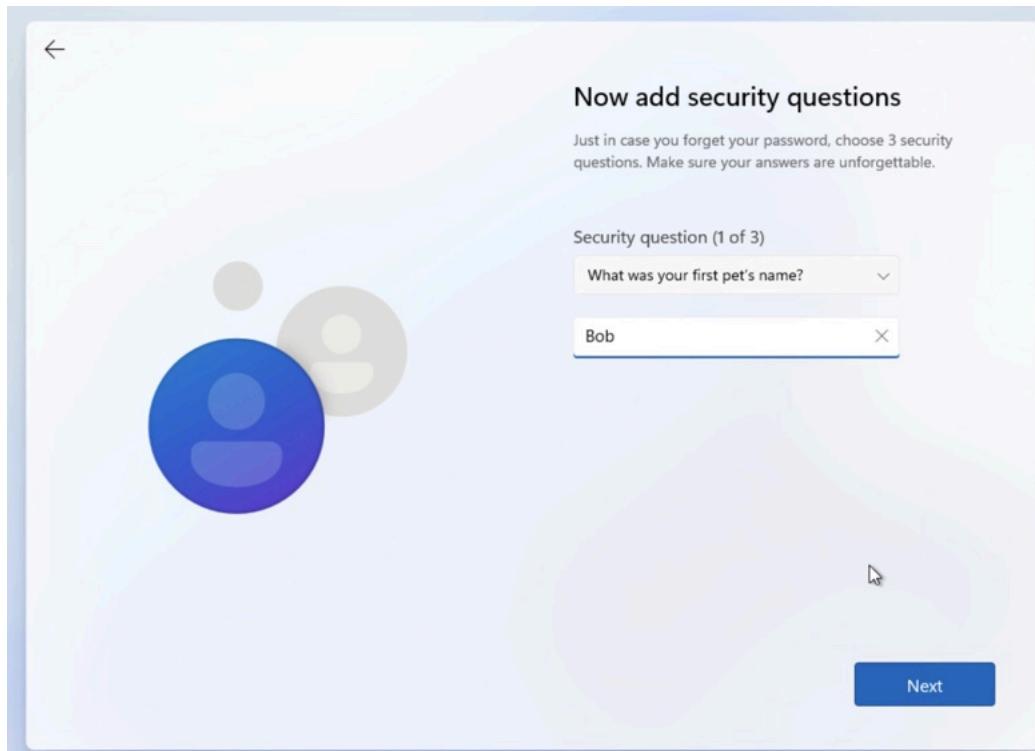
- Hit Continue with limited setup



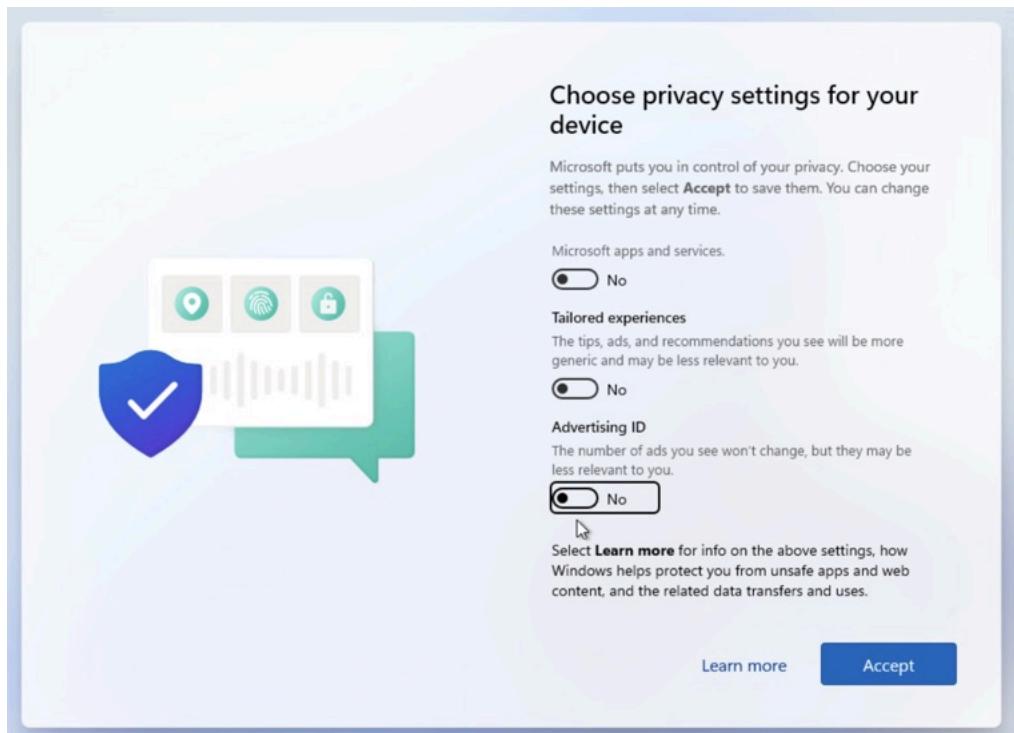
- Create your username and password



- Set your password: Gummybear020128



- Fill in security questions. All my answers are Bob.



- Deselect all options for privacy settings and hit "Accept"

## Edit Settings | Win 11 Desktop 01

X

Virtual Hardware VM Options

ADD NEW DEVICE ▾

|                       |                                                           |    |                                                                   |
|-----------------------|-----------------------------------------------------------|----|-------------------------------------------------------------------|
| Encryption            | VM configuration files are encrypted. <a href="#">(i)</a> |    |                                                                   |
| > CPU                 | 4                                                         | v  | <a href="#">(i)</a>                                               |
| > Memory              | 16                                                        | v  | GB v                                                              |
| > Hard disk 1         | 60                                                        | GB | v                                                                 |
| > SCSI controller 0   | LSI Logic SAS                                             |    |                                                                   |
| > Network adapter 1*  | SysAdmin031                                               | v  | <input checked="" type="checkbox"/> Connected <a href="#">(X)</a> |
| > CD/DVD drive 1      | Datastore ISO File                                        |    | <input checked="" type="checkbox"/> Connected                     |
| > USB xHCI controller | USB 3.1                                                   |    |                                                                   |
| > Video card          | Specify custom settings v                                 |    |                                                                   |
| > Security Devices    | TPM                                                       |    |                                                                   |
| VMCI device           |                                                           |    |                                                                   |

CANCEL OK

- Go back to vSphere and reconnect the network adapter
- Repeat these steps to create another Windows 11 virtual machine

```
wonh@hoolinuxserver:~$ ls /etc/netplan/
50-cloud-init.yaml
wonh@hoolinuxserver:~$ _
```

- Open Linux Server virtual machine and locate the .yaml file in directory /etc/netplan/
- ```
wonh@hoolinuxserver:~$ sudo nano /etc/netplan/50-cloud-init.yaml
[sudo] password for wonh:
```
- Use command “sudo nano /etc/netplan/50-cloud-init.yaml” to use nano to edit the file

```
GNU nano 7.2                                     /etc/netplan/50
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    ens192:
      dhcp4: false
      addresses:
        - 192.168.2.20/24
      gateway4: 192.168.2.1
      nameservers:
        addresses:
          - 10.120.16.10
          - 10.120.16.11
        search: []
      routes:
        - to: default
          via: 10.161.31.1
version: 2
```

- Edit file so that dhcp4 is set to false and the address is set as the DMZ address. Make sure to add the gateway4 address aswell.

```
wonh@hoolinuxserver:~$ sudo netplan apply
```

- Use the command “sudo netplan apply” to apply the changes. Now your Linux Server has a DMZ address!

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

Through this project, I learned how to configure and segment networks into WAN, LAN, and DMZ, and how to manage traffic along these networks through firewalls in pfSense. I learned this by following the guidelines given by Prof. Diesburg and doing this project. Ping testing the servers and making sure all the IP addresses line up with the Lucid Chart created in Project 3A. I ran into some firewall issues while ping testing but it was nothing that broke my initial expectations above.

---

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information>

# Project 4: Internal Caching DNS Server

**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

In this project, I will be creating a new internal caching DNS server that will send requests to UNI's DNS server. This is the first project without a follow along video so I am expecting to run into some walls.

**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



- First, log into pfSense and make your way to DNS Resolver under Services.

A screenshot of the pfSense DNS Resolver configuration page. At the top, there is a section with a 'Enable' checkbox followed by 'Enable DNS resolver' which is checked. Below this is a 'DNS Query Forwarding' section with a 'Enable Forwarding Mode' checkbox which is also checked. A note below says: 'If this option is set, DNS queries will be forwarded to other interfaces such as DHCP, PPP, or OpenVPN'. At the bottom of the page, there is another list item.

- Make sure that "Enable DNS resolver" is checked.

**DNS Query Forwarding**  Enable Forwarding Mode  
If this option is set, DNS queries will be forwarded to other interfaces such as DHCP, PPP, or OpenVPN

- Make sure that "Enable Forwarding Mode" is checked.

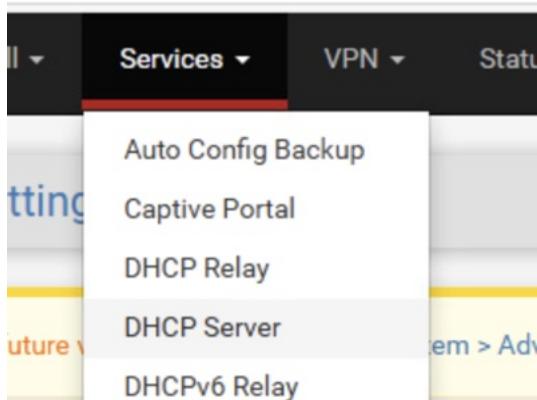
**DNSSEC**  Enable DNSSEC Support

- Make sure that “Enable DNSSEC Support” is unchecked.



Interface IP addresses used by the DNS Resolver for responding to queries from used. Queries to addresses not selected in this list are discarded. The default address.

- Make sure that Network Interfaces is set to “All” so that it responds to both LAN and DMZ.
- Make sure to “Save” at the bottom and “Apply Changes”!!



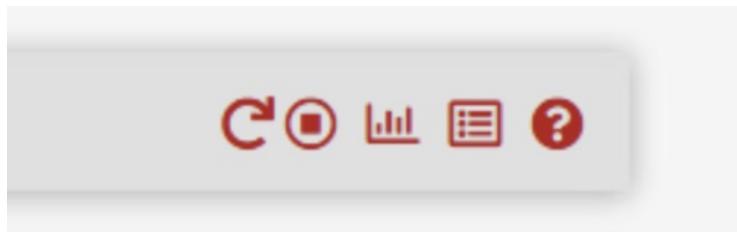
- Next, find your way to DHCP Server under Services.

**DNS Servers** 192.168.1.1

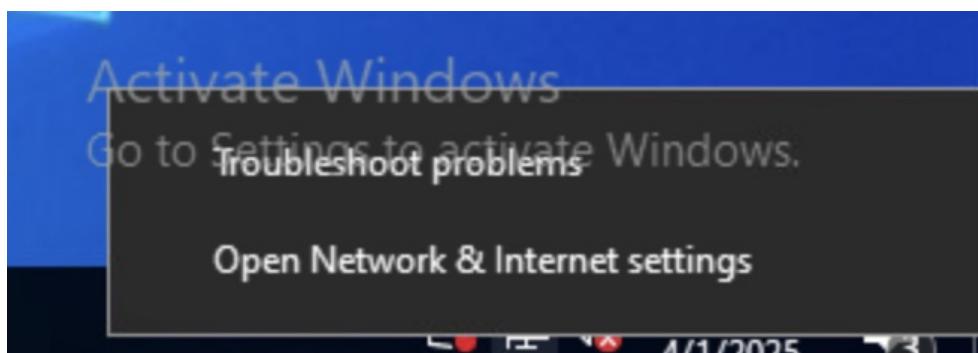
- Under the LAN tab, fill in the LAN IP (192.168.1.1) for DNS Servers.

**DNS Servers** 192.168.2.1

- Under the DMZ tab, fill in the DMZ IP (192.168.2.1) for DNS Servers.
- Make sure to “Save” and “Apply Changes”.



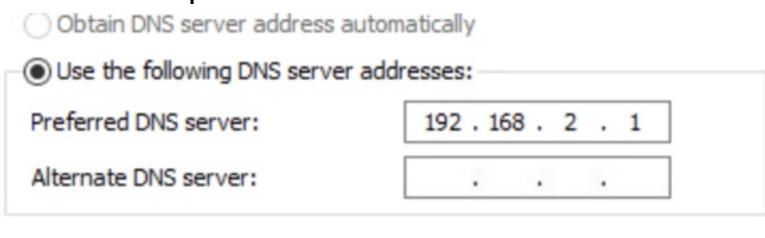
- Hit the refresh button on the top right to restart DHCP Services.



- Now, log into your Windows Server to update the dns settings in network adapter properties.



- Go to Change Adapter Options -> Ethernet0 -> Properties -> Internet Protocol Version 4 -> Properties



- Type in the DMZ IP (192.168.2.1) into Preferred DNS Server.

```
wonh@hoolinuxserver:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

- Finally, let's change the DNS settings for the Linux Server. Type the command: sudo nano /etc/netplan/50-cloud-init.yaml

```
nameservers:  
    addresses:  
        - 192.168.2.1  
        - 192.168.2.1
```

- Now that NetPlan configuration is open, find where it says "nameservers:" and type in the DMZ IP (192.168.2.1) under "addresses:".
- Hit "Save" and "Exit".

```
wonh@hoolinuxserver:~$ sudo netplan apply
```

- Type the command: sudo netplan apply
- This will apply the changes made to NetPlan.

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

I learned how to create a new internal caching DNS server that sends requests to UNI's DNS server. I did run into some problems with this project but as mentioned above, I expected to run into some walls. Although there were some issues, I was able to figure it out and found out that it is simpler than I expected.

---

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

# Project 5: External DNS Server

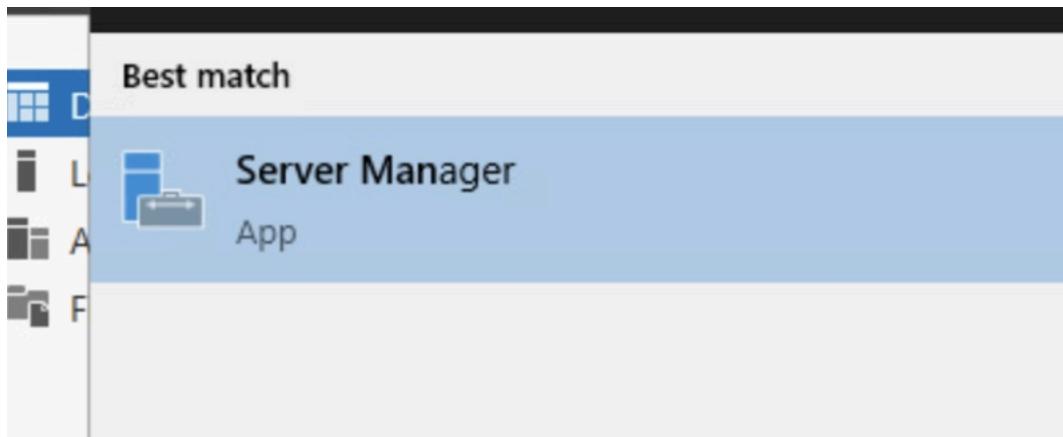
---

**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

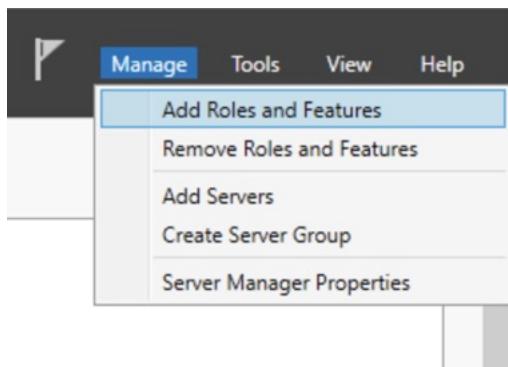
For this project, I will be choosing a domain name to use on a new external DNS server setup on my windows server. I will be trying to make sure that both LAN and DMZ servers can resolve off of my DNS server. I am expecting to get stuck on some parts of this project but with some research/help, I think this project will be pretty straightforward.

---

**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



First, let's start by opening Server Manager in your Windows 2022 Server.



In Server Manager, click "Manage" on the top right and select "Add Roles and Features".

## Select installation type

DESTINATION SERVER  
WIN-KHV7TRSMBOA

Before You Begin

**Installation Type**

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

**Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

**Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous Next > Install Cancel

Select “Role-based or feature-based installation” and hit “Next”.

## Select destination server

DESTINATION SERVER  
WIN-KHV7TRSMBOA

Before You Begin

Installation Type

**Server Selection**

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool

Select a virtual hard disk

Server Pool

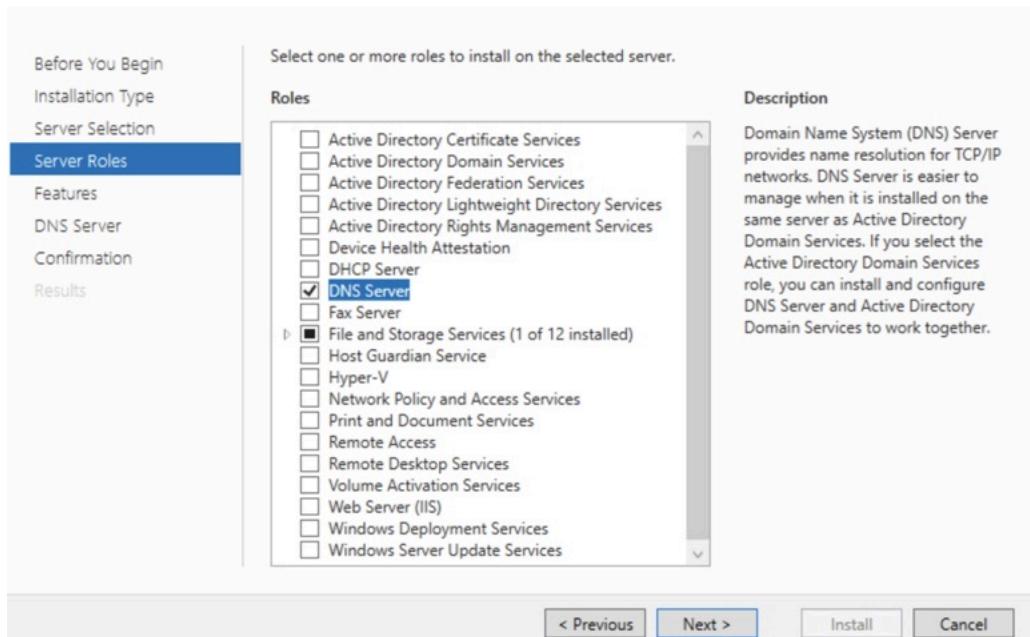
Filter:		
Name	IP Address	Operating System
WIN-KHV7TRSMBOA	192.168.2.10	Microsoft Windows Server 2022 Standard

1 Computer(s) found

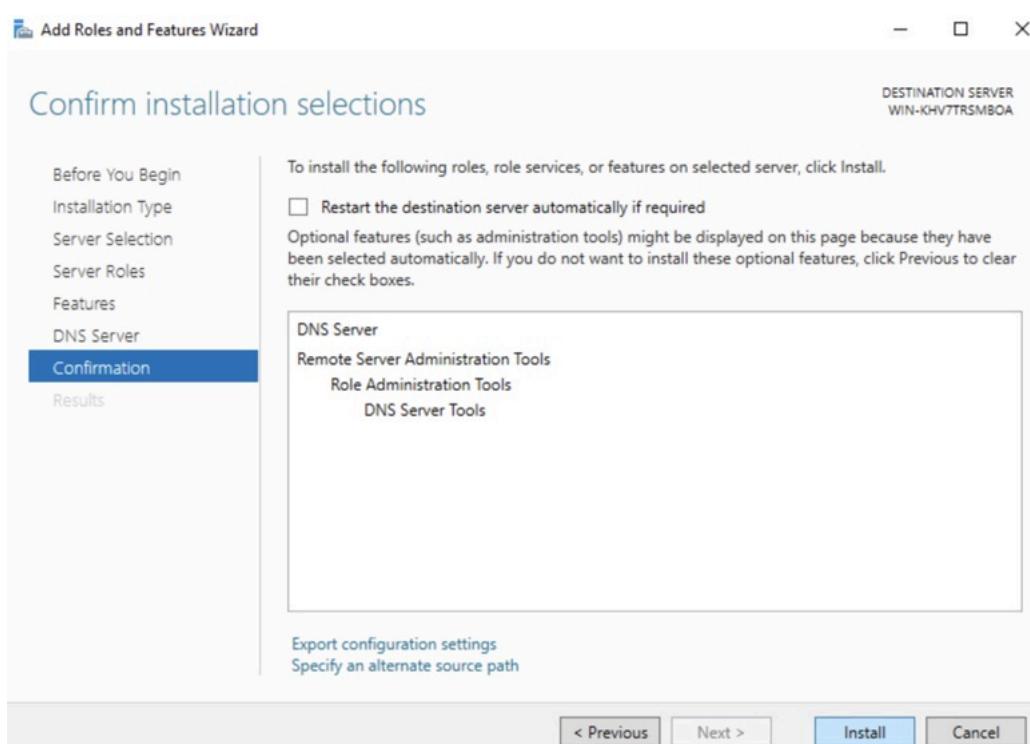
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous Next > Install Cancel

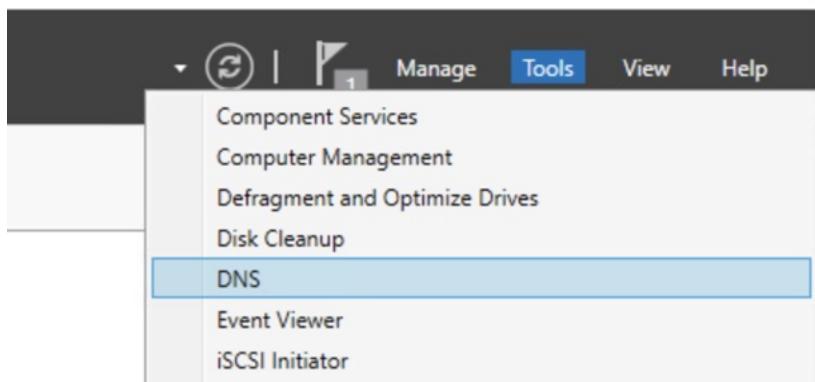
Select your server (192.168.2.10) from the server pool and hit “Next”.



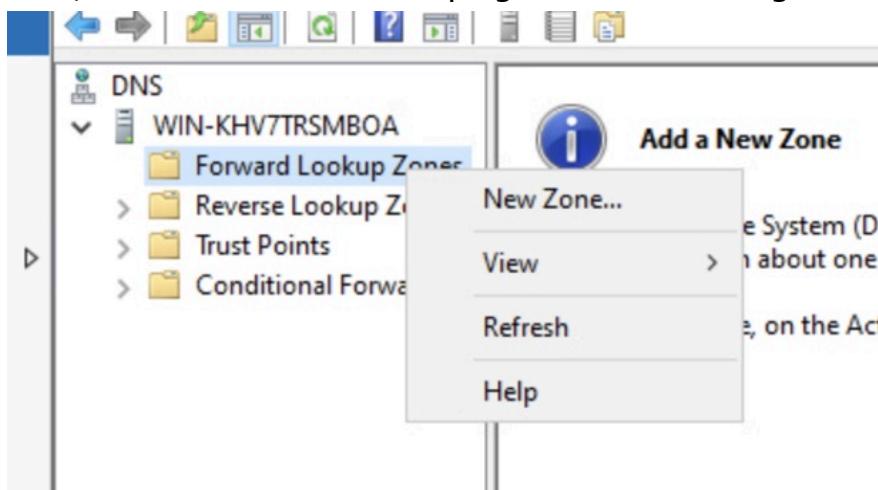
Select "DNS Server" in Server Roles and hit "Next".



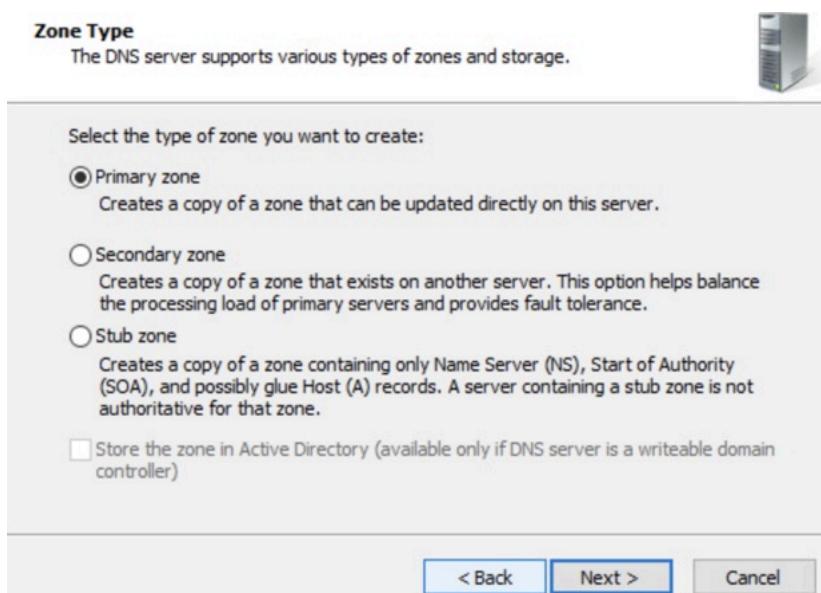
Hit "Install" and "Close" after installation is complete!



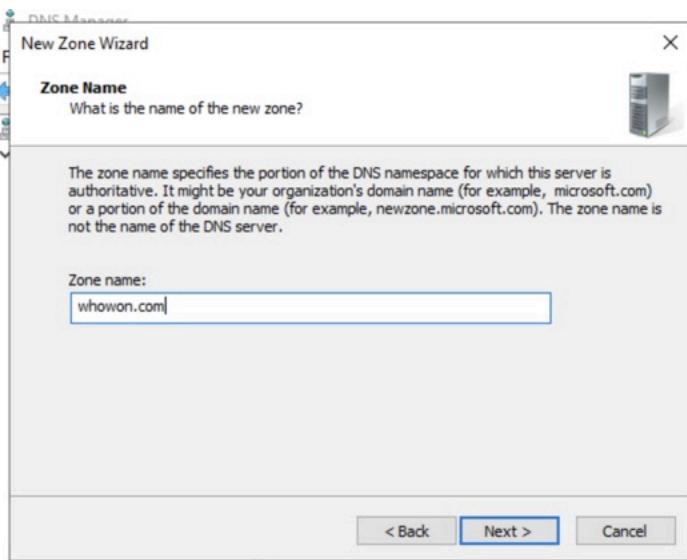
Next, click on "Tools" on the top right of Server Manager then select "DNS".



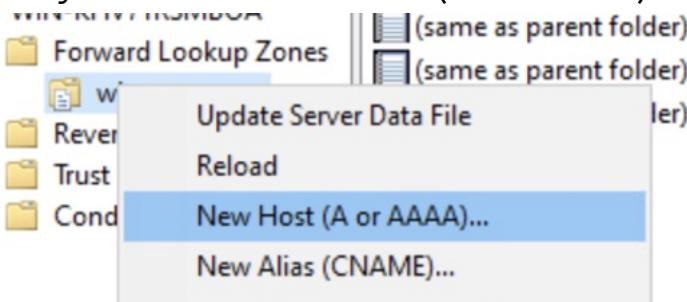
This will bring up the DNS Manager. In DNS Manager, right click on the "Forward Lookup Zones" folder and select "New Zone...".



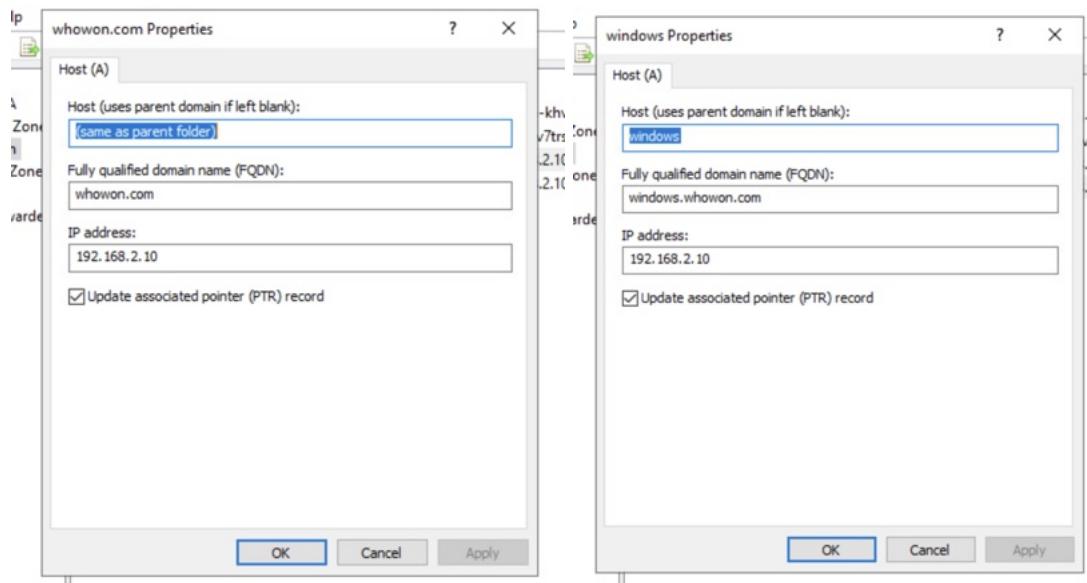
Select "Primary zone" and hit "Next".



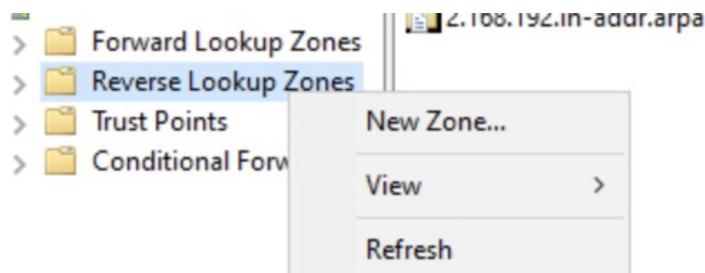
Give your zone a domain name (whowon.com) and hit “Next” until you are done.



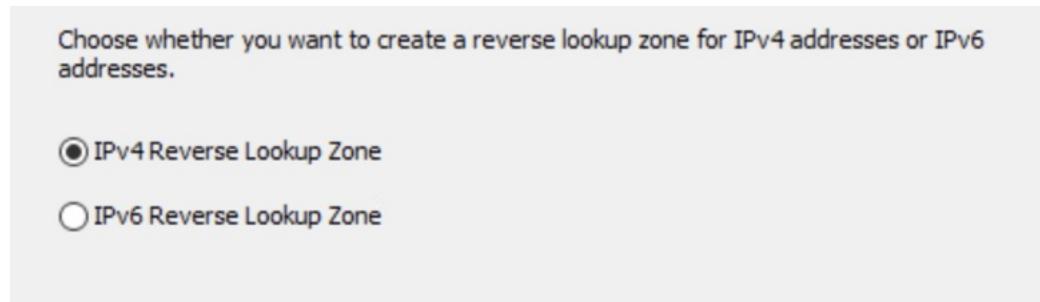
You will not see your new zone in the Forward Lookup Zones folder. Right click on your new zone and select “New Host (A or AAAA)...”



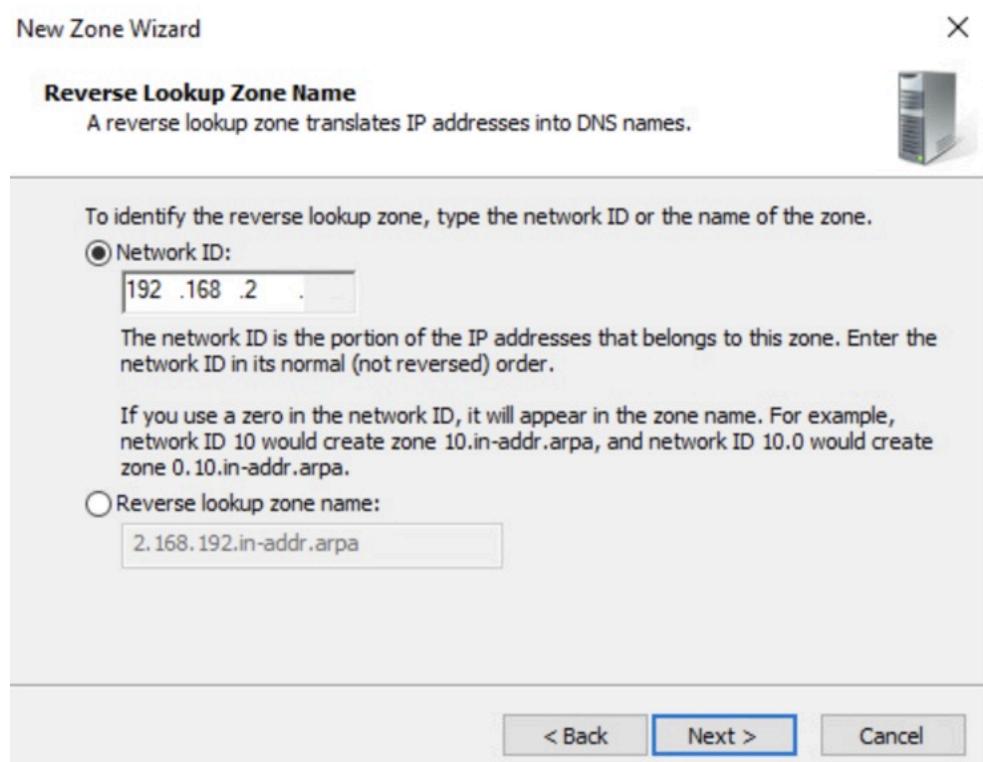
Create two new hosts, one that uses the same host as the parent folder and one with the host “windows”. Both will have the DNS server IP address. (192.168.2.10)



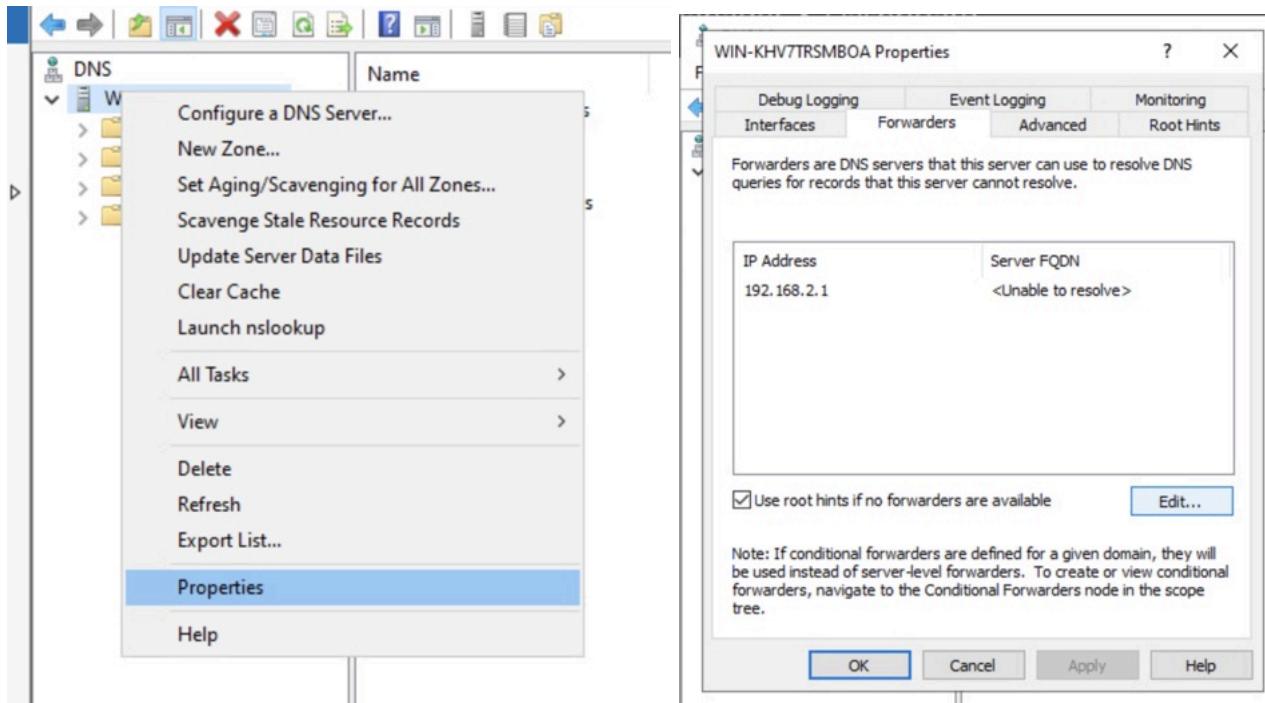
Next, right click on the folder “Reverse Lookup Zones” and select “New Zone...”.



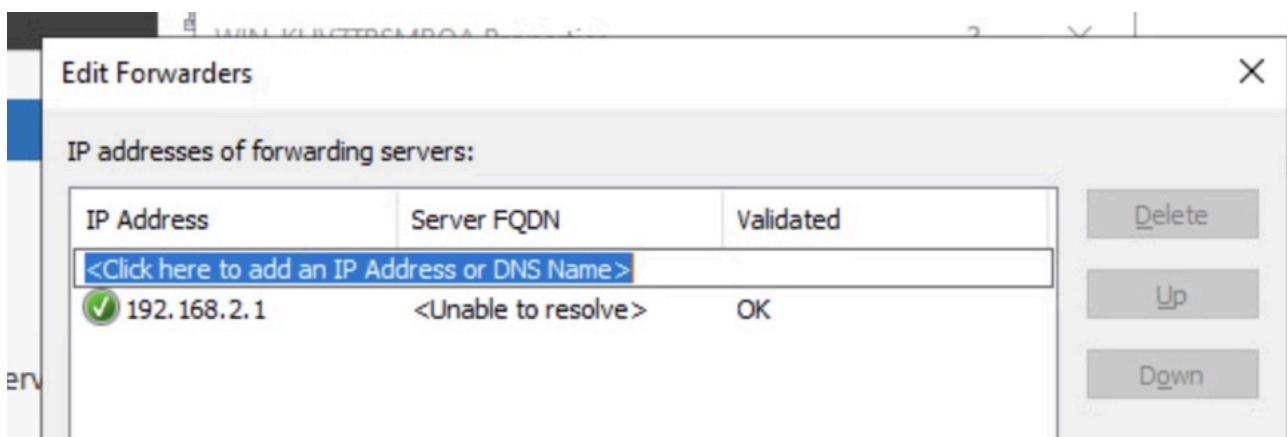
Make sure to select “IPv4 Reverse Lookup Zone”.



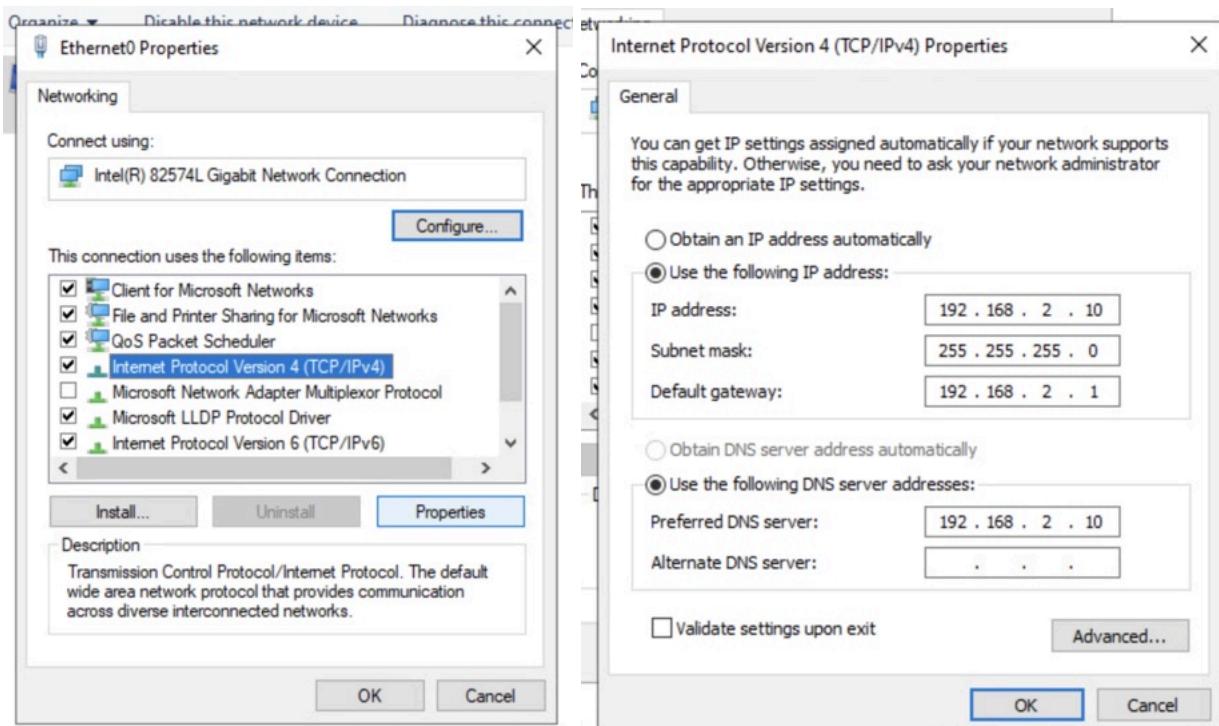
In Network ID, put in the first three segments of your DNS server IP address. Hit “Next” until you’re done.



Next, right click on your DNS server and go to properties. In properties, make your way to "Forwarders" and select "Edit".



In Edit Forwarders, enter in your pfSense IP address (192.168.2.1). Make sure to hit "Apply" and "OK".



Now make your way into Ethernet Properties -> Internet Protocol Version 4 -> Properties and type in the Windows Server IP into the “Preferred DNS server” section.

```
C:\Users\Administrator>nslookup windows.whowon.com
Server: whowon.com
Address: 192.168.2.10

Name:    windows.whowon.com
Address: 192.168.2.10
```

Open up the command prompt and try “nslookup <yourdomainname>” to see if your domain is correctly configured. If your output looks like this, then it is running correctly.

```
wonh@hoolinuxserver:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

Now that the Windows Server is connected to the domain, let's do the same for the Linux Server. Type in the command: "sudo nano /etc/netplan/50-cloud-init.yaml".

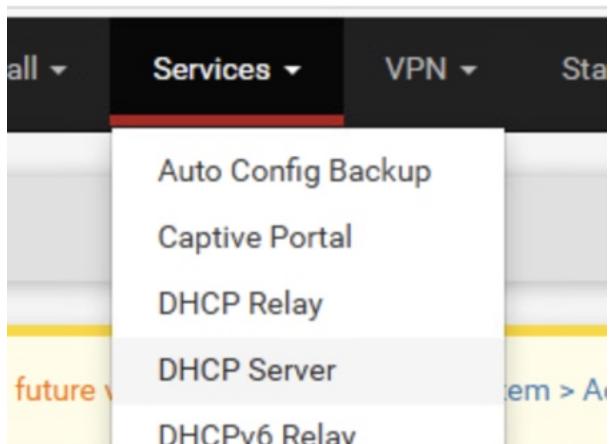
```
network:
  ethernets:
    ens192:
      dhcp4: false
      addresses:
        - 192.168.2.20/24
      gateway4: 192.168.2.1
      nameservers:
        addresses:
          - 192.168.2.10
        search: []
      routes:
        - to: default
          via: 10.161.31.1
  version: 2
```

This will open an editor with this information inside. Under "nameservers", make sure the address that is typed in there is the Windows Server IP address (192.168.2.10). Hit "Exit" and "Yes" to save.

```
wonh@hoolinuxserver:~$ sudo netplan apply
```

Type in the command: "sudo netplan apply" to apply changes.

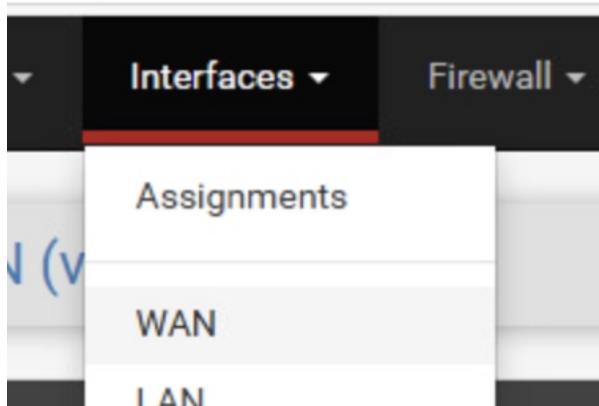
For the next steps, I will be following the documentation of Project 3 to create a Windows 11 virtual machine. It will be made exactly like how the other 2 Windows 11 virtual machines have been created. Once the virtual machine is downloaded, we will be giving it a WAN IP address and port forwarding the external DNS server to it.



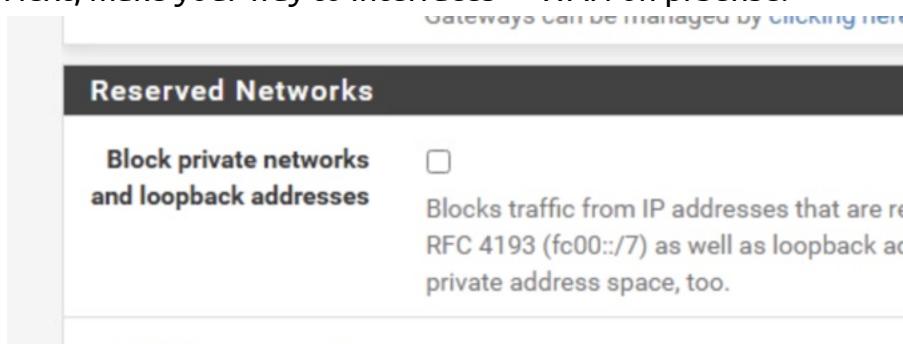
Log into pfSense and make your way to Services -> DHCP Server -> LAN tab.



Under the LAN tab, in DNS Servers, type in the Windows Server IP address (192.168.2.10).  
[taces.php?it=wan](#)



Next, make your way to Interfaces -> WAN on pfSense.



Make sure that "block private networks and loopback addresses" is unchecked.

The screenshot shows the pfSense web interface. The top navigation bar includes 'System' and 'Interfaces' dropdowns, and tabs for 'Access', 'Firewall & NAT' (which is selected), and 'Networking'. Below the navigation is a sub-menu with 'Advanced' and 'Certificates' options. The main content area is titled 'Firewall Processing'.

Next, make your way to System -> Advanced -> Firewall & Nat in pfSense.

This screenshot shows the 'Network Address Translation' configuration page. A dropdown menu for 'NAT Reflection mode for port forwards' is set to 'Pure NAT'. A note below it states: 'The Pure NAT mode uses a set of NAT rules to direct packets to the target of the port forward. It can accurately determine the interface and gateway IP used for communication with the target at the limits to the number of ports other than the limits of the protocols. All protocols available for port forwarding are supported.' Another note below says: 'Individual rules may be configured to override this system setting on a per-rule basis.'

Make sure that "NAT Reflection mode for port forwards" is set to "Pure NAT".

Note: Only applies to Reflection on port forwards in NAT + proxy mode.

This screenshot shows the 'Firewall' configuration page with the 'Reflection' tab selected. Under 'Enable NAT Reflection for 1:1 NAT', there is a checked checkbox for 'Automatic creation of additional NAT redirect rules from within the internal networks'. A note below it says: 'Note: Reflection on 1:1 mappings is only for the inbound component of the 1:1 mappings. This function forwards. For more details, refer to the pure NAT mode description above. Individual rules may be overridden on a per-rule basis.'

Make sure that "Enable NAT Reflection for 1:1 NAT" is checked.

This screenshot shows the 'Firewall' configuration page with the 'NAT' tab selected. The left sidebar lists 'Aliases', 'NAT', and 'Rules'.

Now, make your way to Firewall -> NAT in pfSense.

This screenshot shows the 'NAT' configuration page. At the top, there are dropdown menus for 'Destination port range' (set to 'DNS'), 'From port' (set to 'Custom'), 'To port' (set to 'Custom'), and 'Protocol' (set to 'Custom').

Make sure that "Destination port range" is from DNS to DNS.

<u>Redirect target IP</u>	Address or Alias	Type	192.168.2.10
			Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope".

Set “Redirect target IP” to the Windows Server IP address (192.168.2.10).

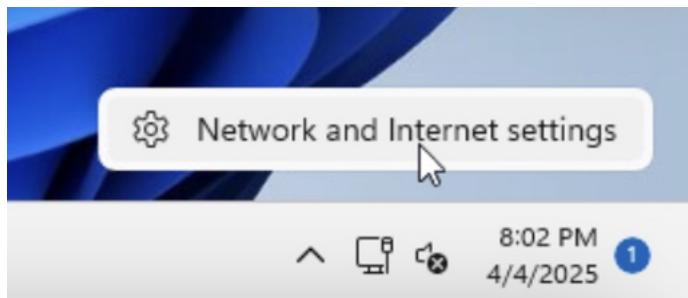
<u>Redirect target port</u>	DNS
	Port

Specify the port on the machine with the IP address entered above. In case of DNS, this is the port number.

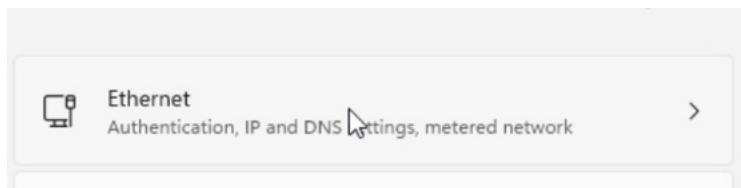
Set “Redirect target port” to DNS.

<u>Protocol</u>	UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.	

Set “Protocol” to UDP. Make sure to hit “Save” and “Apply Changes” on all of pfSense configurations.



Log into your WAN Windows 11 desktop and go to Network and Internet settings.

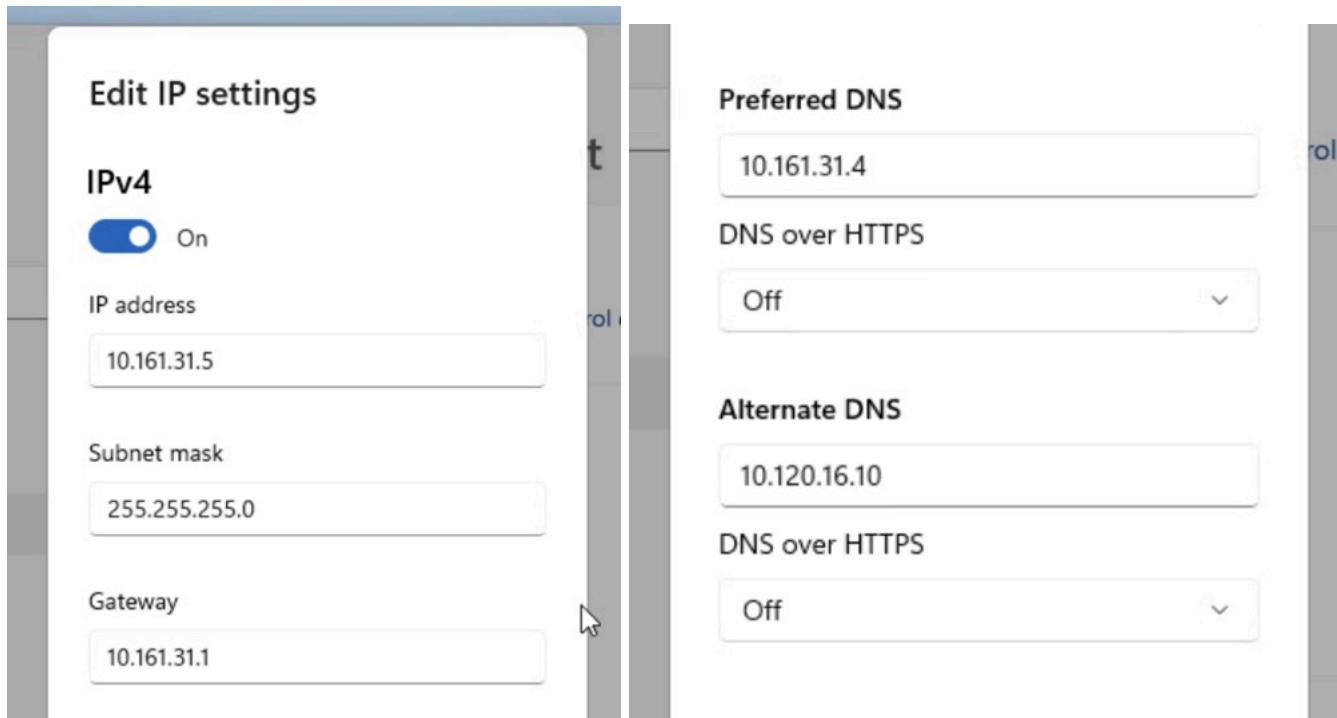


Select “Ethernet”.

IP assignment:	Manual
IPv4 address:	10.161.31.5
IPv4 mask:	255.255.255.0
IPv4 gateway:	10.161.31.1

Edit

Hit “Edit” IP Address.



Type in new WAN IP address (10.161.31.5) for IP address, 255.255.255.0 for subnet mask, WAN gateway IP address (10.161.31.1) for gateway, WAN IP (10.161.31.4) for preferred DNS, and the UNI DNS Server address (10.120.16.10) for alternate DNS. Hit “save”.

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

I learned how to create external DNS servers and how to use fully qualified domain names with them. Through these projects I am getting a better understanding of networking and how to configure them. I did run into some issues but with some helpful tips from Prof. Diesburg, I was able to finish the project. Nothing in the project broke my initial expectations as I expected to run into some problems.

---

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

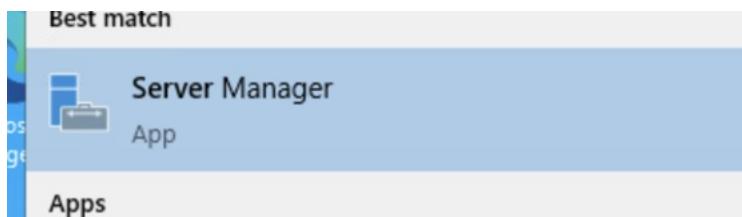
# Project 6: Static HTTPS Web Server

---

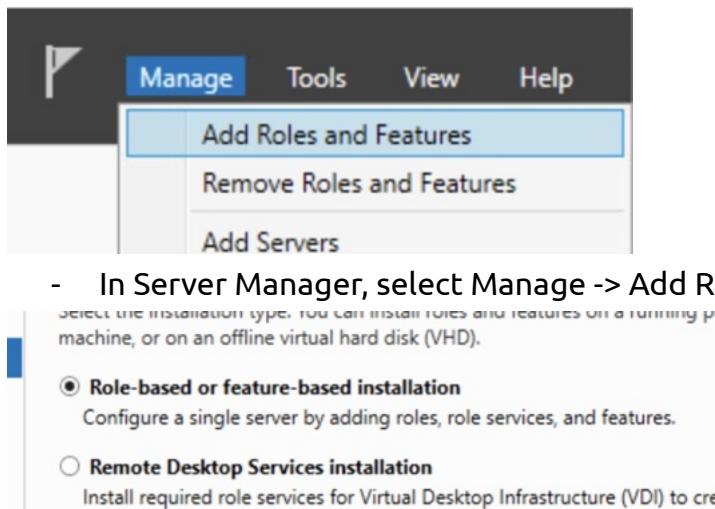
**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

For this project, I will be setting up a web server to serve static web content over a secure connection. My webpage will display my company's name and an "Under Construction" GIF. I expect this project to be pretty straightforward but I will not be surprised if I make some configuration errors.

**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



- First, make your way to Server Manager in your Windows 2022 Server.



- In Server Manager, select Manage -> Add Roles and Features.

SELECT THE INSTALLATION TYPE. YOU CAN INSTALL ROLES AND FEATURES ON A RUNNING SERVER, OR ON AN OFFLINE VIRTUAL HARD DISK (VHD).

**Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

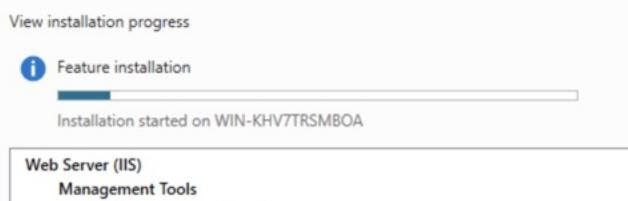
**Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create

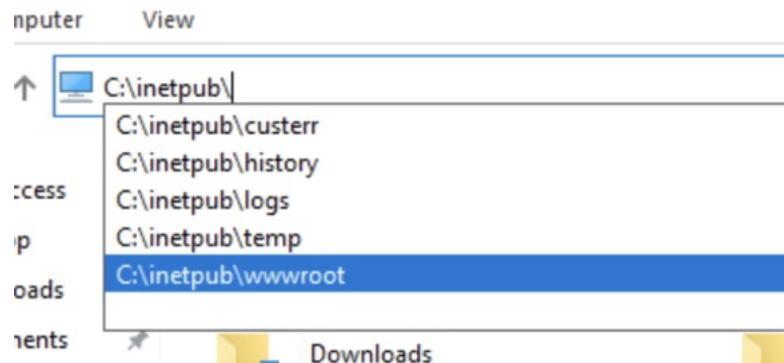
- Make sure "Role-based or feature-based installation" is selected.

- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

- Select “Web Server (IIS)” for your role and hit “Next” until you see the installation page.



- Select and hit “Install”.

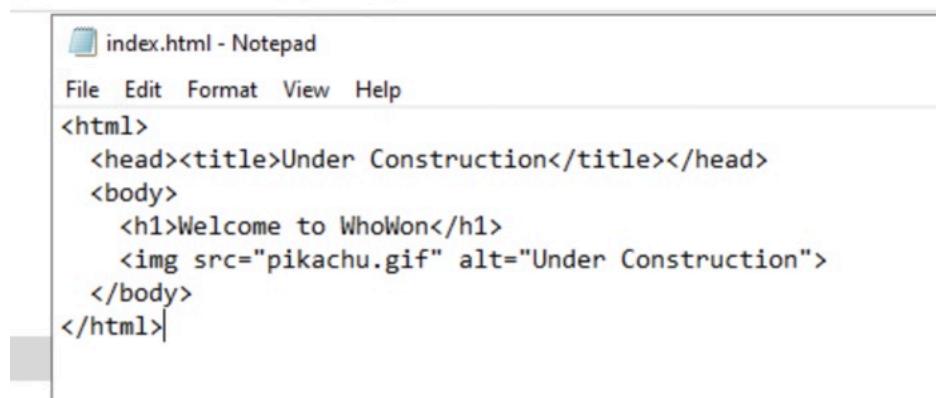


- Once Web Server (IIS) is installed, make your way to the new directory created by Windows IIS (C:\inetpub\wwwroot) in File Explorer.

	Name	Date modified	Type	Size
Quick access	iisstart	4/7/2025 10:52 AM	Microsoft Edge H...	1 KB
Desktop	iisstart	4/7/2025 10:52 AM	PNG File	98 KB
Downloads	index.html	4/7/2025 5:24 PM	Text Document	1 KB
Documents	pikachu	4/7/2025 5:27 PM	GIF File	1,009 KB
Pictures				

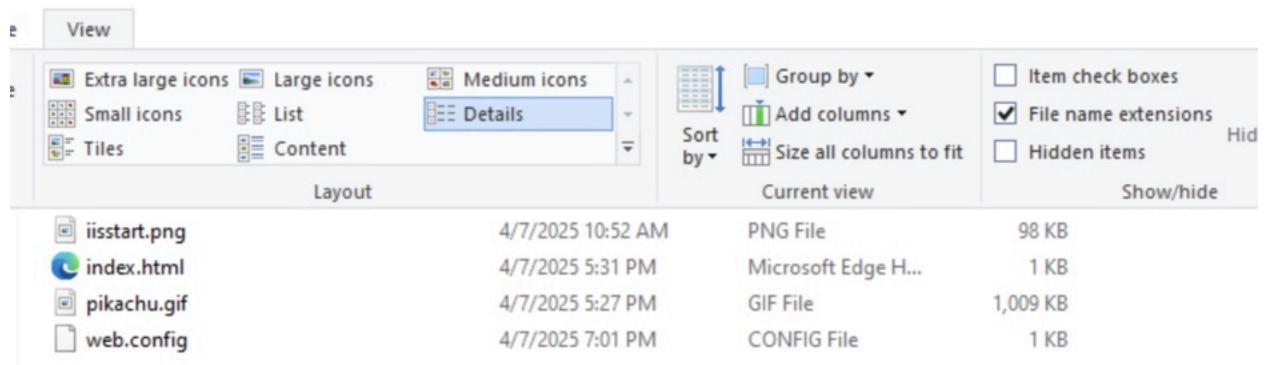
- There should be two files in the “C:\inetpub\wwwroot” directory: iistart.htm and iistart.png
- You will want to create an index.html file and place your “Under Construction” GIF in this directory.

| > This PC > Local Disk (C:) > inetpub > wwwroot



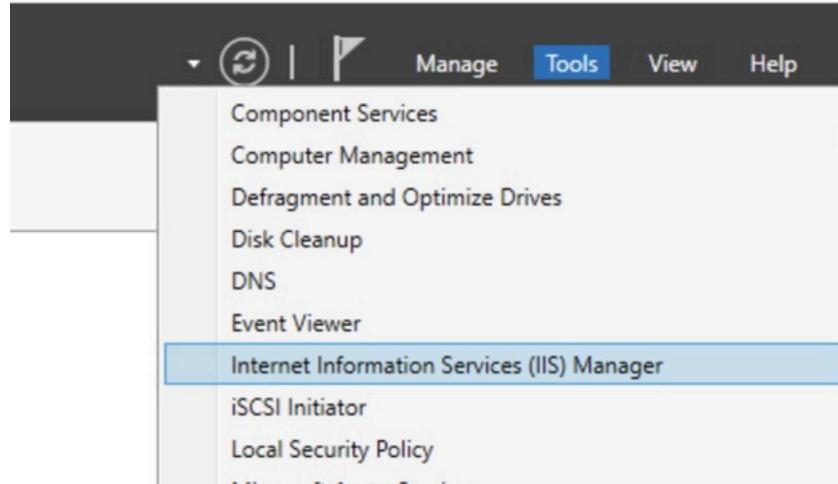
```
<html>
  <head><title>Under Construction</title></head>
  <body>
    <h1>Welcome to WhoWon</h1>
    
  </body>
</html>
```

- The contents of your index.html file should look like this. Make sure to save.

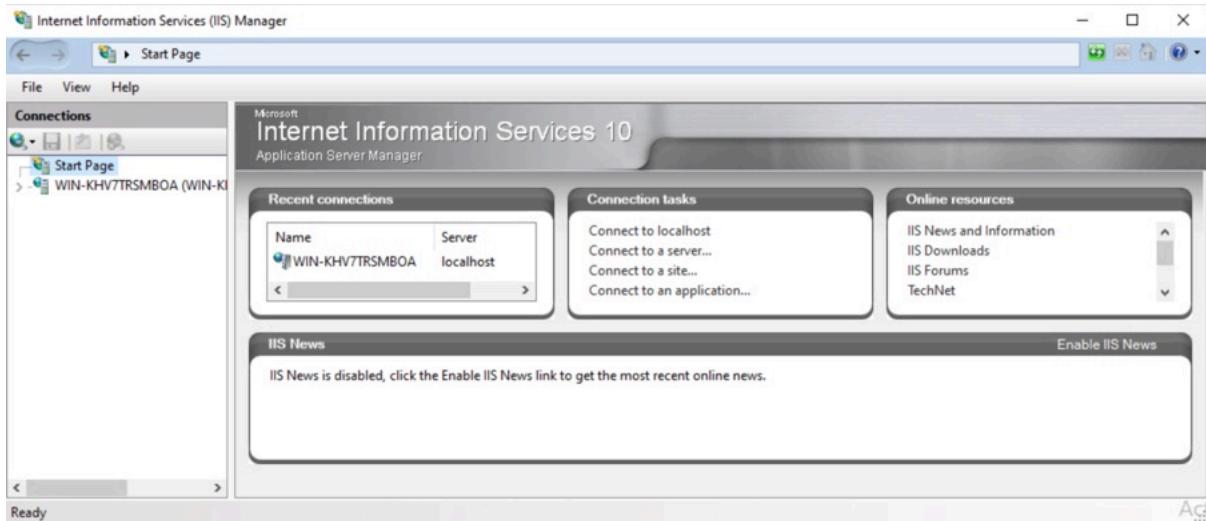


Layout				Current view		Show/hide	
Extra large icons	Large icons	Medium icons	Details	Group by	Add columns	Size all columns to fit	Item check boxes
Small icons	List	Tiles	Content	Sort by			File name extensions
 iisstart.png			4/7/2025 10:52 AM	PNG File	98 KB		
 index.html			4/7/2025 5:31 PM	Microsoft Edge H...	1 KB		
 pikachu.gif			4/7/2025 5:27 PM	GIF File	1,009 KB		
 web.config			4/7/2025 7:01 PM	CONFIG File	1 KB		

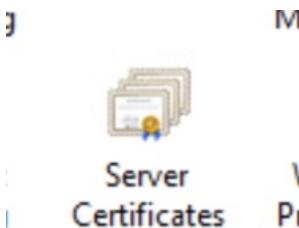
- Make sure to check that index.html is a proper html file. You can do this by going to File Explorer -> View -> Select "File name extensions".



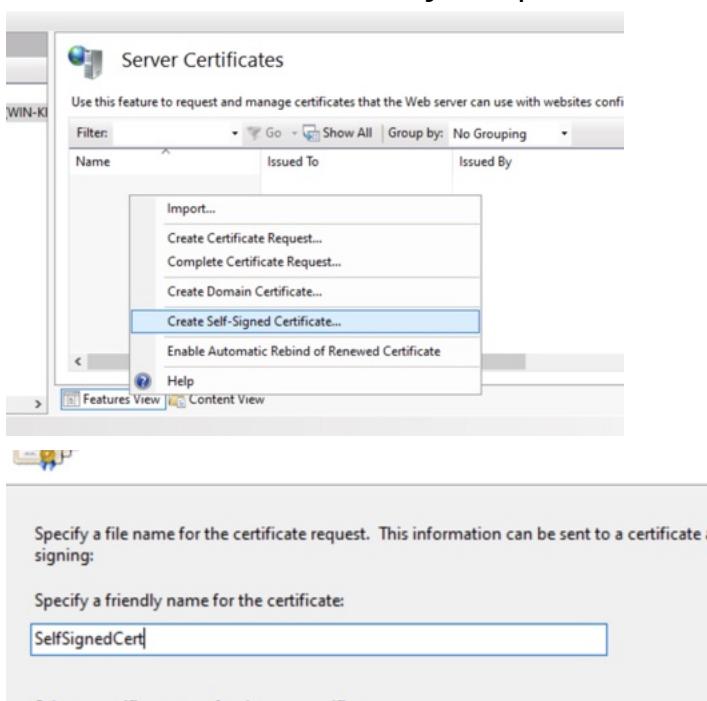
- Make your way back to Server Manager and select Tools -> Internet Information Services (IIS) Manager.



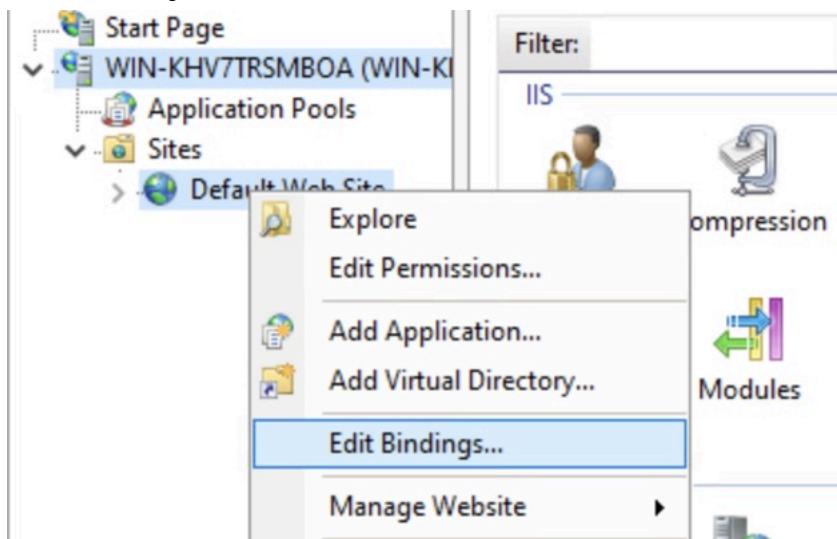
- This is what your IIS Manager should look like. You will want to select your server on the left-side under "Start Page".



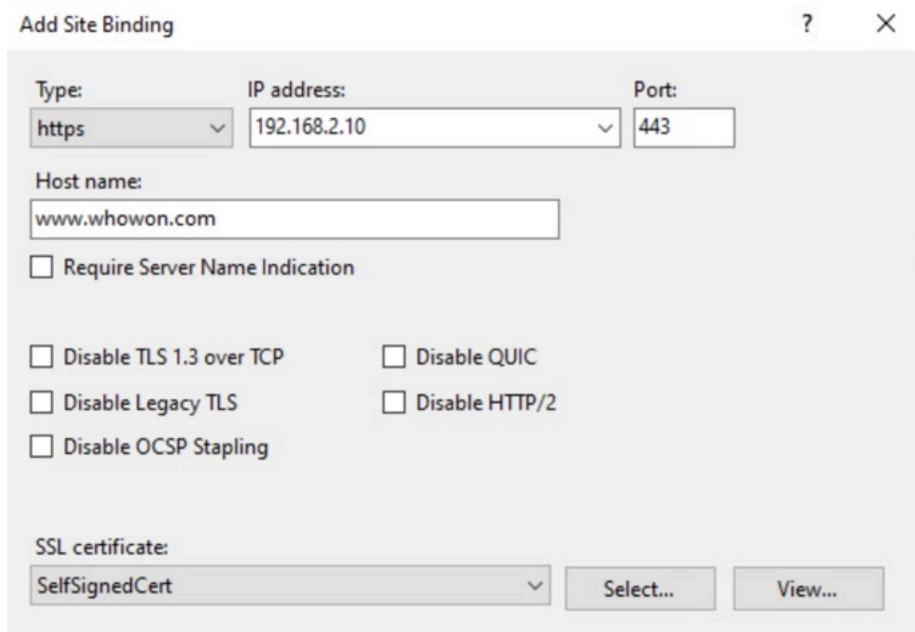
- Once you have your server selected, you should be able to see "Server Certificates" as one of your options.



- Click on Server Certificates, right-click, and select “Create Self-Signed Certificate”.
- Give your certificate a name and hit “OK”.



- In IIS Manager, right click on the Default Web Site under your server and select “Edit Bindings...”.



- Set the Type to: https
- Set IP address to: 192.168.2.10
- Set Port to: 443
- Put in your host name ([www.whowon.com](http://www.whowon.com))
- Select your self-signed certificate (SelfSignedCert) you made earlier for SSL certificate.
- Hit “Apply”.

t Bing

microsoft iis url rewrite module download 

 ALL

 SEARCH

IMAGES

VIDEOS

MAPS

NEWS

COPilot

 M

About 962,000 results



The Official Microsoft IIS Site

<https://www.iis.net/downloads/microsoft/url-rewrite>

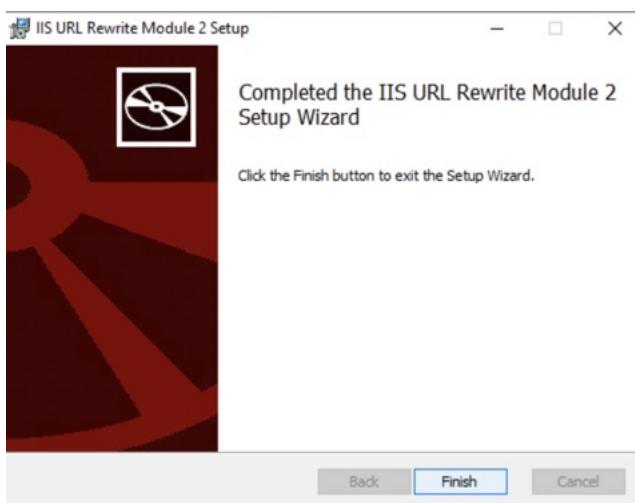
### URL Rewrite : The Official Microsoft IIS Site

URL Rewrite allows Web administrators to easily build powerful rules using rewrite providers written in .NET, regular expression pattern matching, and wildcard mapping to examine ...

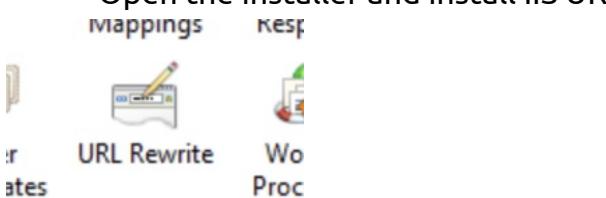
- Next, make your way to a browser and lookup “Microsoft IIS URL Rewrite Module download”.

#### Download URL Rewrite Module 2.1

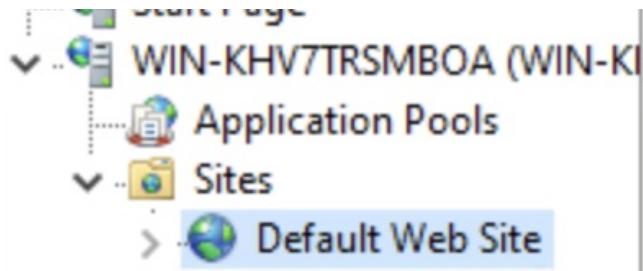
- English: [x86 installer / x64 installer](#)
- Download x64 installer in your language.



- Open the installer and install IIS URL Rewrite Module.



- Now if you make your way to your IIS Manager, you will be able to see the URL Rewrite Module next to Server Certificates.



## URL Rewrite

Provides rewriting capabilities based on rules for the request  
Inbound rules that are applied to the requested URL address:

Name	Input
<	Add Rule(s)...
>	View Server Variables...

- Select your **Default Web Site** in IIS Manager and click on URL Rewrite.
- Then right click and select "Add Rule(s)..."

Select a rule template:

Inbound rules

- Blank rule
- Rule with rewrite map
- Request blocking

Inbound and Outbound Rules

User-friendly URL

Outbound rules

- Blank rule
- Search Engine Optimization (SEO)
- Enforce lowercase URLs

- Select "Blank rule" under Inbound Rules.

Name:

Redirect to HTTPS

Match URL

Requested URL:

Matches the Pattern

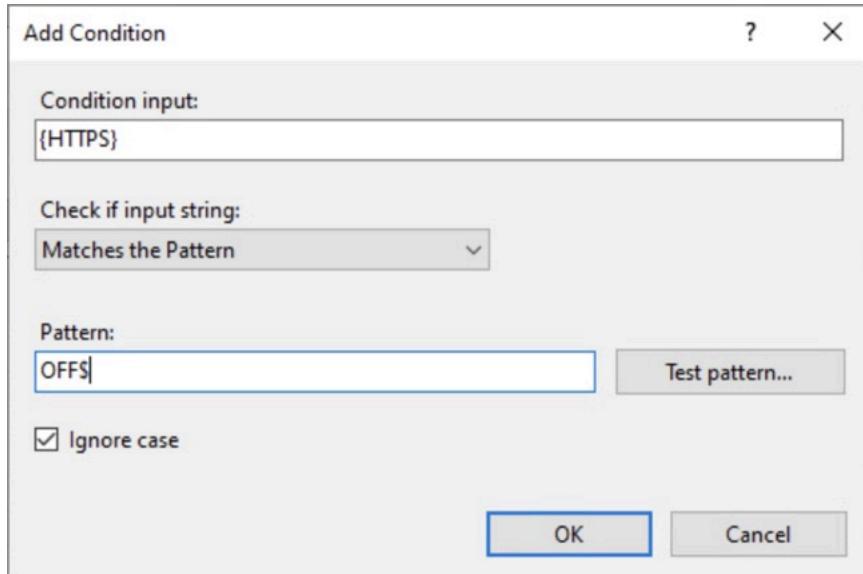
Using:

Regular Expressions

Pattern:

(.\*|)

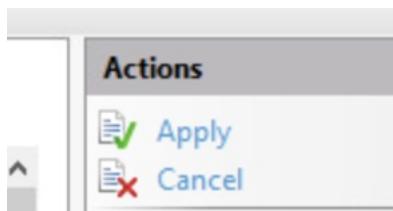
- Give it a name (Redirect HTTPS) and fill in “(.\*)” for the pattern.



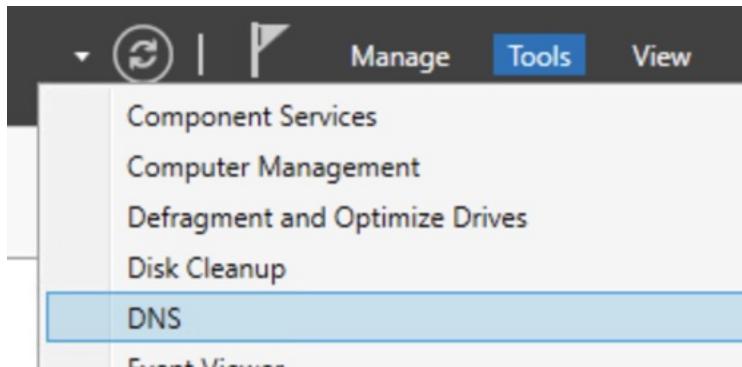
- For Conditions:
  - Hit “Add”
  - Set condition input to: {HTTPS}
  - Set pattern to: ^OFF\$
  - Hit “OK”.



- For Actions:
  - Set action type to: Redirect
  - Type “[https://{{HTTP\\_HOST}}/{R:1}](https://{{HTTP_HOST}}/{R:1})” in the redirect URL.
  - Set redirect type to: Permanent (301)



- Once everything is done, hit “Apply”.



- Next, make your way to Server Manager -> Tools -> DNS.

	Name	Type	Data
WIN-KHV7TRSMBOA	(same as parent folder)	Start of Authority (SOA)	[5], win-khv7trsmboa, ho...
Forward Lookup Zones	(same as parent folder)	Name Server (NS)	win-khv7trsmboa.
whowon.com	(same as parent folder)	Host (A)	192.168.2.10
Reverse Lookup Zones	windows	Host (A)	192.168.2.10
2.168.192.in-addr.arp	www	Host (A)	192.168.2.10
Trust Points	www	Host (A)	10.161.31.4
Conditional Forwarders			

- In Forward Lookup Zones -> whowon.com, you will want to create two new A Hosts with "www" as the host.

**www Properties**

Host (A)

Host (uses parent domain if left blank):

Fully qualified domain name (FQDN):

IP address:

Update associated pointer (PTR) record

**OK**   **Cancel**   **Apply**

**www Properties**

Host (A)

Host (uses parent domain if left blank):

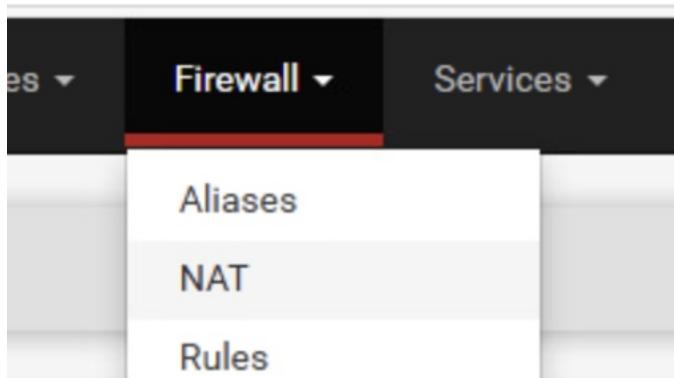
Fully qualified domain name (FQDN):

IP address:

Update associated pointer (PTR) record

**OK**   **Cancel**   **Apply**

- Set one of your A Host IP address to your Windows Server (192.168.2.10) and the other to your WAN IP address (10.161.31.4)



- Now that everything is IIS and DNS Manager is configured, make your way to Firewall -> NAT in pfSense.
- Select “^Add” to create a new NAT rule.

Protocol  Interface

Choose which protocol this rule should ma Choose which inter

---

- Make sure the protocol is set to “TCP” and the interface is set to “WAN”.

Destination  Invert match.

---

- Make sure the destination is set to “WAN address”.

Destination port range

From port To port

Specify the port or port range for the destination of the packet for this mapping. The ‘to’ field may be left empty if only mapping a single port.

---

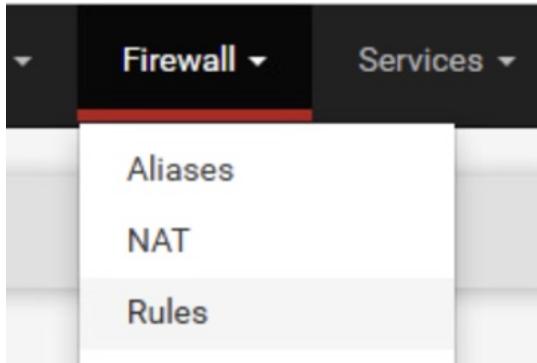
- Make sure the destination port range is from HTTPS to HTTPS (443).

Redirect target IP

---

- Set the redirect target IP to your Windows server IP address (192.168.2.10).

- Hit “Save” and “Apply Changes”.



- Finally, make your way to Firewall -> Rules in pfSense.

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/1.85 MiB	IPv4 UDP	*	*	192.168.2.10	53 (DNS)	*	none	NAT		
<input type="checkbox"/>	✓ 0/1.07 MiB	IPv4 TCP	*	*	192.168.2.10	443 (HTTPS)	*	none	NAT HTTP webserver		
<input type="checkbox"/>	✗ 0/2 KiB	IPv4 TCP	*	*	DMZ subnets	*	*	none	Block inbound WAN to DMZ traffic		
<input type="checkbox"/>	✗ 0/390 B	IPv4 *	*	*	LAN subnets	*	*	none	Do not allow traffic from WAN to LAN		

- In WAN, make sure your NAT rules are prioritized and at the top of the list.

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

I learned how to configure a web server through Windows IIS to host a static HTTPS web server with a qualified domain name. I ran into some configuration errors/issues while doing this project but was able to correct them with the help of Prof. Diesburg.

---

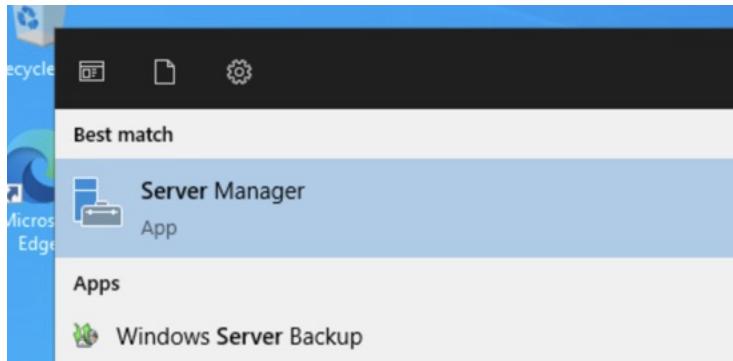
**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.  
<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

# Project 7: Active Directory Setup

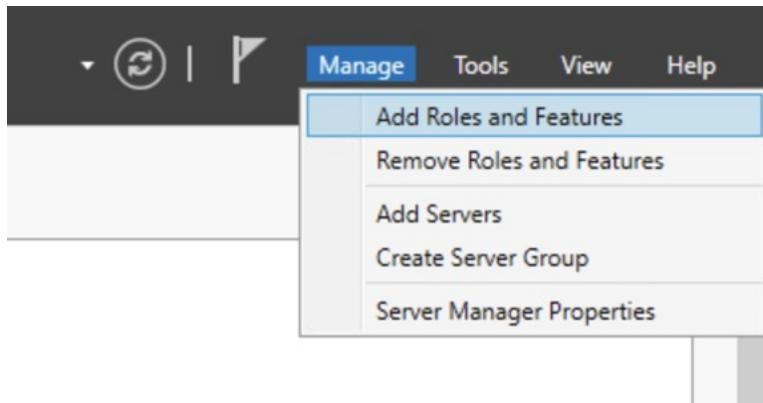
**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

In this project, I will be configuring active directory settings so that multiple users can log into different machines and still be able to access their active directory from before. I expect this project to be straightforward but will not be surprised if I run into some configuration errors.

**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



1. Make your way to Server Manager in your Windows 2022 server.



2. Select "Add Roles and Features" under Manage.

## Select server roles

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

Select one or more roles to install on the selected server.

**Roles**

- Active Directory Certificate Services
- Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server

3. In Server Roles, select “Active Directory Domain Services”.

Confirm installation selections

DESTINATION SERVER  
WIN-KHV7TRSMBOA

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

4. Hit “Next” until you see “Install” and hit it.

The screenshot shows a 'Post-deployment Configuration' window with a yellow warning icon. It displays a message: 'Configuration required for Active Directory Domain Services at WIN-KHV7TRSMBOA' and a link 'Promote this server to a domain controller'. Below the window, a 'Feature installation' status bar is visible.

5. After AD DS is installed, you will see this notification in Server Manager. Click on “Promote this server to a domain controller”.

## Deployment Configuration

TARGET SERVER  
WIN-KHV7TRSMBOA

### Deployment Configuration

- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

ad.net

6. Select “Add a new Forest” and type in your root domain name (ad.net).

## Domain Controller Options

TARG  
WIN-KHV7

### Deployment Configuration

#### Domain Controller Options

- DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select functional level of the new forest and root domain

Forest functional level:

Windows Server 2016

Domain functional level:

Windows Server 2016

Specify domain controller capabilities

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

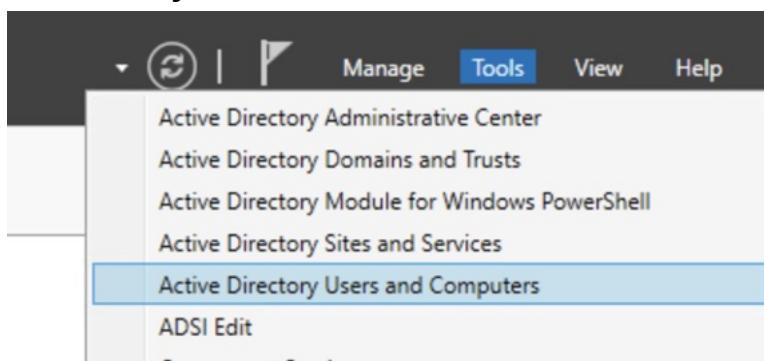
Password:

\*\*\*\*\*

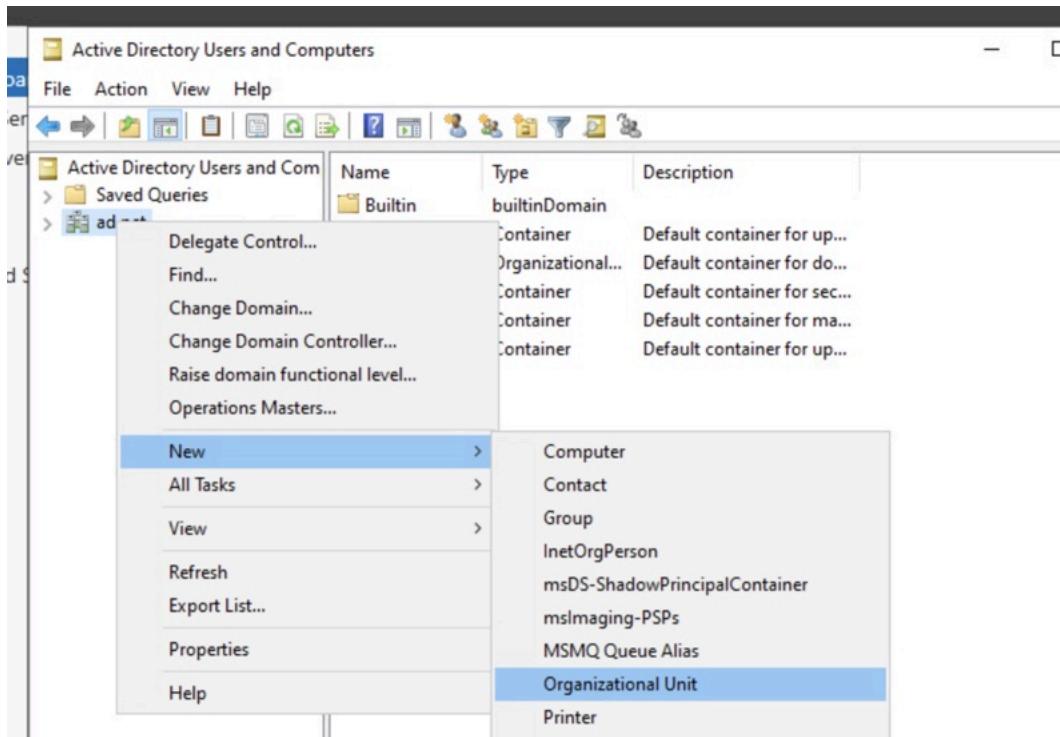
Confirm password:

\*\*\*\*\*

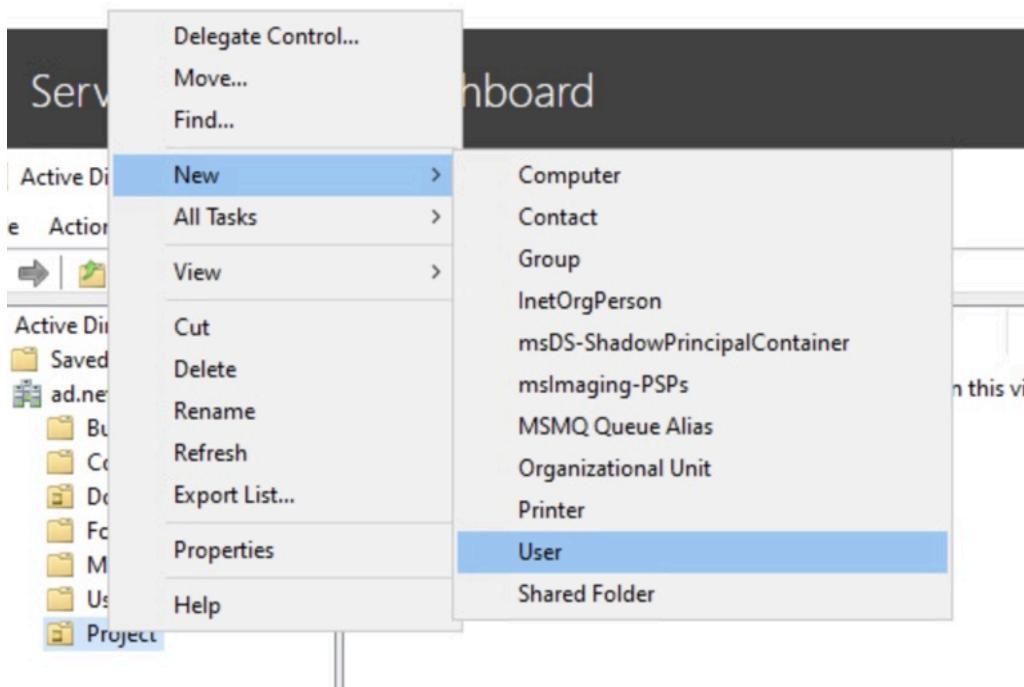
7. In Domain Controller Options, set and confirm your password (Juspen6h). Hit “Next” until you see “Install” and hit it. Once it is done installing, reboot your system.



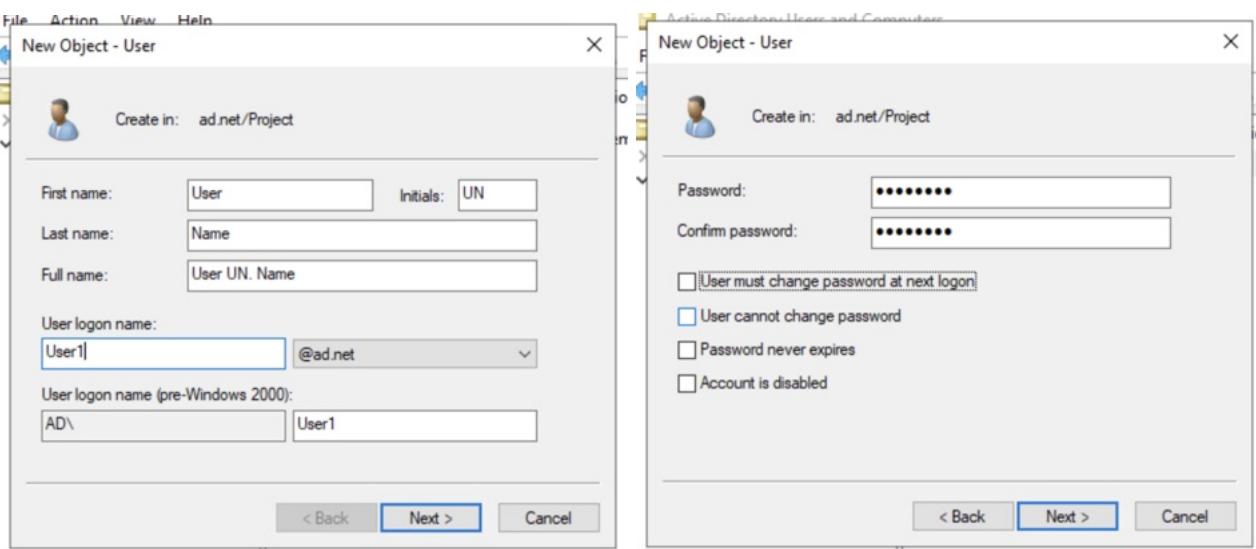
8. In Server manager, select “Active Directory Users and Computers” under Tools.



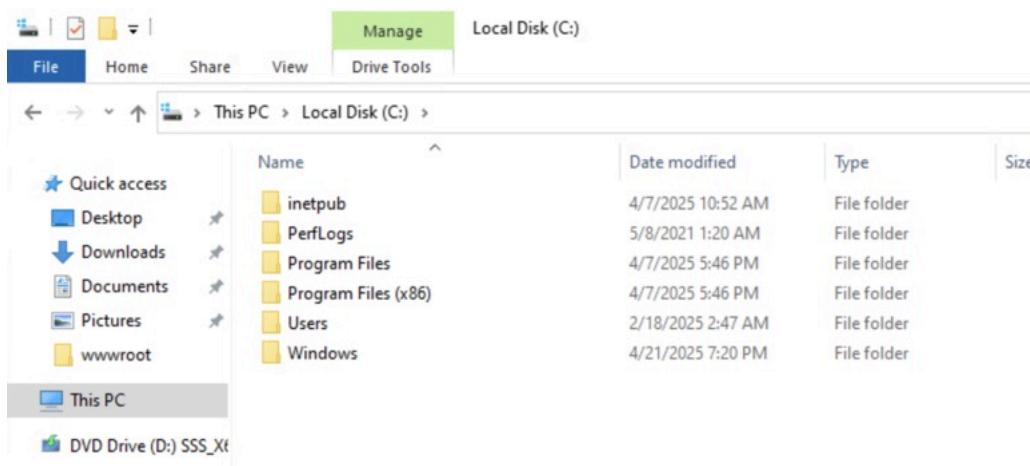
9. Right click on your domain (ad.net) and select New -> Organizational Unit. Give it a name (Project).



10. Right click on the new folder created and select New -> User.



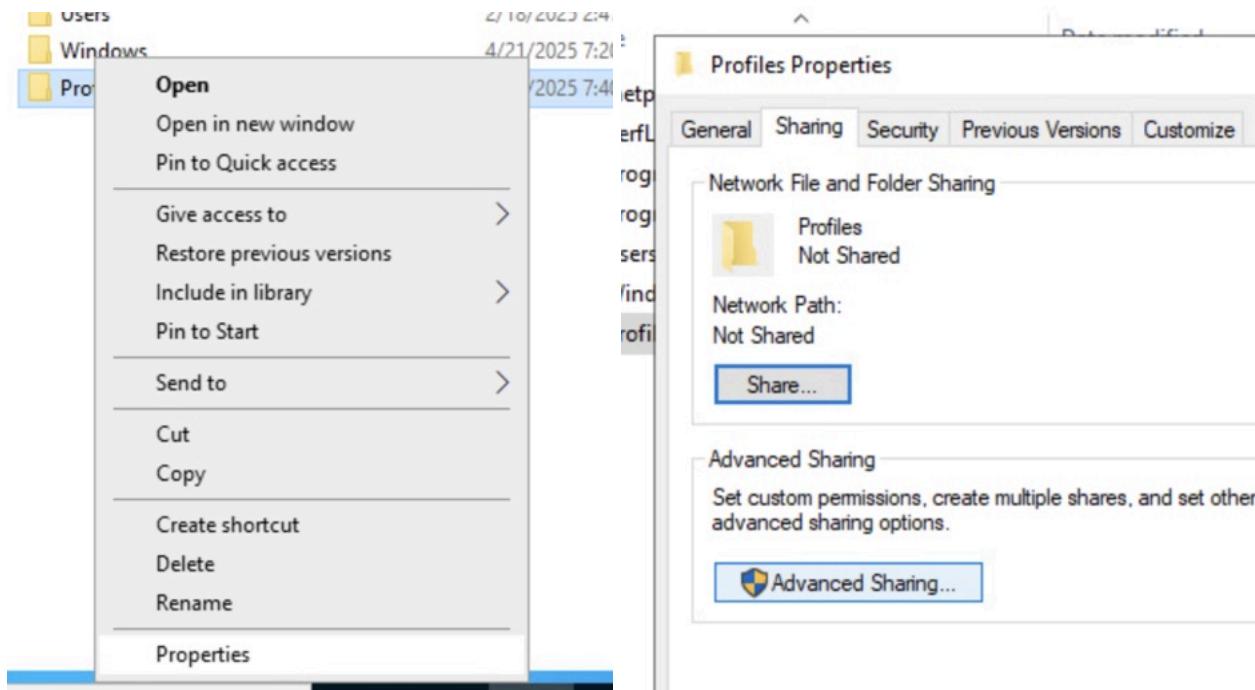
11. Fill in user information and set the password. Repeat steps 10 and 11 to create another user.



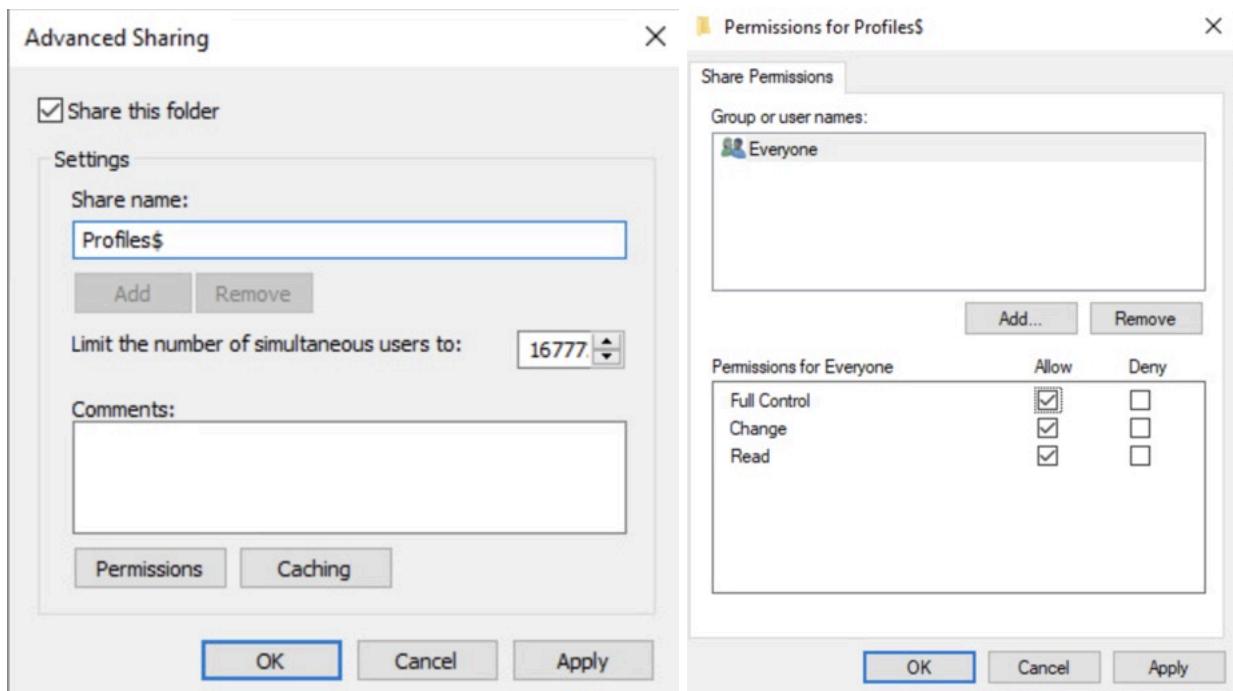
12. Make your way to your local disk on your desktop.

Name	Date modified	Type	Size
inetpub	4/7/2025 10:52 AM	File folder	
PerfLogs	5/8/2021 1:20 AM	File folder	
Program Files	4/7/2025 5:46 PM	File folder	
Program Files (x86)	4/7/2025 5:46 PM	File folder	
Users	2/18/2025 2:47 AM	File folder	
Windows	4/21/2025 7:20 PM	File folder	
Profiles	4/21/2025 7:40 PM	File folder	

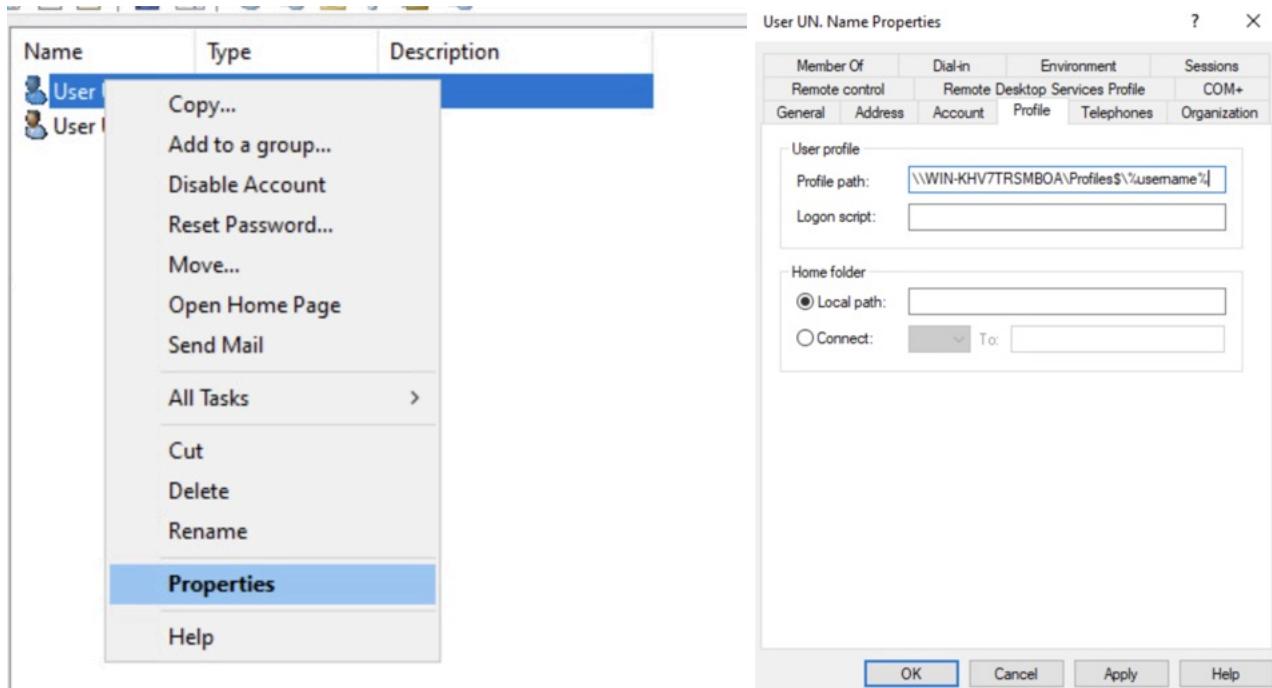
13. Right click and create a new folder called "Profiles".



14. Right click on your new folder and select "Properties". Go to the "Sharing" tab and select "Advanced Sharing...".



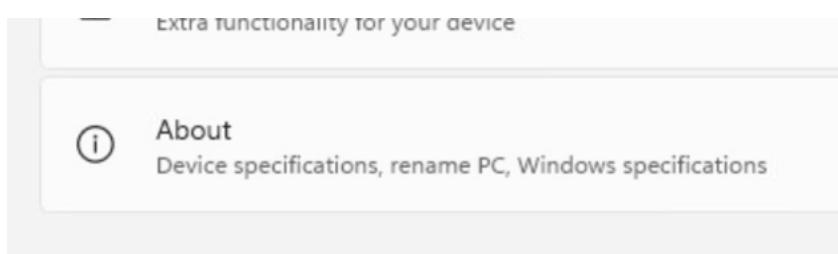
15. Select "Share this folder" and put "Profiles\$" in the share name. The "\$" hides it from casual browsing.  
 16. Click on "Permissions" and make sure everyone is added and has full control. Hit "Apply" and "OK".



17. Make your way back to “Active Directory Users and Computers” under Tools. Right click on one of your users and select “Properties”. In the Profile tab, type in “\\(YourServerName)\\Profiles\$\\%username%” in the profile path.

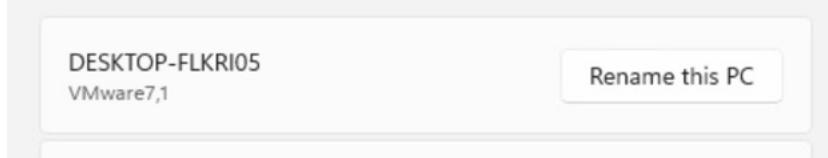
```
C:\Users\Administrator>hostname
WIN-KHV7TRSMBOA
```

HINT: If you do not know your server's name, type in “hostname” in CMD.

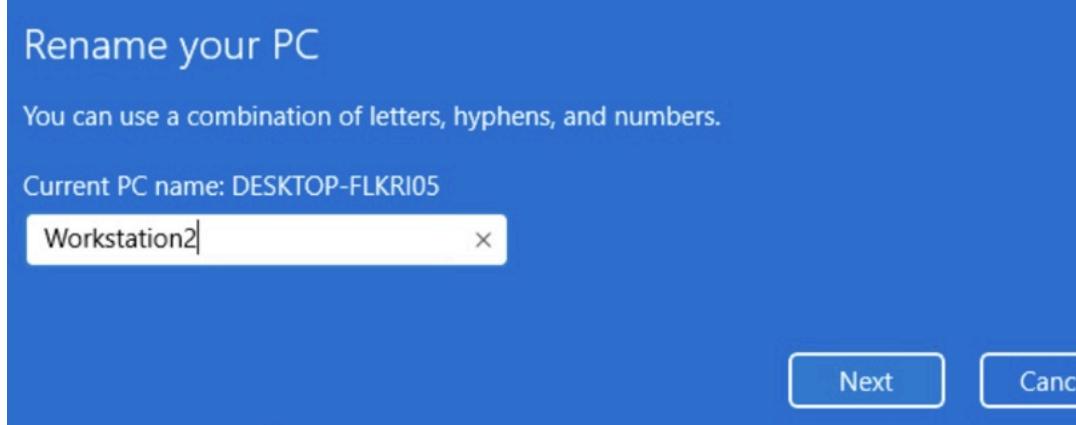


18. Now, make your way to Settings -> System -> About.

**System > About**



19. Click on “Rename this PC”.



20. Give your PC a new name (Workstation1, Workstation2) and reboot. Repeat steps 18-20 for your other machine.

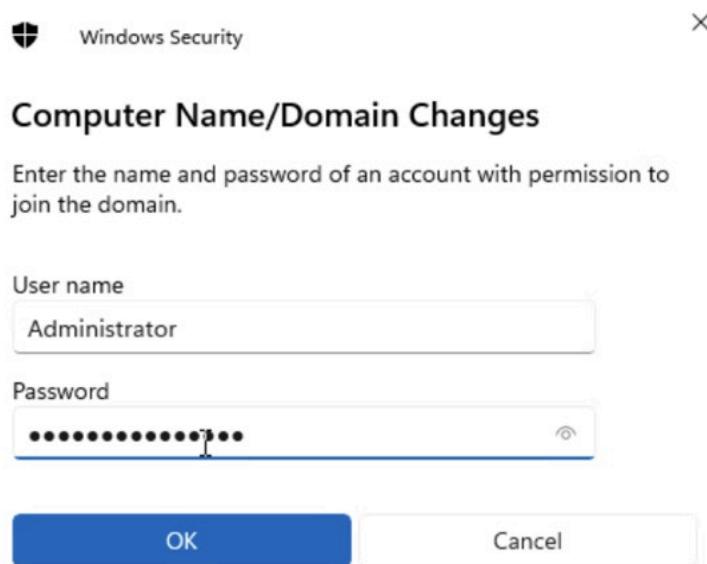
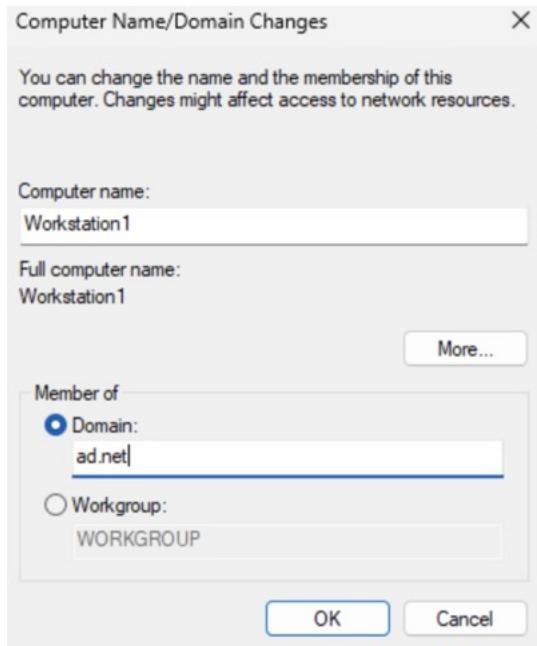
The screenshot shows the "System > About" page. At the top, there are links for "Related links", "Domain or workgroup", "System protection", and "Advanced system settings".

21. In Settings -> System -> About, click on "Domain or workgroup".

The screenshot shows the "Computer Name / Domain Changes" dialog box. The "Computer Name" tab is selected. It displays the following information:

- Icon: A computer monitor icon.
- Text: "Windows uses the following information to identify your computer on the network."
- Section: "Computer description:" with a text input field containing "Workstation1".  
Description: "For example: 'Kitchen Computer' or 'Mary's Computer'."
- Section: "Full computer name:" with the value "Workstation1".
- Section: "Workgroup:" with the value "WORKGROUP".
- Text: "To use a wizard to join a domain or workgroup, click Network ID..." with a "Network ID..." button.
- Text: "To rename this computer or change its domain or workgroup, click Change..." with a "Change..." button.

22. Click on "Change..."



23. Type in your root domain name (ad.net) in the domain. Hit “OK” and enter your administrative user/password to apply changes. Reboot your system and everything should be set up.

---

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

In this project, I learned how to set up an Active Directory Domain Controller to manage user accounts. I created 2 user accounts, configured a shared profile folder, and joined the Windows 11 machines to the domain so users can log into different machines and seamlessly access their active directory from before. The project went as expected and none of my initial expectations were broken.

---

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

<https://woshub.com/add-computer-to-active-directory-domain/#:~:text=name%20and%20an%20access%20the>

# Project 8: Configure a VPN for Remote Workers

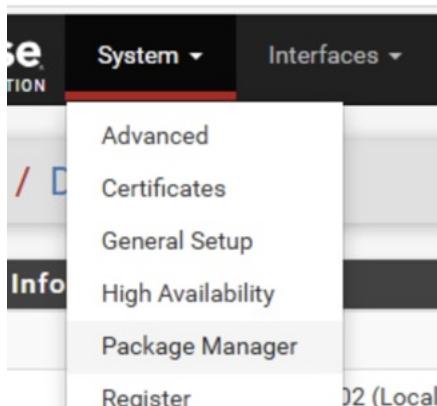
---

**Project Baseline:** This section should include the Topic, Expectations, and Additional Pre-work Notes.

In this project, I will be installing and configuring a VPN in pfSense so that it allows users from outside the organization to obtain an IP address from inside the organization. I will be using WireGuard in this project because it was recommended by my professor. I have used VPNs before but have never configured one myself. I am not too sure what to expect from this project but I will not be surprised if I run into configuration issues.

---

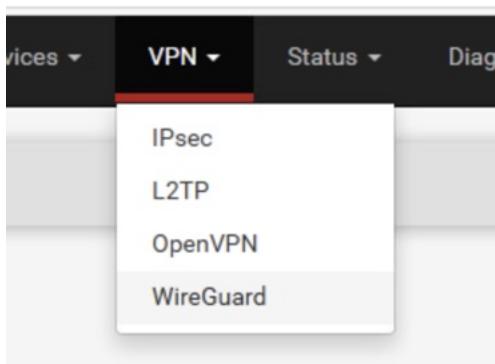
**Project Steps:** This section should cover the steps you took to install the application or create whatever it was that was created. These steps are for your system administration handbook that you can use in the future. Build this section with the future in mind.



1. Log into pfSense and make your way to System -> Package Manager.

A screenshot of the pfSense Package Manager. It shows two tabs at the top: 'Installed Packages' (which is active) and 'Available Packages'. Below is a table titled 'Installed Packages' with columns: Name, Category, Version, and Description. One package is listed: 'WireGuard net 0.2.1'. The description for WireGuard states: 'WireGuard(R) is an extremely simple yet fast and more leaner, and more useful than IPSec, while avoiding the overhead of OpenVPN. WireGuard is designed as a general purpose VPN for many different circumstances. Initially released for the Linux kernel under heavy development, but already it might be ready for industry.' At the bottom right of the table is a blue link labeled '⟳ = Update'.

2. Go to Available Packages and install "WireGuard".



3. Once WireGuard is installed, make your way to VPN -> WireGuard in pfSense.

A screenshot of the WireGuard Tunnels configuration page. The top navigation bar shows 'VPN / WireGuard / Tunnels'. Below it is a toolbar with icons for Tunnels, Peers, Settings, and Status. The main area is titled 'WireGuard Tunnels' and contains a table with one row. The table columns are Name, Description, Public Key, Address / Assignment, Listen Port, Peers, and Actions. The row shows 'tun\_wg0' with 'wg-server' as the description, a long public key, 'VPN (opt2)' as the address, port '51820', and 1 peer. The Actions column has icons for edit, download, and delete. A green button at the bottom right says '+ Add Tunnel'.

4. In the Tunnels tab, click "+Add Tunnel".

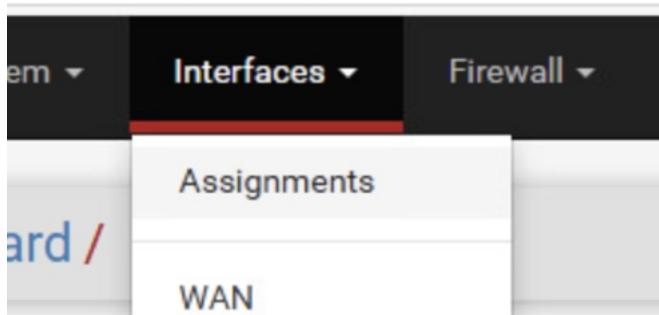
A screenshot of the Tunnel Configuration page for 'tun\_wg0'. The title is 'Tunnel Configuration (tun\_wg0)'. It has sections for Enable (checkbox checked), Description ('wg-server'), Listen Port ('51820'), and Interface Keys. The Interface Keys section shows a private key field with placeholder dots, a public key field with a long string, and a 'Generate' button. There is also a 'New Keys' link.

5. Give your tunnel a description and click on "Generate" in Interface Keys.

A screenshot of the General Settings page. The top navigation bar shows 'VPN / WireGuard / Settings'. Below it is a toolbar with Tunnels, Peers, Settings (selected), and Status. The main area is titled 'General Settings' and contains an 'Enable' checkbox which is checked. A note below it states 'Note: WireGuard cannot be disabled when on'.

6. Make sure that WireGuard is enabled in the Settings.

vg/vpn\_wg\_settings.php



7. Now make your way to Interfaces -> Assignments in pfSense.

A screenshot of the 'Interface Assignments' page in pfSense. The top navigation bar shows 'Interfaces / Interface Assignments'. Below it is a table with columns 'Interface' and 'Network port'. The table rows are: WAN (vmx0), LAN (vmx1), DMZ (vmx2), VPN (tun\_wg0). Each row has a dropdown arrow and a red 'Delete' button.

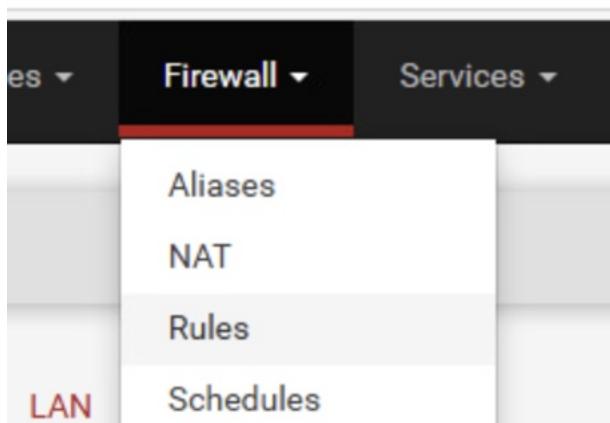
8. You should see your new WireGuard interface listed with a "+Add" button next to it. Click on "+Add" then click on your new interface to make configurations.

A screenshot of the 'General Configuration' page for the 'VPN' interface. It includes fields for 'Enable' (checked), 'Description' (VPN), 'IPv4 Configuration Type' (Static IPv4), and 'IPv6 Configuration Type' (None).

9. Give your interface the name VPN and make sure that IPv4 configuration type is set to "Static IPv4"

A screenshot of the 'Static IPv4 Configuration' page. It shows an 'IPv4 Address' field containing '192.168.3.1' and a 'IPv4 Upstream gateway' field containing 'None'. A green button at the bottom right says '+ Add a new gateway'.

10. Set the static IPv4 address to "192.168.3.1/24". Hit "Save".



## 11. Make your way to Firewall -> Rules in pfSense.

**Edit Firewall Rule**

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	UDP
Choose which IP protocol this rule should match.	

Activate Window

## 12. Make a new rule in WAN with UDP protocol.

**Destination**

Destination	<input type="checkbox"/> Invert match	VPN address	Destination
Destination Port Range	any	From	any
	Custom	To	Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a			

## 13. Make sure that the destination is set to the VPN address. Hit "Save".

Floating	WireGuard	WAN	LAN	DMZ	VPN					
<b>Rules (Drag to Change Order)</b>										
Actions	Description	Schedule	Queue	Gateway	Port	Destination	Source	Protocol	States	

## 14. Make your way to the new VPN tab in Rules. Click "+Add".

**Edit Firewall Rule**

<b>Action</b>	<input type="text" value="Pass"/> <input type="button" value="▼"/>
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICM) whereas with block the packet is dropped silently. In either case, the original packet is dis-	
<b>Disabled</b>	<input type="checkbox"/> <input type="text" value="Disable this rule"/> Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="text" value="VPN"/> <input type="button" value="▼"/> Choose the interface from which packets must come to match this rule.
<b>Address Family</b>	<input type="text" value="IPv4"/> <input type="button" value="▼"/> Select the Internet Protocol version this rule applies to.
<b>Protocol</b>	<input type="text" value="TCP"/> <input type="button" value="▼"/> Choose which IP protocol this rule should match.

15. Make sure the action is set to “Pass” and the interface is set to “VPN”.

<b>Source</b>	
<b>Source</b>	<input type="checkbox"/> Invert match <input type="text" value="Network"/> <input type="button" value="▼"/> <input type="text" value="192.168.3.0"/> <input type="button" value="/"/> <input type="text" value="24"/> <input type="button" value="▼"/>
<input type="button" value="Display Advanced"/> The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.	
<b>Destination</b>	
<b>Destination</b>	<input type="checkbox"/> Invert match <input type="text" value="DMZ subnets"/> <input type="button" value="▼"/> <input type="text" value="Destination Address"/> <input type="button" value="/"/> <input type="button" value="▼"/>
<b>Destination Port Range</b>	<input type="text" value="any"/> From <input type="text" value="Custom"/> To <input type="text" value="any"/> To <input type="text" value="Custom"/>
Specify the destination port or port range for this rule. The “To” field may be left empty if only filtering a single port.	

16. Set the source to “192.168.3.0/24” and the destination to “DMZ subnets”. Hit “Save”.

**Edit Firewall Rule**

<b>Action</b>	<input type="button" value="Block"/>
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable) whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="button" value="VPN"/>
Choose the interface from which packets must come to match this rule.	
<b>Address Family</b>	<input type="button" value="IPv4"/>
Select the Internet Protocol version this rule applies to.	
<b>Protocol</b>	<input type="button" value="TCP"/>
Choose which IP protocol this rule should match.	

17. Add another rule. Make sure that the action is set to “Block” and the interface is “VPN.”

**Source**

<b>Source</b>	<input type="checkbox"/> Invert match	<input type="button" value="Network"/>	192.168.3.0	/ 24
<input type="button" value="Display Advanced"/>				
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.				

**Destination**

<b>Destination</b>	<input type="checkbox"/> Invert match	<input type="button" value="LAN subnets"/>	<input type="button" value="Destination Address"/>	
<b>Destination Port Range</b>	any	any	any	
From	Custom	To	Custom	
Specify the destination port or port range for this rule. The “To” field may be left empty if only filtering a single port.				

18. Set the source to “192.168.3.0/24” and the destination to “LAN subnets”. Hit “Save”.

Microsoft Bing

wireguard download

ALL SEARCH VIDEOS IMAGES MAPS NEWS SHOPPING

WireGuard

Available On

wireguard.com Google Play

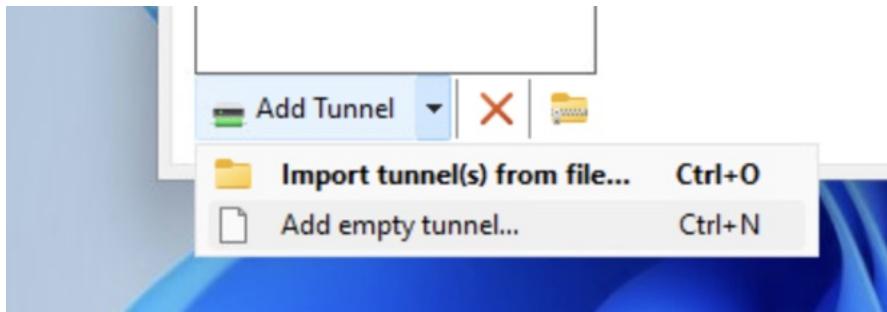
WireGuard

https://www.wireguard.com/install/ Software · Tools · WireGuard Development ...

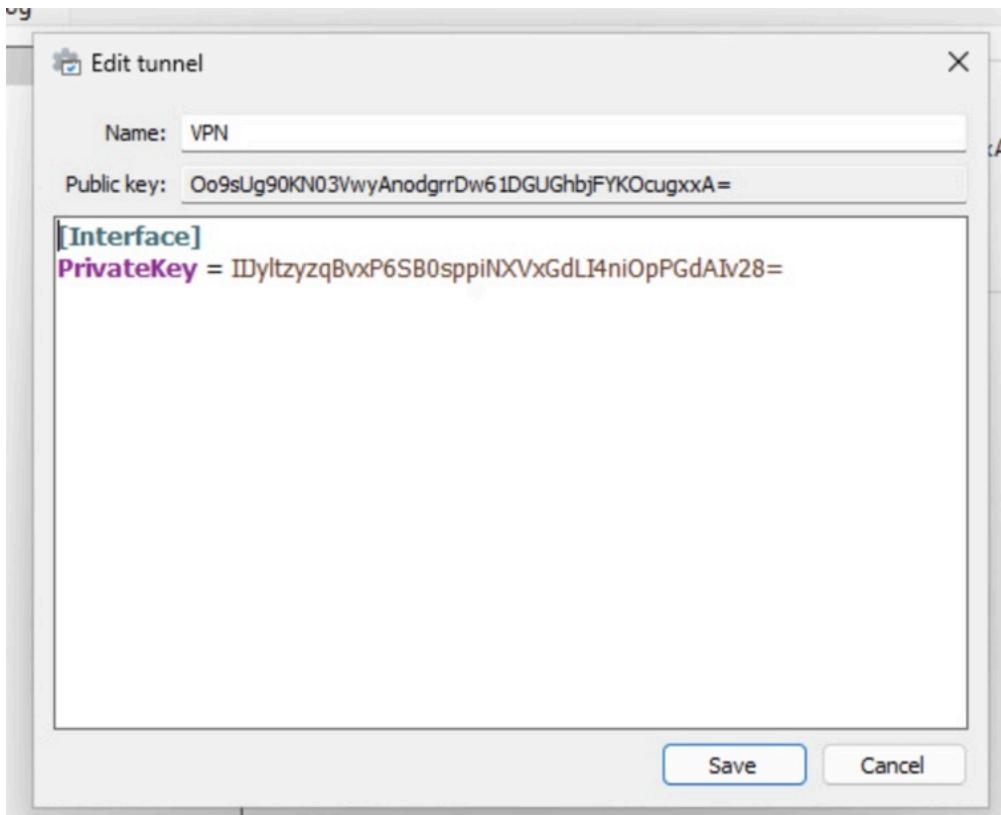
WireGuard is a fast and modern VPN designed to provide ease of use and high performance. It available for Windows, Linux, Ubuntu 20.04, Debian, AlmaLinux, Rocky Linux, CentOS an...

Download

19. Next, log into your WAN desktop and download WireGuard from your browser.



20. Open WireGuard and select “Add empty tunnel...” on the bottom left.



21. Name your tunnel (VPN) and copy the public key to use in the next steps.

A screenshot of the pfSense WebUI under the "VPN" section, specifically the "WireGuard Peers" table. The "Peers" tab is selected. The table has columns: Description, Public key, Tunnel, Allowed IPs, Endpoint : Port, and Actions. One row is present: "project" with Public key "Oo9sUg90KN03VwyA...", Tunnel "tun\_wg0", Allowed IPs "192.168.3.2/32", and Endpoint : Port "Dynamic". The Actions column shows edit, copy, and delete icons. A green "Add Peer" button is located at the bottom right of the table.

22. Log back into pfSense and make your way to VPN -> WireGuard -> Peers. Click “Add Peer”.

Default is empty (disabled).

**Public Key** Oo9sUg90KN03VwyAnodgrDw61DGUGhbjFYK0cugxxA=

WireGuard public key for this peer.

23. Copy and paste the public key from step 20.

The screenshot shows the 'Address Configuration' screen with the 'Allowed IPs' section selected. A hint at the top states: 'Hint Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries must list multiple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.' Below this, there is a table with one row. The first column is 'Allowed IPs' with the value '192.168.3.2 / 32'. The second column is 'Description' with the value 'IPv4 or IPv6 subnet or host reachable via this peer.'. At the bottom left is a green button labeled '+ Add Allowed IP'.

Allowed IPs	Description
192.168.3.2 / 32	IPv4 or IPv6 subnet or host reachable via this peer.

24. Type in "192.168.3.2/32" in Allowed IPs. Make sure to hit "Save" and "Apply Changes".

**Project Reflection:** What did you learn and how did you learn it? Did anything break your initial expectations outlined above?

In this project, I learned how to install and set up a VPN so that remote users can obtain IP addresses from outside the network. I didn't know what to expect when starting the project but I found it to be pretty straightforward. I ran into some configuration issues with WireGuard in pfSense but it was because it was not automatically enabled in settings.

**Project Resources:** In this section I will steal the resources that you have linked/provided. Additionally, I will add any additional resources I used here.

<https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html#figure-general-information-screen>

<https://docs.netgate.com/pfsense/en/latest/recipes/wireguard-ra.html>

# Appendix

This course taught me several important skills that will be useful in real-world IT environments. The three that I thought were the most important skills I learned are setting up virtual machines and servers, configuring DNS, and using pfSense to manage networks.

First, I learned how to set up virtual machines and install systems like Windows Server 2022, Linux servers, and Windows 11 desktops. I also learned how to set up Active Directory on the Windows Server, join machines to the domain, and create and manage users. This gave me a solid understanding of how network systems are built and how different machines are connected and managed through centralized authentication.

Secondly, I became much more comfortable with DNS. I learned how to configure DNS records, connect domain names to static IP addresses, and set up a DNS server for local testing. I got practice assigning domains to HTTPS servers and troubleshooting name resolution problems. Before this course, I didn't understand DNS at all, but now I have a good grasp of how it works and how to set it up properly.

Last of all, I learned how to use pfSense to manage networks. I was able to create firewall rules, set up VPNs, and isolate different parts of a network using subnets. I learned how pfSense can act as a router, DNS resolver, and firewall all in one. This helped me understand how network security is configured and how traffic is controlled between devices and services.

Overall, this class was very helpful and gave me real hands-on experience with system administration. I found the configuration hints provided with the projects to be a huge help for me, especially when something didn't work right away. I don't have any major suggestions for improvement, but I do recommend continuing to include these hints and adding examples of common mistakes to avoid. The little bit of extra guidance made it easier for me to troubleshoot and understand what was going on.