Exercise 1 - Remote Access Network Services

Every day, many network services and protocols are used. You will learn how to install and configure DNS, DHCP, FTP, and other well-known services in this practice.

Connectionless Vs. Connection-Oriented Services

Network services are used to make it easier for certain network applications, such as email and database servers, to communicate with one another. These unique network services operate at the OSI model's application layer. Different services can be distinguished by their name, port (e.g., 21, 443, 80...), and protocol (UDP or TCP).

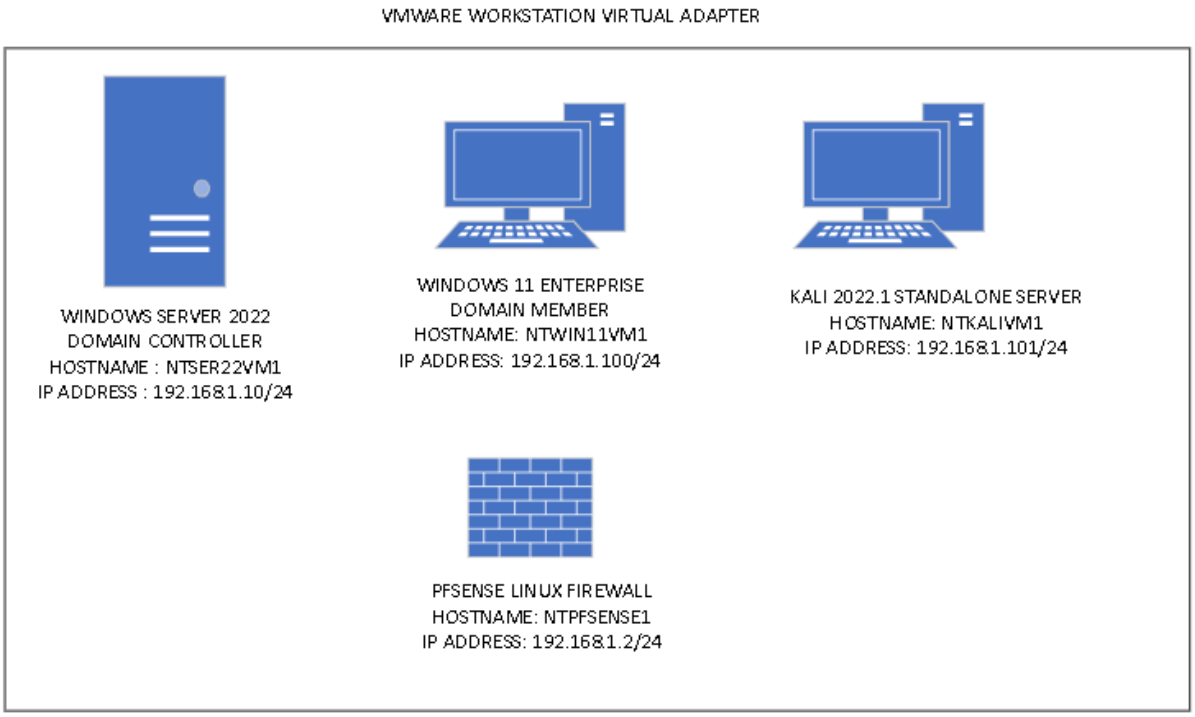
Transmission Control Protocol (TCP) is a connection-oriented protocol that stands for Transmission Control Protocol. This means that data cannot be transmitted until communication has been established. It is built on acknowledgments and sequencing, and it includes mistake checking and correction. It is a trustworthy protocol. UDP, on the other hand, stands for User Datagram Protocol, and it's a connectionless protocol. It is unreliable because it lacks acknowledgments and error checking. UDP is faster than TC because of these features.

- Examples of TCP services are FTP, HTTP, HTTPS and SMTP
- Examples of UDP services are DNS and SYSLOG

In this exercise,

1. Install and Configure FTP Server Role on Windows Server
2. Access Share Folder using SMB Protocol
3. Access Pfsense Firewall using SSH Protocol
4. Examine and Configure DNS Server on Domain Controller
5. Configure DHCP Server on Pfsense Firewall

Topology



DOMAIN = networktute.com

- NTPFSENSE1 = Linux - Virtual Firewall)
- NTSER22VM1 = Windows Server 2022 – Domain Controller
- NTWIN11VM1 = Windows 11 – Domain Member
- NTKALIVM1 = Kali 2022.1 - Standalone Server

Prerequisite

- *VMware Workstation 16 Pro*
    - When making this tutorial, we used the “Windows Server 2019” VM Template and “Windows 10 & later” VM Template. Since VMware didn’t have the updated templates.
- *Microsoft Windows Server 2022*
- *Microsoft Windows 11*
- *PFSense Linux Firewall*

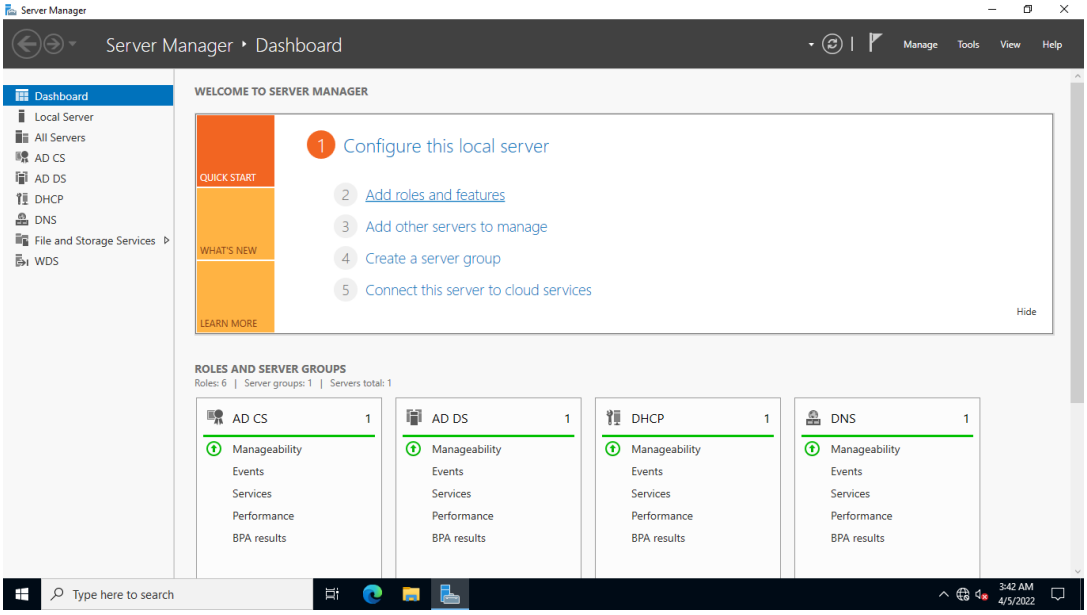
Task 1: Install and Configure FTP Server Role on Windows Server

FTP is a protocol for copying and transferring files between servers, typically the file server and the file client. It employs two ports and is based on TCP. The data transfer protocol TCP 20 is utilized, and the connection control protocol TCP 21 is used. Because the data is transferred in clear text format, it is not a secure protocol. In practice, you should always use Secure File Transfer Protocol (SFTP) instead of FTP

because SFTP runs over SSL and allows for protected data transfer. It's also a TCP protocol that runs on port 22.

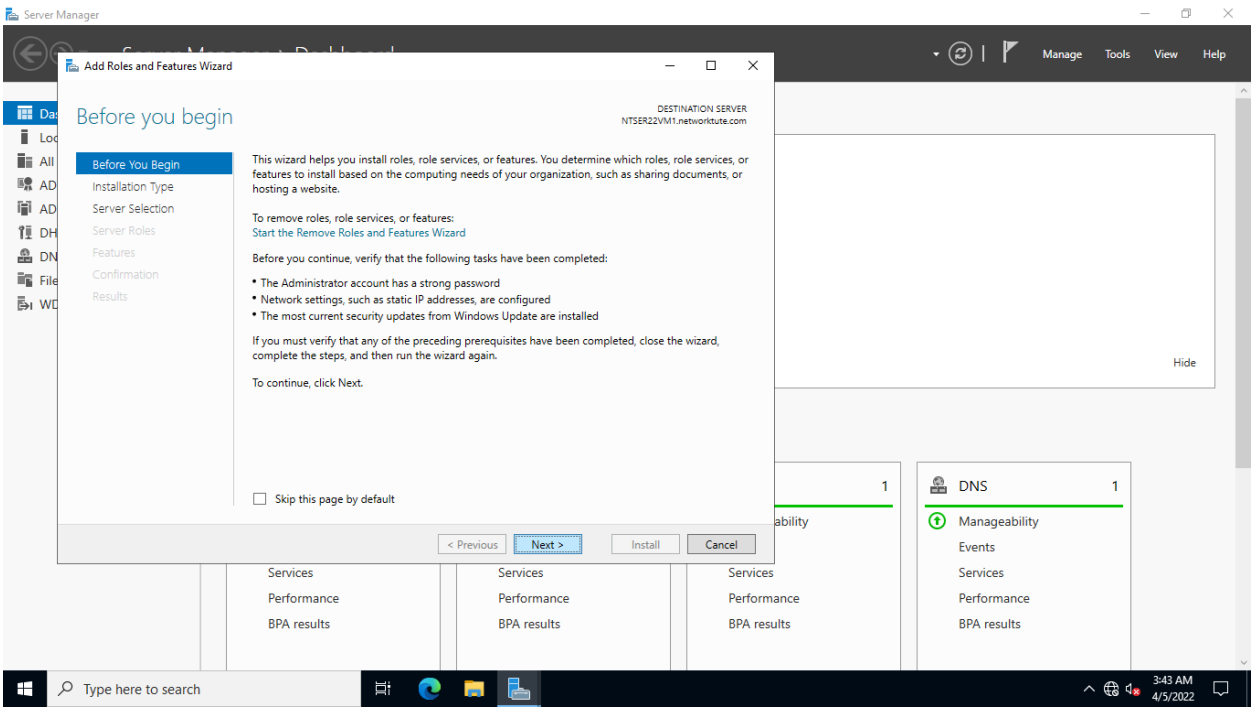
Step 1:

Connect to **NTSER22VM1**. From the **Server Manager** > **Dashboard** window, click Add roles and features.



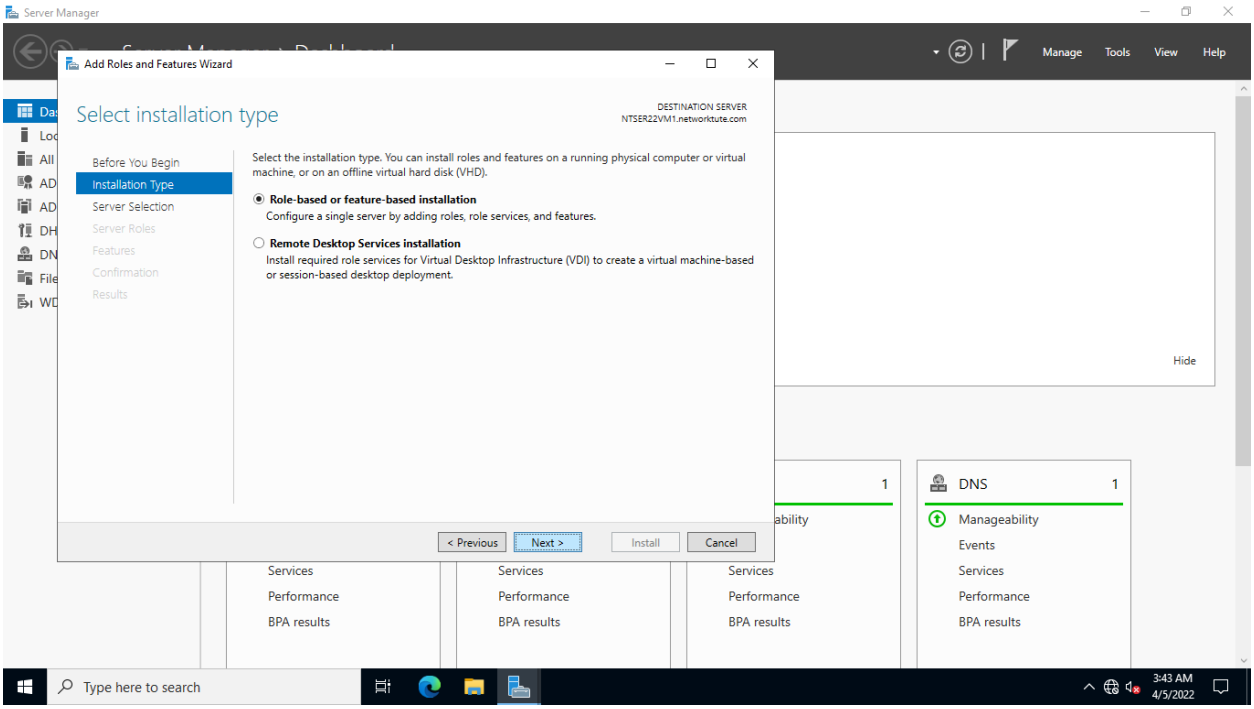
Step 2:

In the **Add Roles** and **Features Wizard** - **Before you begin** page, select Next.



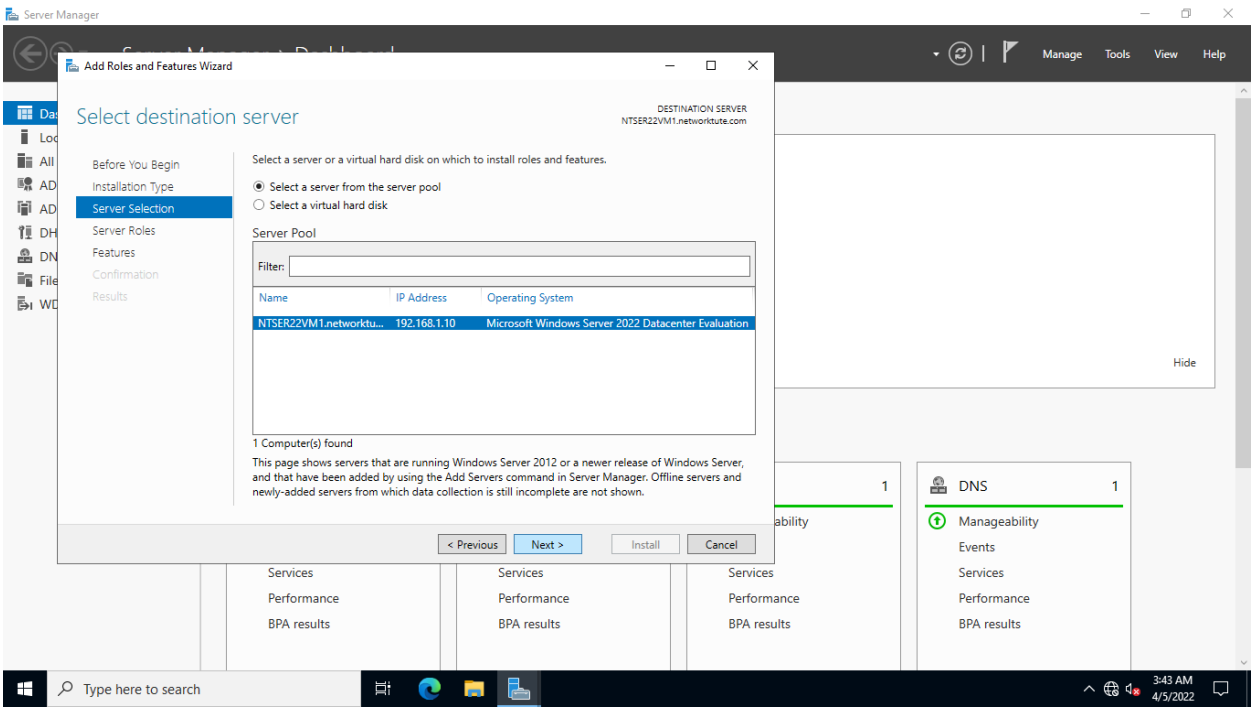
Step 3:

In the **Select installation type** page, leave the default selection and click Next



Step 4:

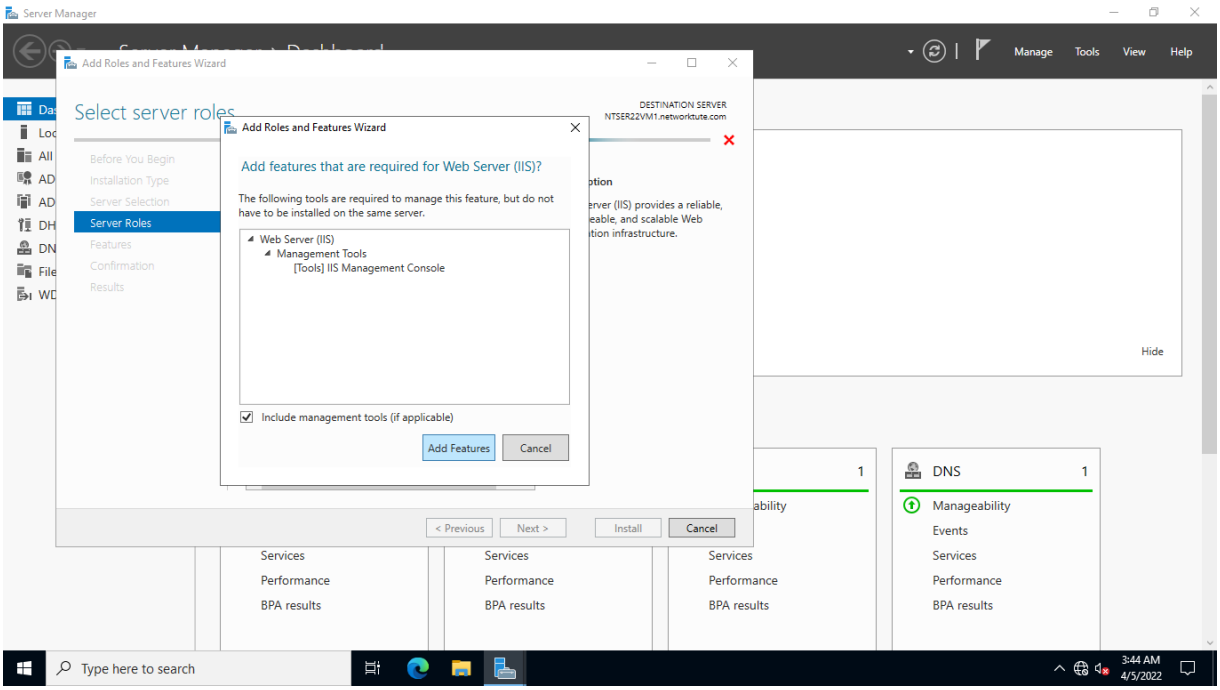
Click **Next** on the **Select destination server** page.



Step 5:

On the **Select server roles** page, select **Web Server (IIS).**

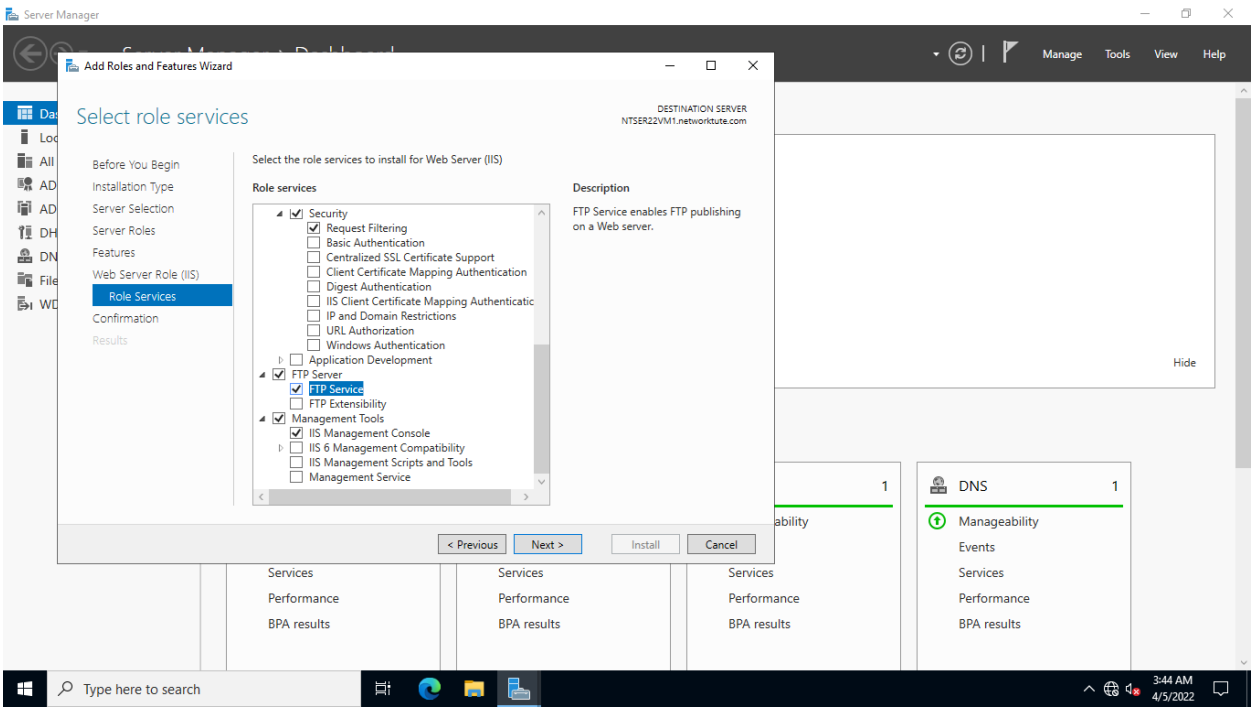
Click **Add Features** on the **Add Roles and Features Wizard** pop-up window. Click **Next**.



Step 6:

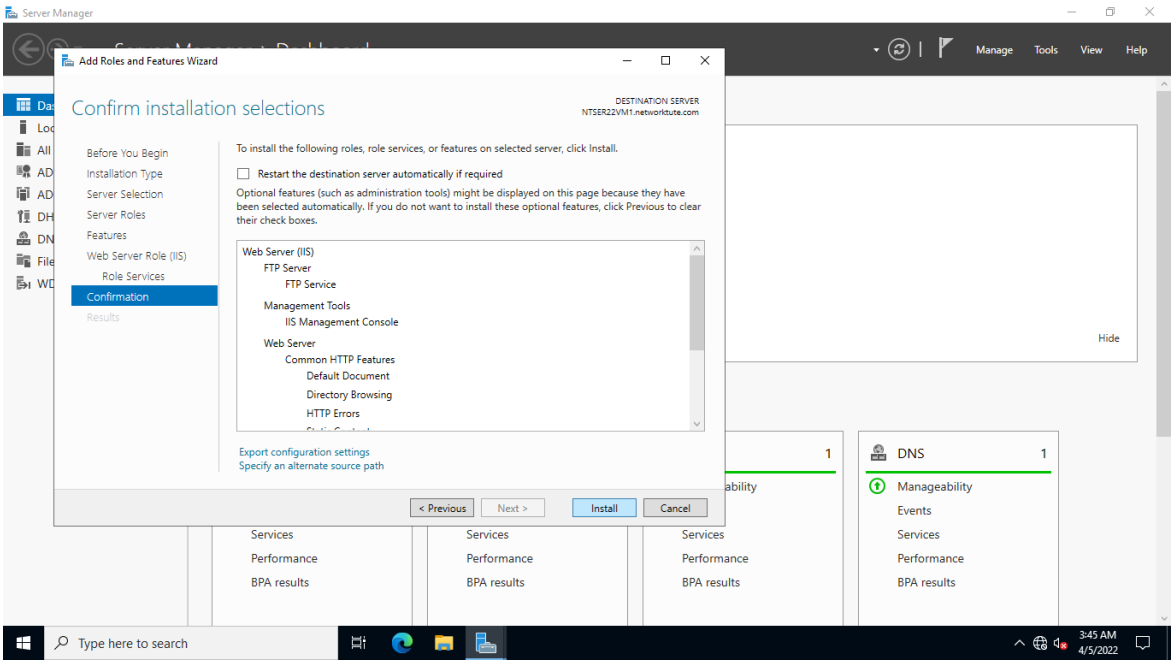
Click **Next** on the **Select features** and **Web Server Role** (**IIS**) page.

On the **Select role services** page, enable **FTP Server** and click **Next.**



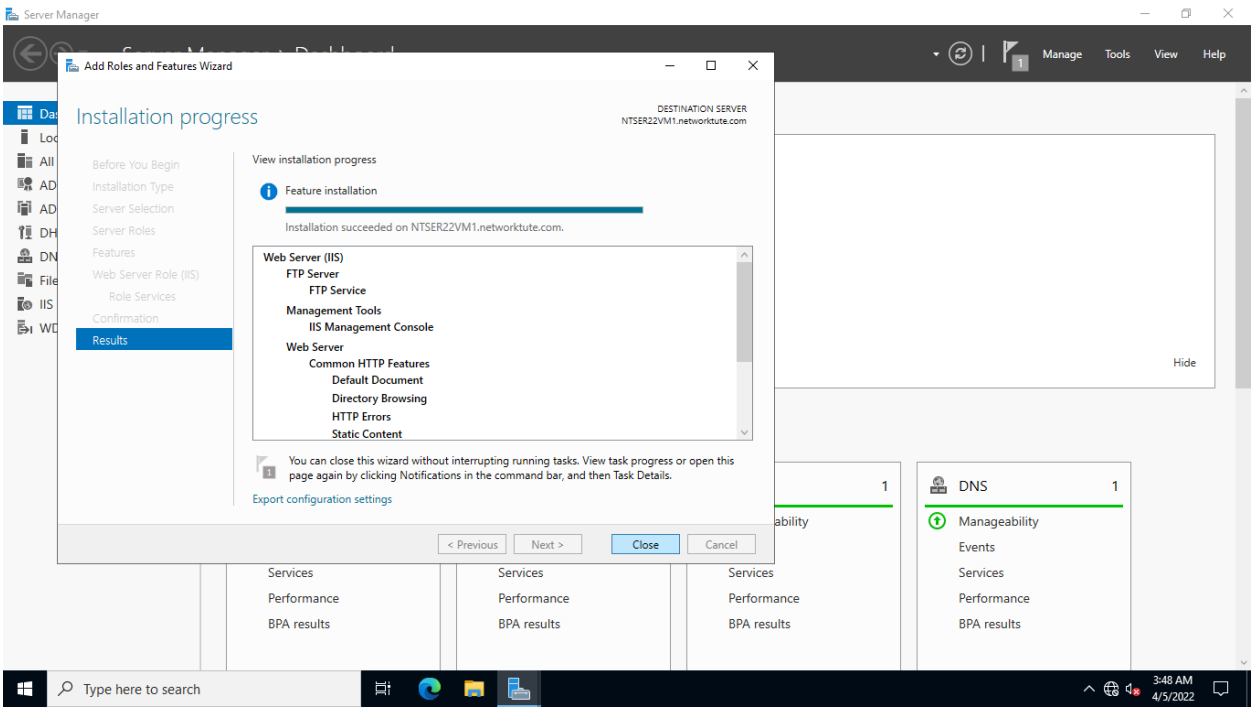
Step 7:

On the **Confirm installation selections** page, click **Install**.



Step 8:

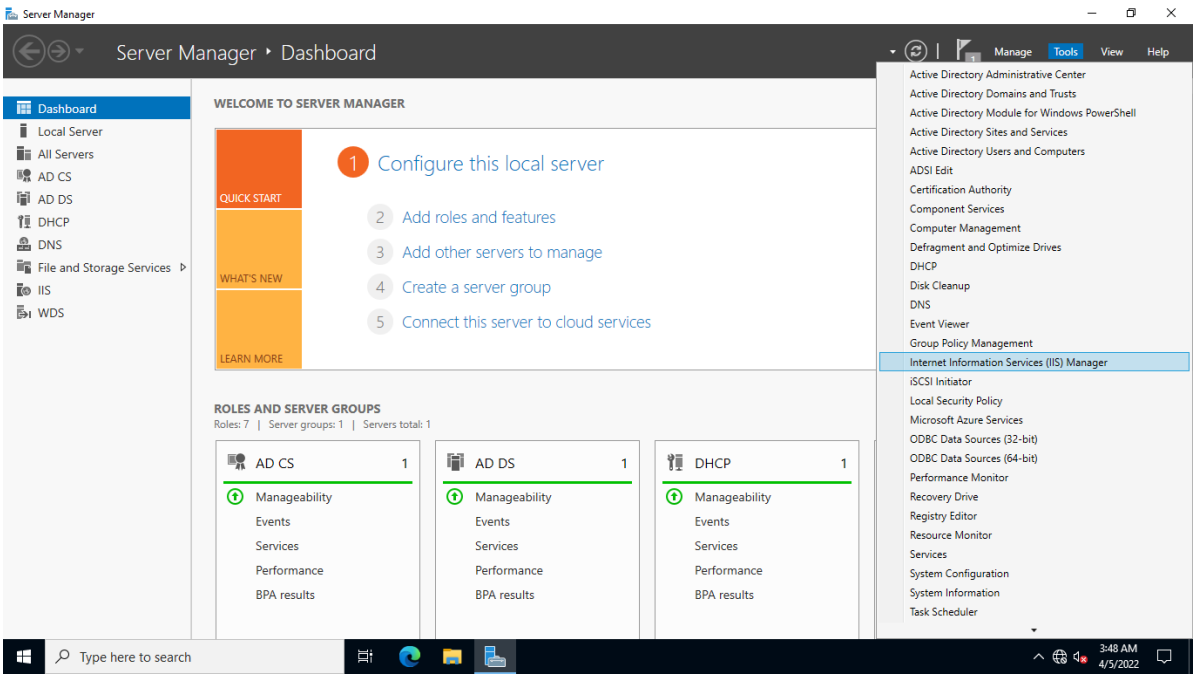
Once the installation is complete, click **Close** on the **Installation progress** page.



Step 9:

Next, you will configure the FTP server in Passive mode.

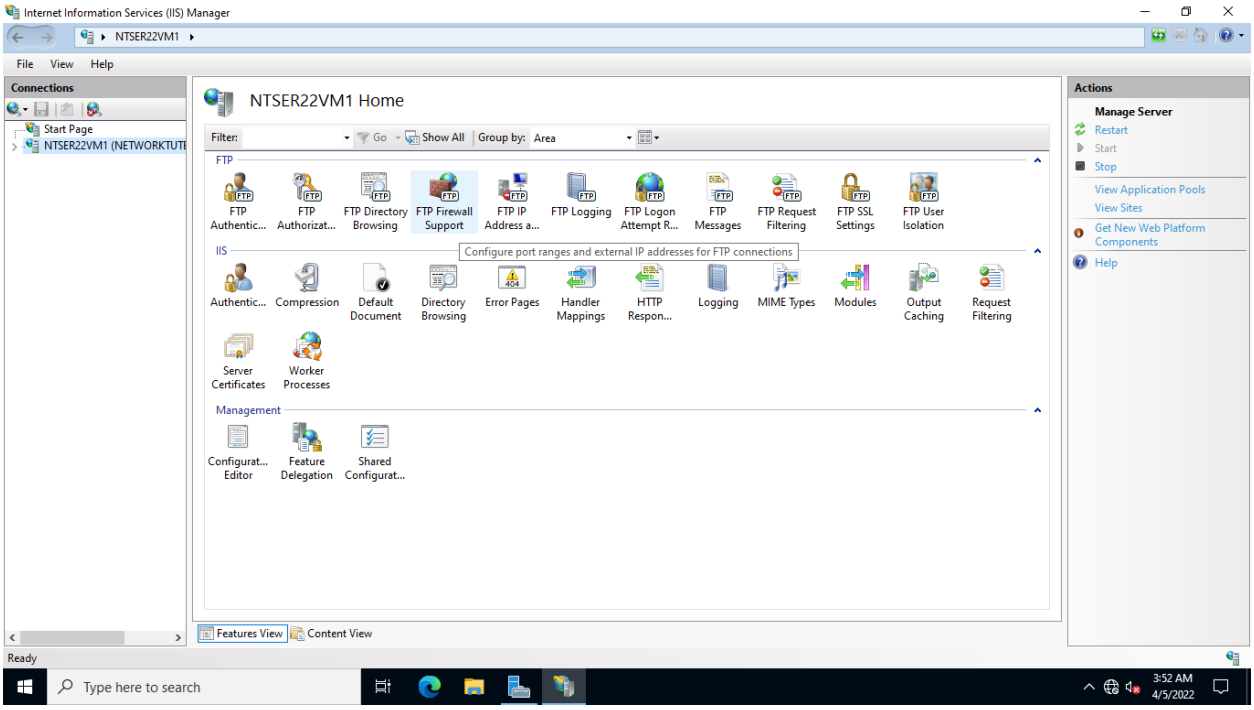
Back on the **Server Manager** page, click **Tools** and select **Internet Information Services (IIS) Manager**



Step 10:

On the **Internet Information Services (IIS) Manager** window, double-click **NTSER22VM1**.

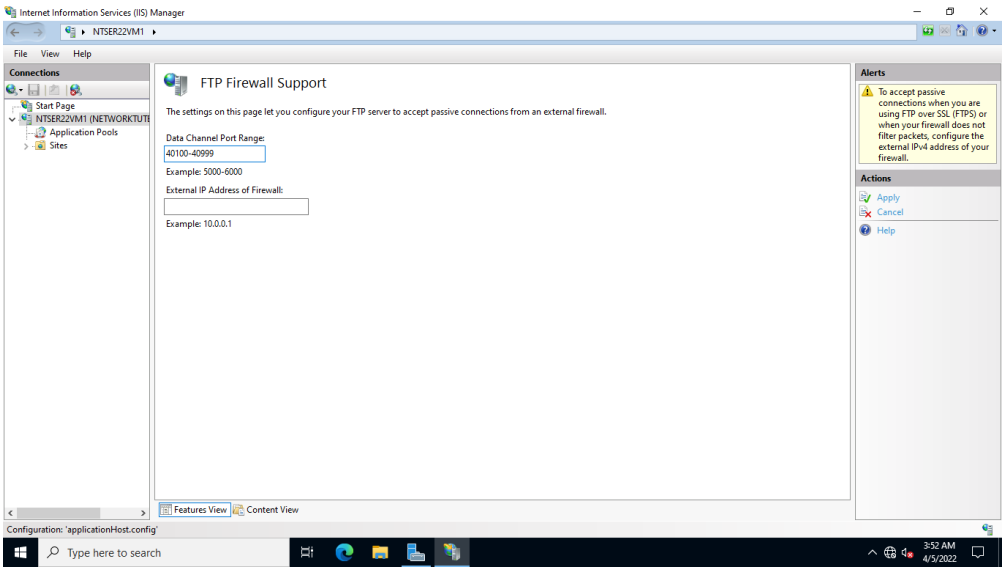
Double-click **FTP Firewall Support** on the **NTSER22VM1 Home** pane.



Step 11:

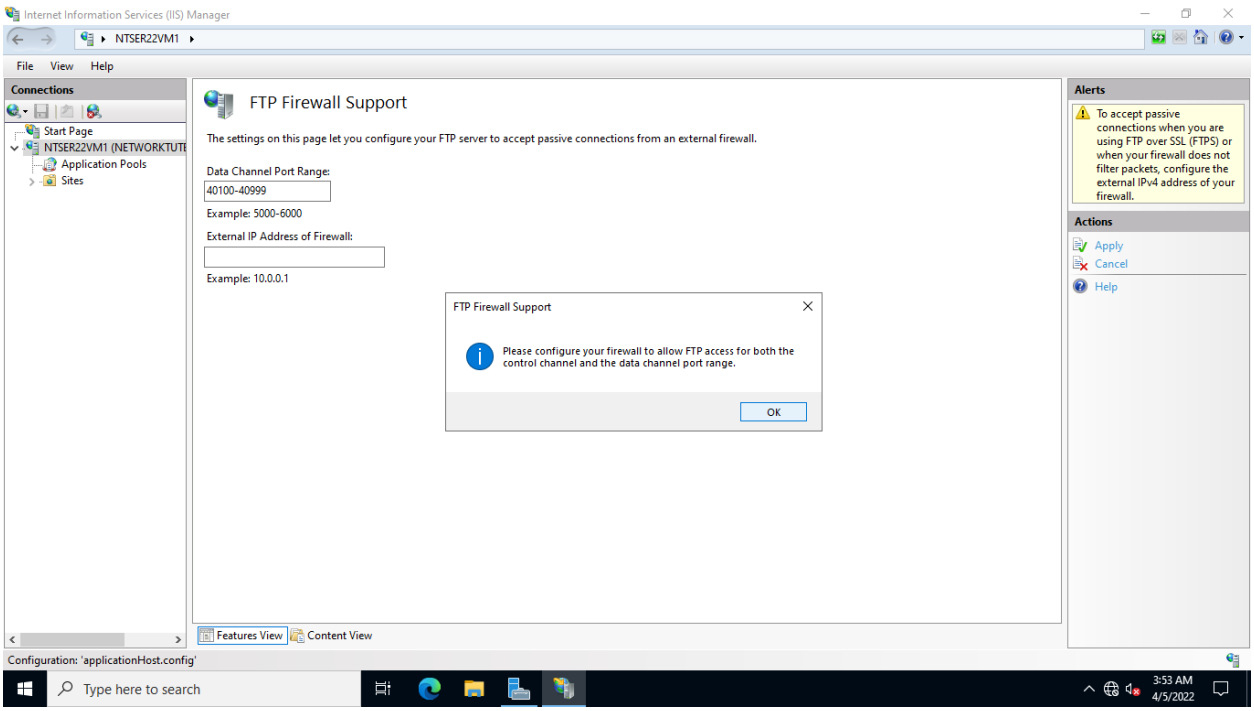
On the **FTP Firewall Support** pane, type the following on the **Data Channel Port Range** field: ***40100-40999***

Click **Apply** on the right pane.



Step 12:

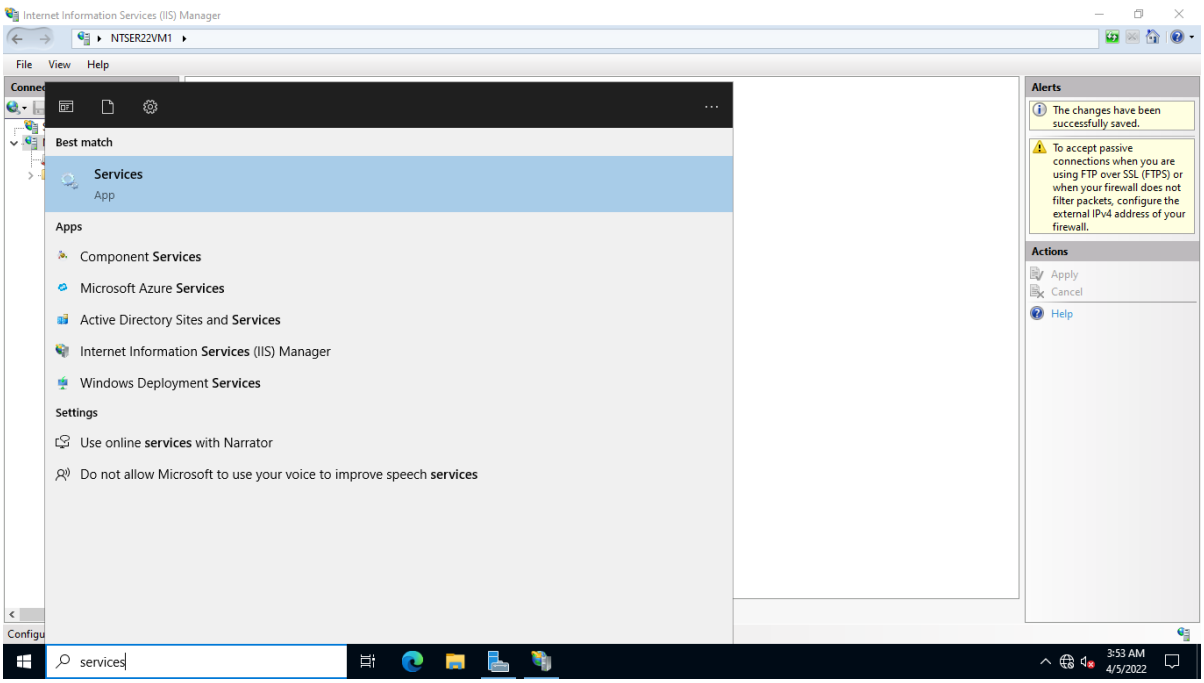
Click **OK** on the **FTP Firewall Support** pop-up window.



Step 13:

Click Start and type: ***services***

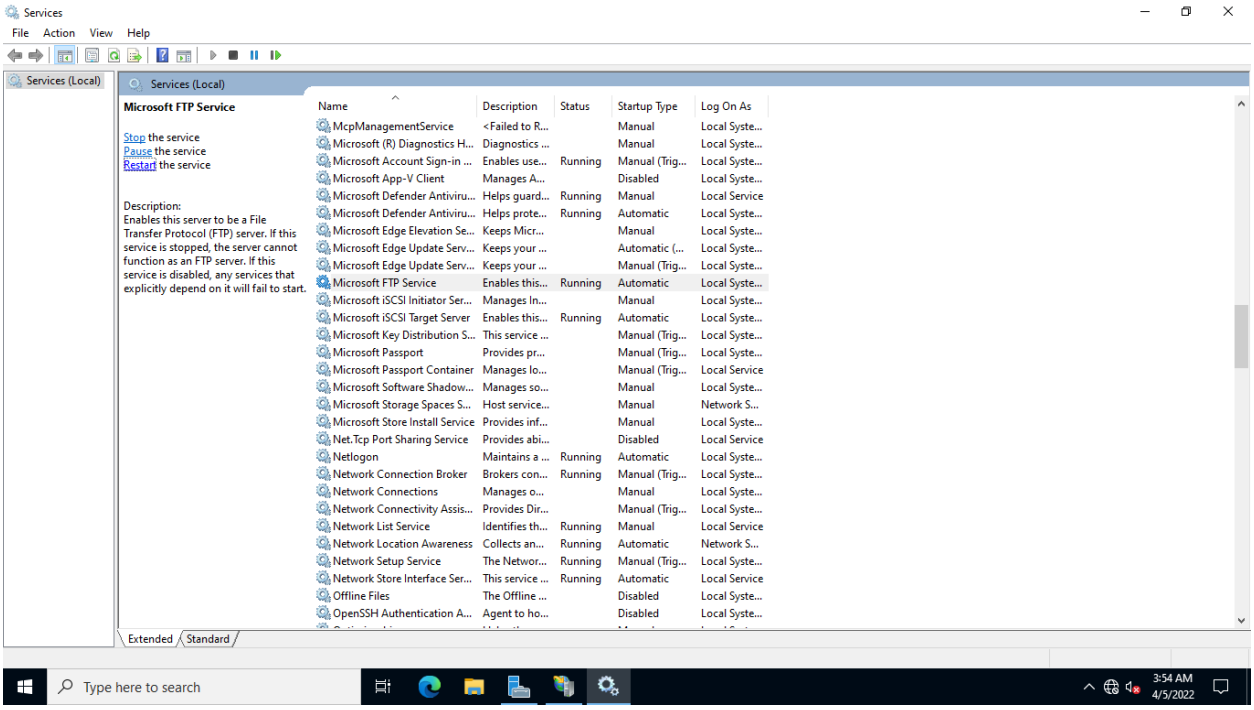
Select **Services**.



Step 14:

On the **Services** window, scroll down the middle pane and select **Microsoft FTP Service**.

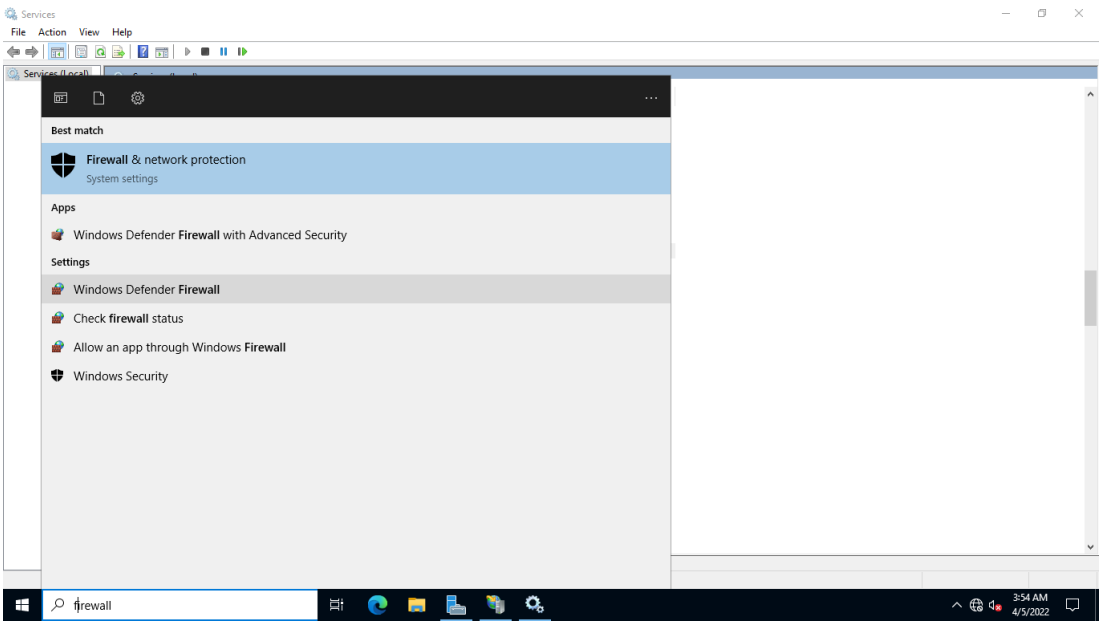
Click the **Restart** link.



Step 15:

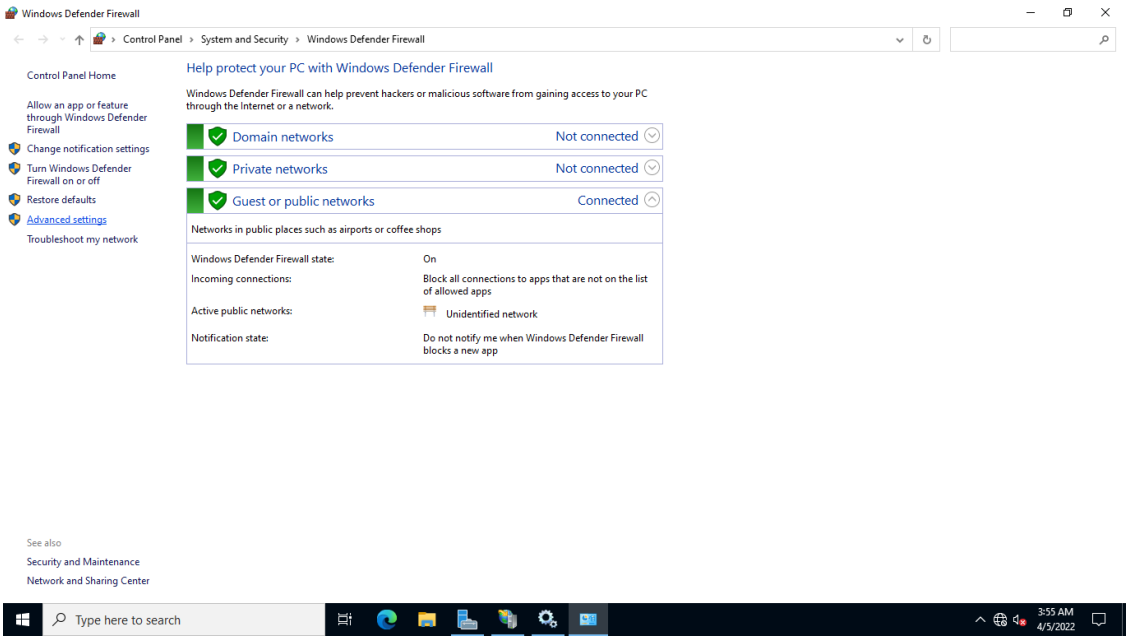
Click on **Start** and type: ***firewall***

Select **Windows Defender Firewall**.



Step 16:

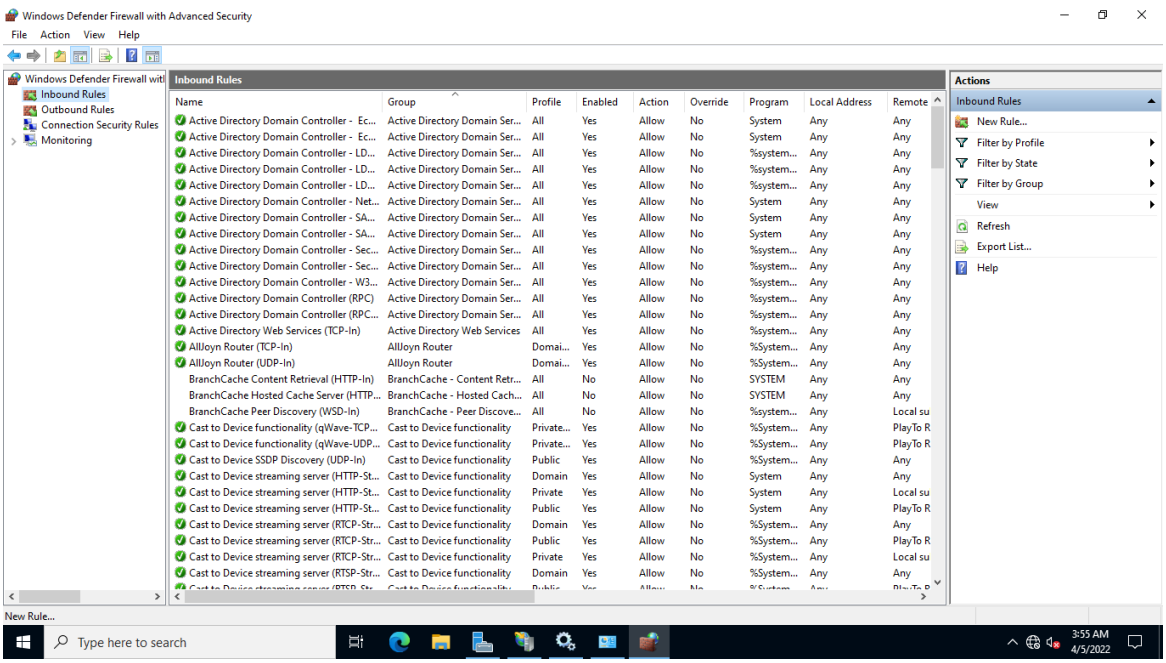
From the **Windows Defender Firewall** window, click the **Advanced settings** link on the left pane.



Step 17:

On the **Windows Defender Firewall with Advanced Security** window, select **Inbound rules** on the left pane.

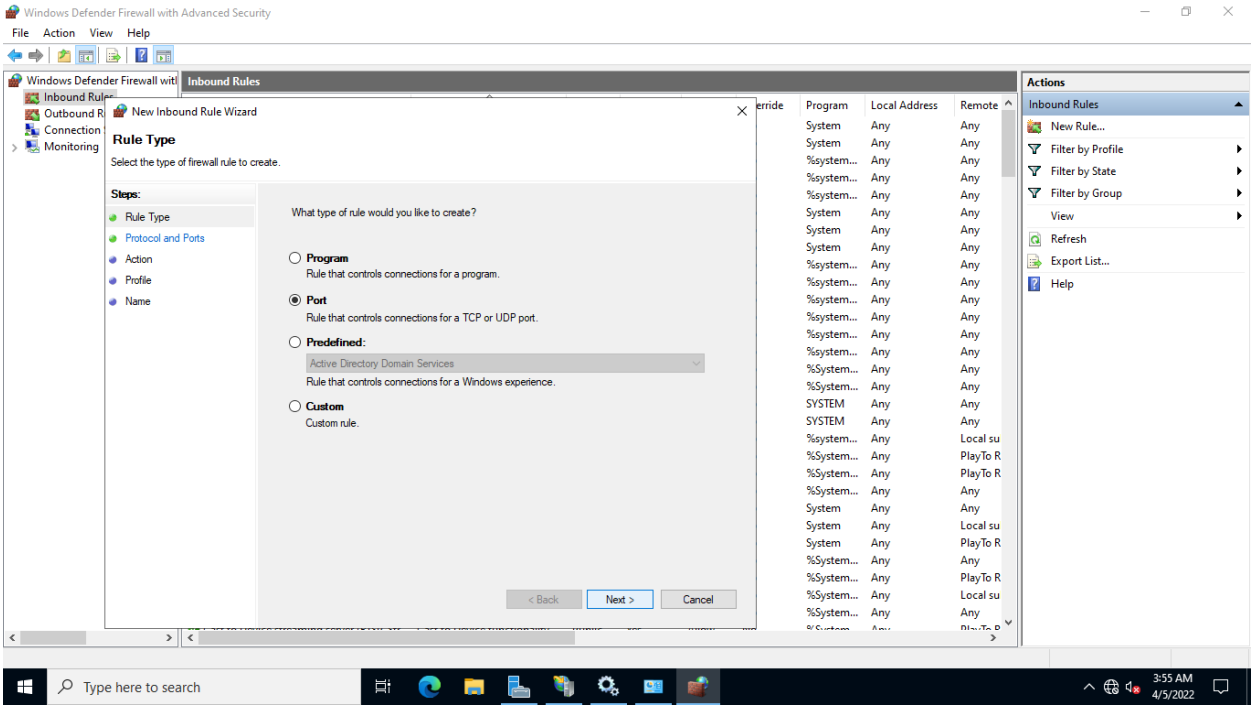
Click **New Rule** on the right pane.



Step 18:

On the **New Inbound Rule Wizard** - **Rule type** page, select **Port**.

Click **Next**.

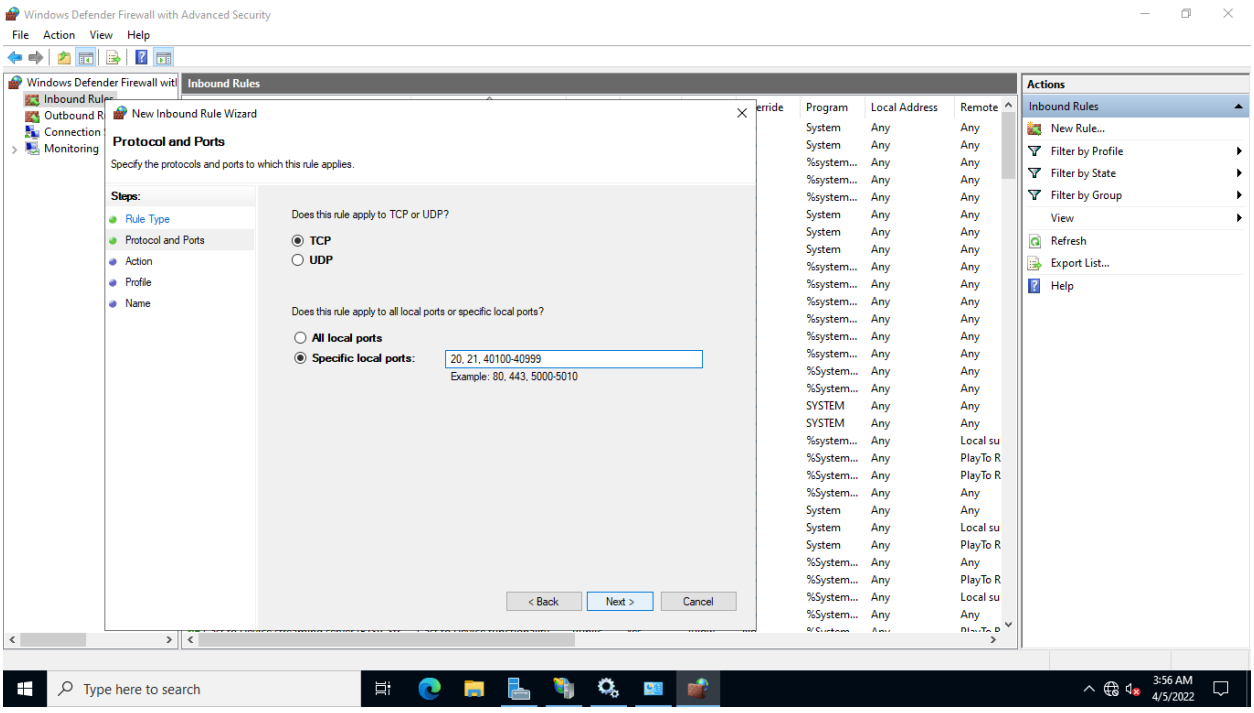


Step 19:

From the **Protocol and Ports** page, ensure **TCP** is selected.

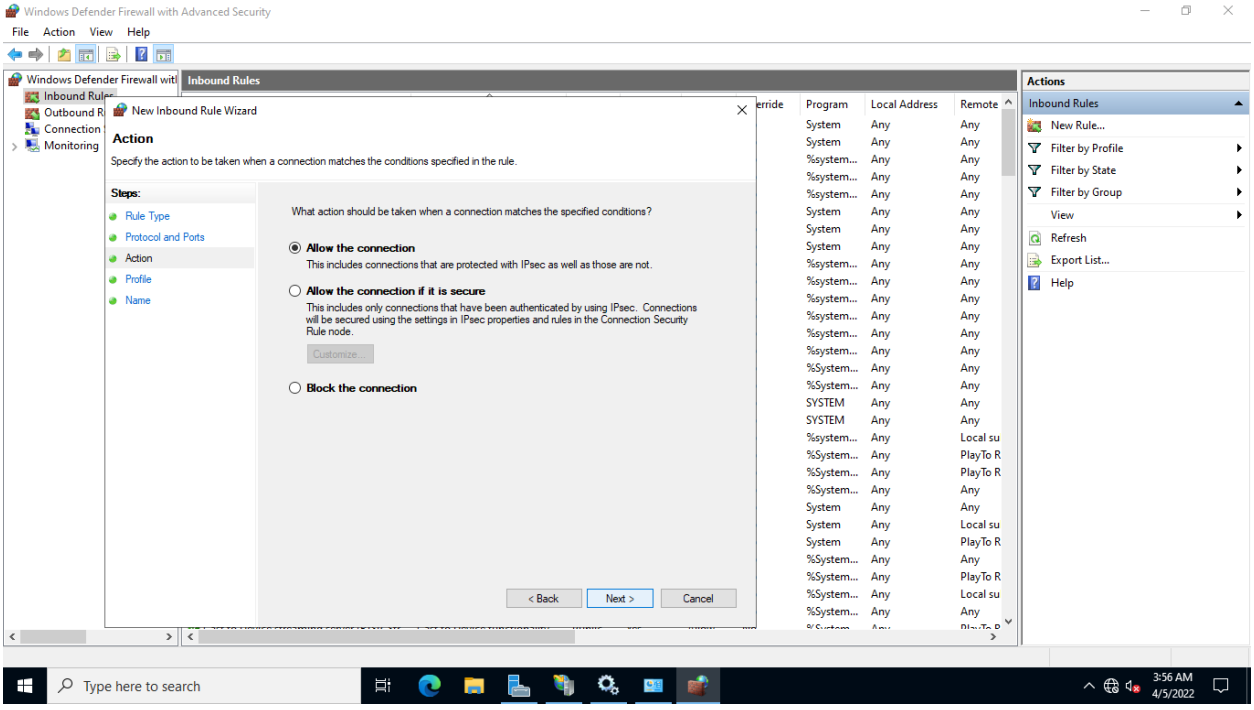
Under the **Does the rule apply to all local ports or specific local ports**? field, select **Specific local ports** and type: ***20, 21, 40100-40999***

Click **Next**.



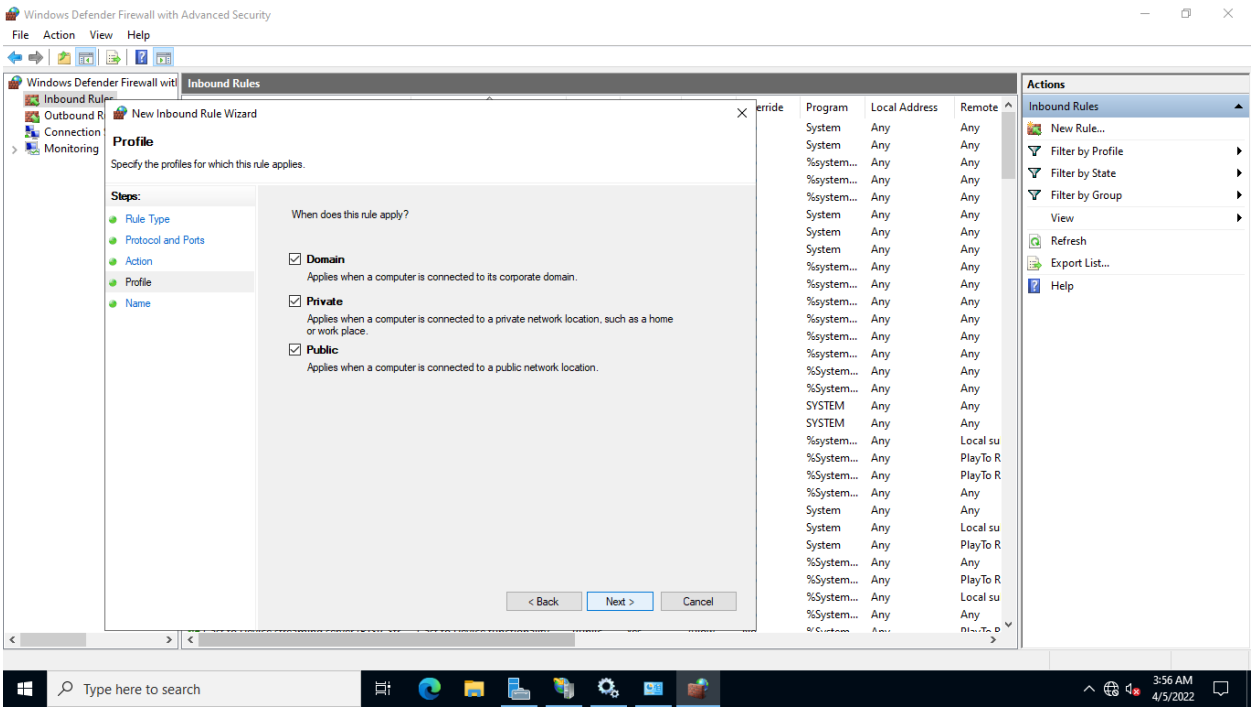
Step 20:

On the **Action** page, leave the default selection and click **Next**.



Step 21:

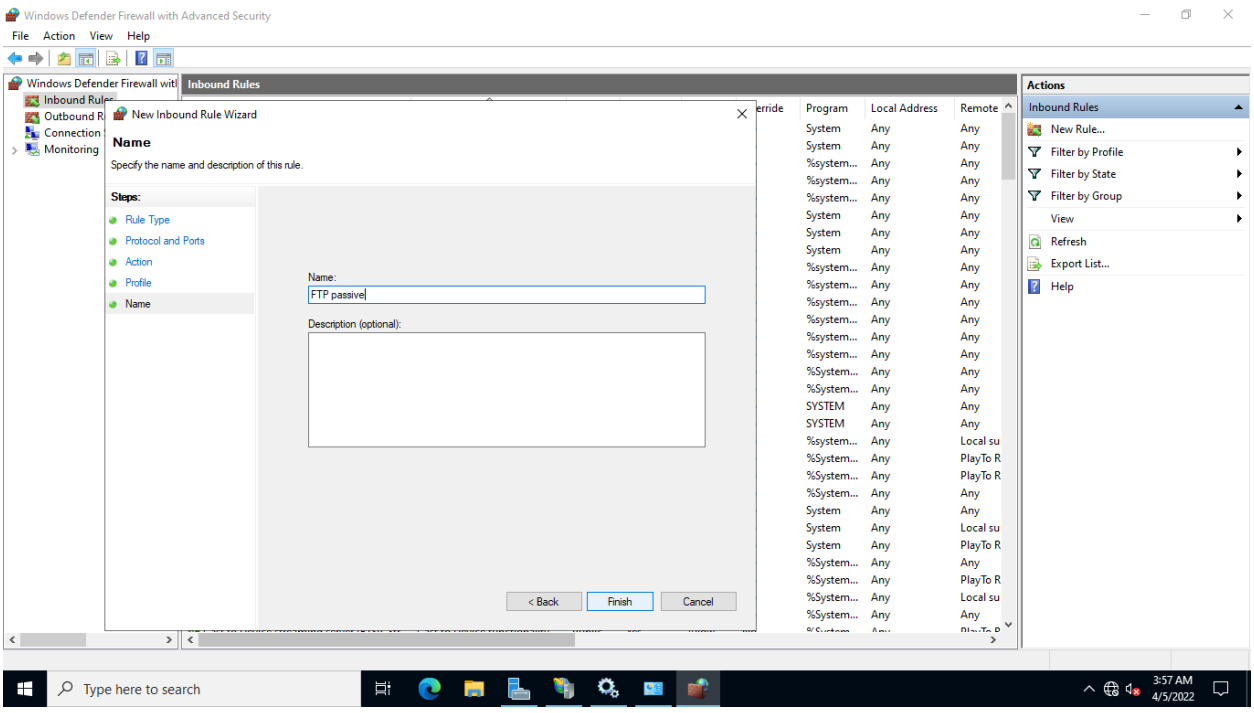
On the **Profile** page, click **Next.**



Step 22:

From the **Name** page, on the **Name** field, type: ***FTP passive***

Click **Finish**.

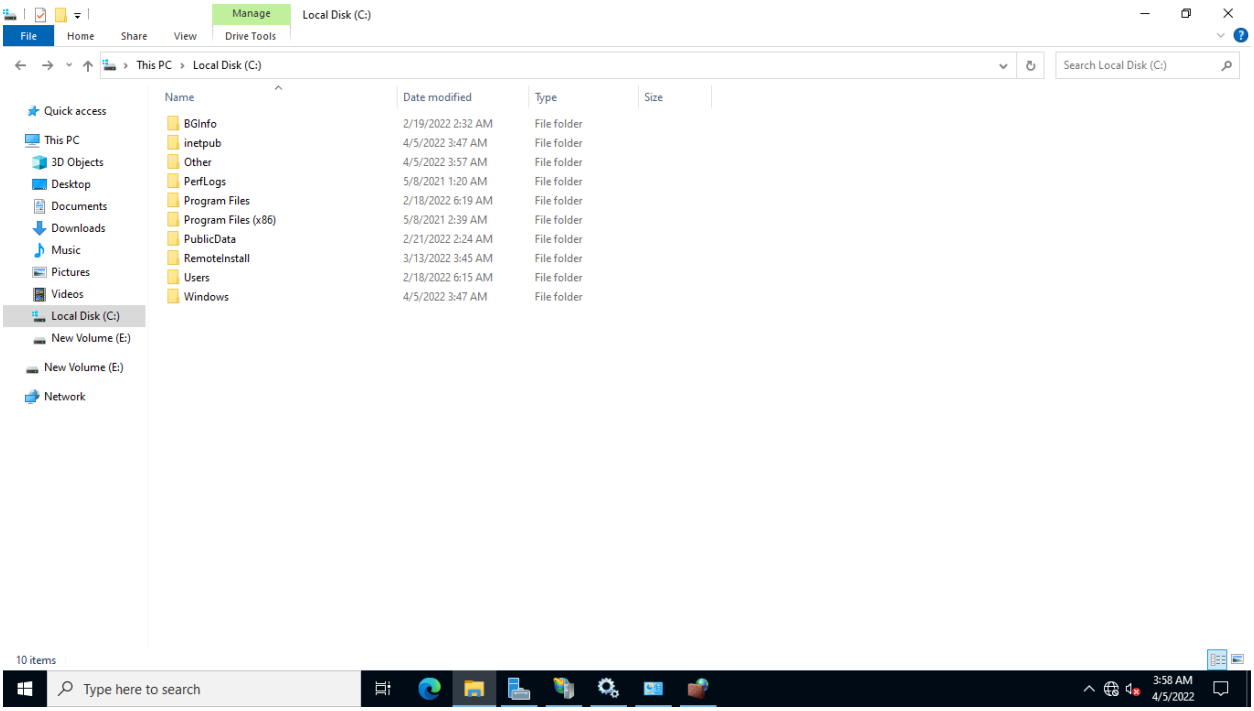


Step 23:

You will now create a folder for the FTP site.

Open **File Explorer** from the taskbar.

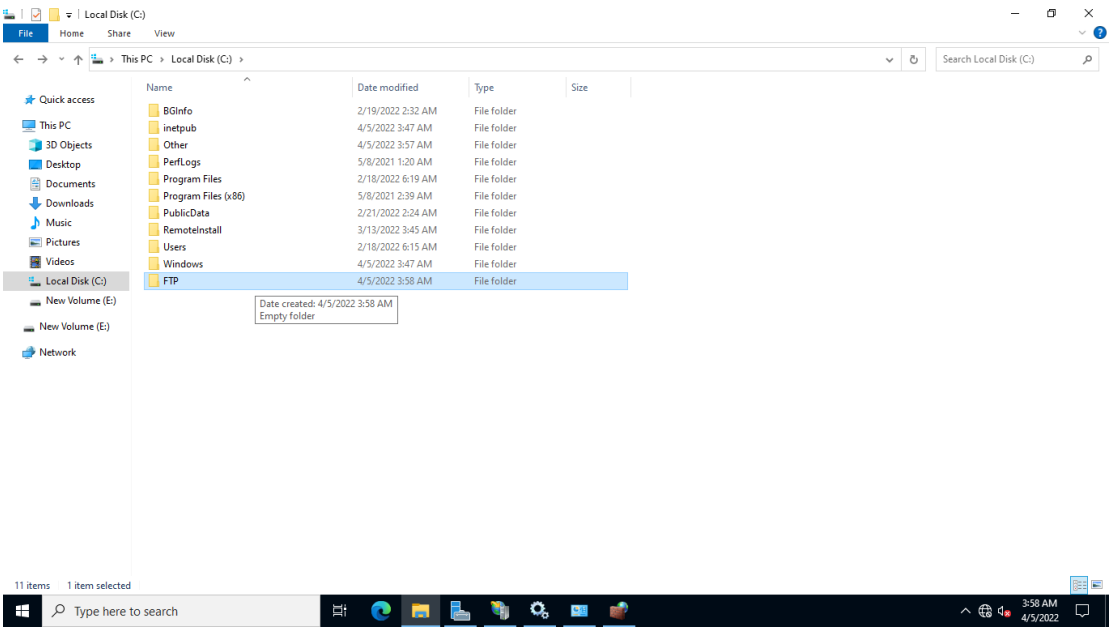
On the **File Explorer** window, navigate to **This PC** > **Local Disk** (**C**:).



Step 24:

Right click anywhere on the contents pane and select **New** > **Folder**.

Rename the folder to: ***FTP***

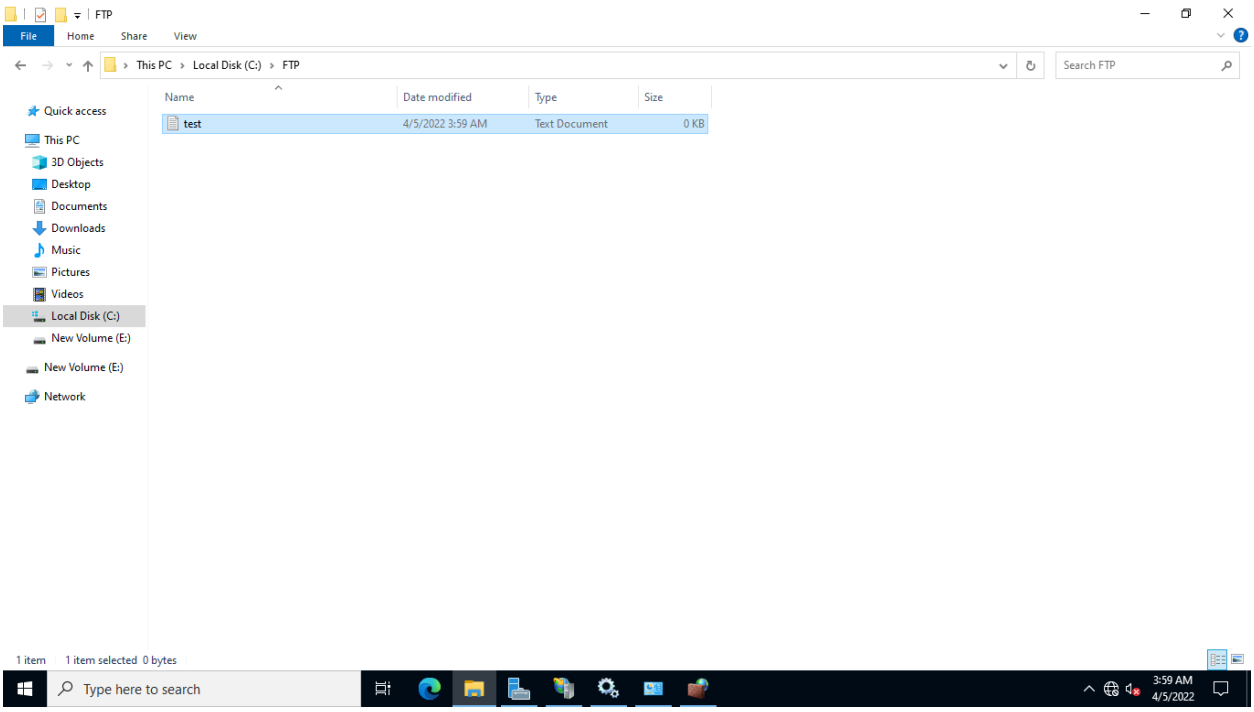


Step 25:

Double-click on the **FTP** folder.

Right-click anywhere on the content pane, and select **New** > **Text Document**.

Rename the text document to: ***test***



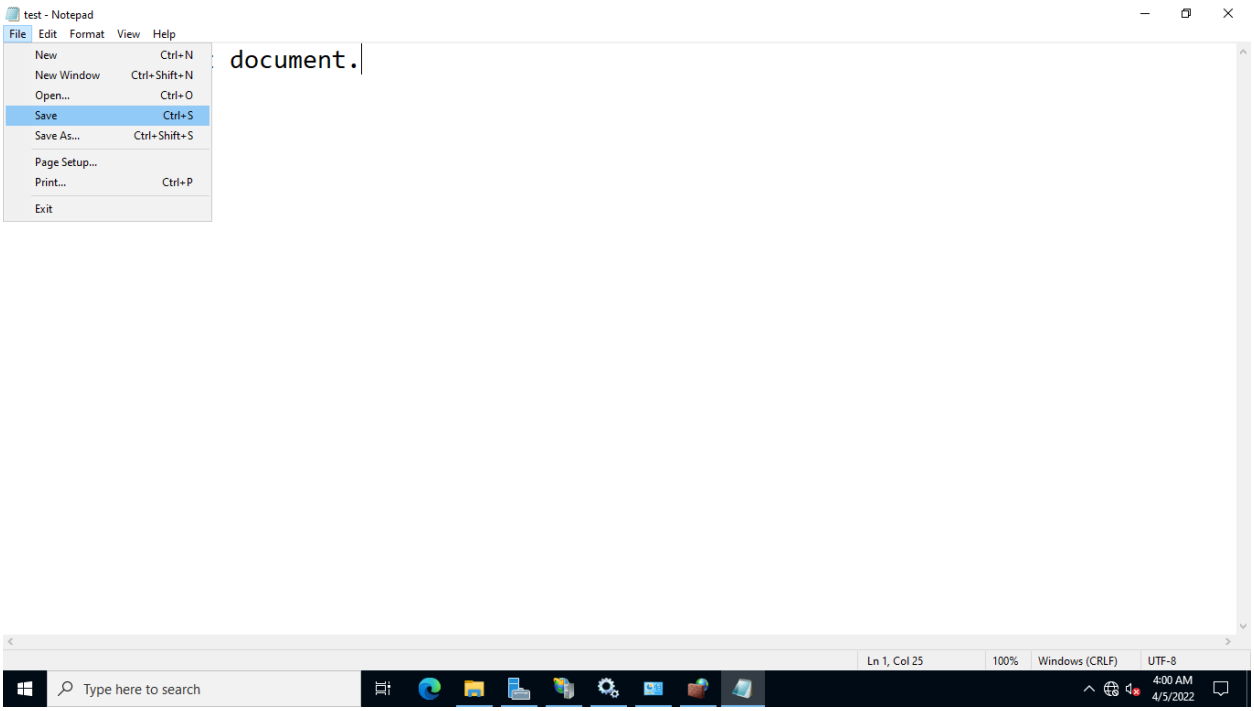
Step 26:

Double-click on the **test** document to open it.

On the **test** - **Notepad** window, type: ***This is a test document***.

Step 27:

Click the **File** menu and select **Save**.

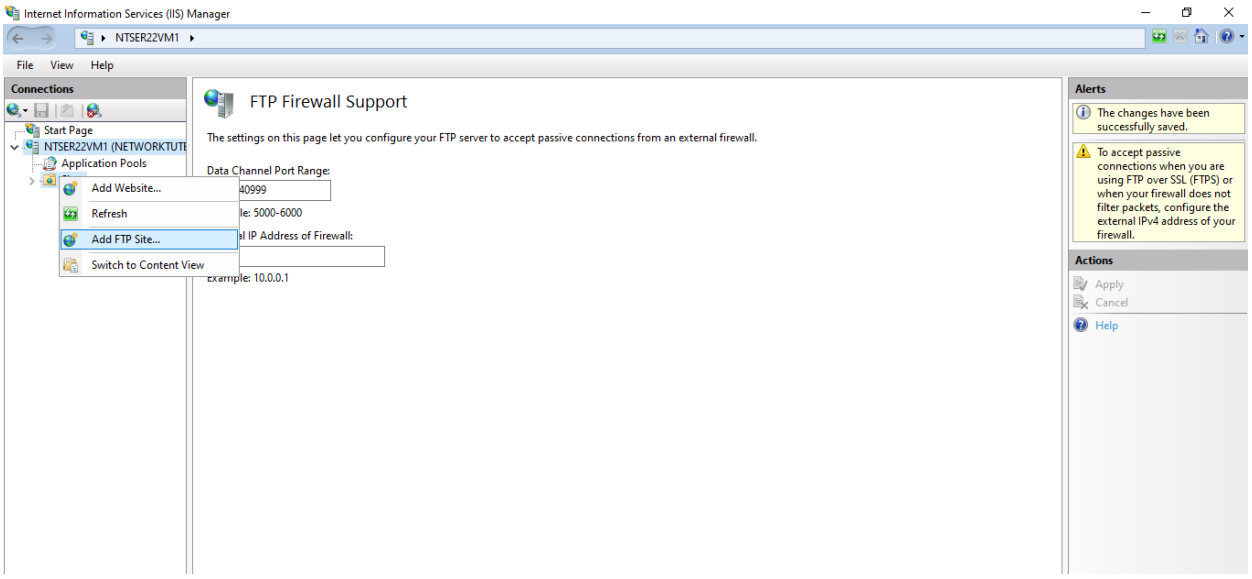


Close the **test** - **Notepad** window.

Step 28:

Restore the **Internet Information Services** (**IIS**) **Manager** window from the taskbar.

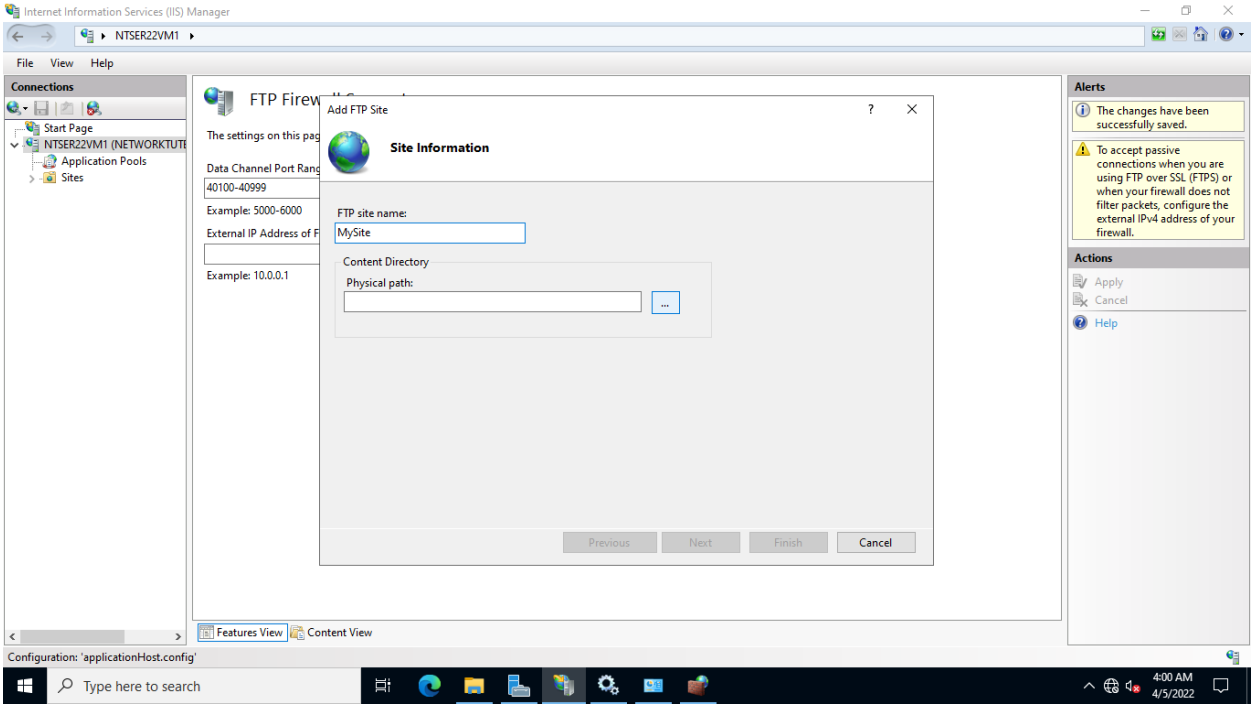
Select and right-click on **Sites**, click **Add FTP Site**.



Step 29:

From the **Add FTP Site** - **Site Information** page, under the **FTP site name** field, type: ***MySite***

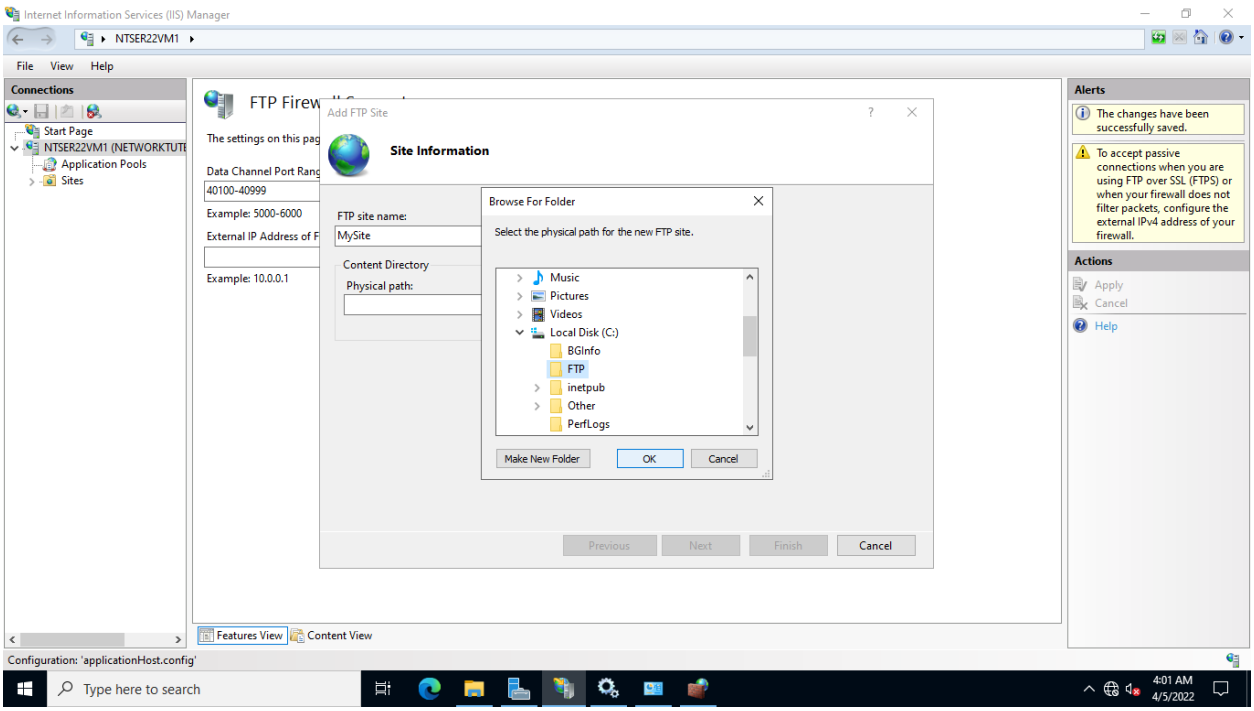
Click on … under the **Physical path** field.



Step 30:

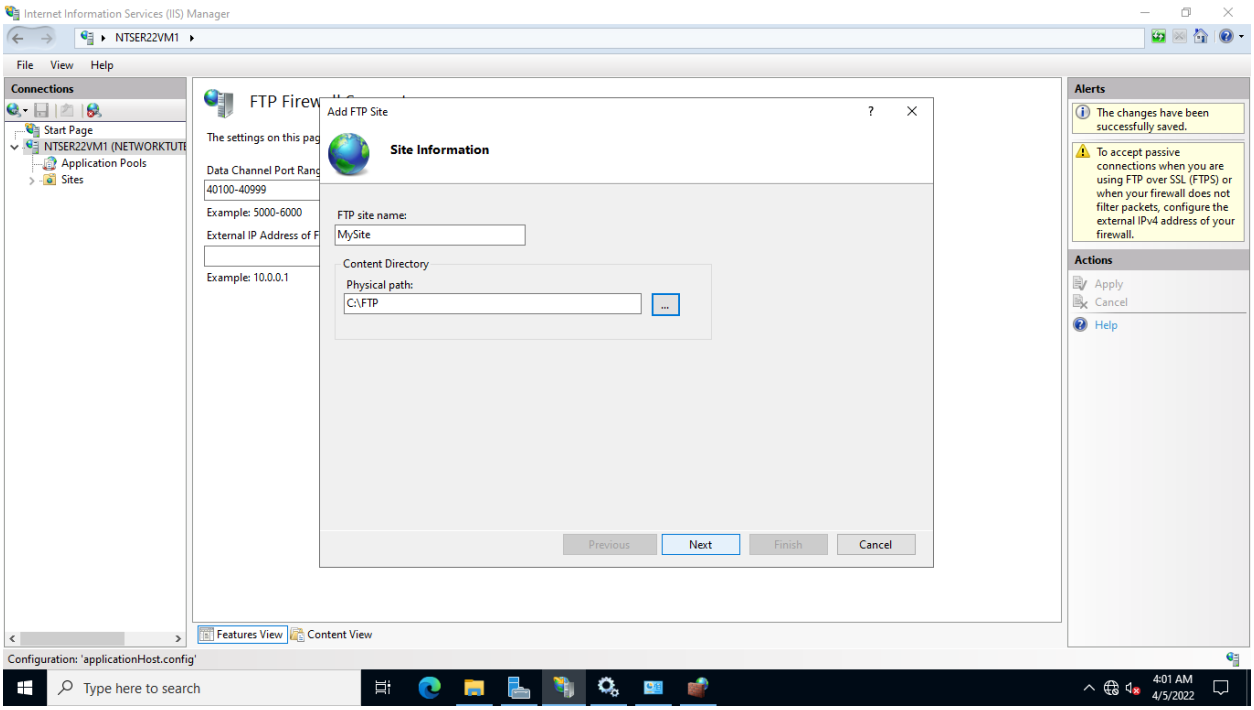
On the **Browse for Folder** dialog box, expand **Local Disk** (**C**:) and select the **FTP** folder.

Click **OK**.



Step 31:

Back on the **Add FTP Site** - **Site Information** page, click **Next**.



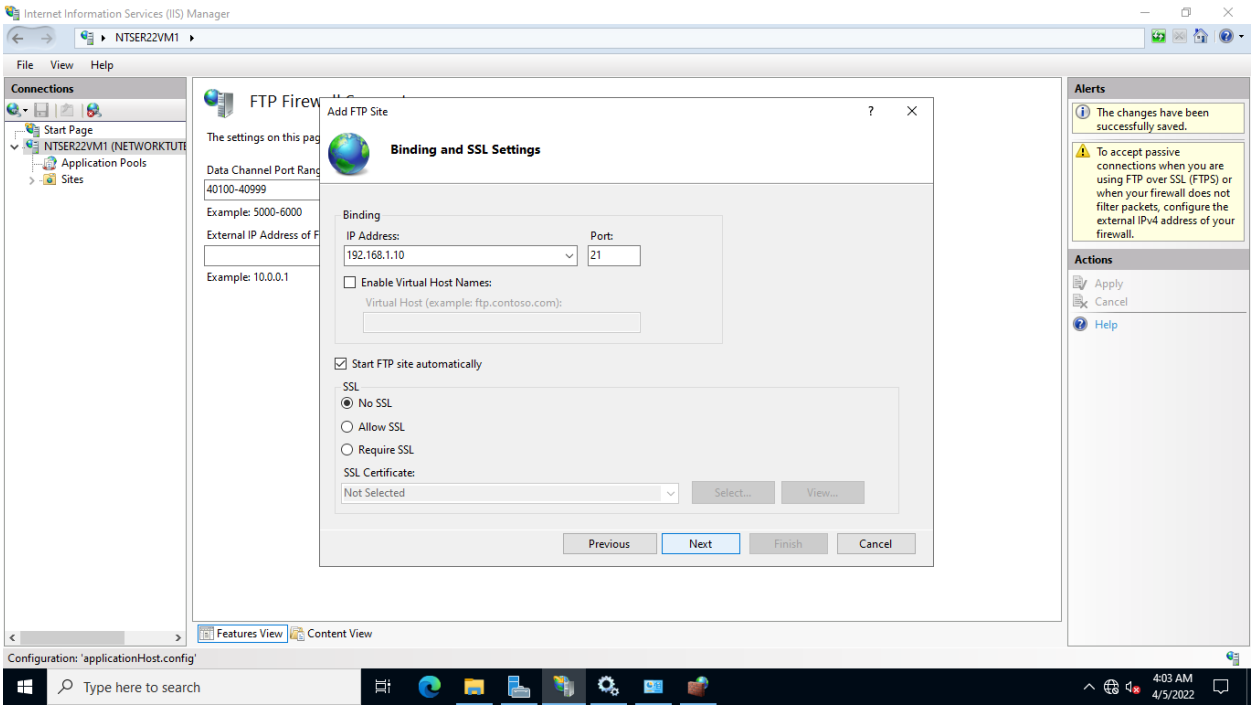
Step 32:

On the **Binding and SSL Settings** page, under the **Binding** field, type the following for the **IP Address**:

192.168.1.10

For the **SSL** field, select the **No SSL** option.

Click **Next.**



Step 33:

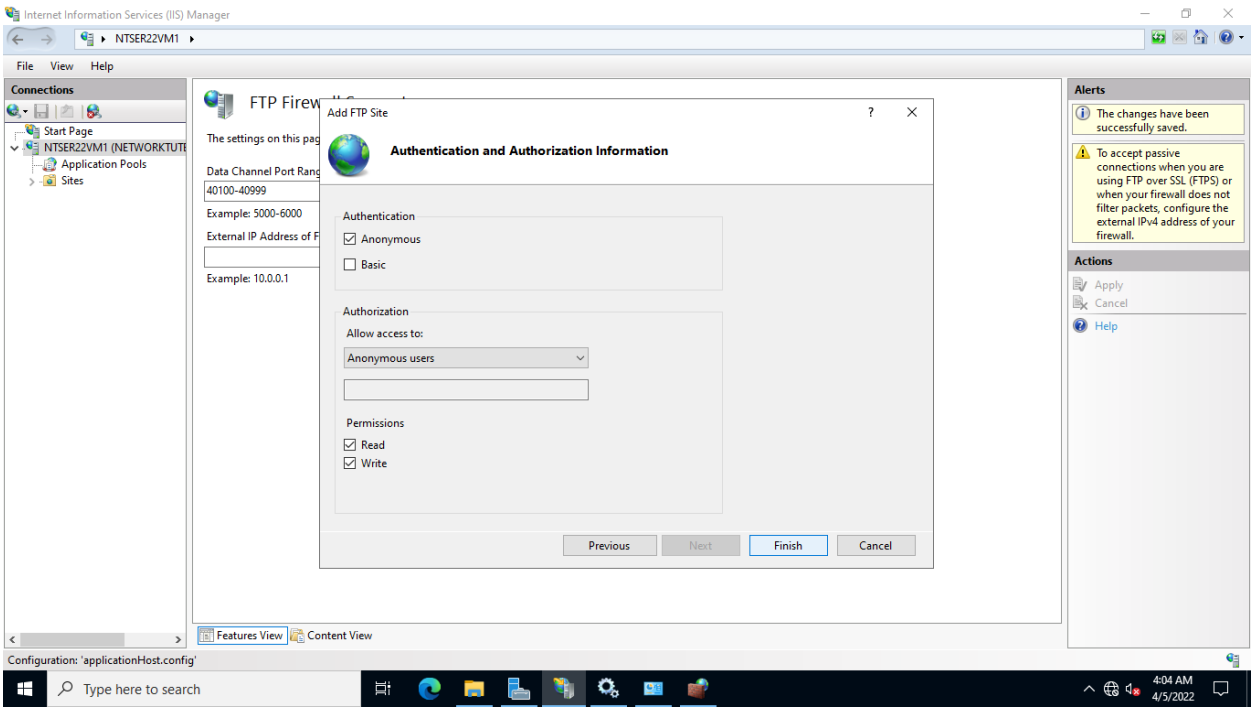
From the **Authentication and Authorization Information** page, enable **Anonymous** for the **Authentication** field.

Under the **Authorization** section, select **Anonymous** users from the Allow access to drop-down.

Enable **Read** and **Write** checkboxes for **Permissions.**

Click **Finish**.

Note: Please note this is a basic setup without any security implemented. In a real-time environment, proper security measures need to be in place.



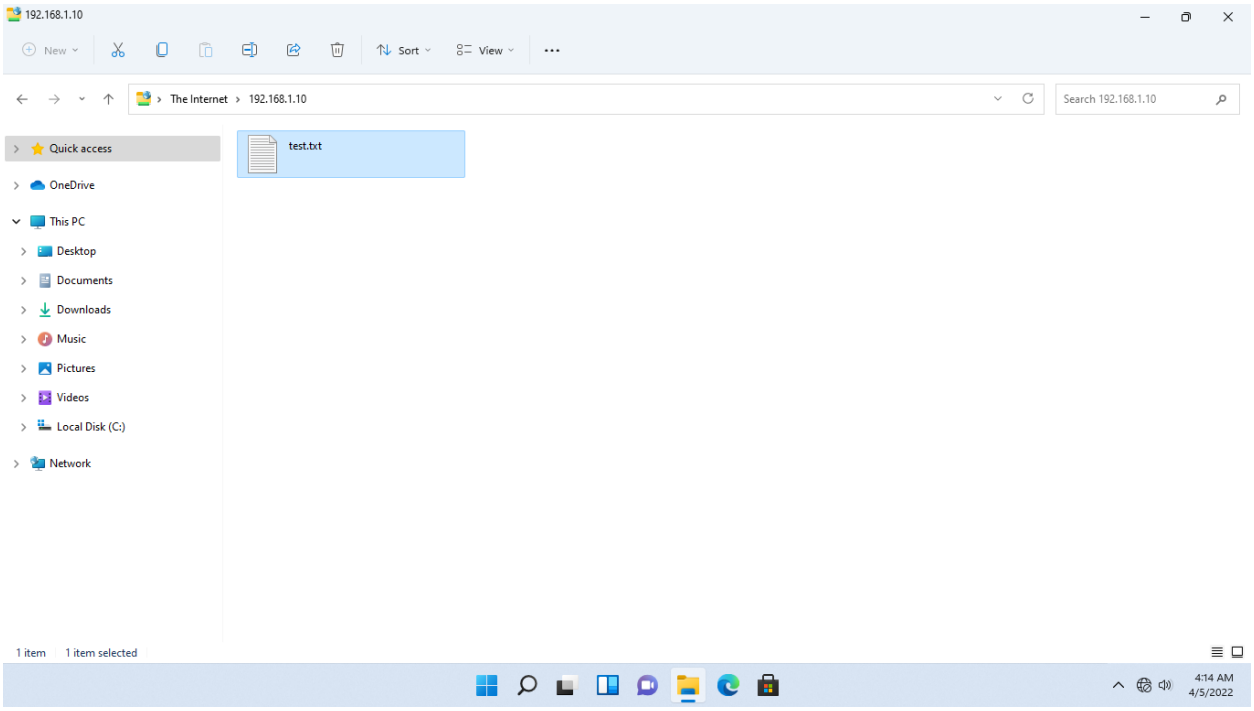
Step 34:

You will now test the FTP connection.

Connect to **NTWIN11VM1.**

Open **File Explorer** from the taskbar. On the **Quick access** bar, type: ***ftp://192.168.1.10***

Press **Enter**.



Task 2: Access Shared Folder using SMB Protocol

In computer networks, the Server Message Block (SMB) protocol is used for file sharing. It allows different users and applications to access and edit shared network resources and files.

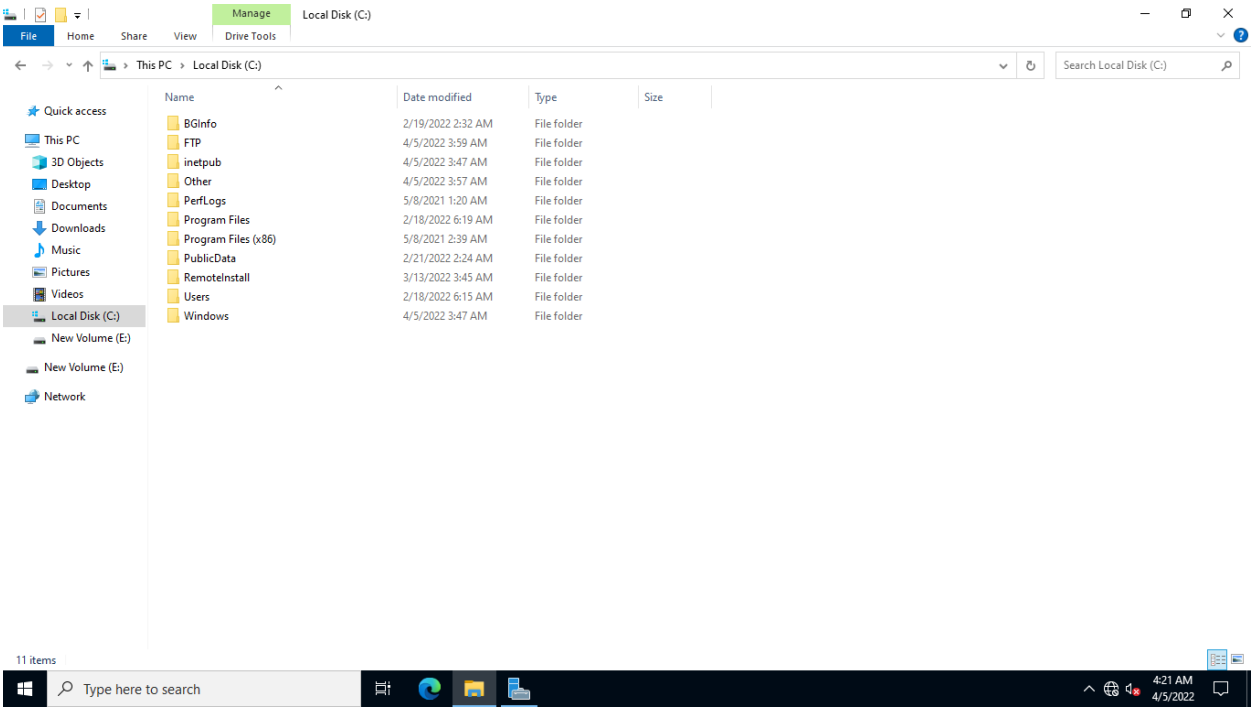
To create a client/server connection, SMB uses TCP port 445 and a large number of request-response packets. It has one major flaw: vulnerability, and when installed on hosts, it poses a security risk. The SMB vulnerability is used by ransomware. SMB is available in three versions: SMBv1, SMBv2, and SMBv3.

Now let's, On the Windows server, file sharing will be enabled via SMB. The enabled SMB version will then be detected using Windows PowerShell.

Step 1:

Connect to **NTSER22VM1**.

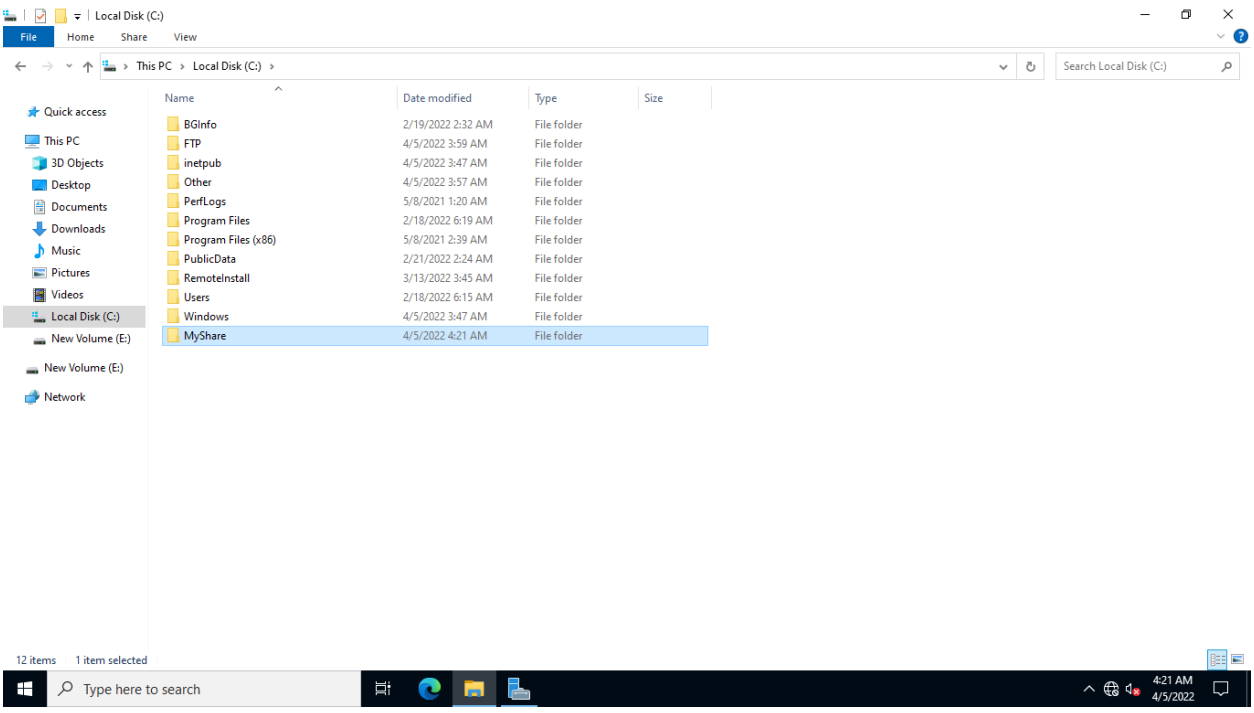
Open **File Explorer** from the taskbar. Navigate to **This PC** > **Local Disk** (**C**:).



Step 2:

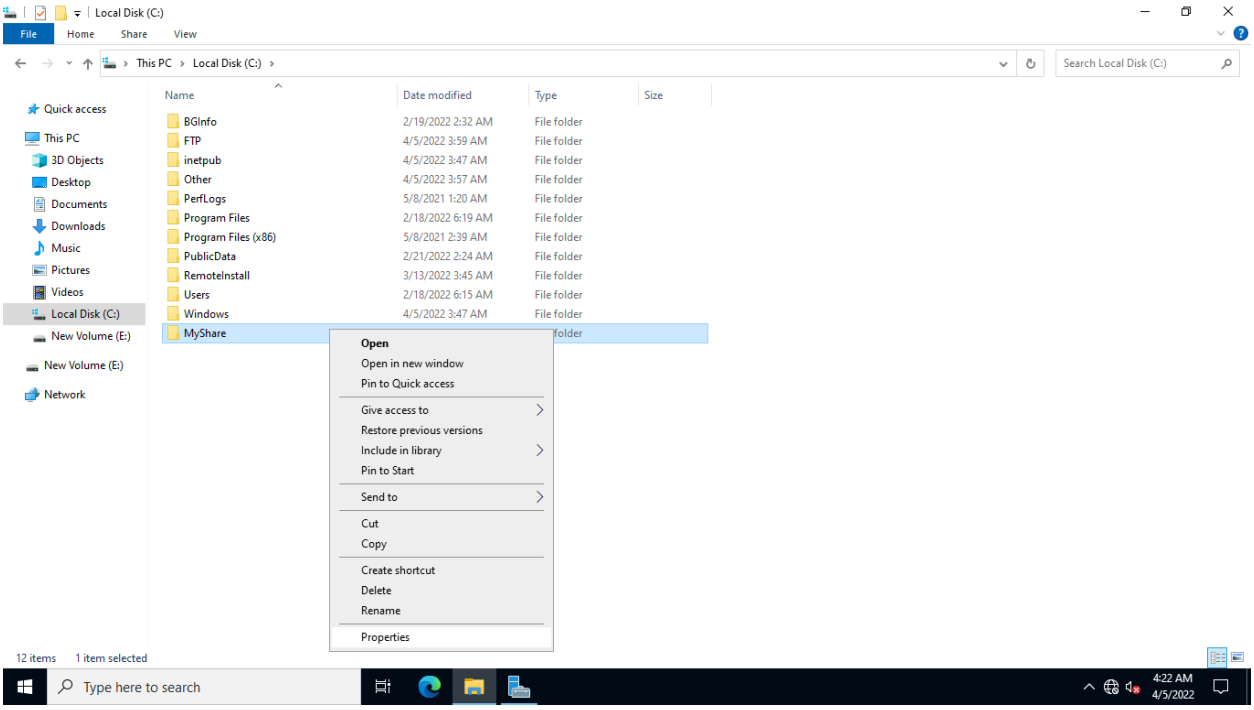
Right click anywhere on the contents pane and select **New** >**Folder**.

Name it to: ***MyShare***



Step 3:

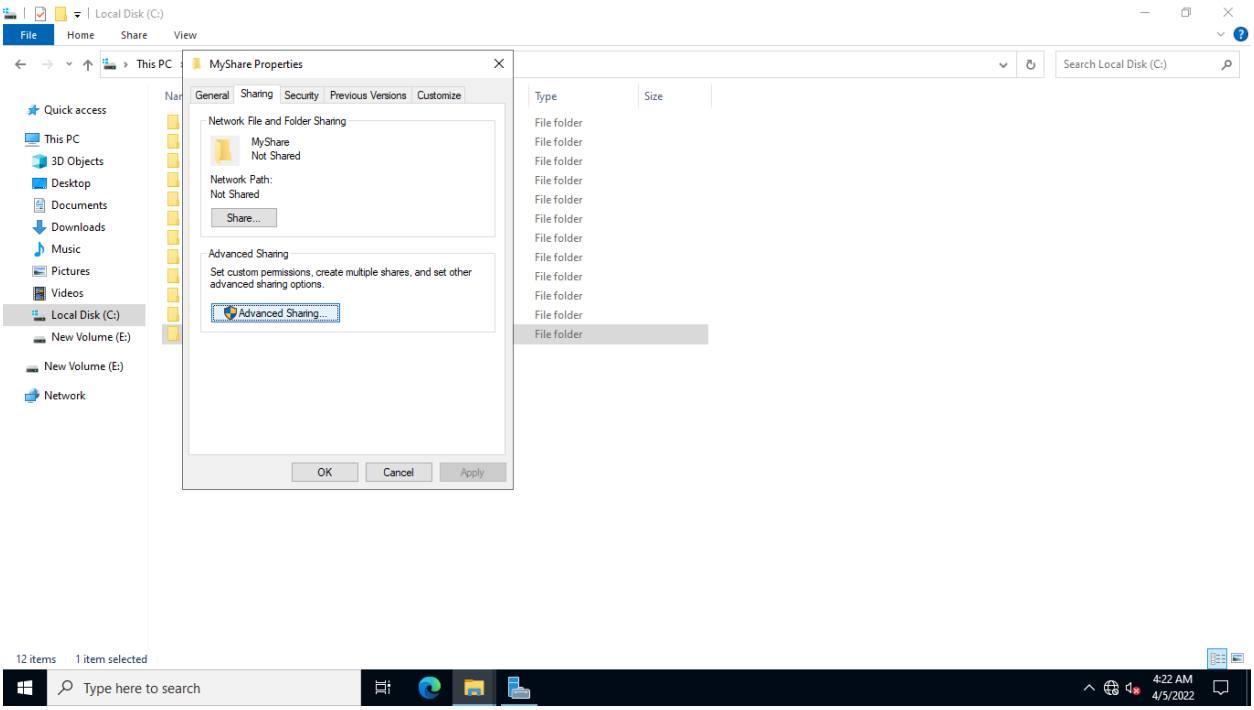
Right-click on **MyShare** and select **Properties**.



Step 4:

On the **MyShare Properties** dialog box, click the **Sharing** tab.

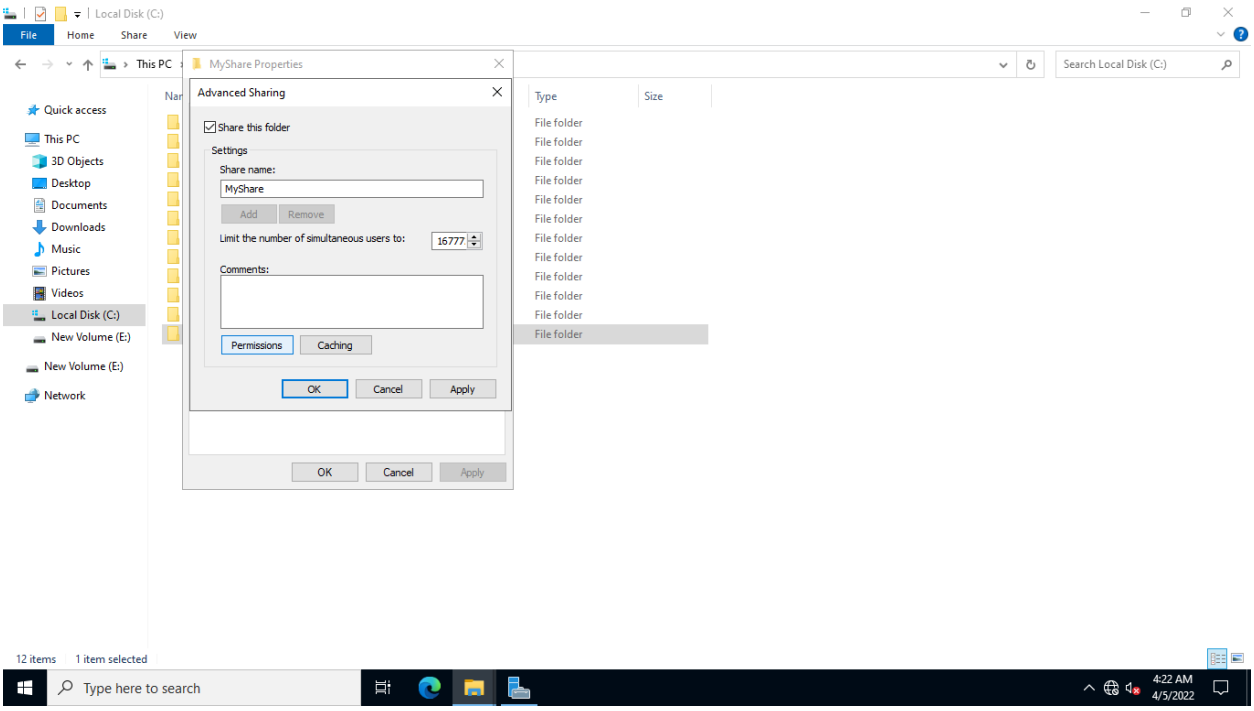
Select **Advanced Sharing**.



Step 5:

From the **Advanced Sharing** dialog box, enable the **Share this folder** checkbox.

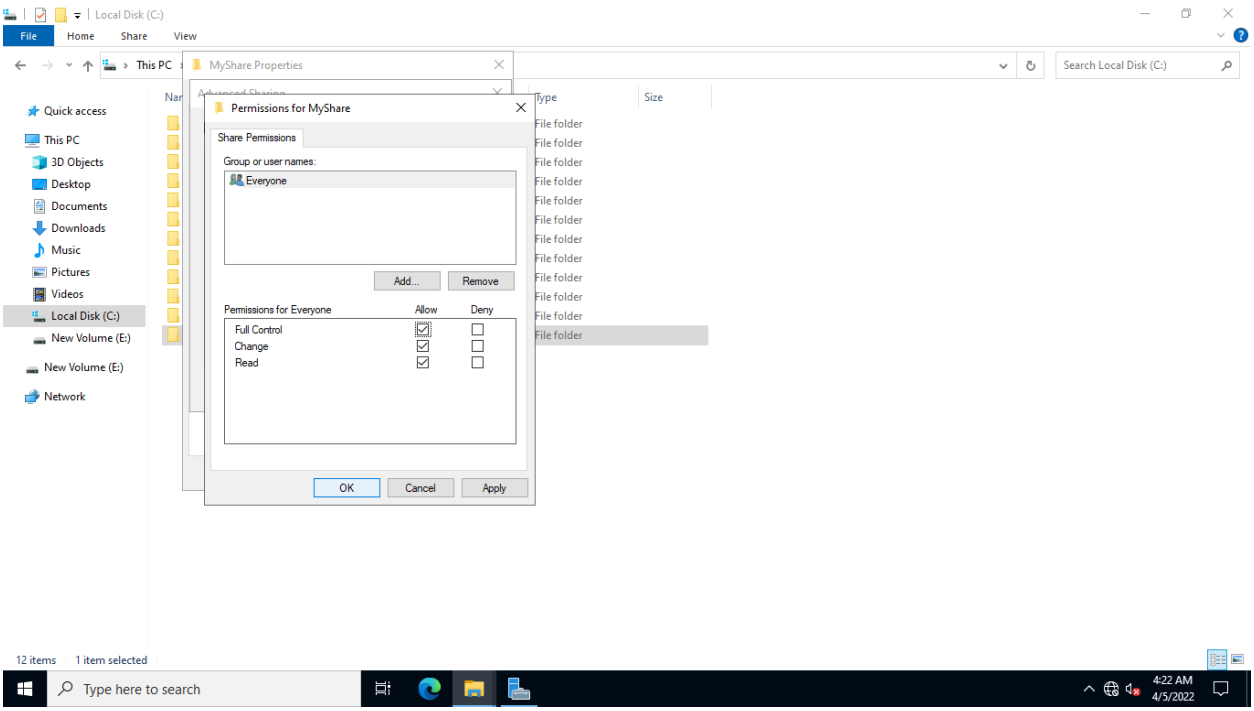
Click the **Permissions** button.



Step 6:

On the **Permissions for MyShare** dialog box, enable **Full Control** under the **Allow** section.

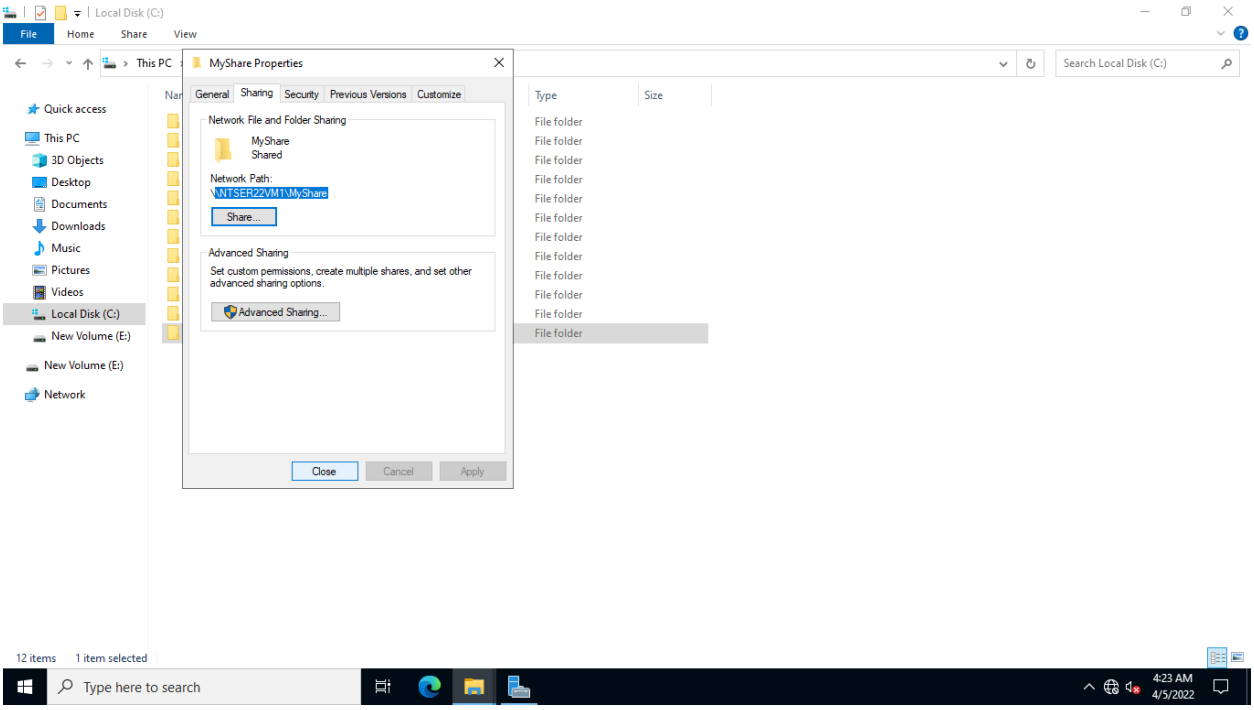
Click **OK** twice.



Step 7:

On the **MyShare Properties** dialog box, take note of the **Network Path** for the shared folder. It is set to: ***\\NTSER22VM1\MyShare***

Click **Close**.



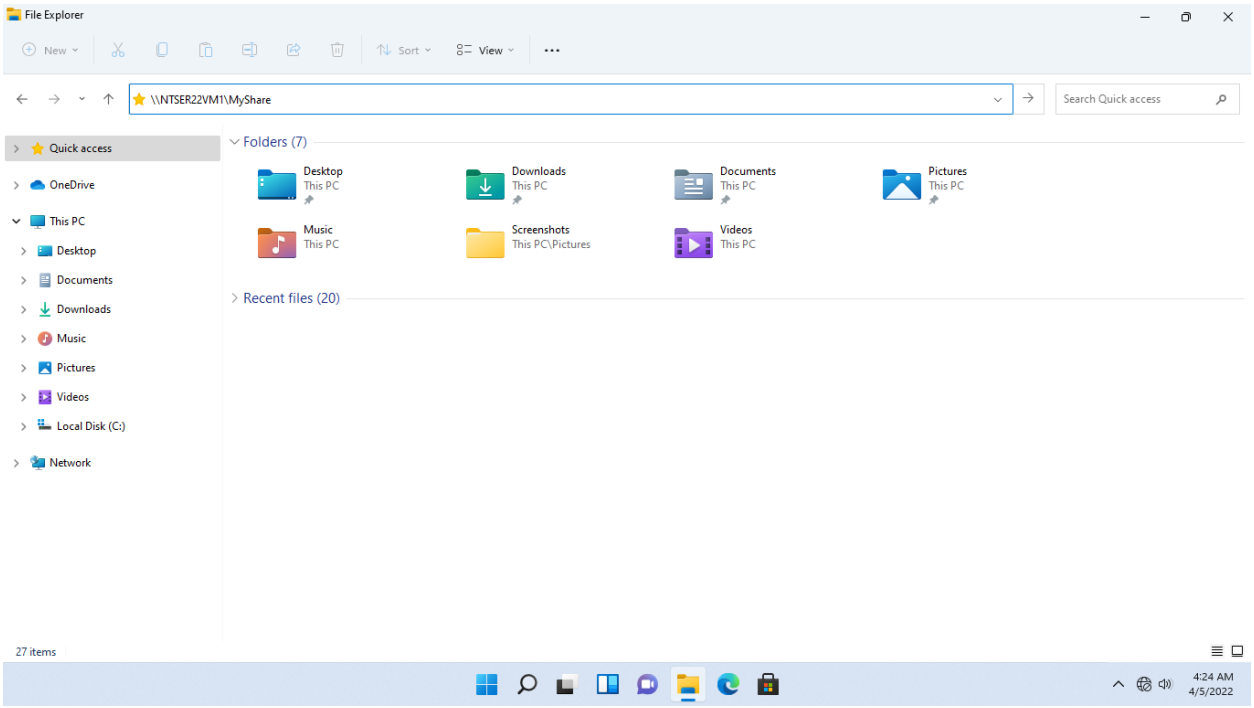
Step 8:

You will now access the shared folder. Connect to **NTWIN11VM1**.

Open **File Explorer** from the taskbar.

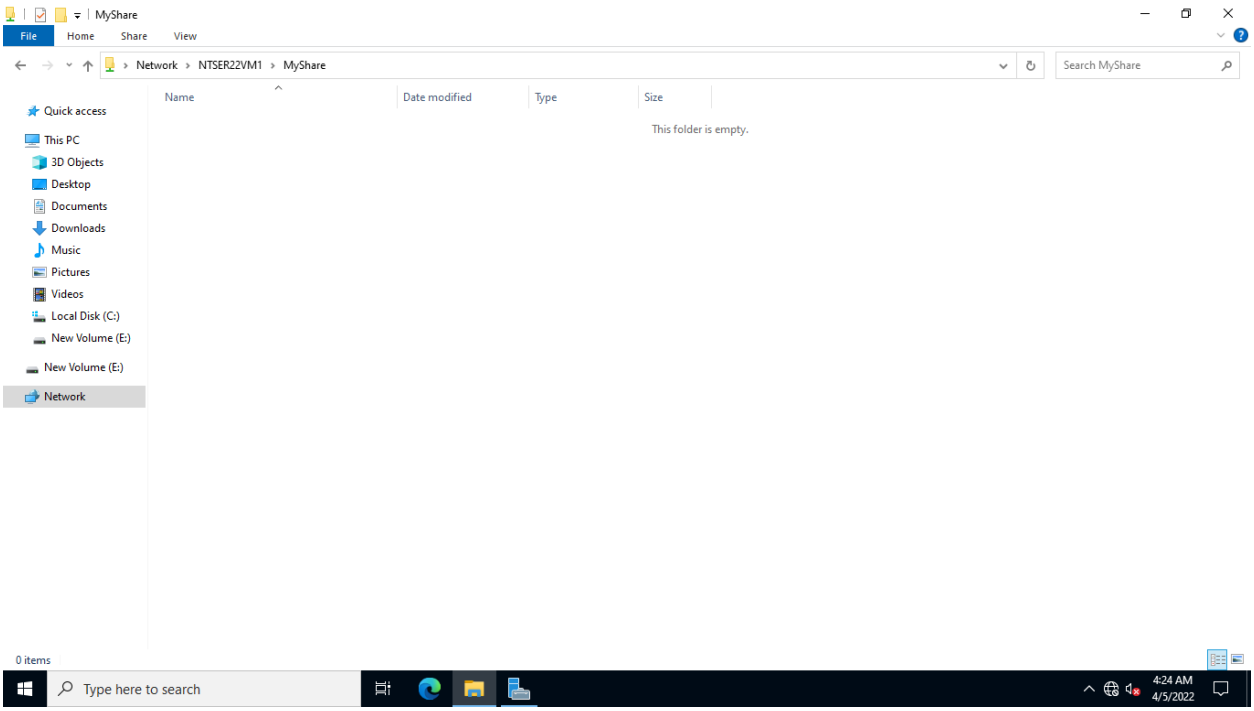
On the File Explorer window., type the following network path on the Quick access bar:
\\NTSER22VM1\MyShare

Press **Enter.**



Step 9:

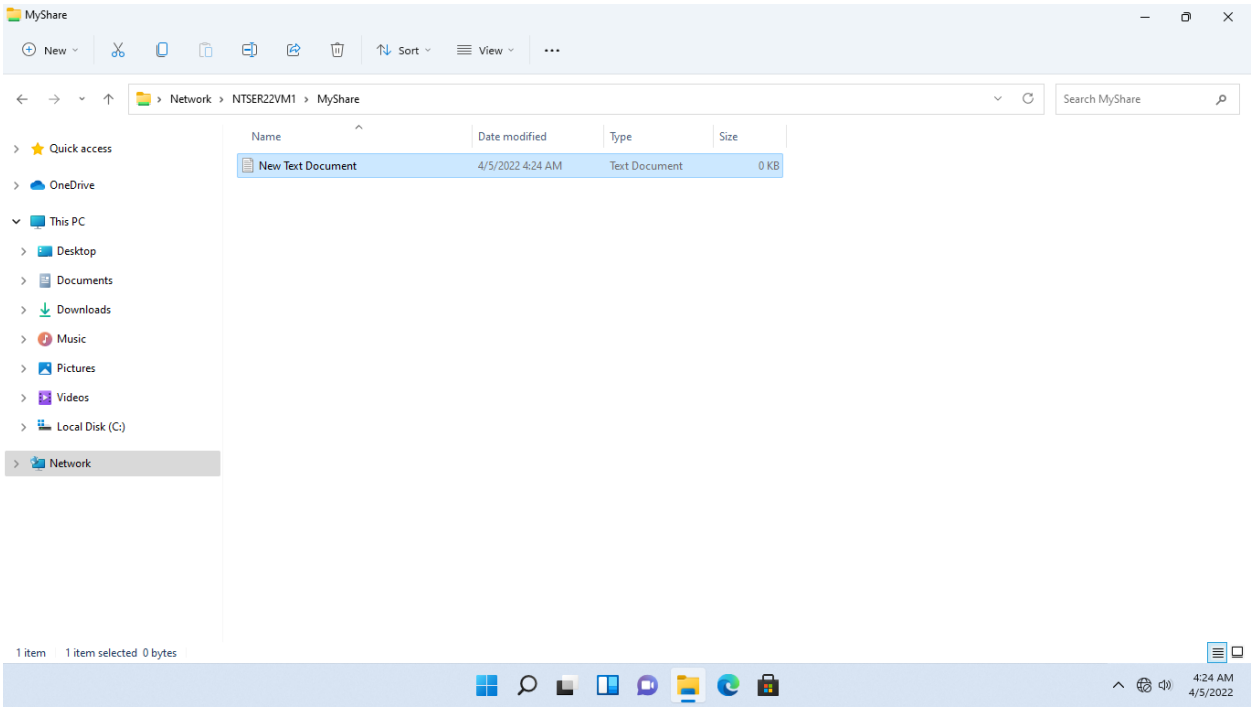
Notice you now have access to the **MyShare** shared folder.



Step 10:

Since **Everyone** has full control on this folder, you can create a new text document.

Right click anywhere on the contents pane and select **New** > **Text Document**.



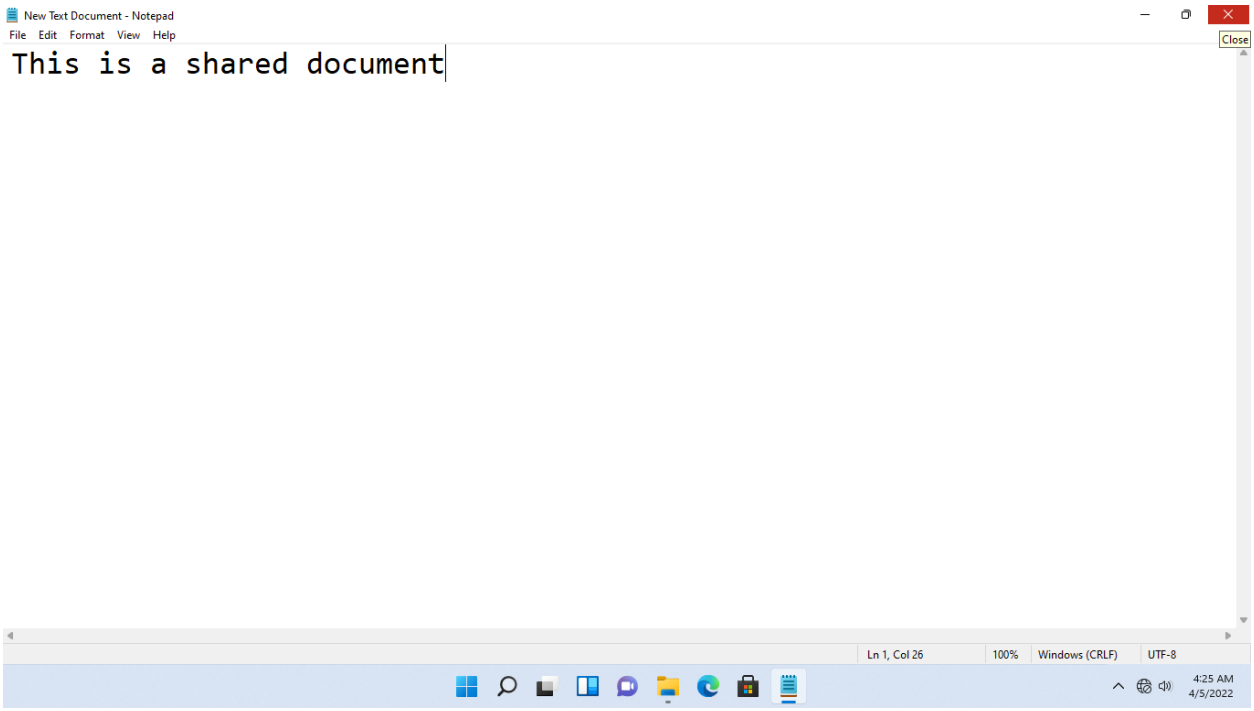
Step 11:

Double-click on **New Text Document** and type:

This is a shared document

Click the **File** menu and select **Save**.

Close the **Notepad** and **File Explorer** window.

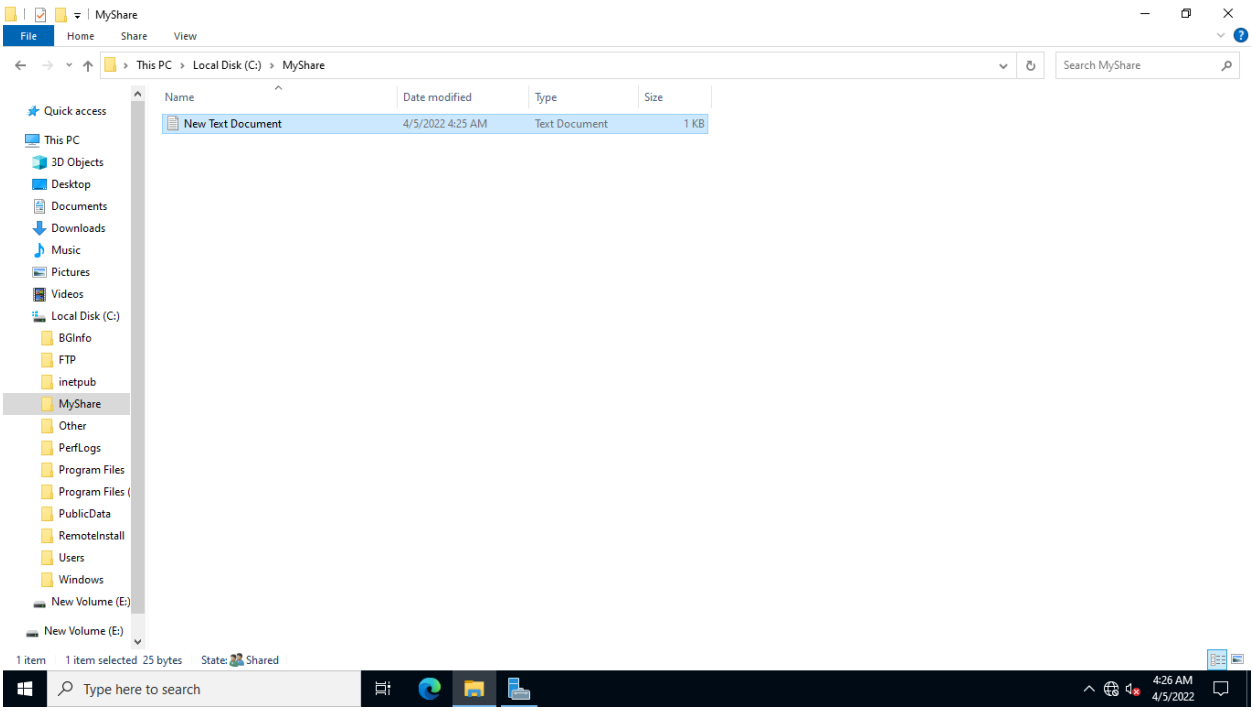


Step 12:

Connect to **NTSER22VM1**.

Open **File Explorer** from the taskbar and navigate to **This PC** > **LocalDisk**(**C**:) > **MyShare** folder

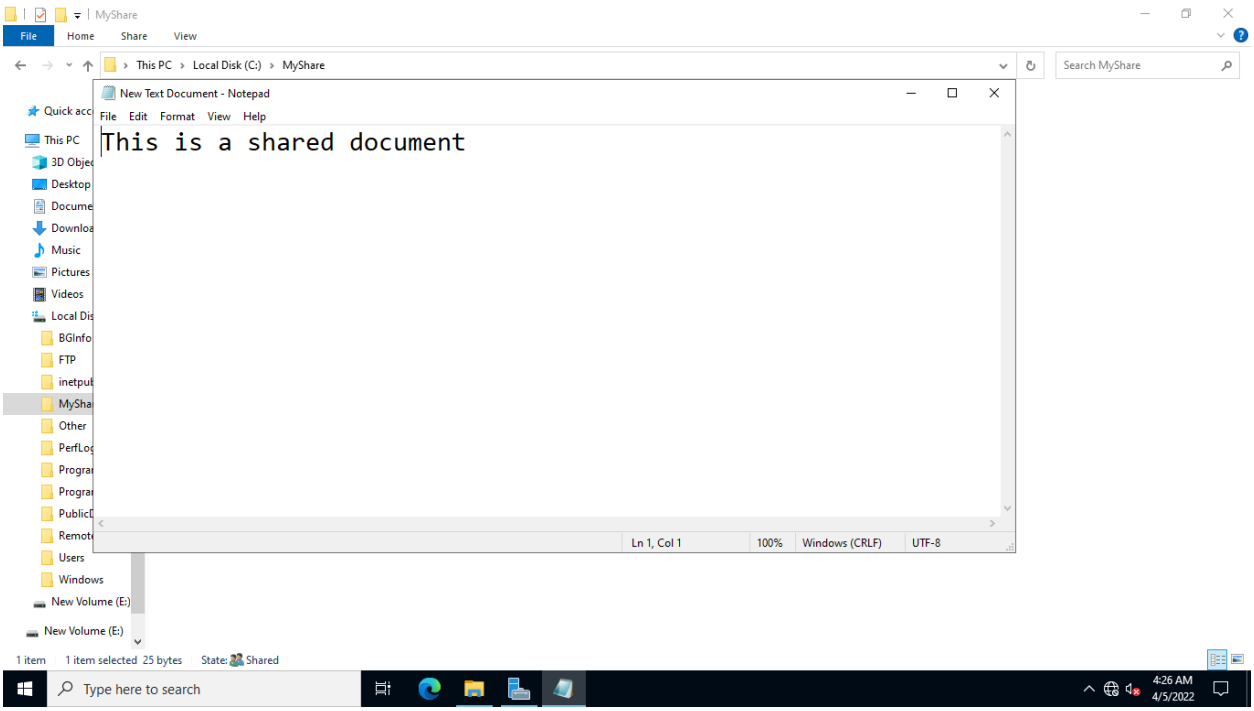
Notice the **New Text Document** you created earlier.



Step 13:

Double-click on **New Text Document**.

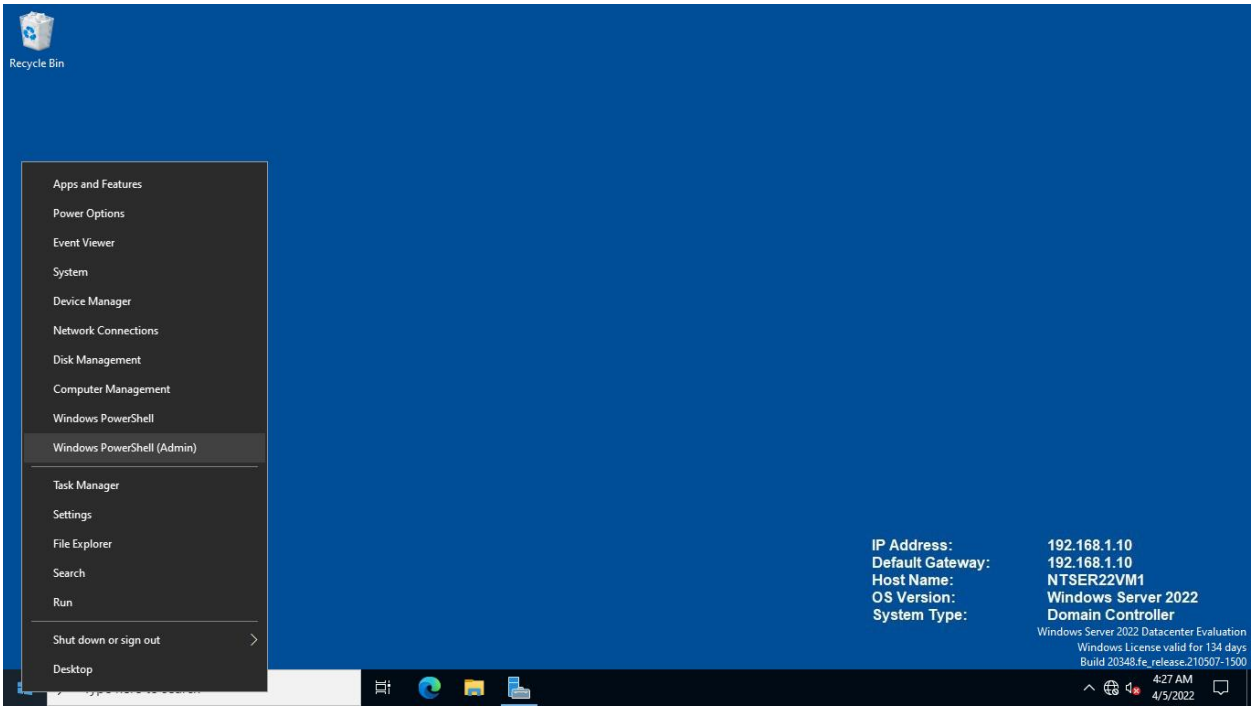
On the **New Text Document** - **Notepad** window, you can view the text that was entered earlier.



Step 14:

Next, you will check the enabled SMB version on the server.

Right-click Start and select **Windows PowerShell Administrator**.



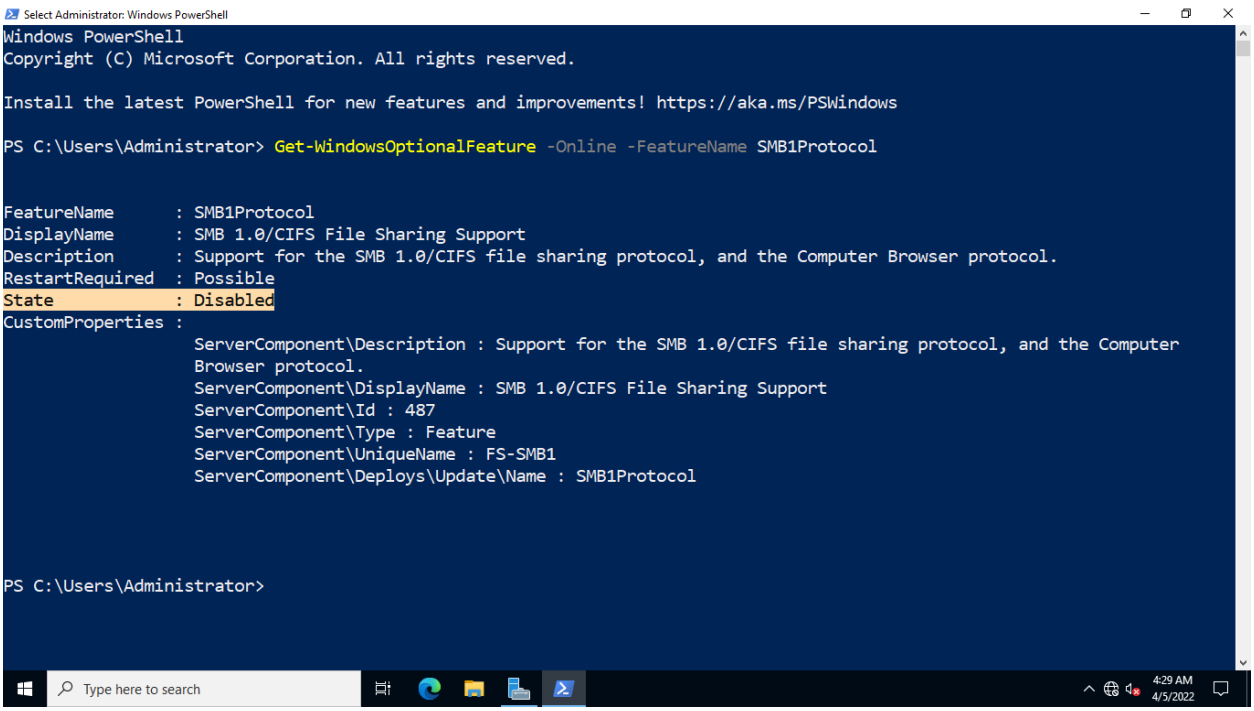
Step 15:

Click **Yes** on the **User Account Control** message box.

On the **Administrator**: **Windows PowerShell** window, type the following command:

```
Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

Press **Enter**.

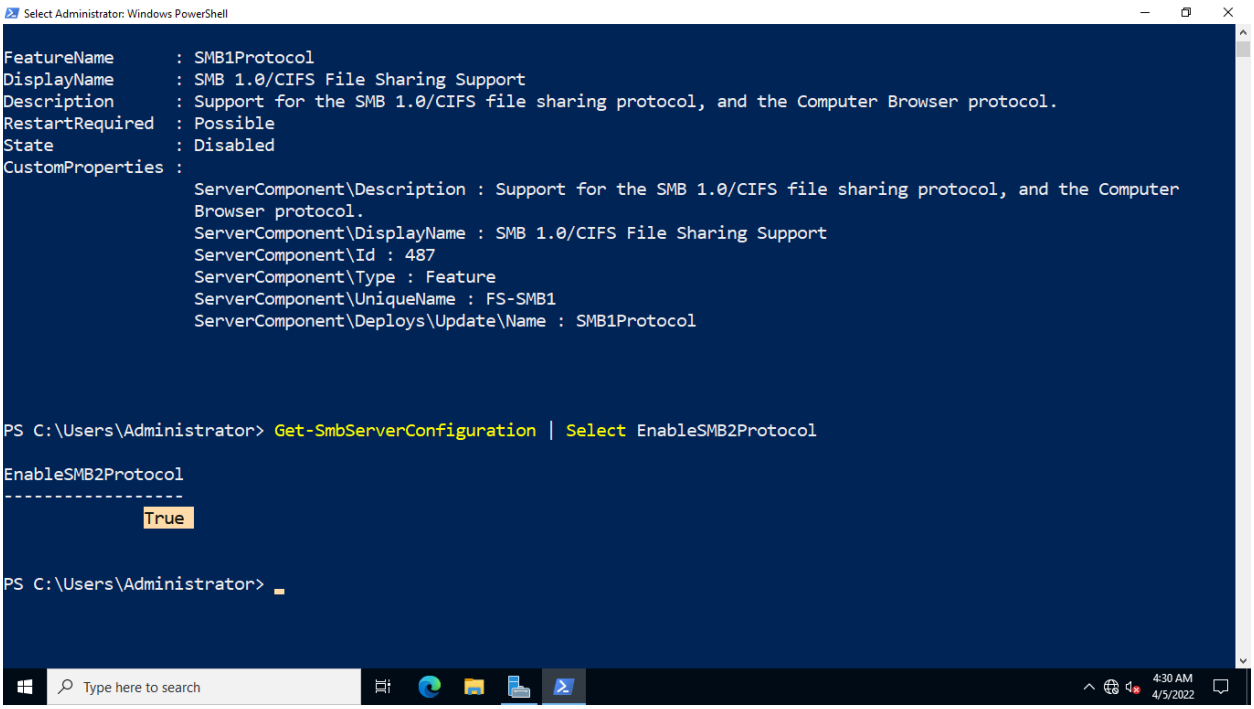


Step 16:

To check if SMBv2 is enabled, type:

```
Get-SmbServerConfiguration | Select EnableSMB2Protocol
```

Press **Enter**.



Task 3: Access Pfsense Firewall using SSH Protocol

TCP protocols such as Telnet and Secure Shell (SSH) are used to get remote access to network devices or hosts such as Linux workstations. Telnet is an insecure protocol that runs on TCP port 23 and sends data in cleartext. SSH, on the other hand, uses port 22, which is a secure port because it encrypts communication. It's commonly used to connect to network devices and Linux servers.

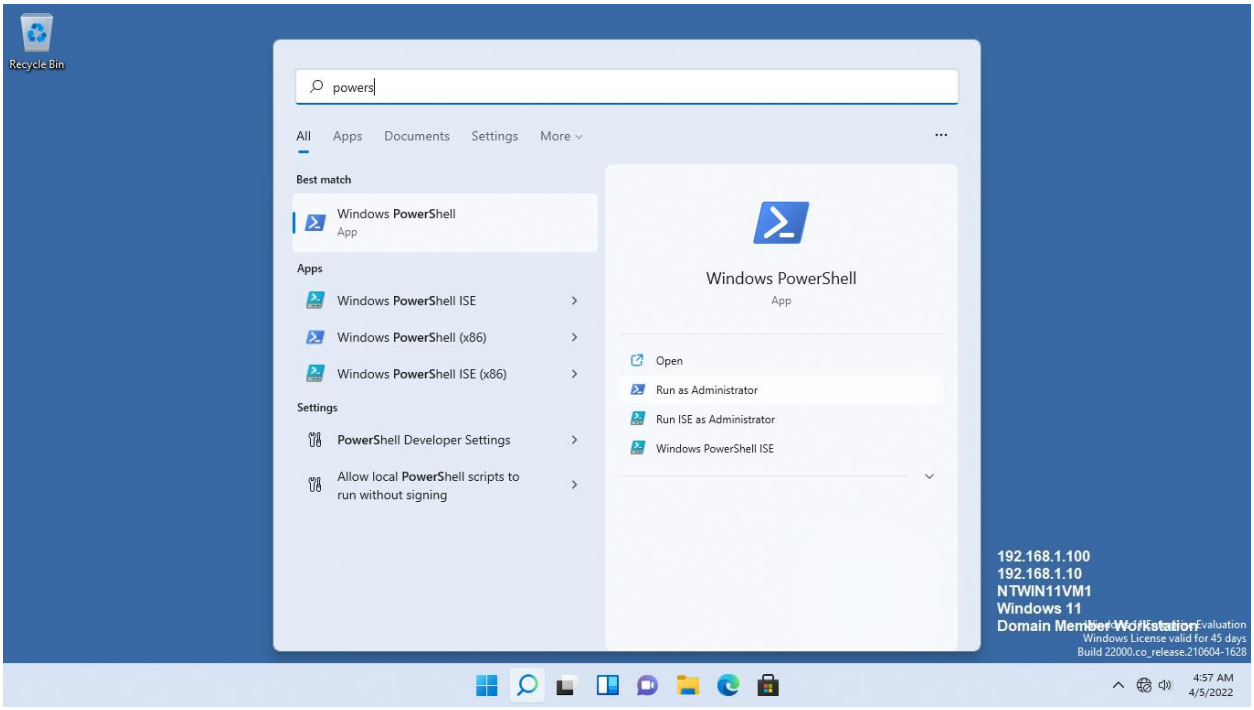
Now let's, Use Windows PowerShell to access the Pfsense firewall via SSH protocol.

Step 1:

Connect to **NTWIN11VM1**.

Click on **Start** and type: ***powershell***

Select **Windows PowerShell** > **Run as Administrator**.



Step 2:

On the **User Account Control** pop-up window, click **Yes**.

On the **Administrator**: **Windows PowerShell** window, type:

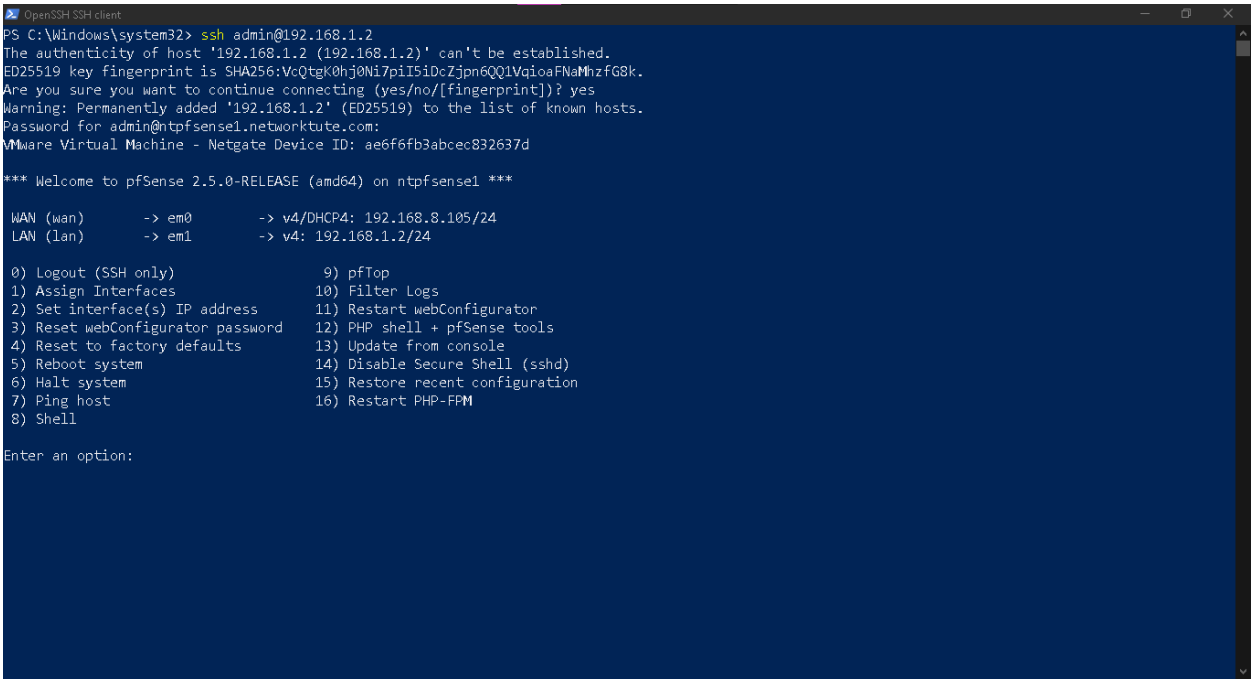
```
ssh admin@192.168.1.1
```

Press **Enter.**

Note: If you get an **Are you sure you want to continue connecting** (**yes**/**no**)? prompt, type **yes**.

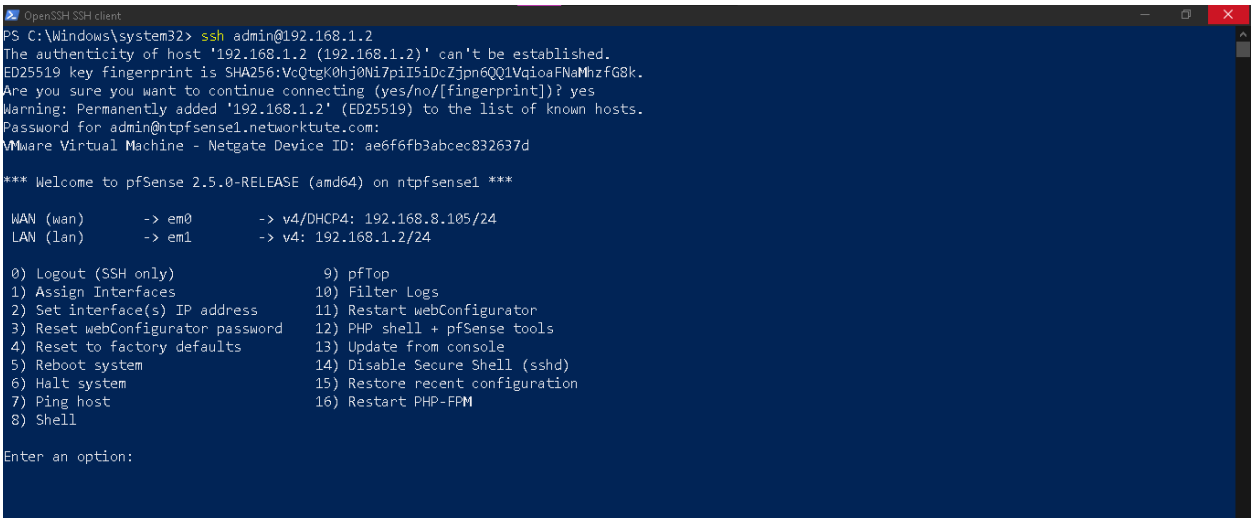
On the Password prompt, type: ***pfsense***

Press **Enter.**



Step 3:

You are now successfully connected to the pfSense firewall and have access to the different configuration options.



Note: This is the same output you'd see if you connected to the pfSense firewall via console. Once connected to the pfsense firewall, you can change the interface IP addresses, reboot the system, access the shell, and restore the system. Default manufacturer settings and more

Since this is a security device, you cannot use Telnet to access it. Telnet is mostly used on switches and routers.

Close the **Administrator**: **Windows PowerShell** window.

Special Notes

SMTP and SMTP TLS

To establish a connection between the sender, recipient, and mail server, email protocols are utilized. SMTP, POP3, IMAP, and their secure variants are the most widely used email protocols.

SMTP (Simple Mail Transfer Protocol) is a network protocol for sending and receiving email over the Internet. It's generally used for mail relaying, or sending and receiving emails between different mail servers. It can also be used to send and receive messages between a client and a mail server. It just transfers text and operates at the application layer of the OSI architecture. For all non-text traffic, the MIME (Multipurpose Internet Mail Extensions) protocol is used, which encodes all non-text traffic into text.

The Mail Transfer Agent (MTA) pushes the new message to the mail server when the sender sends an email. After then, the mail server will communicate with the recipient's mail server, which will receive, process, and deliver the message to the relevant mailbox.

For submission and relay, SMTP uses distinct ports. When an email client connects to the mail server and sends a message, it is called a submission operation. The sending and receiving of emails between two mail servers is known as relay operation. These two procedures are carried out at the following ports:

- **TCP port 25 -** SMTP relay between two email servers is the most common application. It can be used to submit information; however, it is insecure and vulnerable to attack. As a result, most Internet Service Providers (ISPs) block this port due to the high volume of spam messages it receives. transmitted from computers that have been hacked. For the most part, more secure protocols are utilized. submissions.
- **TCP port 587** - It is used for Secure Sockets Layer (SSL)/Transport Layer Security and is the default port for mail submission (TLS). This means that during the client-server handshake, the client will attempt to upgrade to an encrypted connection. A secure TLS connection will be formed if the server is compatible, that is, if it supports SSL/TLS. If the server is incompatible, a connection will be created, but it will be for plain-text communication only.
- **TCP port 465** - It's a different port for sending mail, and it's used for implicit SSL/TLS. This means that during the client-server handshake, the client will attempt to upgrade to an encrypted connection but will not check for server compatibility. The connection will be established and is secure if the server supports SSL/TLS. The connection will be dropped if the server is incompatible, and transmission will not take place.

IMAP and POP3

On the client side, the Internet Message Access Protocol (IMAP) is utilized to connect to the mail server. It's a term that's widely used in the context of email service providers. The protocol for connecting to the mail server is configured when an email program is configured on the host or a phone. All emails that have been downloaded from the server have remained on the server. When an email application is set up to use IMAP, only the email headers are visible at first. When the message is selected and opened, the actual message is downloaded.

TCP port 143 is used by IMAP. IMAP over SSL/TLS, which runs on TCP port 993, is the secure version of IMAP. Unlike IMAP, while using IMAP over SSL, the client communicates with the server through encrypted communication, which is more secure.

On the client side, Post Office Protocol version 3 (POP3) is used to establish a connection to the mail server. The key distinction between IMAP and POP3 is that with POP3, email messages are downloaded from the server to the client and then forwarded to the recipient. The file was removed from the server. POP3 uses TCP port 110, and if you choose the secure option, it uses TCP port 110. TCP port 995 is used for POP3 over SSL/TLS.

Task 4: Examine and Configure DNS Server on Domain Controller

DNS stands for Domain Name Server, and it is a network service that converts domain names to IP addresses. DNS is mostly used on UDP port 53; however, it may also be used on TCP port 53.

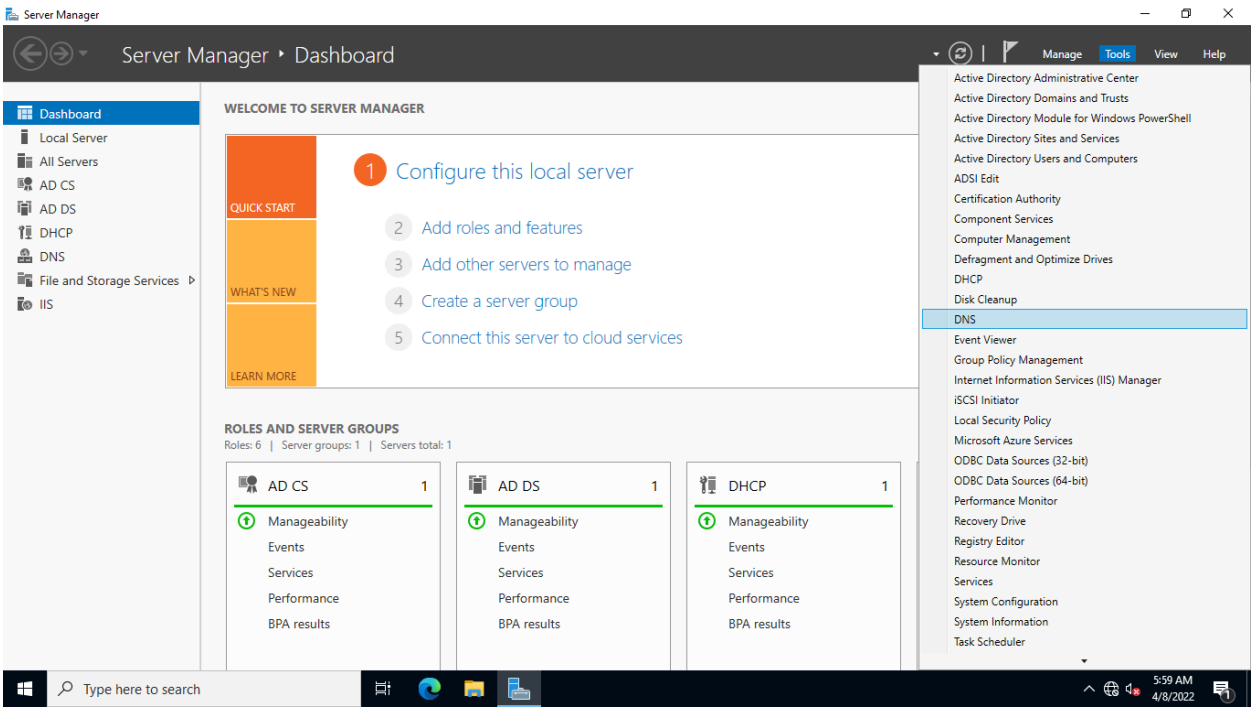
On the Internet and in private networks, DNS is employed. **NTSER22VM1** serves as the domain controller and DNS server for networktute.com in our lab. Because all computers are registered with the DNS, they may be found using their names. (you can put an easy name to the ip address of you existing pc and resolve them too.)

Now let’s, setup the DNS parameters and how they function will be examined. You'll also look at fundamental DNS settings like lookup zones and DNS forwarders, as well as how DNS converts names to IP addresses.

Step 1:

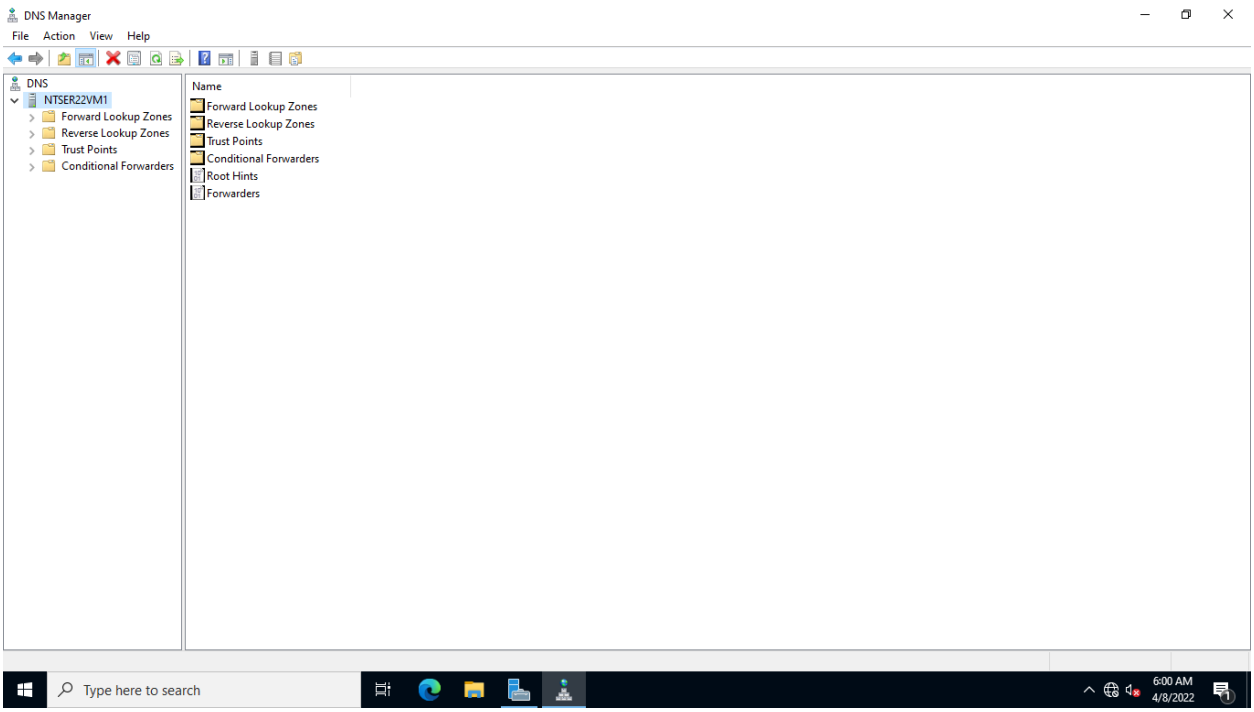
Connect to **NTSER22VM1**, where the **Server Manager** window is open.

On the **Server Manager** window, click **Tools** and select **DNS**.



Step 2:

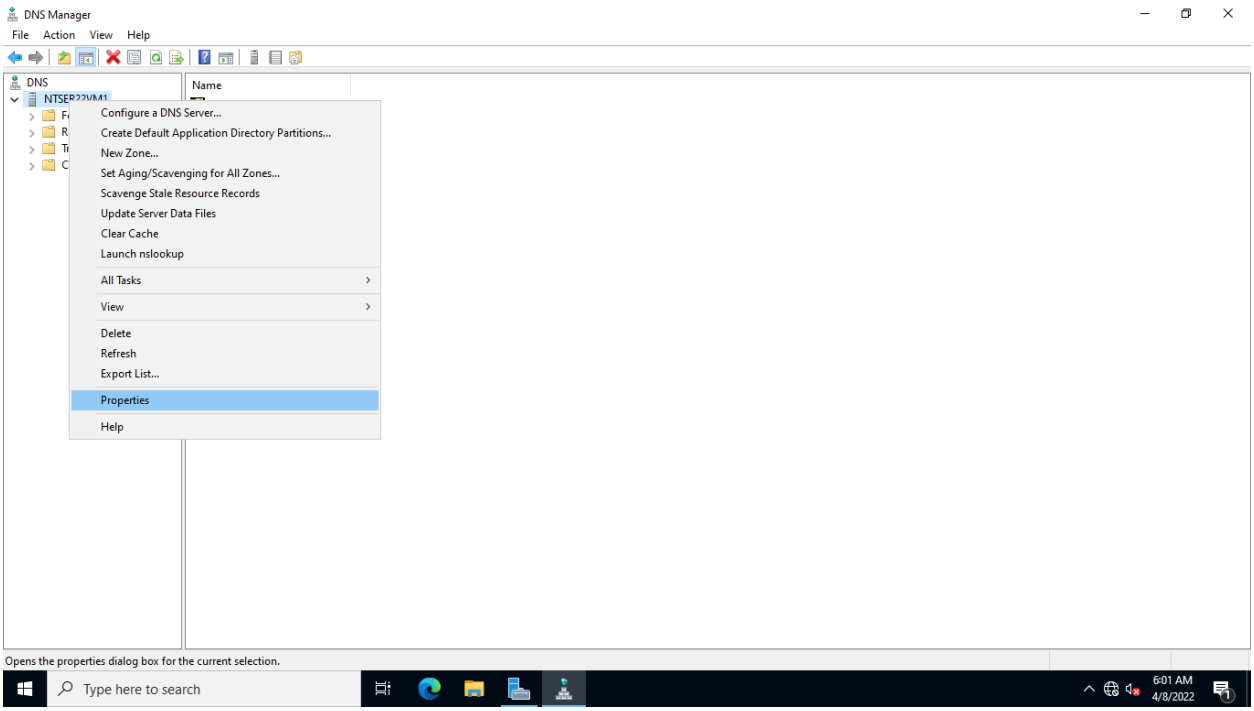
On the **DNS Manager** window, expand **NTSER22VM1**.



Note: Notice that there are Forward and Reverse Lookup zones. Forward lookup zones enable us to resolve the domain name to IP address, while reverse lookup zones do the opposite, resolves the IP address to the resource name.

Step 3:

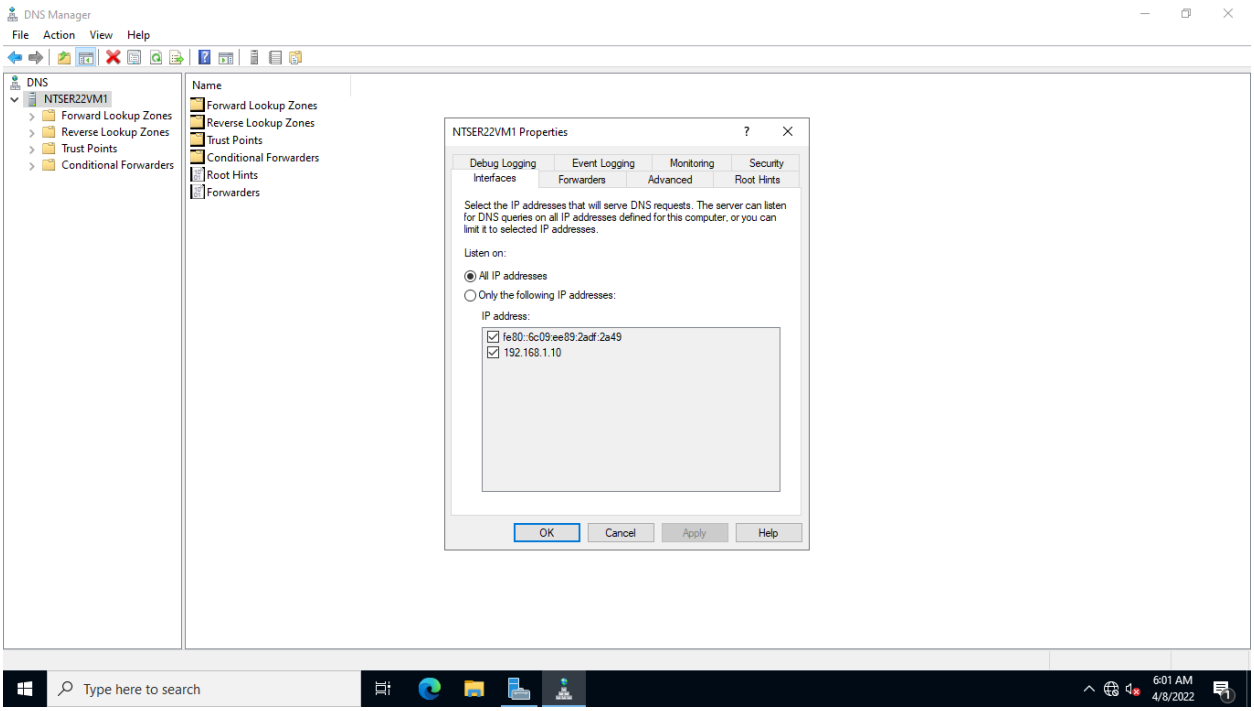
To view basic DNS server settings, right-click on **NTSER22VM1** and select **Properties**.



Step 4:

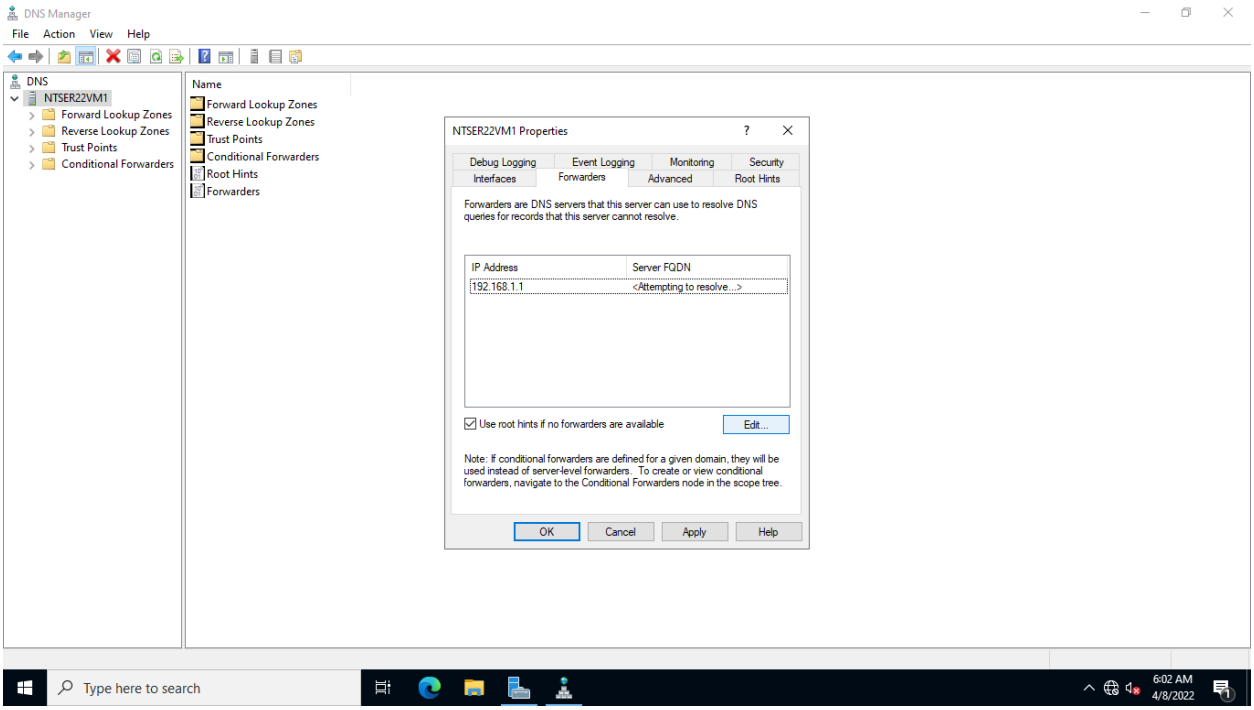
On the **NTSER22VM1 Properties** window, settings related to listener IP address, Forwarders, Root Hints and Debug can be viewed.

Go through each tab and view the options available.



Step 5:

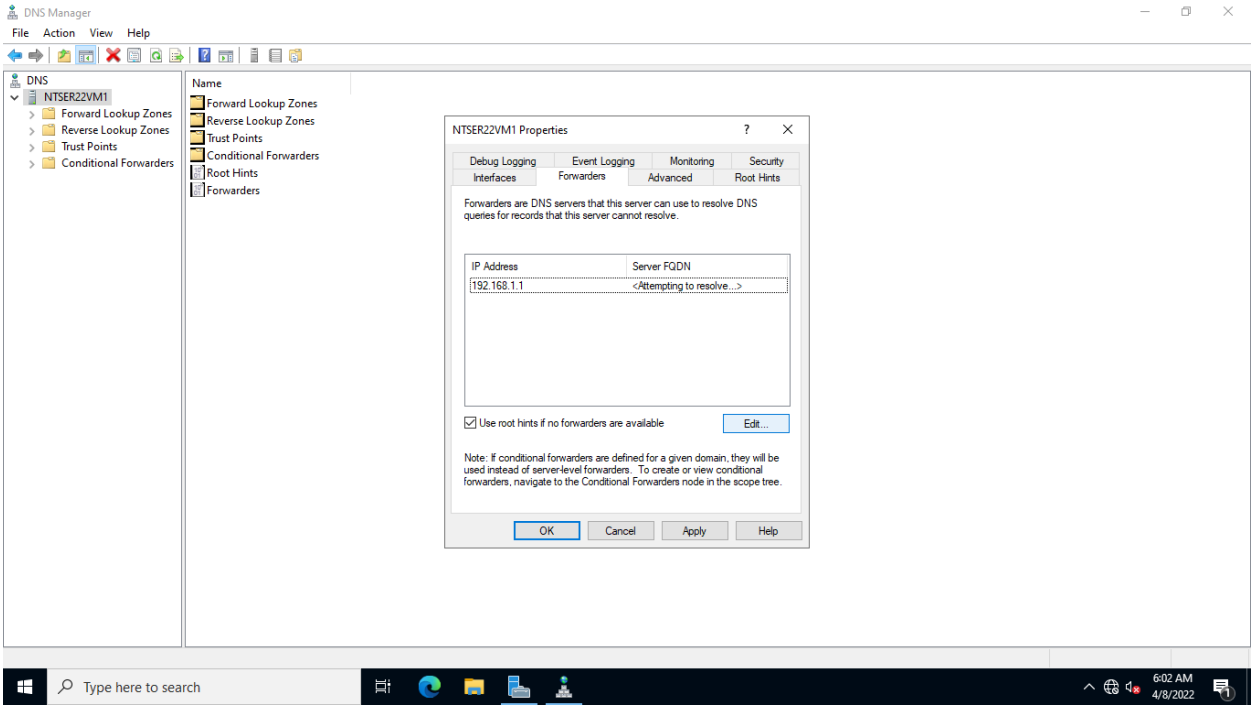
Select the **Forwarders** tab.



Step 6:

You will now add Google's DNS server to the forwarders list.

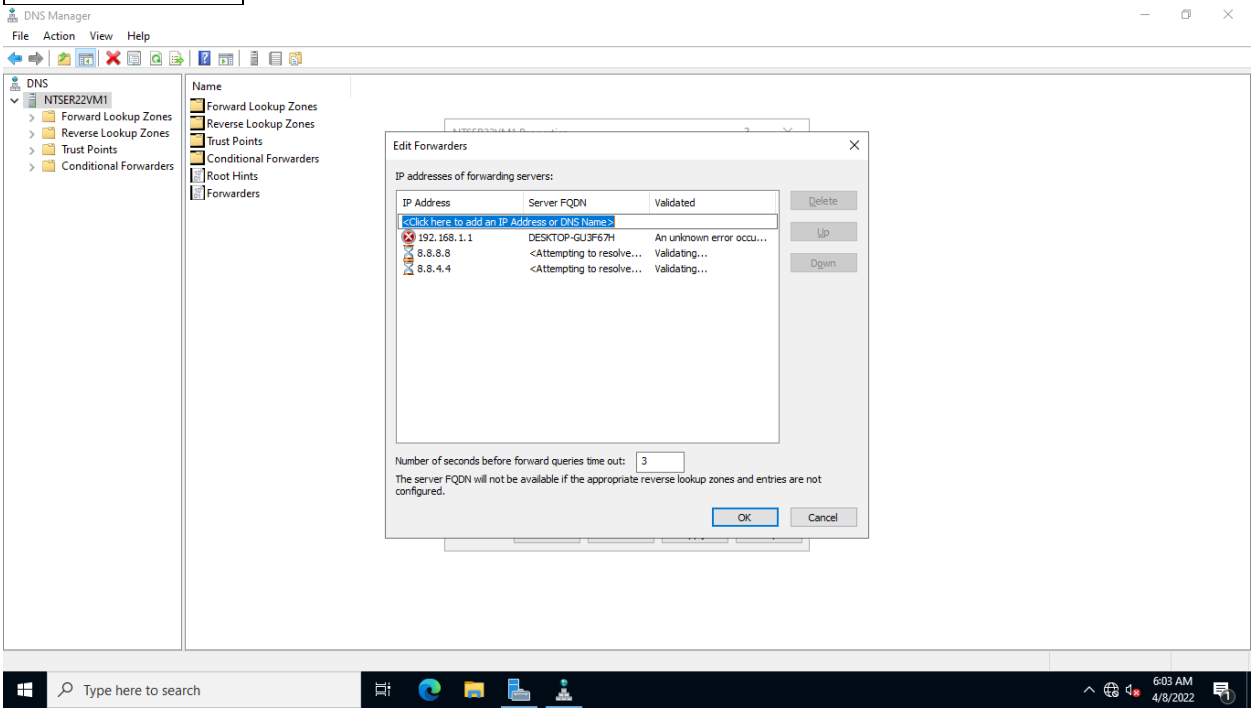
Click **Edit.**



Step 7:

On the **Edit Forwarders** dialog box, type the following IP addresses on the <**Click here to add an IP Address or DNS Name**> (Press **Enter** after entering each IP address):

8.8.8.8
8.8.4.4



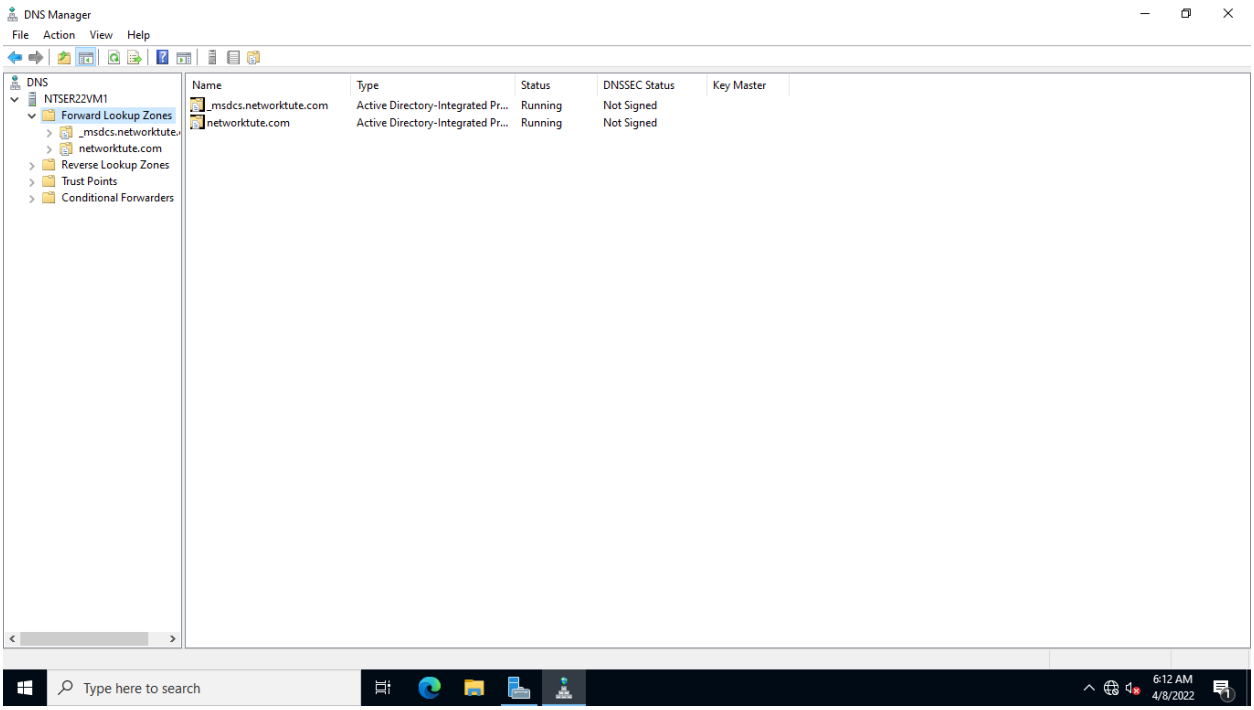
Note: From the output, it can be seen that though the servers are validated as OK, you get. This is because this server has no access to the Internet.

Click **OK**.

Close the **NTSER22VM1 Properties** window.

Step 8:

Back on the **DNS Manager** window, expand **Forward Lookup Zones**.

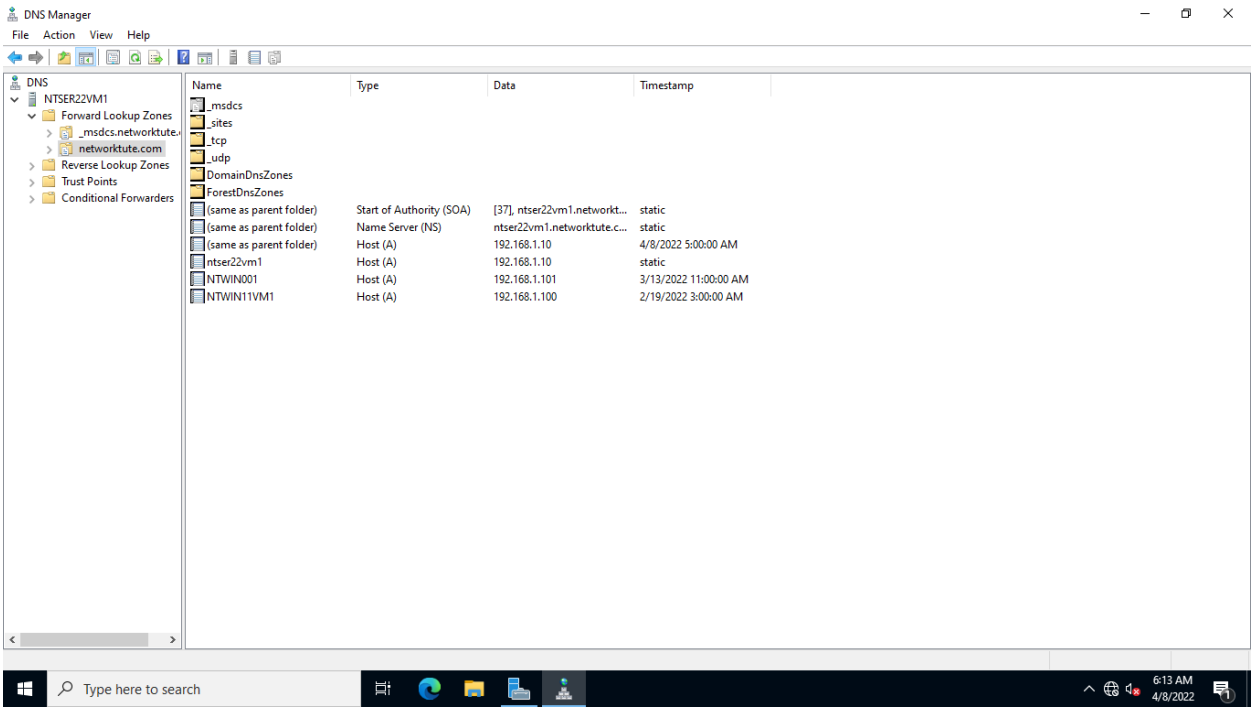


Note: Notice that you only have forward lookup zones for the NETWORKTUTE.com domain.

Step 9:

On the left pane, click on **NETWORKTUTE.COM**.

On the right pane, you will notice computers that are registered to the DNS. These names can be resolved by any client that uses **NTSER22VM1** as a DNS server.

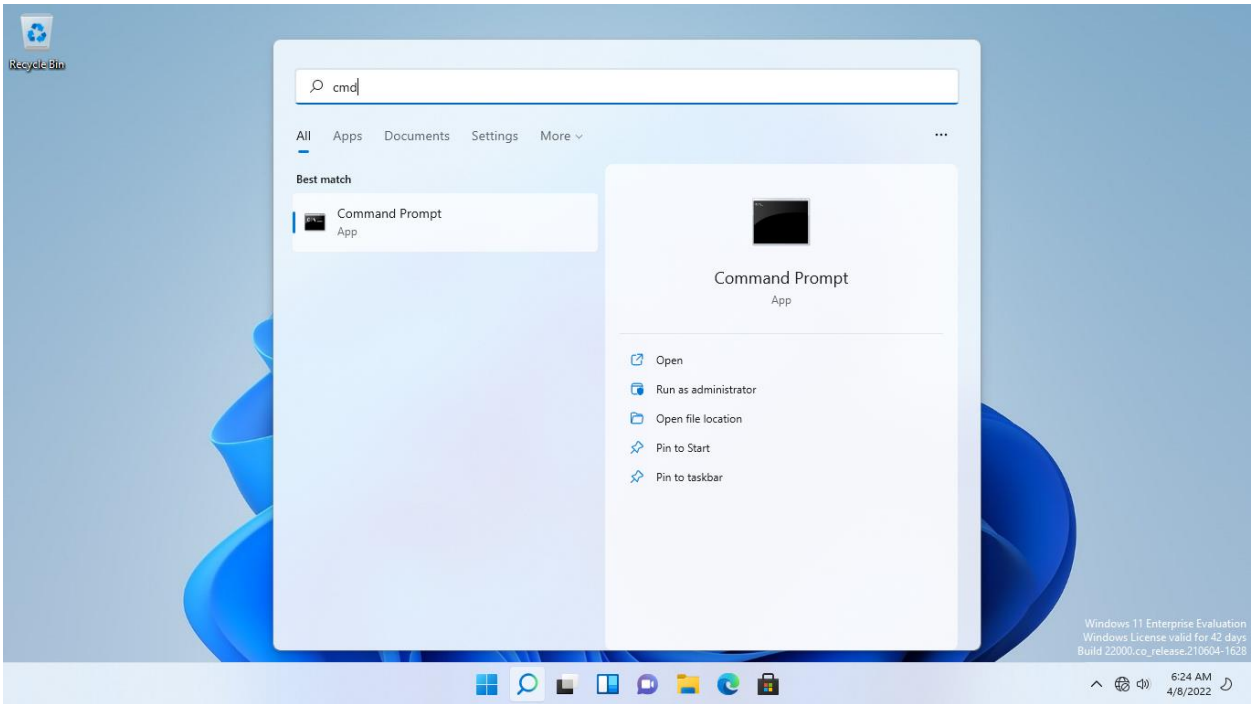


Step 10:

Connect to **NTWIN11VM1**.

Click on **Start** and type: ***cmd***

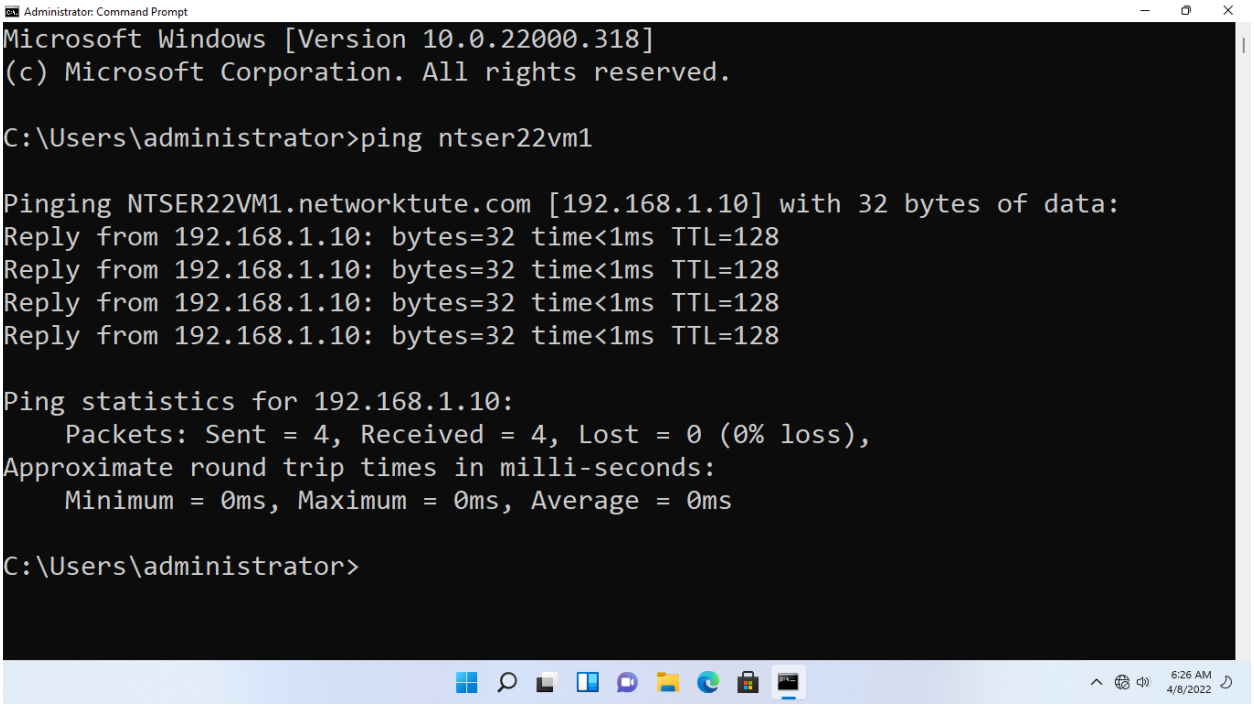
Select **Command Prompt**.



Step 11:

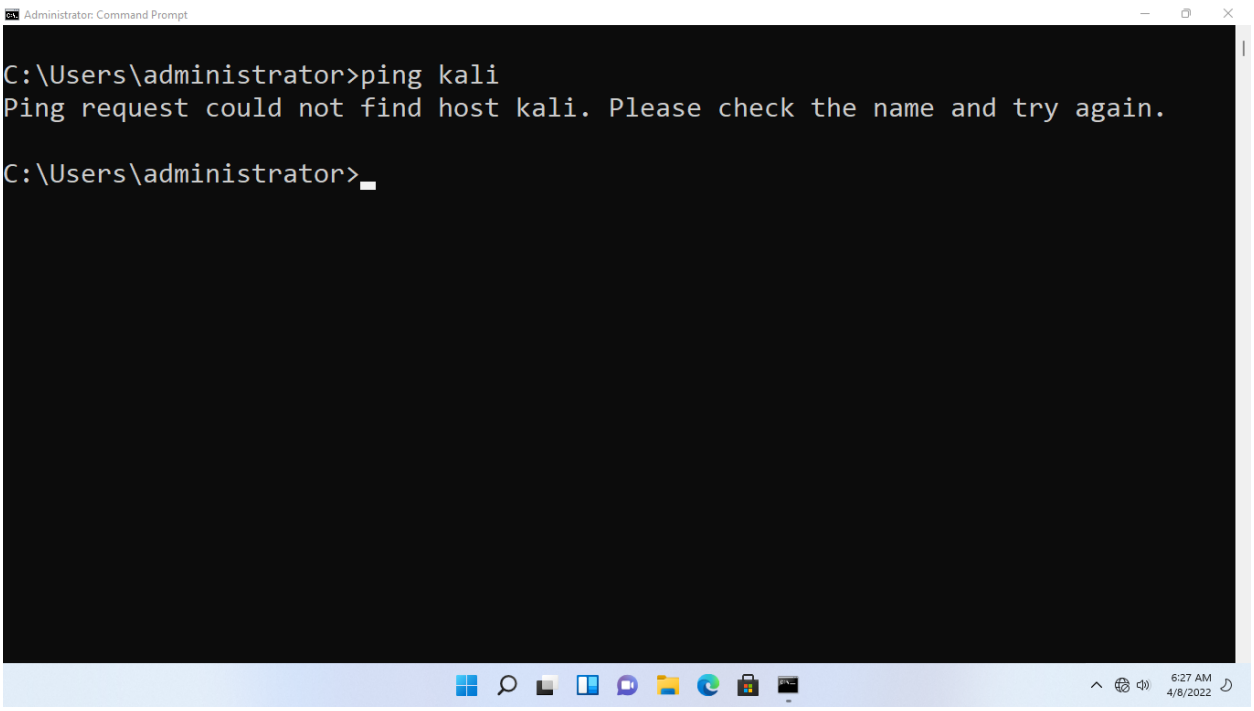
You will now test the DNS to see if it will be resolved to the IP address.

On the **Command Prompt** window, type the following and press **Enter**: ***ping ntser22vm1***



Step 12:

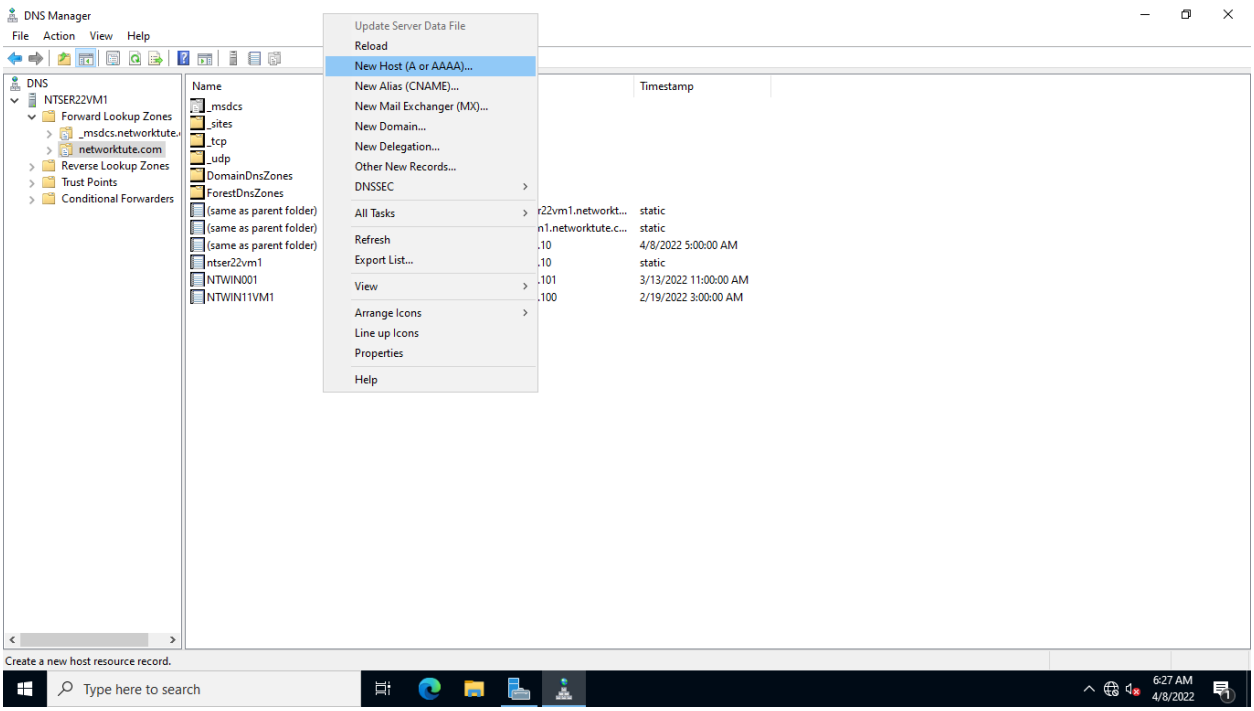
Next, you will try to ping the Kali Linux server. Type the following and press Enter: ***ping kali***



Step 13:

Connect to **NTSER22VM1**. You will be on the **DNS Manager** window.

You will add an A record for Kali Linux. Right click on an empty space in the right pane and select **New Host** (**A or AAAA**)

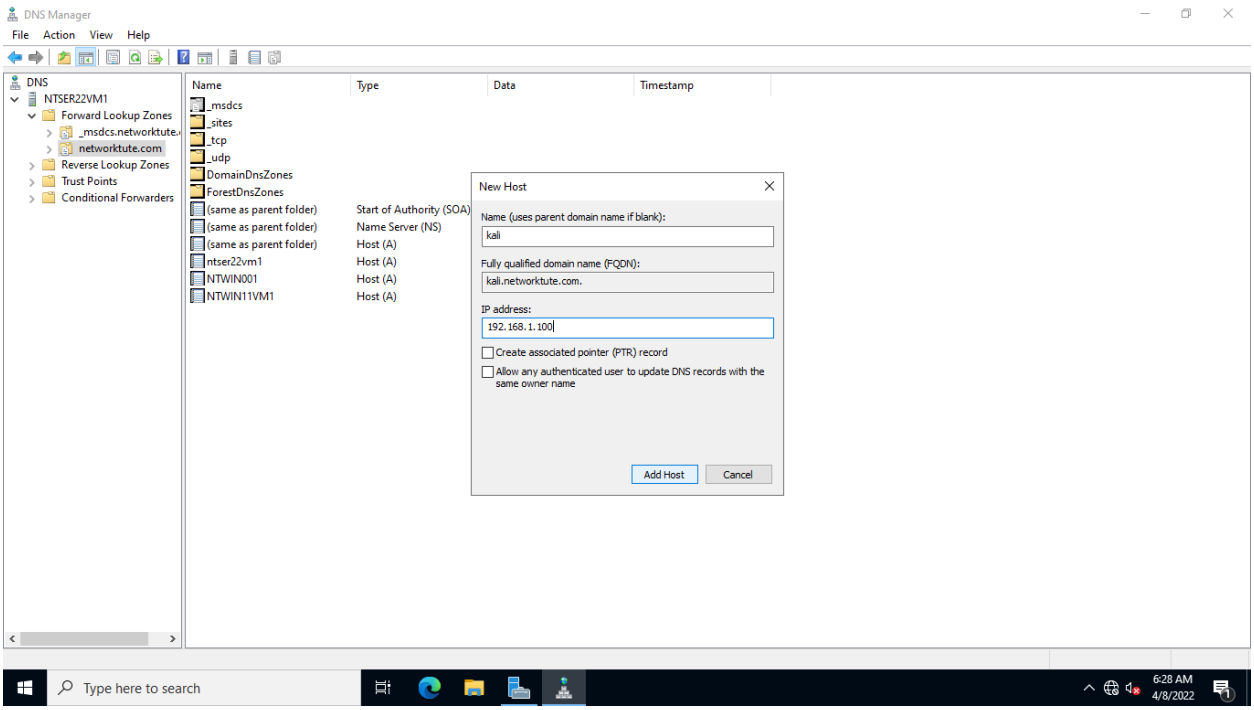


Step 14:

On the **New Host** dialog box, type the following in the **Name** and **IP address** field:

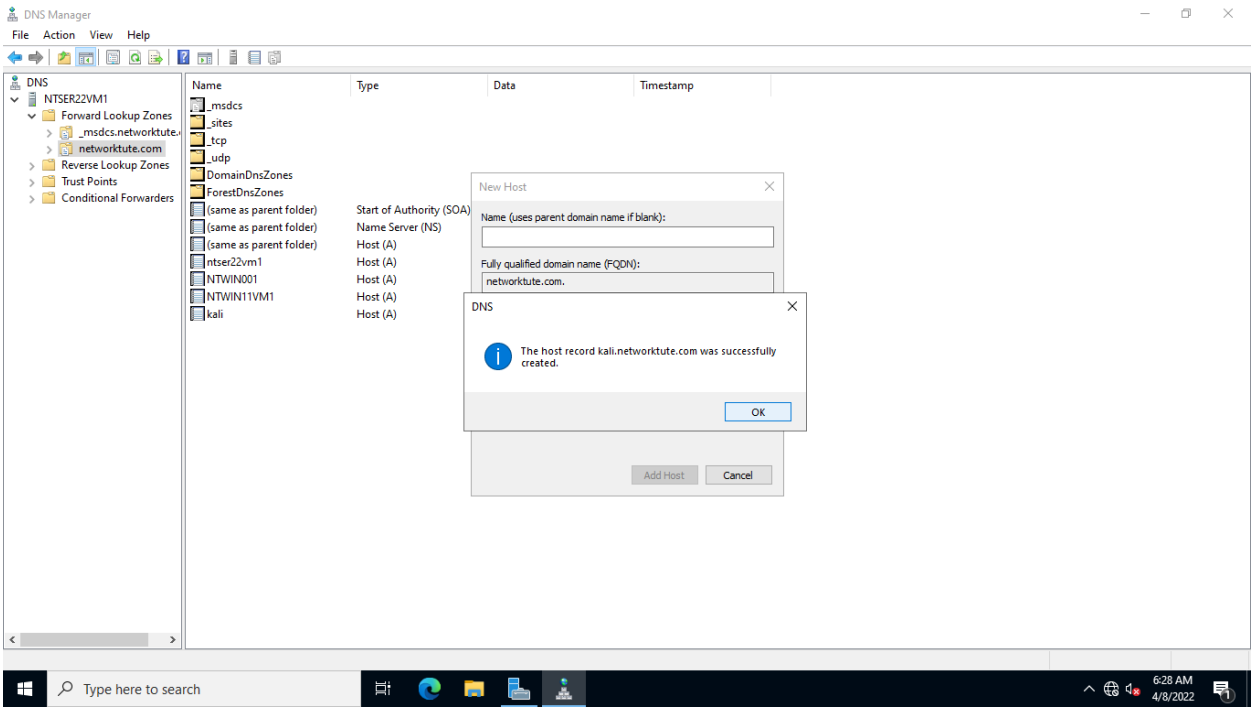
Name: kali IP address: 192.168.1.100

Click **Add Host**.



Step 15:

Click **OK** on the **DNS** message box.

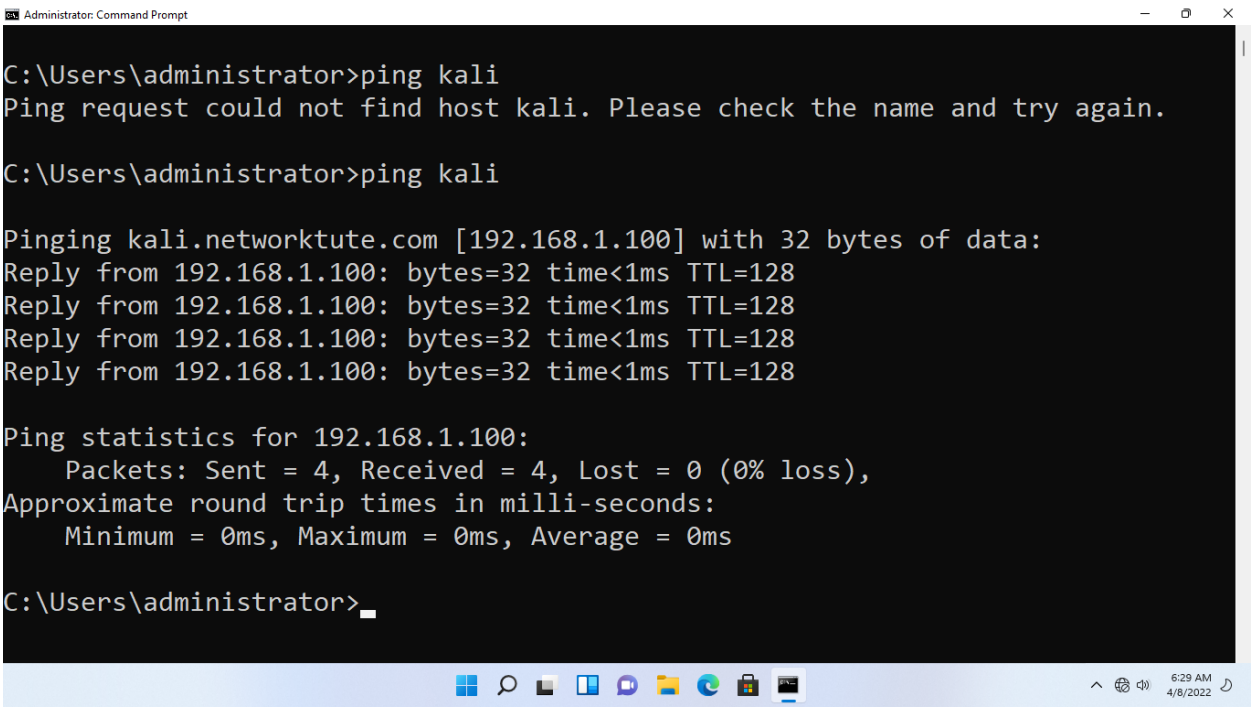


Close the **New Host** and **DNS Manager** window.

Step 16:

Connect to **NTWIN11VM1**.

On the **Command Prompt** window, type the following command and press **Enter**: ***ping kali***



Task 5: Configure DHCP Server on PfSense Firewall

DHCP (Dynamic Host Configuration Protocol) allocates an IP address to a host together with the default gateway and other network characteristics like DNS. If your environment does not have a DHCP server, each computer will need to be manually assigned an IP address. If you have a network with 100 or even 1,000 PCs, this can take a long time.

On a Windows server, Linux system, router, or firewall, a DHCP server can be set up. Even better, DHCP software tools can be downloaded for free and utilized on your own computer. DHCP is an UDP-based protocol that communicates over two ports. Clients to server communication takes place on UDP port 67, whereas server to client communication takes place on UDP port 68. When a server transmits a DHCP offer to a client, it uses UDP port 68 to do so.

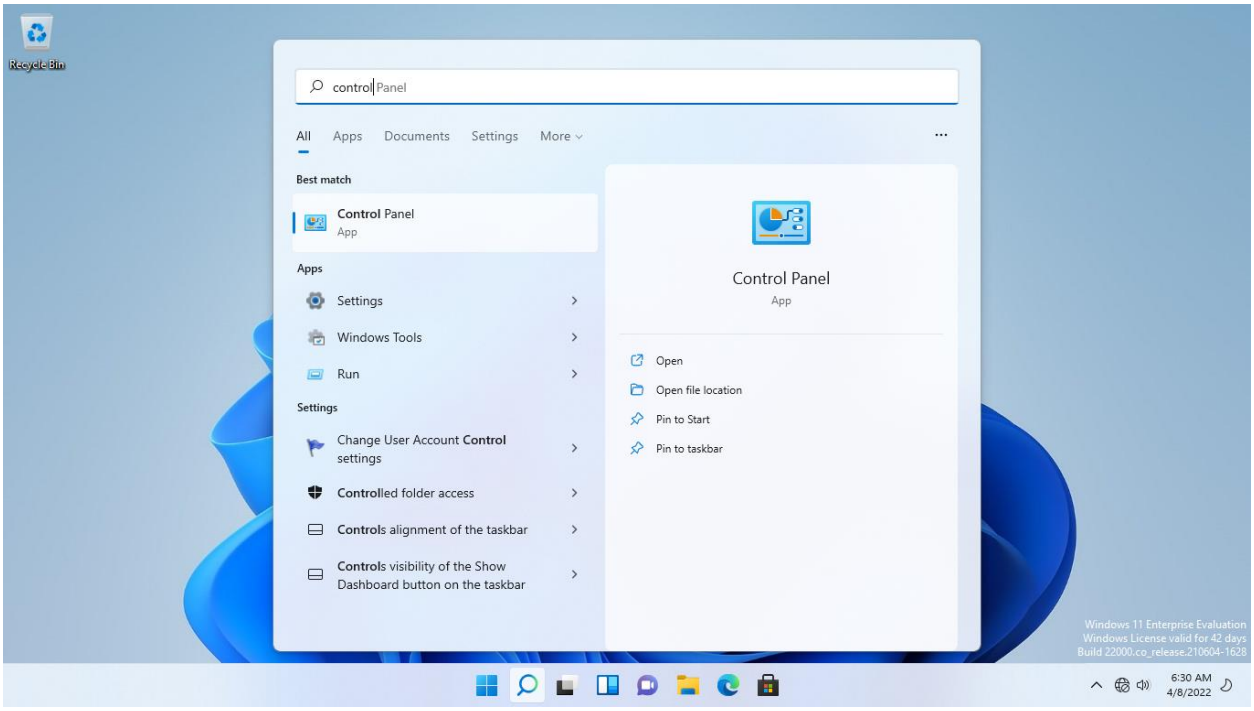
In this task, DHCP will be configured on the pfsense firewall. You will then see how it assigns an IP address to a host.

Step 1:

Connect to **NTWIN11VM1**.

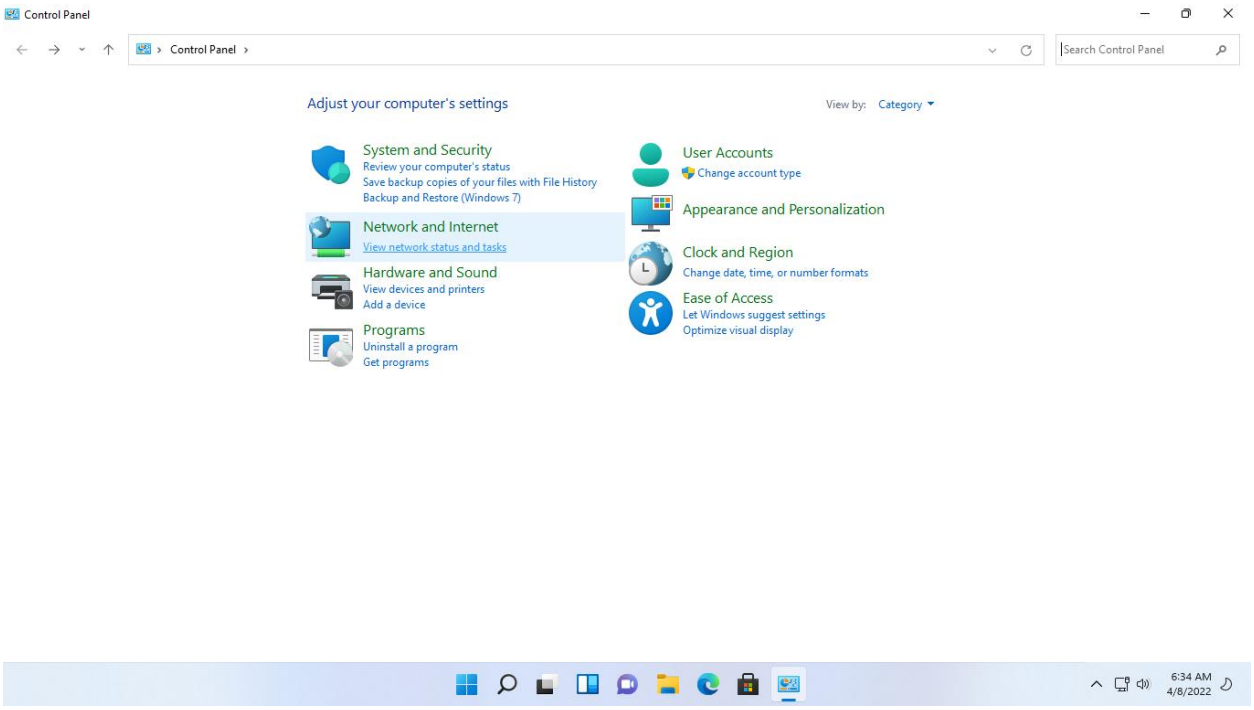
Click on the **Start** menu and type: ***control***

Select **Control Panel**.



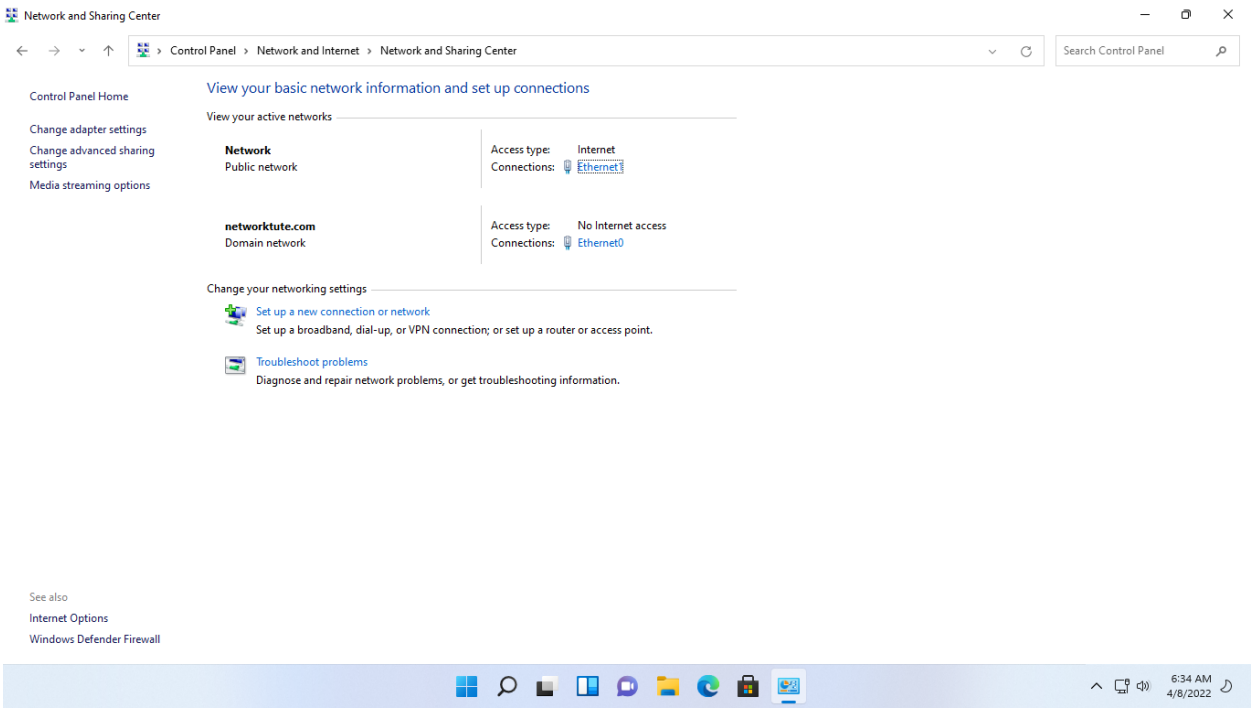
Step 2:

On the **Control Panel** window, under **Network and Internet**, click on the **View network status and tasks** link



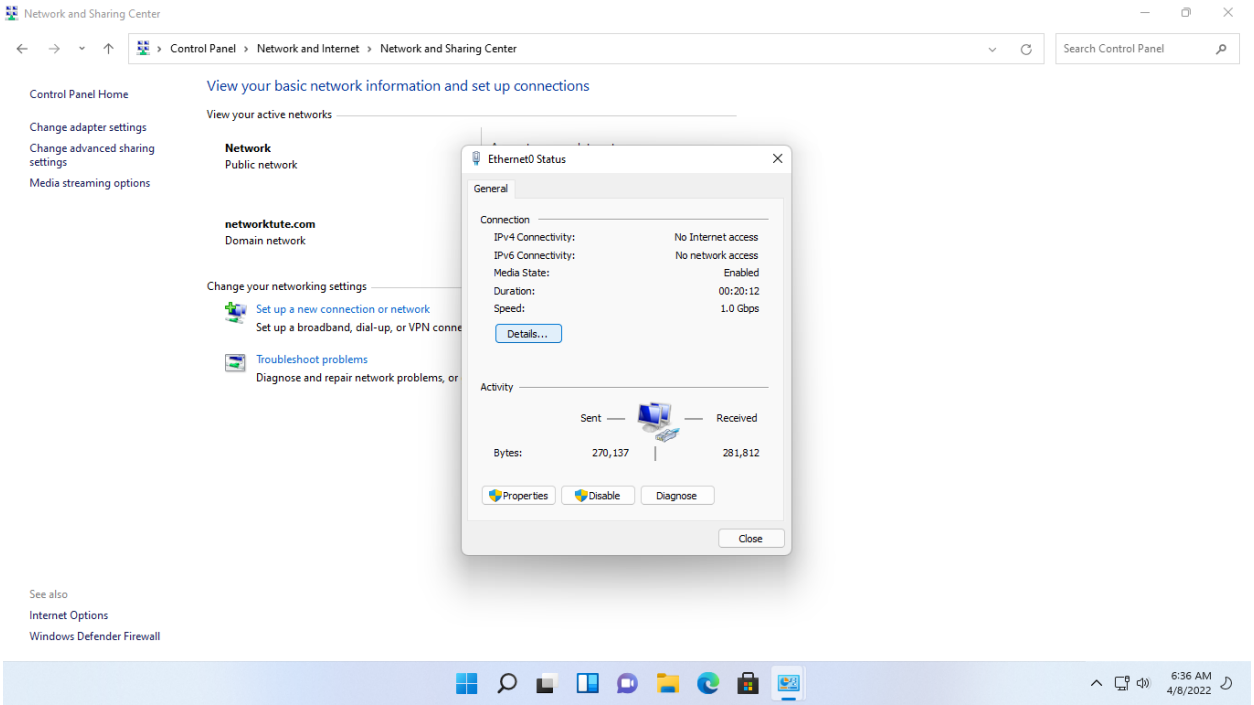
Step 3:

On the **Network and Sharing Center** window, notice that **NTWIN11VM1** has two network interface cards. One is the domain network - **Ethernet**, and the other is the Public Network - **Ethernet 1.**



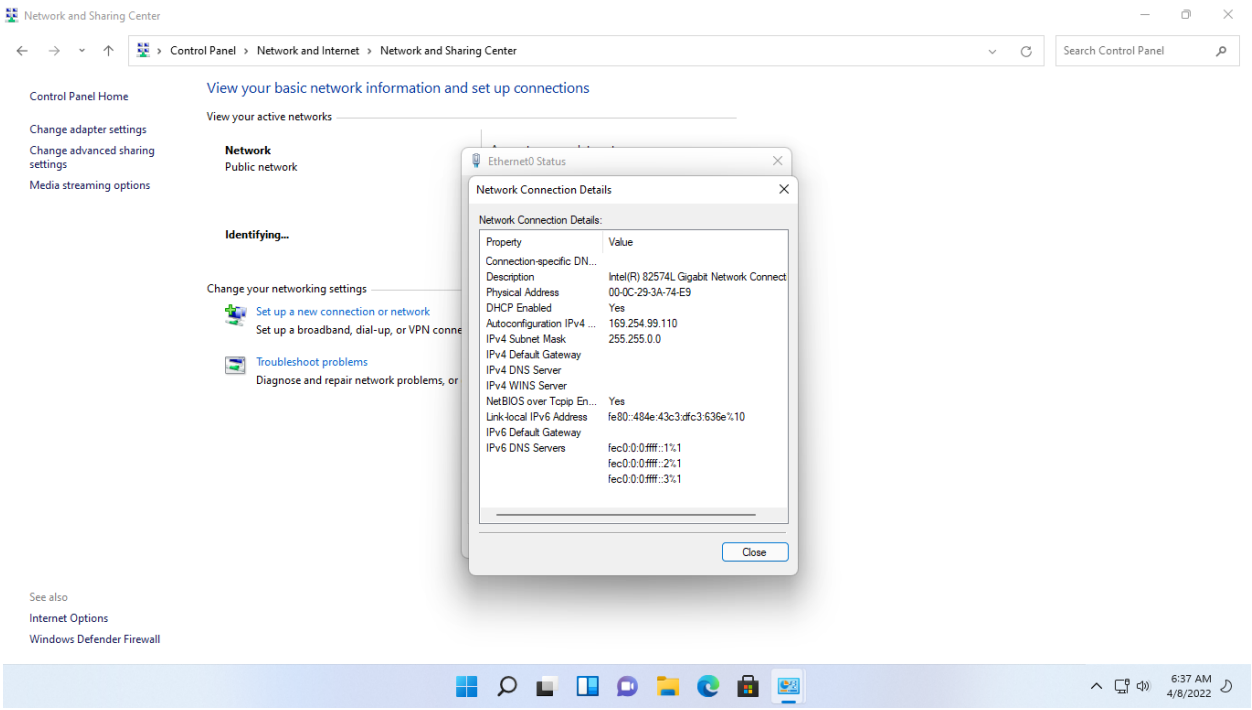
Step 4:

On the **Ethernet 1pra Status** dialog box, click the **Details** button.



Step 5:

On the **Network Connection Details** dialog box, notice that you don't have a valid IP address on this interface and that DHCP is enabled



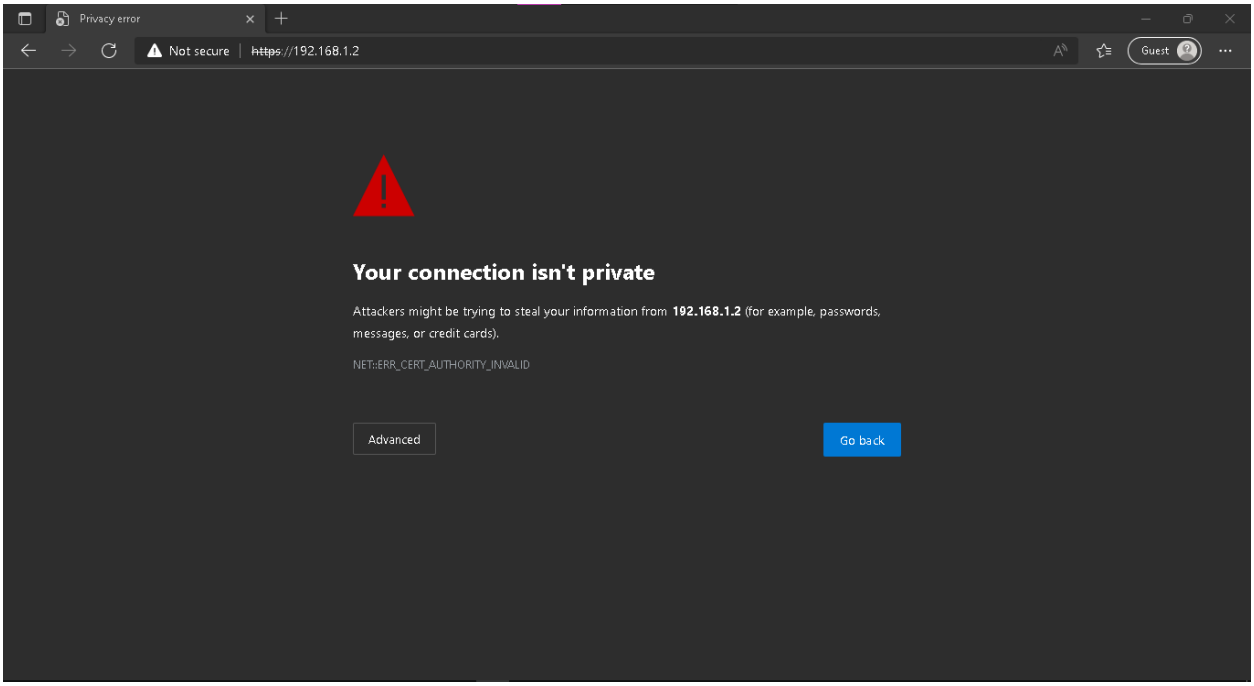
Step 6:

Open **Microsoft Edge** browser from the taskbar.

In the Microsoft Edge browser, click in the address bar and type:

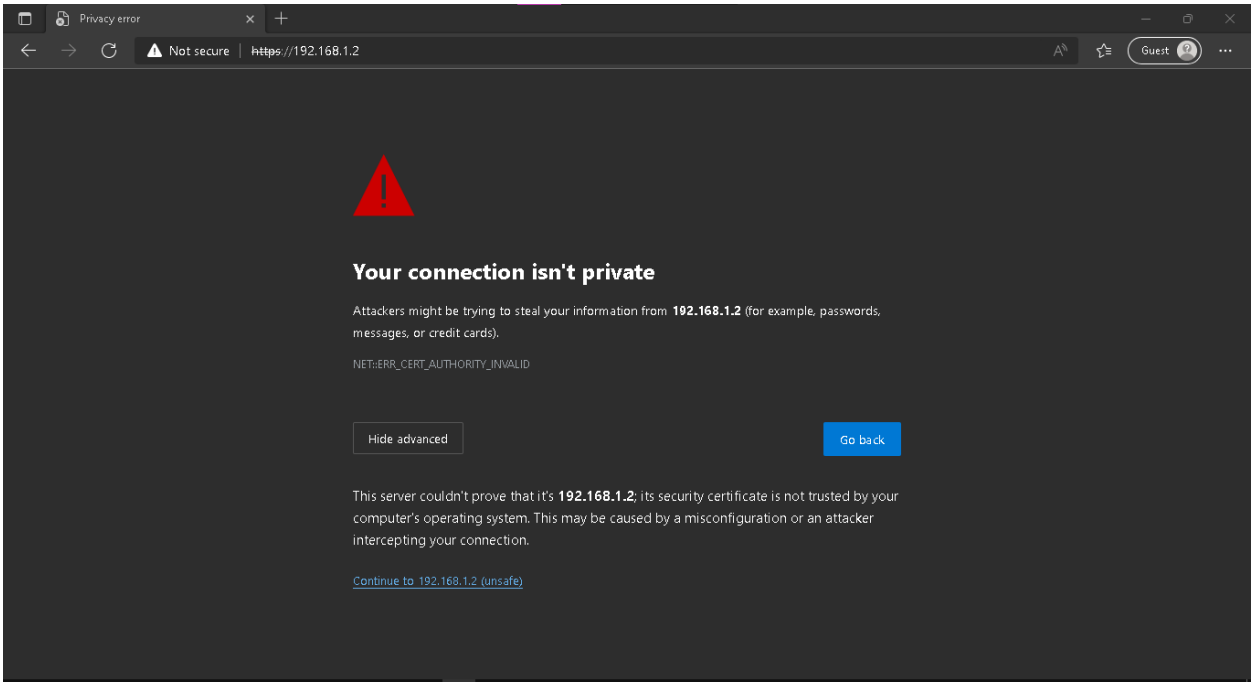
https://192.168.1.1

Press **Enter**.



Step 7:

Click **Advanced** in the **Microsoft Edge** browser and click the **Continue to 192.168.1.2** (**unsafe**) link.



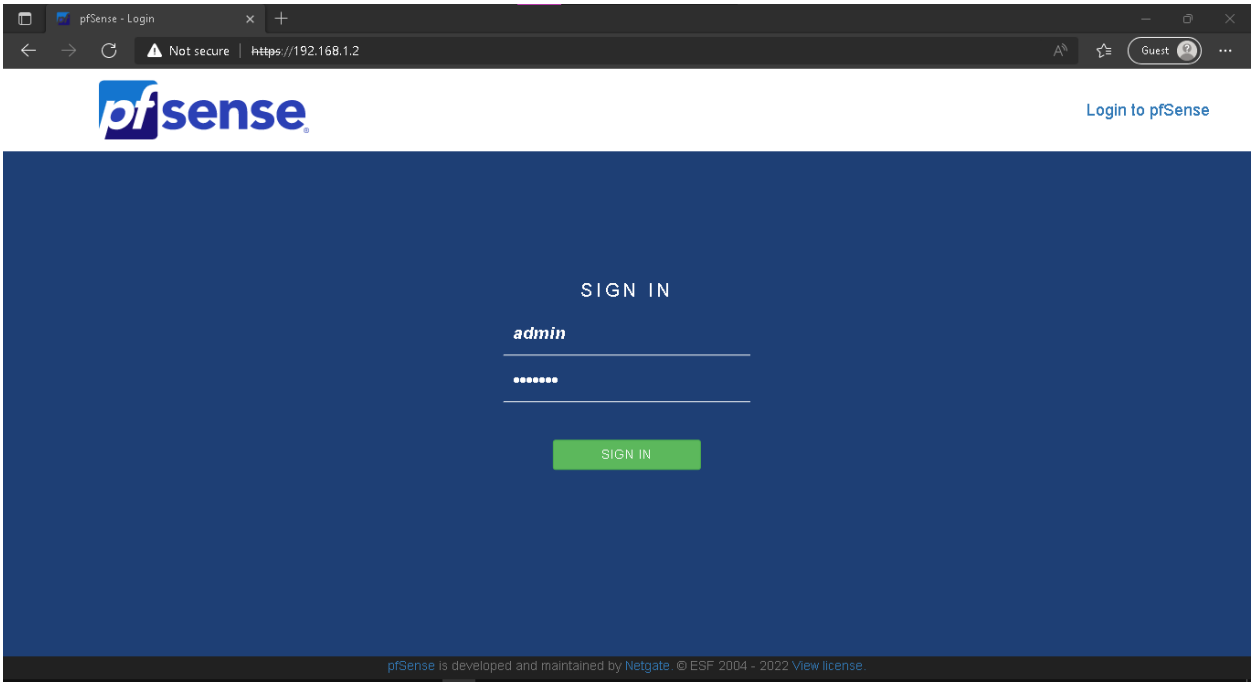
Step 8:

On the **pfsense** web page, log in with the following credentials:

Username: admin

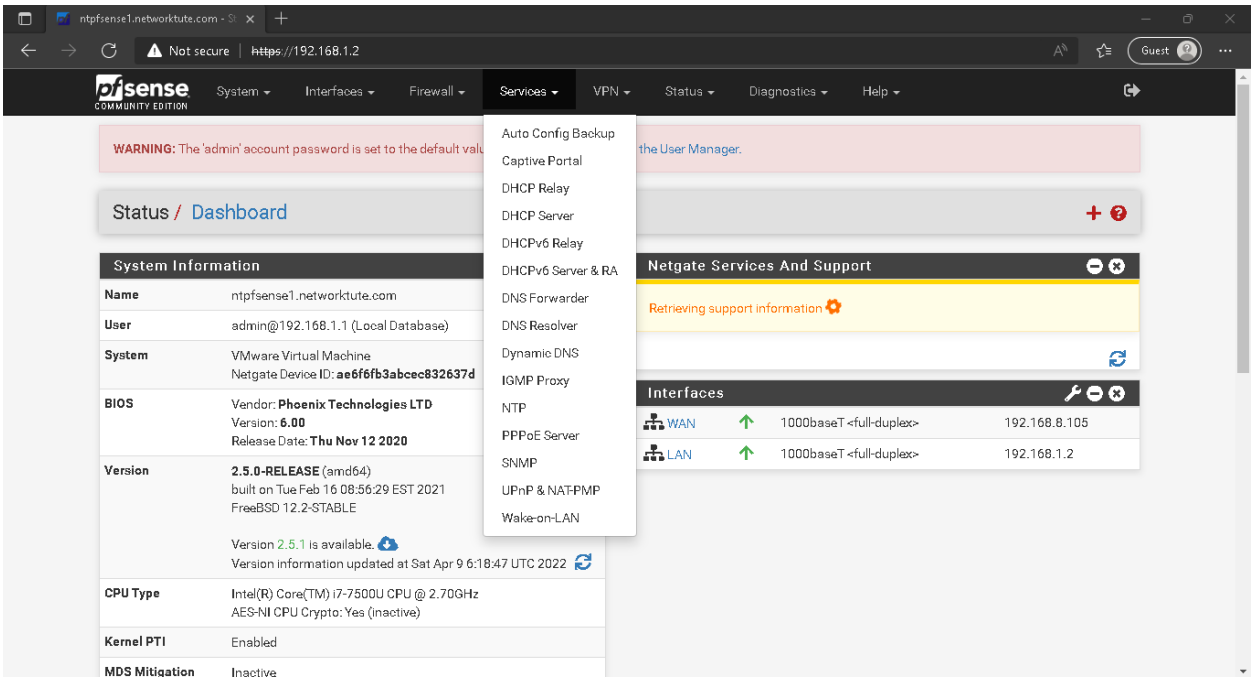
Password: pfsense

Press **Enter**.



Step 9:

On the web page, click the **Services** menu drop-down and select **DHCP Server**.



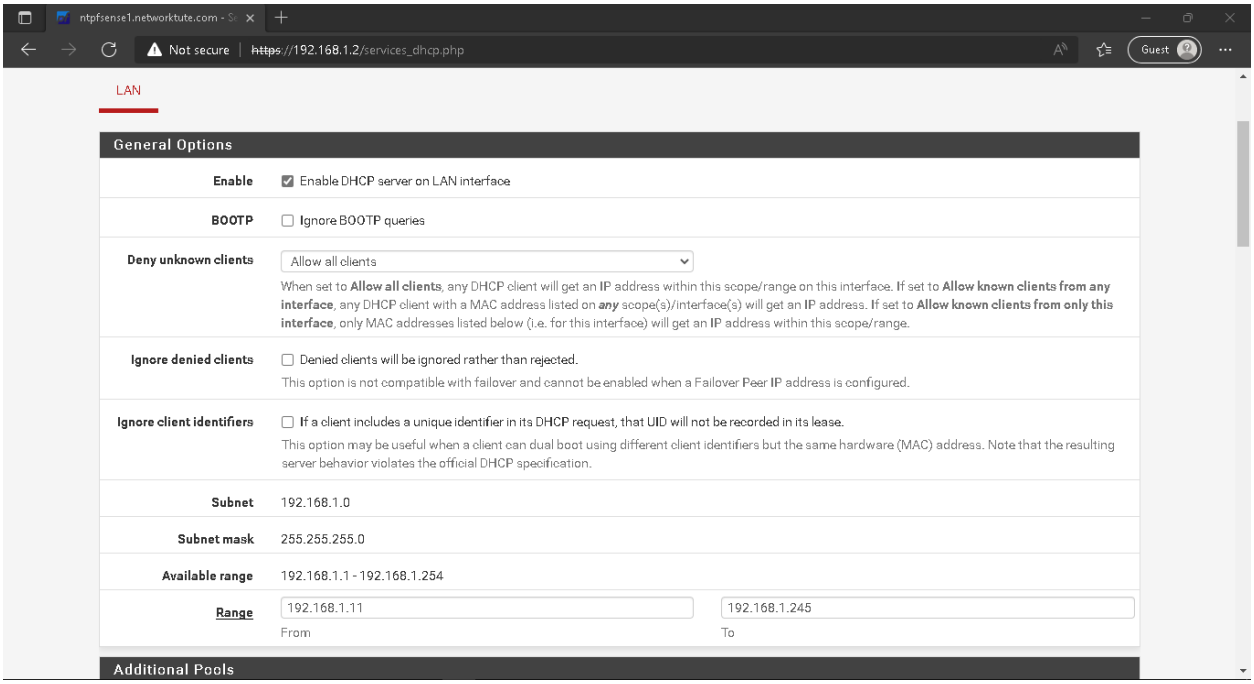
Step 10:

Click the **WAN** tab.

Under **General Options**, do the following:

- Click the **Enable DHCP server on WAN interface** checkbox next to the **Enable** field.
- In the **Range** field, enter the following range:

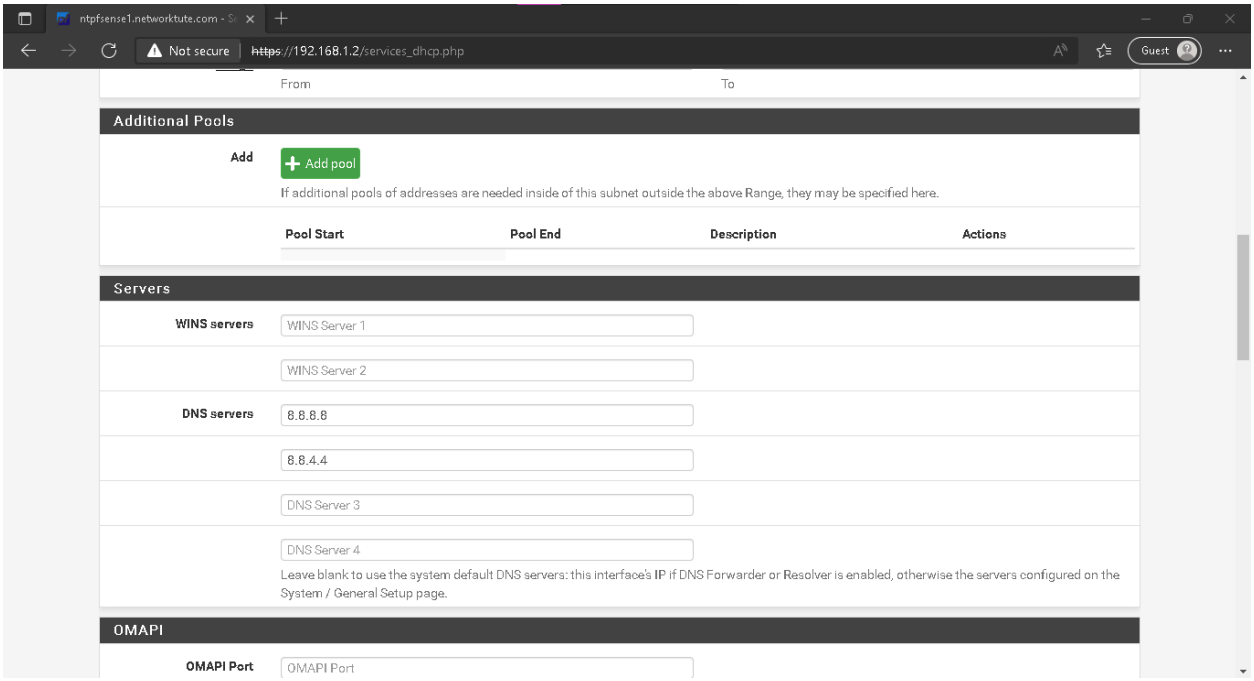
From: 192.168.1.11 To: 192.168.1.245



Step 11:

Scroll down to the **Servers** section and type the following for the **DNS servers**:

8.8.8.8 8.8.4.4

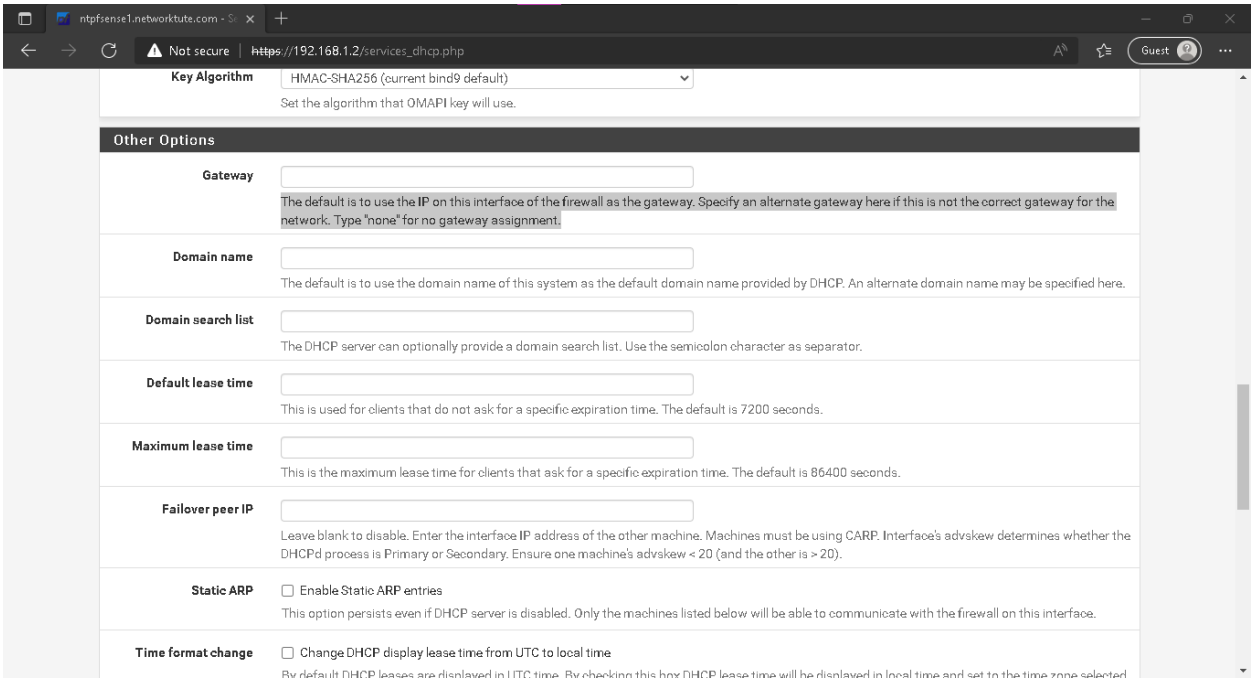


Note: 8.8.8.8 is the primary DNS server, and 8.8.4.4 is the secondary DNS server.

Step 12:

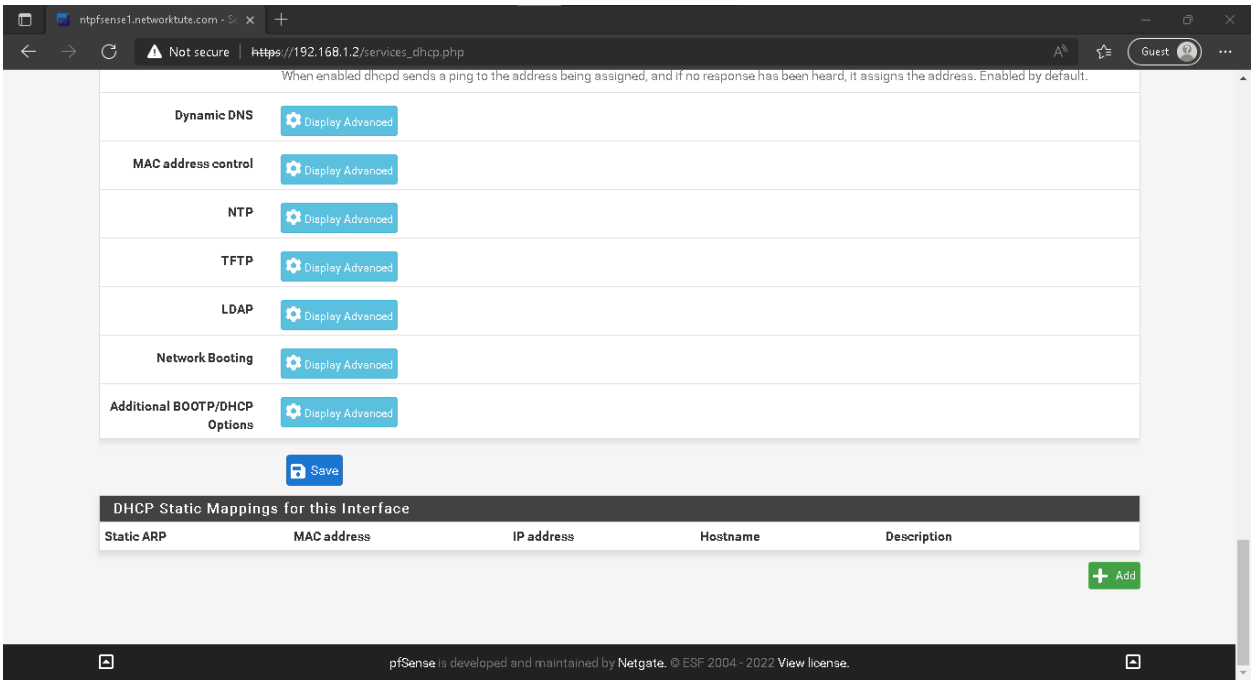
Scroll down further to **Other Options**.

The IP address of the interface of the firewall on which you enabled DHCP is used by default in the Gateway field. In the lab, the IP address is 192.168.1.1, therefore leave this entry blank.



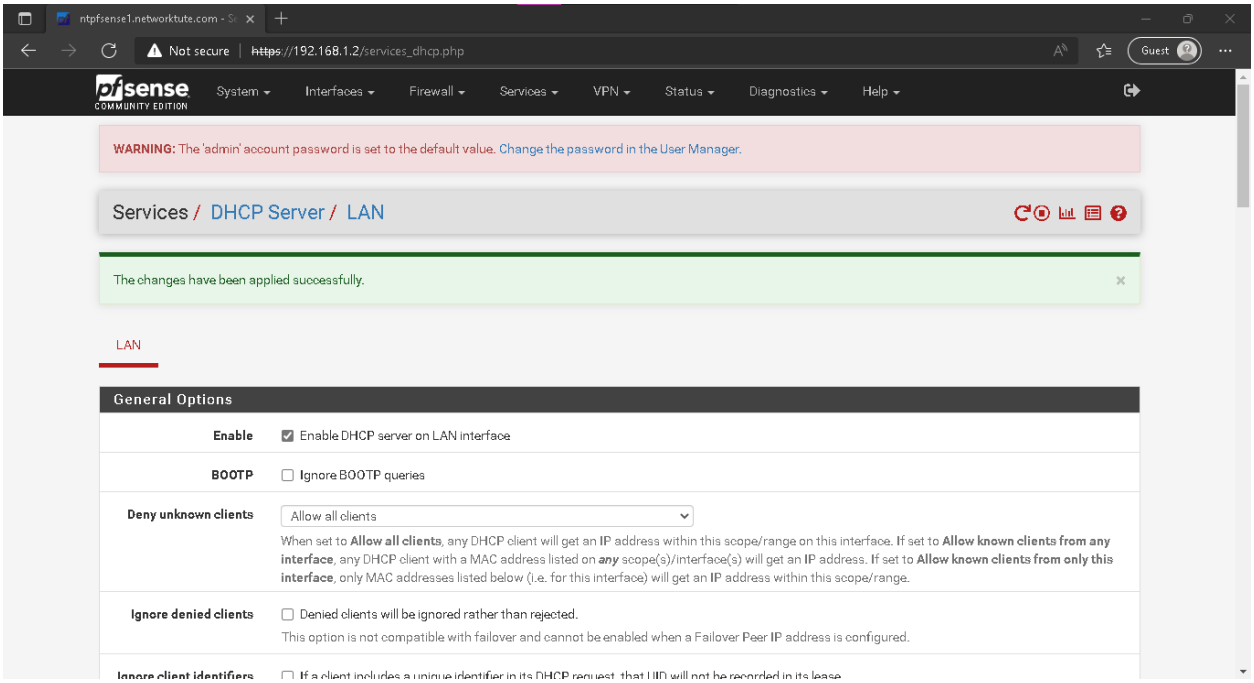
Step 13:

Scroll down to the end of the page and click **Save**.



Step 14:

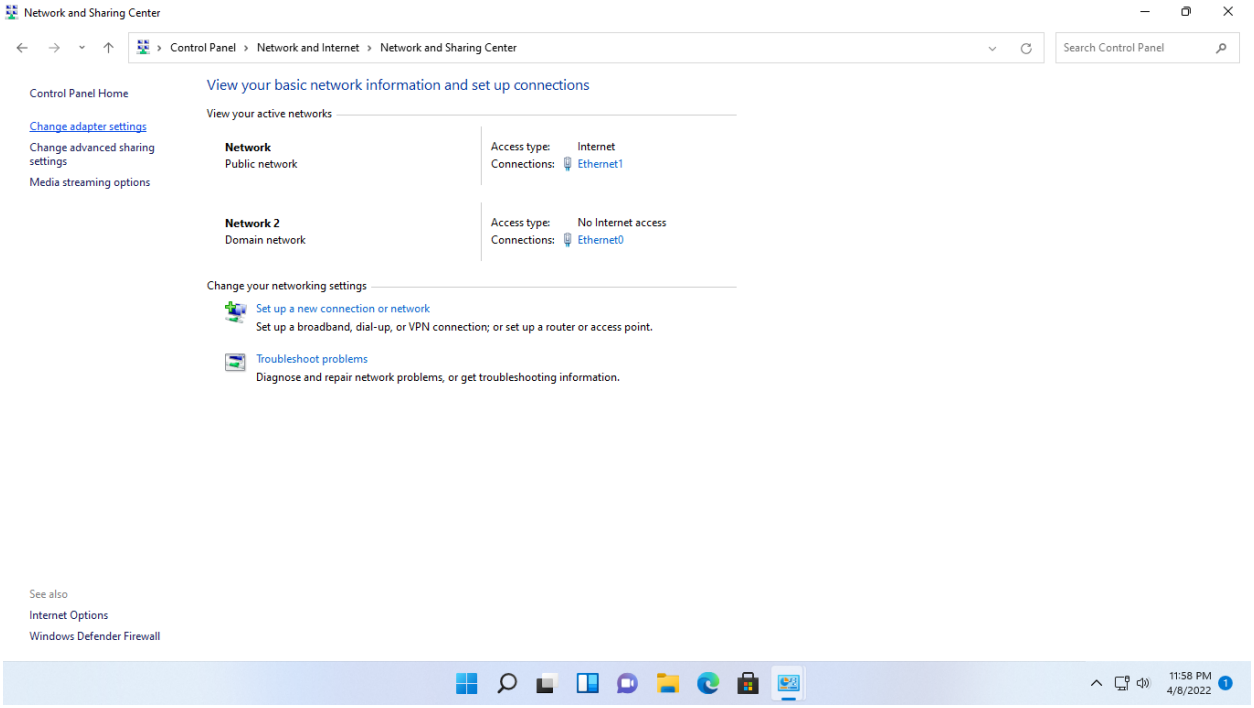
Scroll up to the beginning of the page. You will get the changes applied successfully message.



Step 15:

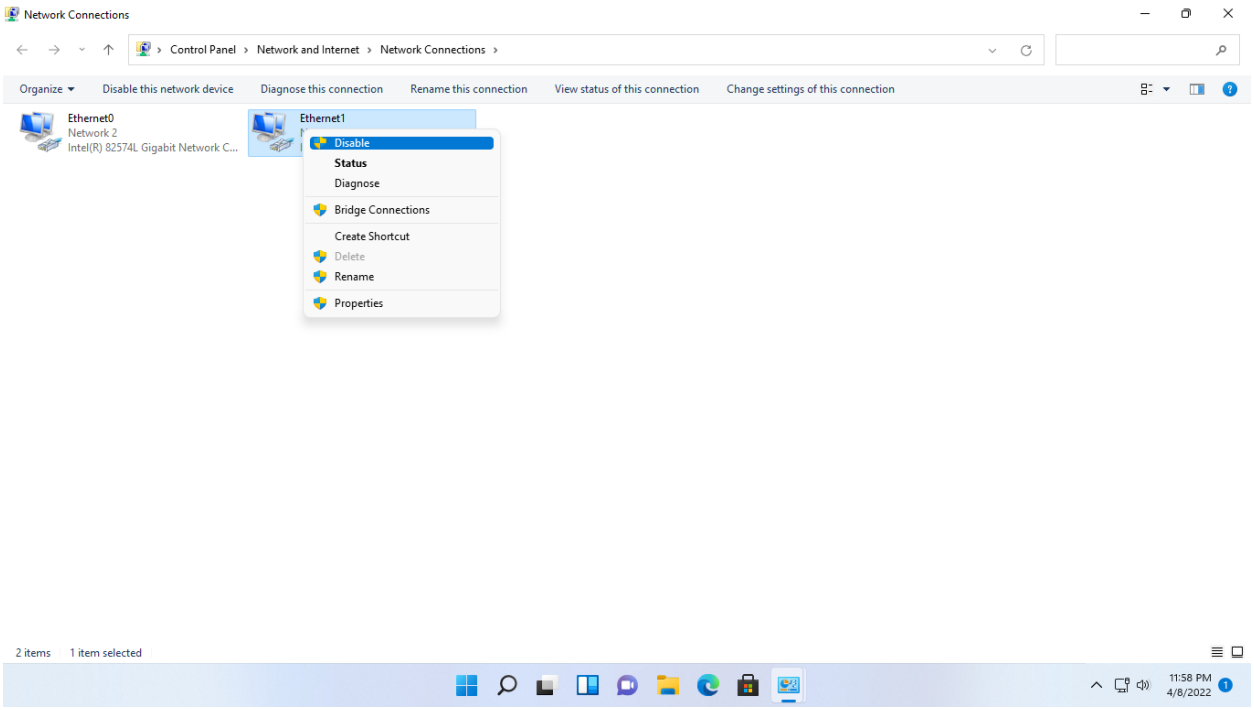
Restore the **Network and Sharing Center** window from the taskbar.

Click the **Change adapter settings** link on the left pane.



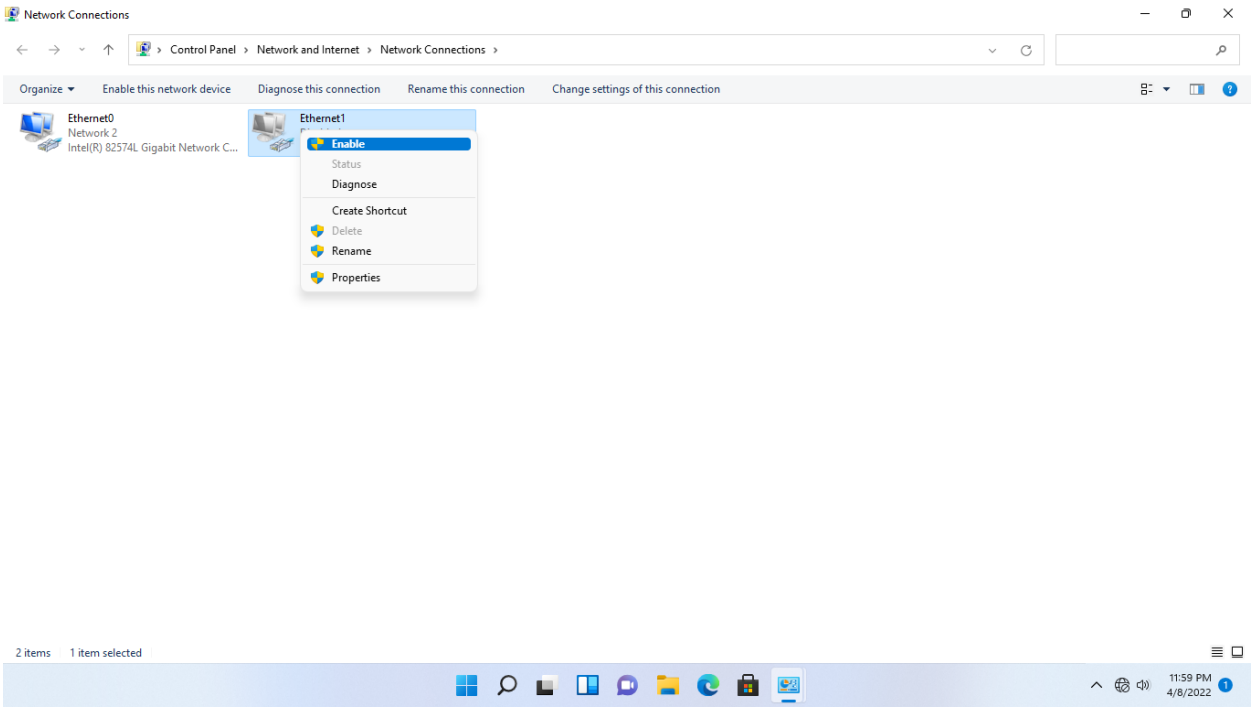
Step 16:

From the **Network Connections** window, right-click on **Ethernet 1** and select **Disable**.



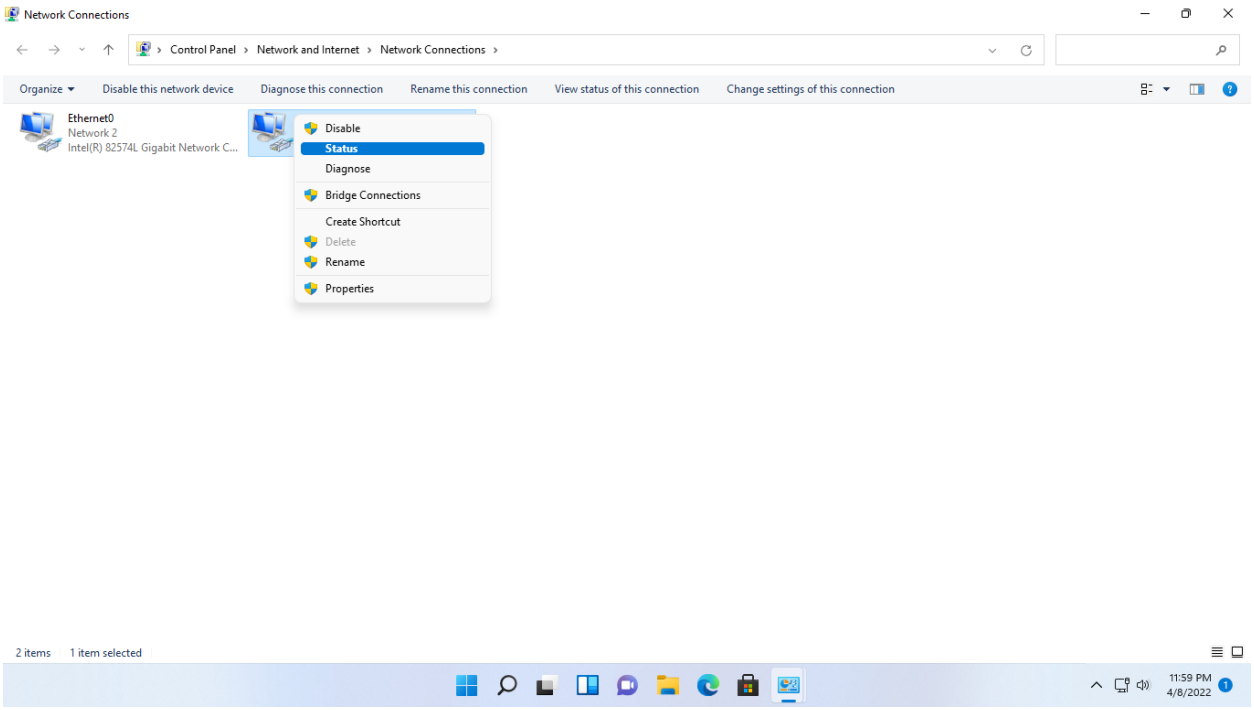
Step 17:

Right-click on **Ethernet 1** and select **Enable**.



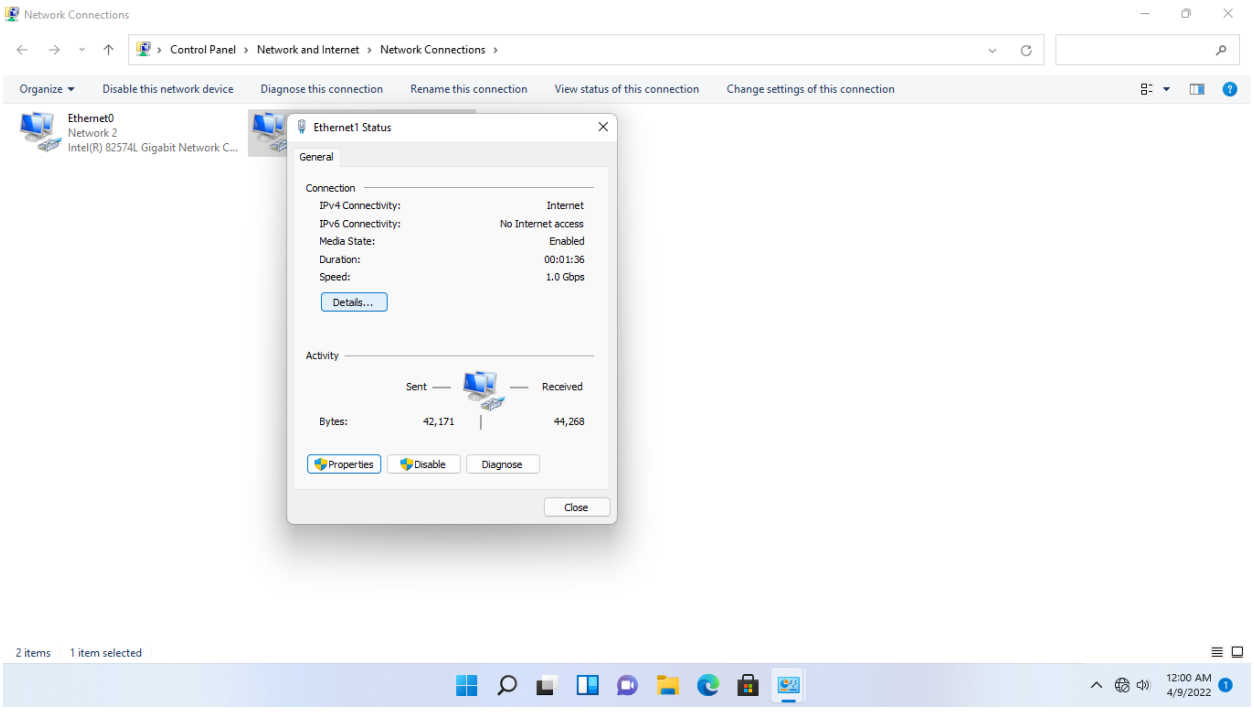
Step 18:

Right-click on **Ethernet 1** and select **Status**.



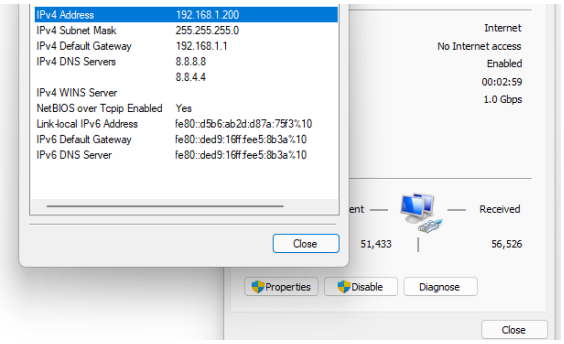
Step 19:

On the **Ethernet 1 Status** dialog box, click **Details**.



Step 20:

On the **Network Connection Details** dialog box, notice that you have received an IP address from the configured DHCP server.



Click **Close**.

Close the **Ethernet 1 Status** dialog box.

Step 21:

Restore **Microsoft Edge** browser from the taskbar.

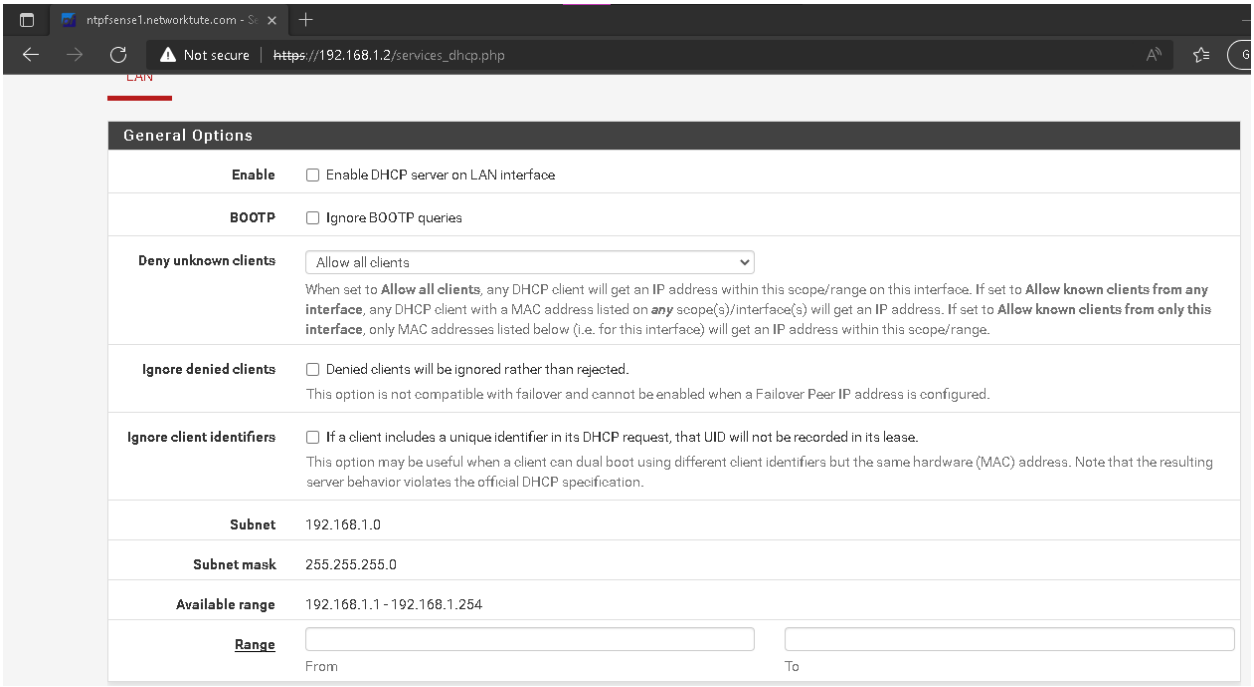
You will be on the pfsense web page.

Apply the following settings:

- Under **General Options**, do the following:
  - Untick the **Enable DHCP server on WAN interface checkbox** next to the **Enable** field
  - Remove the IP addresses from the **Range** field.

- Scroll down to the **Servers** section and remove the addresses entered earlier for the **DNS servers'** field.

Click **Save**.



Step 22:

Restore the **Network Connections** window from the taskbar.

Right-click on **Ethernet 1** and select **Disable**.

Again right-click on **Ethernet 1** and select **Enable**.