

Worksheet 4

Author: Tomos Leggett · **Student Code:** 1901852 · **Module Code:** ACCA5023

Worksheet 4

Task 1: Utilising ARP & Routing Tables

Task 2: Deploying core services (FTP Server)

Task 3: Installing and configuring the Routing and Remote Access Service

Observation: How Routers reference which networks they are able to connect to

Task 4: IP Packet Filtering

Filter 1

Filter 2

Filter 3

Task 5: Failover Clustering for high availability systems/services

Concept 1: Understanding the difference between a hot, warm or cold server

A cold server

A warm server

A hot server

Concept 2: Prerequisites

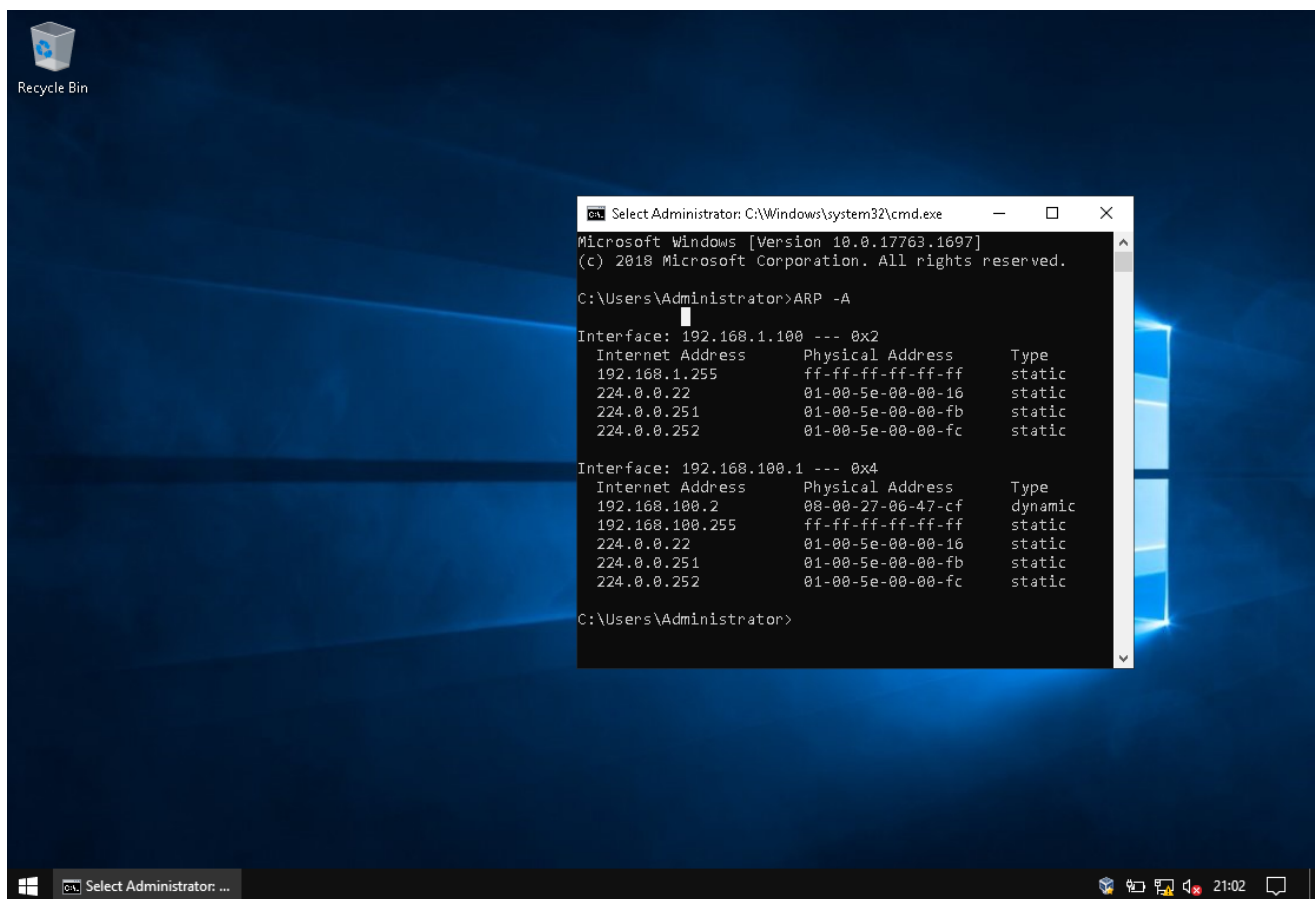
Task 6: Observational Tasks

Architecture

Topology

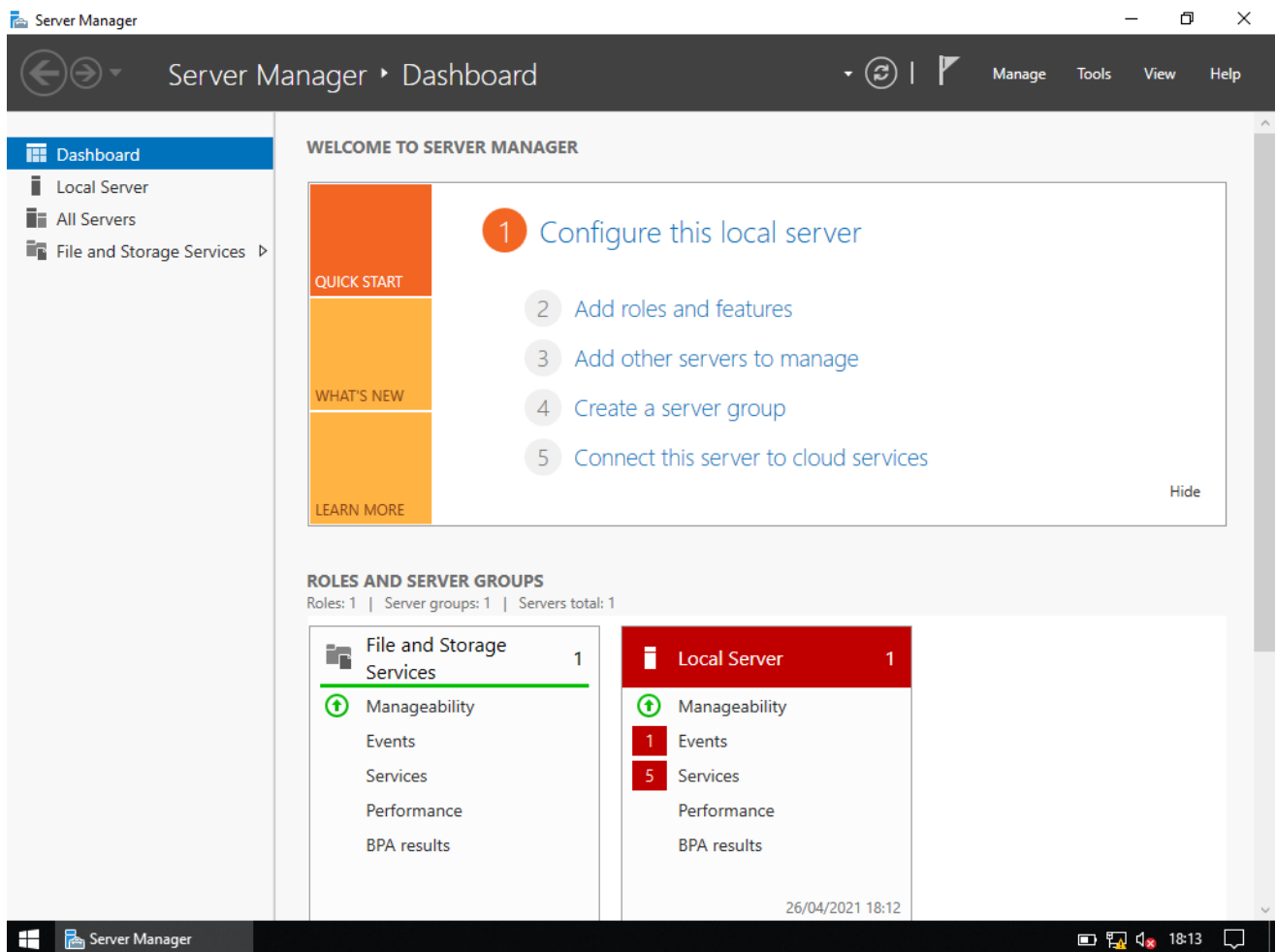
References

Task 1: Utilising ARP & Routing Tables

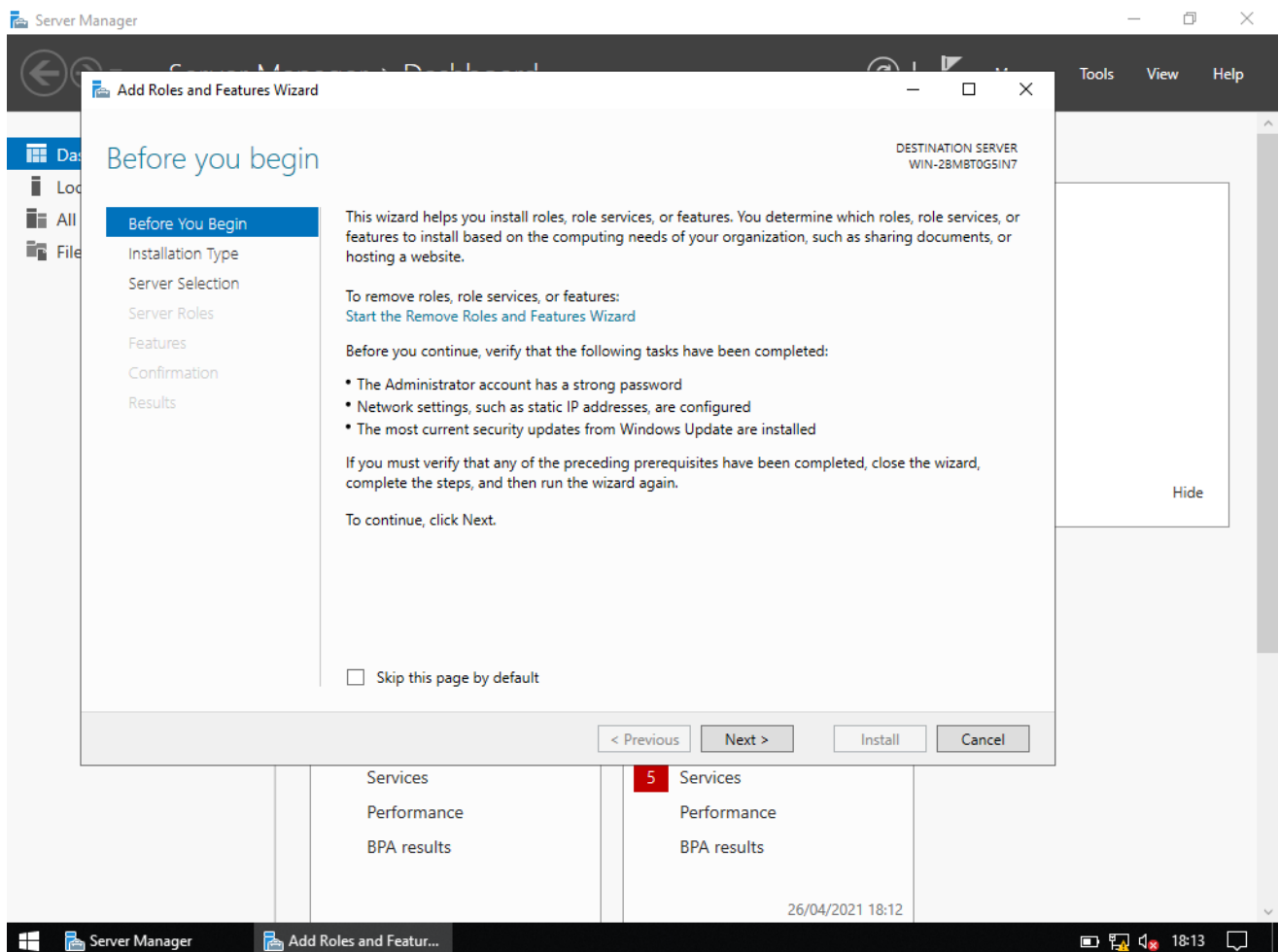


The ARP -A command is run, as you can see, a list of NICs are displayed, each with the interfaces connected to the device.

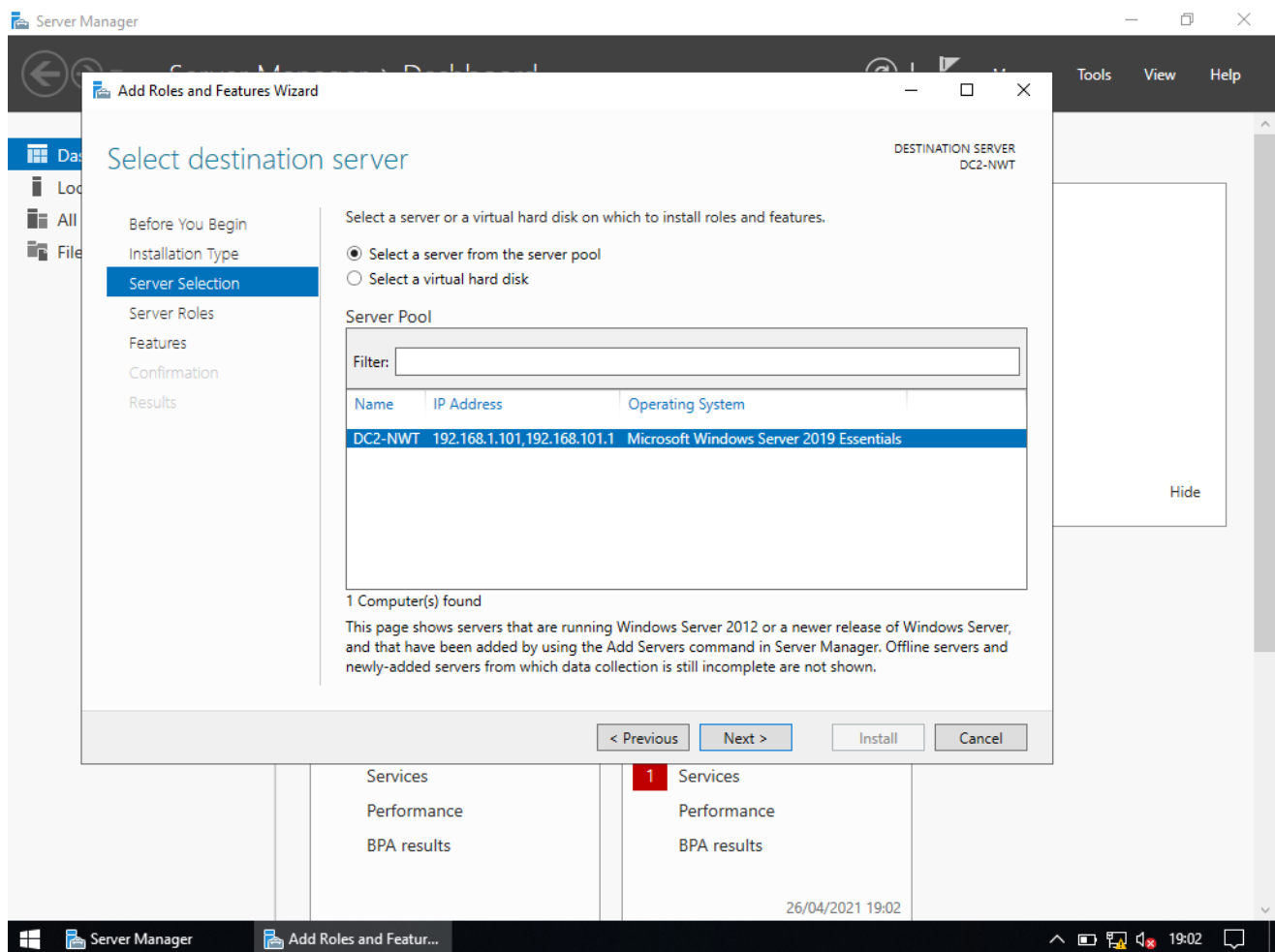
Task 2: Deploying core services (FTP Server)



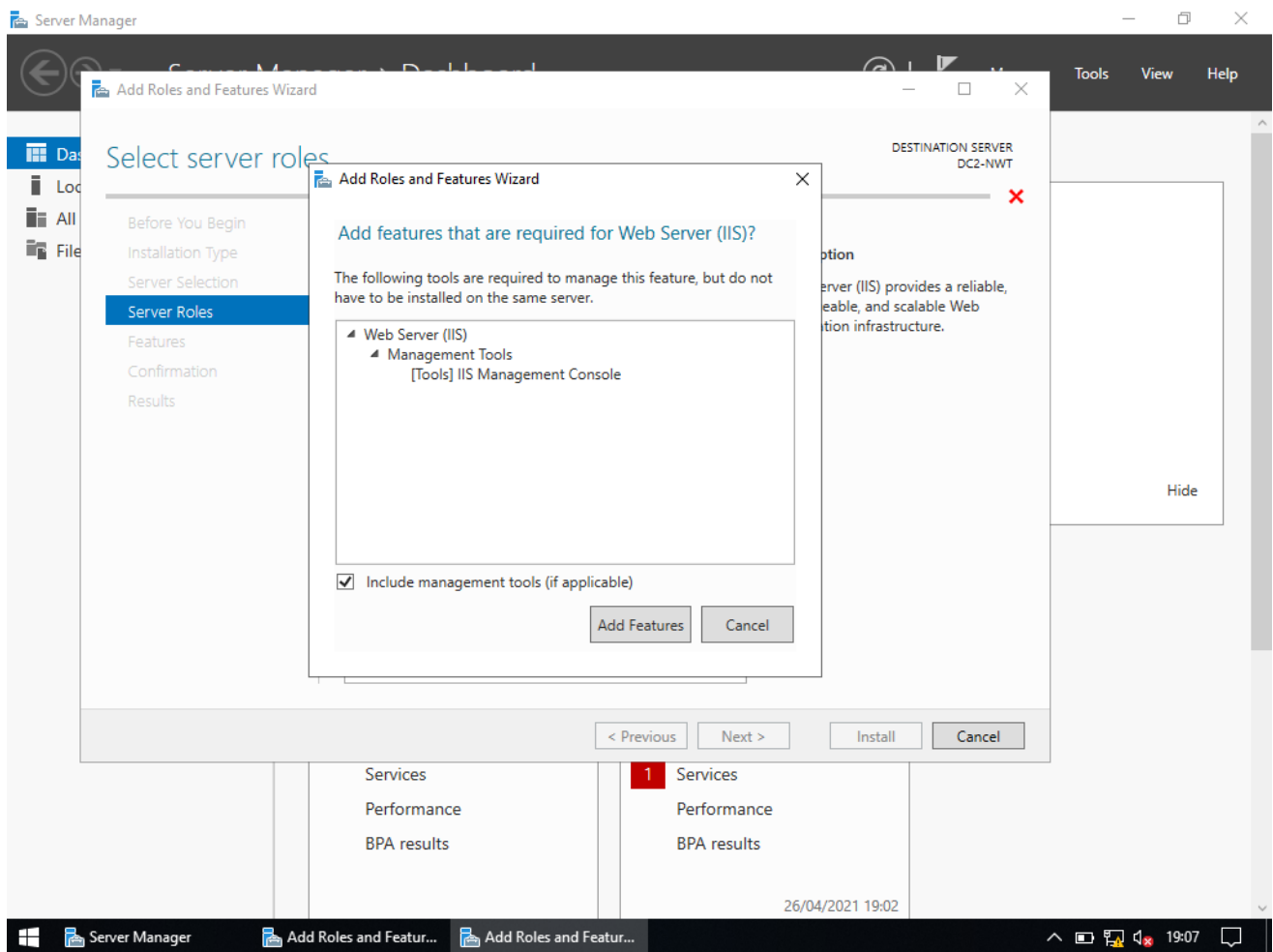
Server 2 is booted, and the Server Manager is launched.



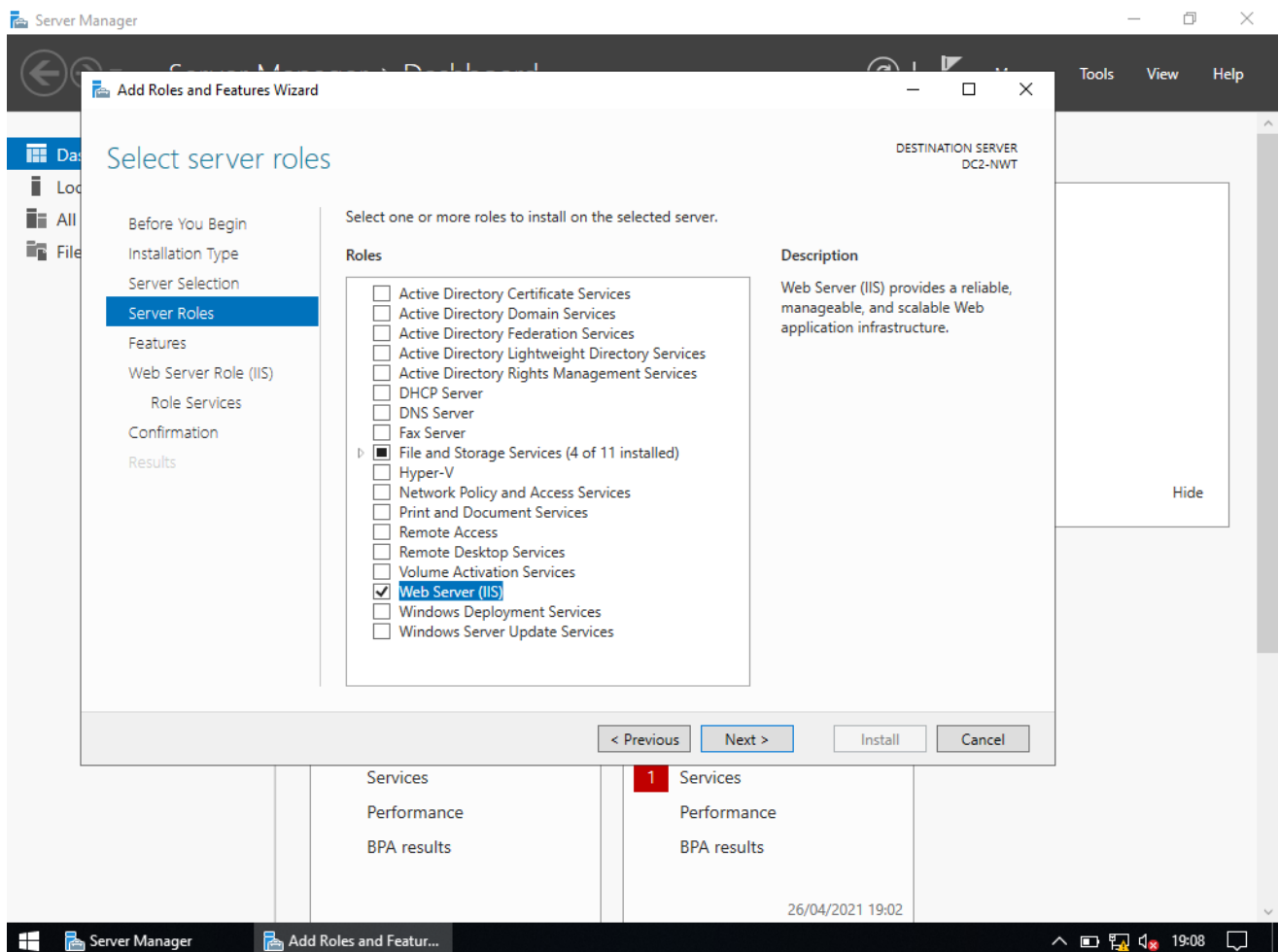
The 'Add Roles and Features' link is clicked, and the 'Add Roles and Features' wizard appears.



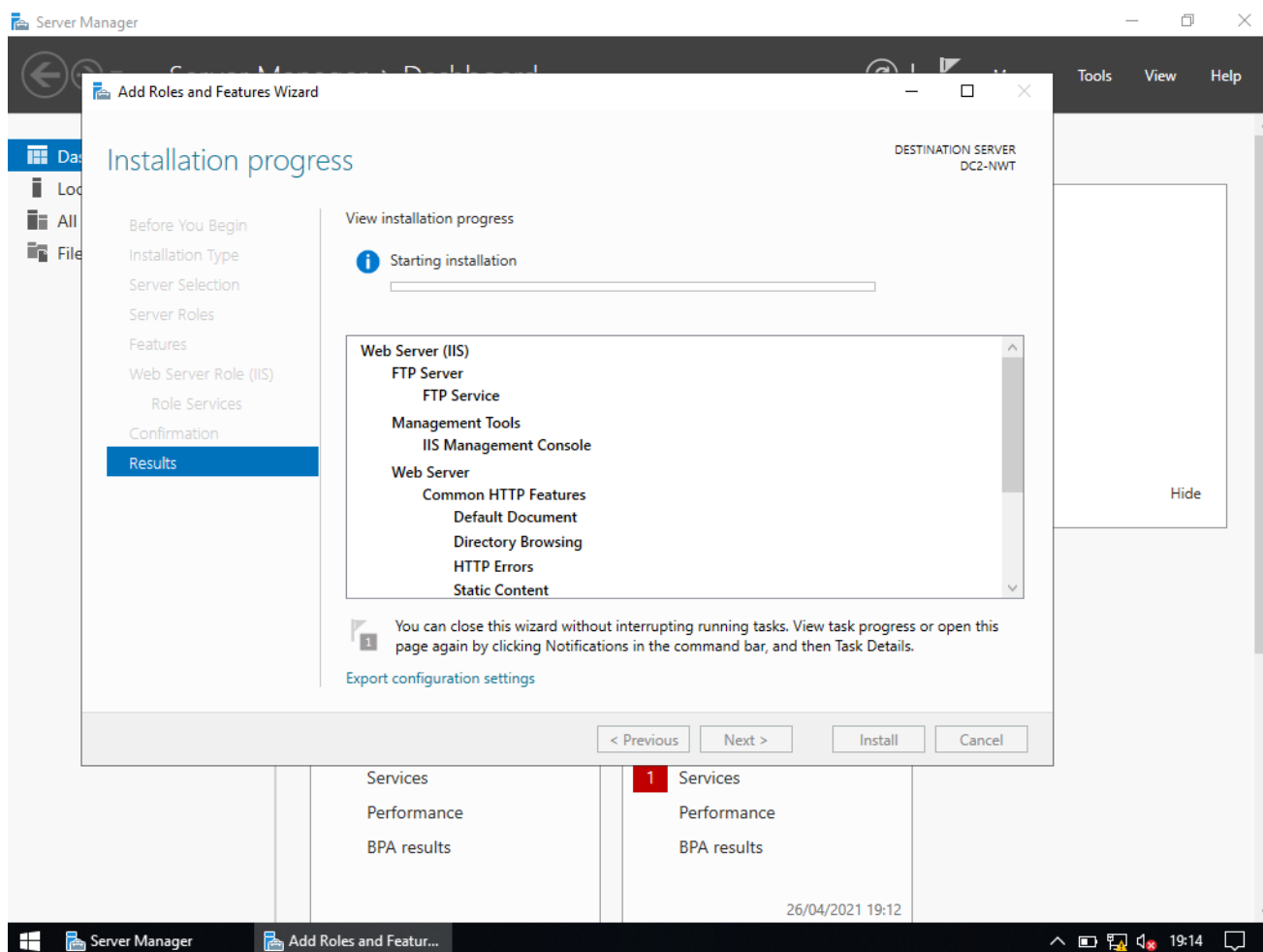
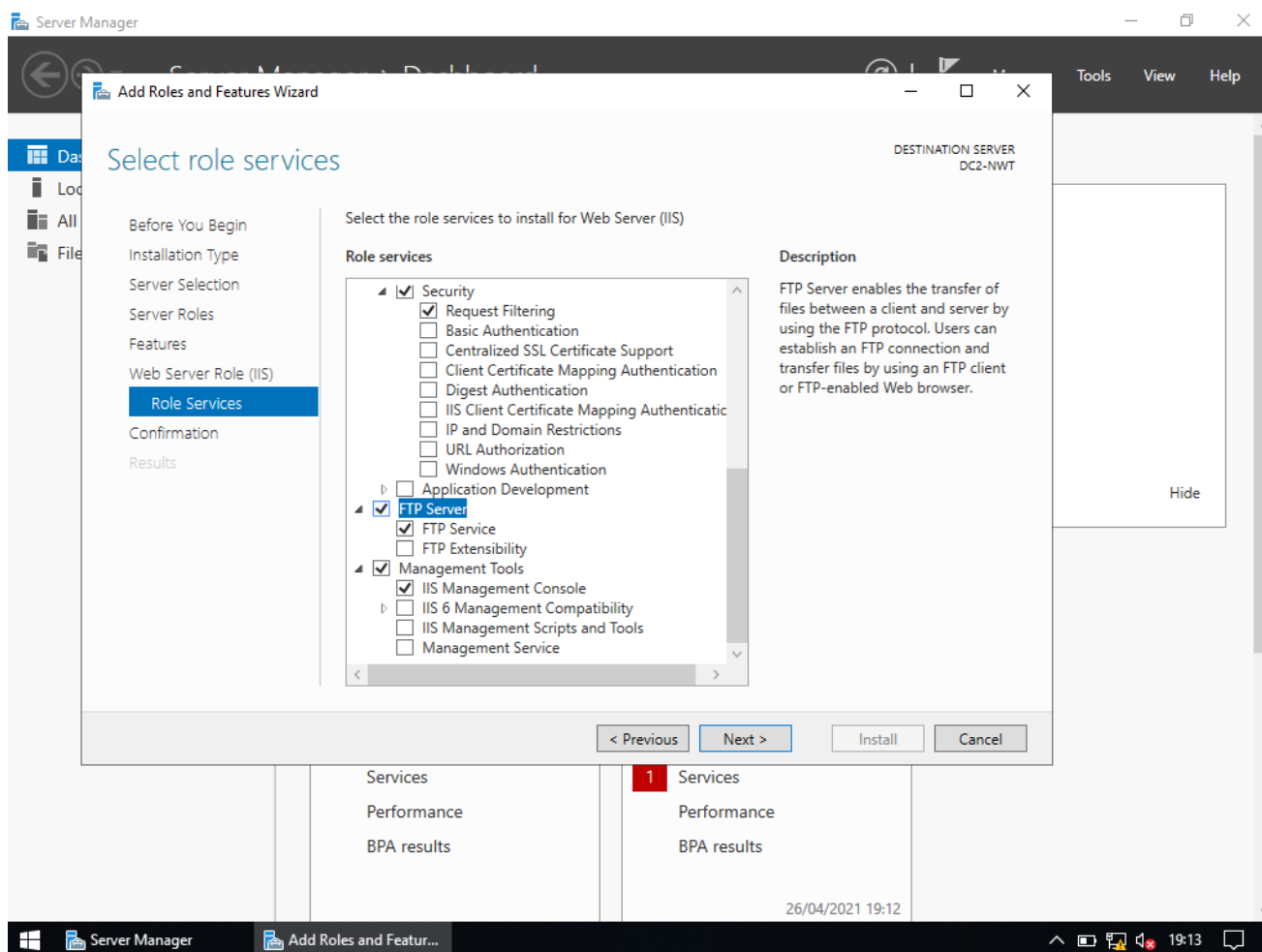
From this screen, confirmation that the correct server is being used can be achieved. The selected server is 'DC2-NWT' which is the second server.



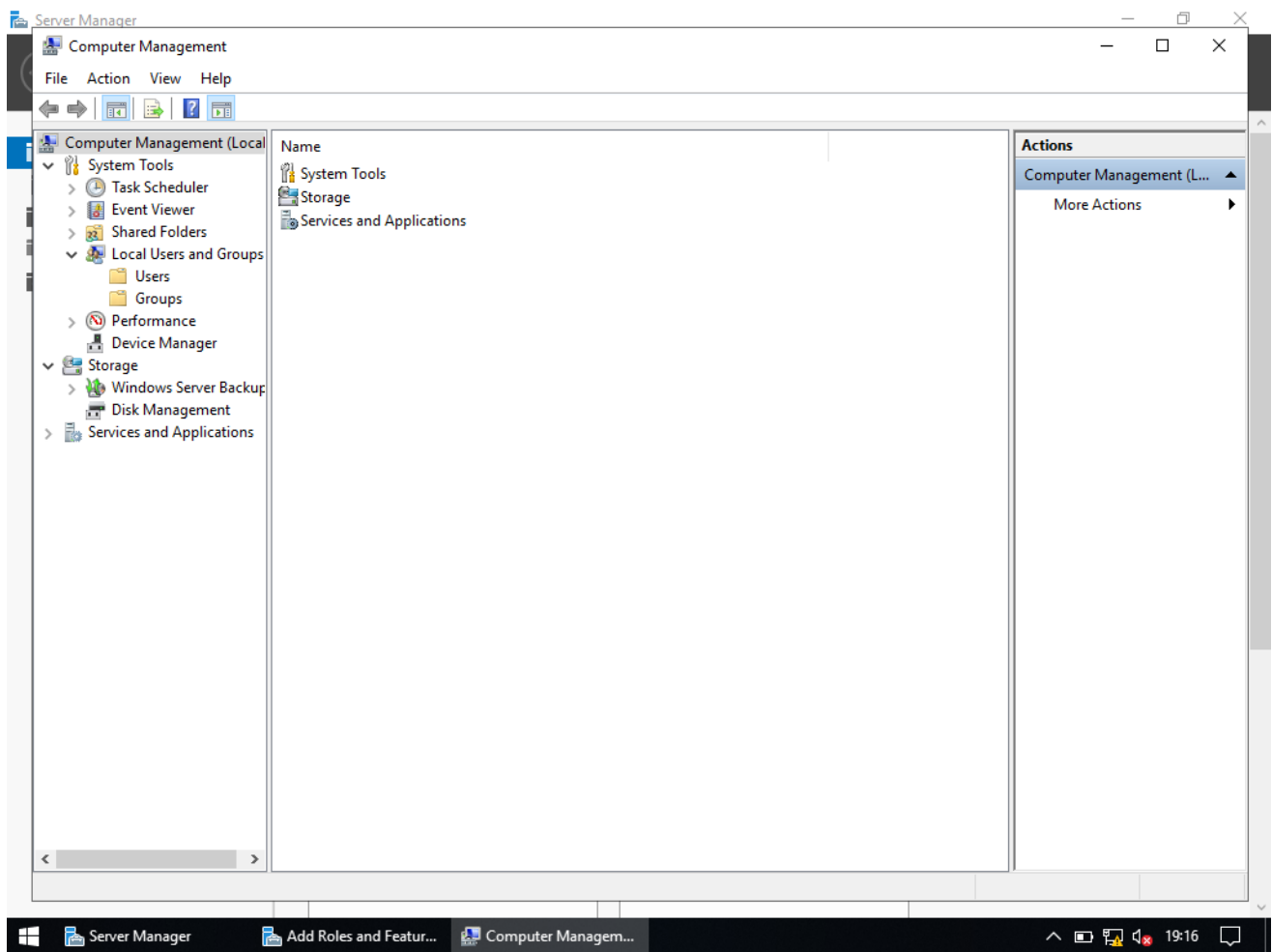
The IIS Management Console will be added (along with the management tools).



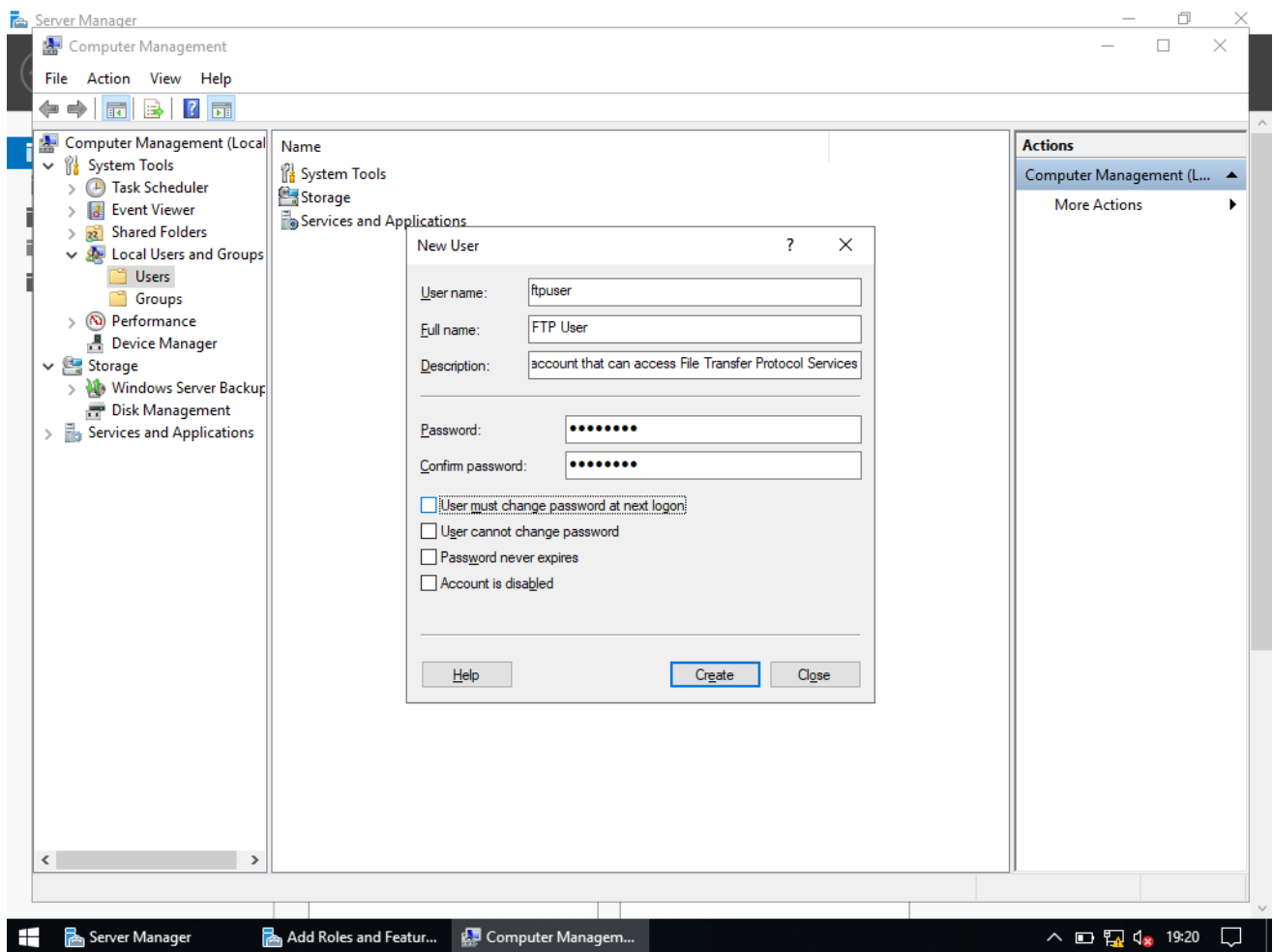
Evidence of the feature being added.



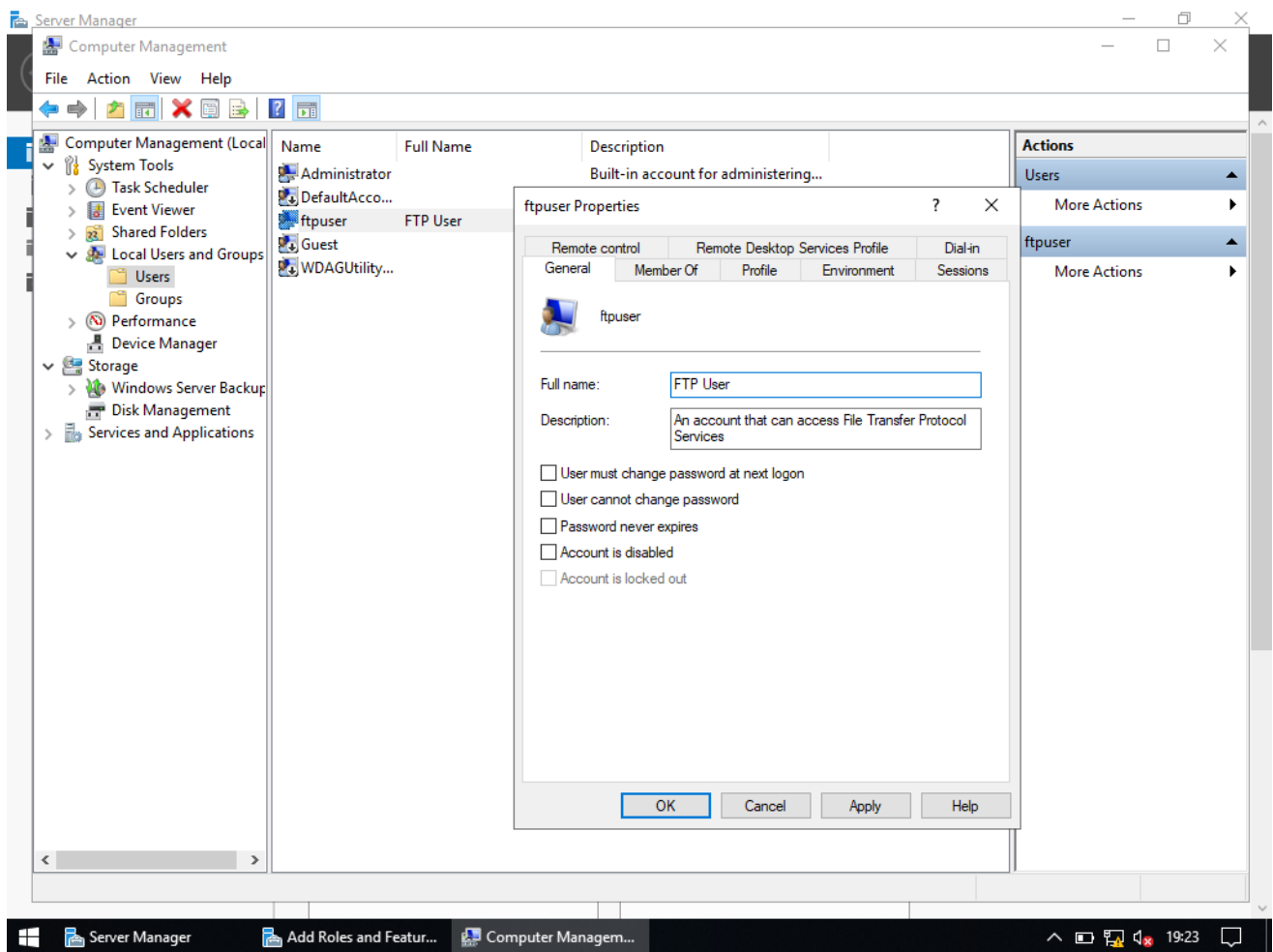
The installation process begins.



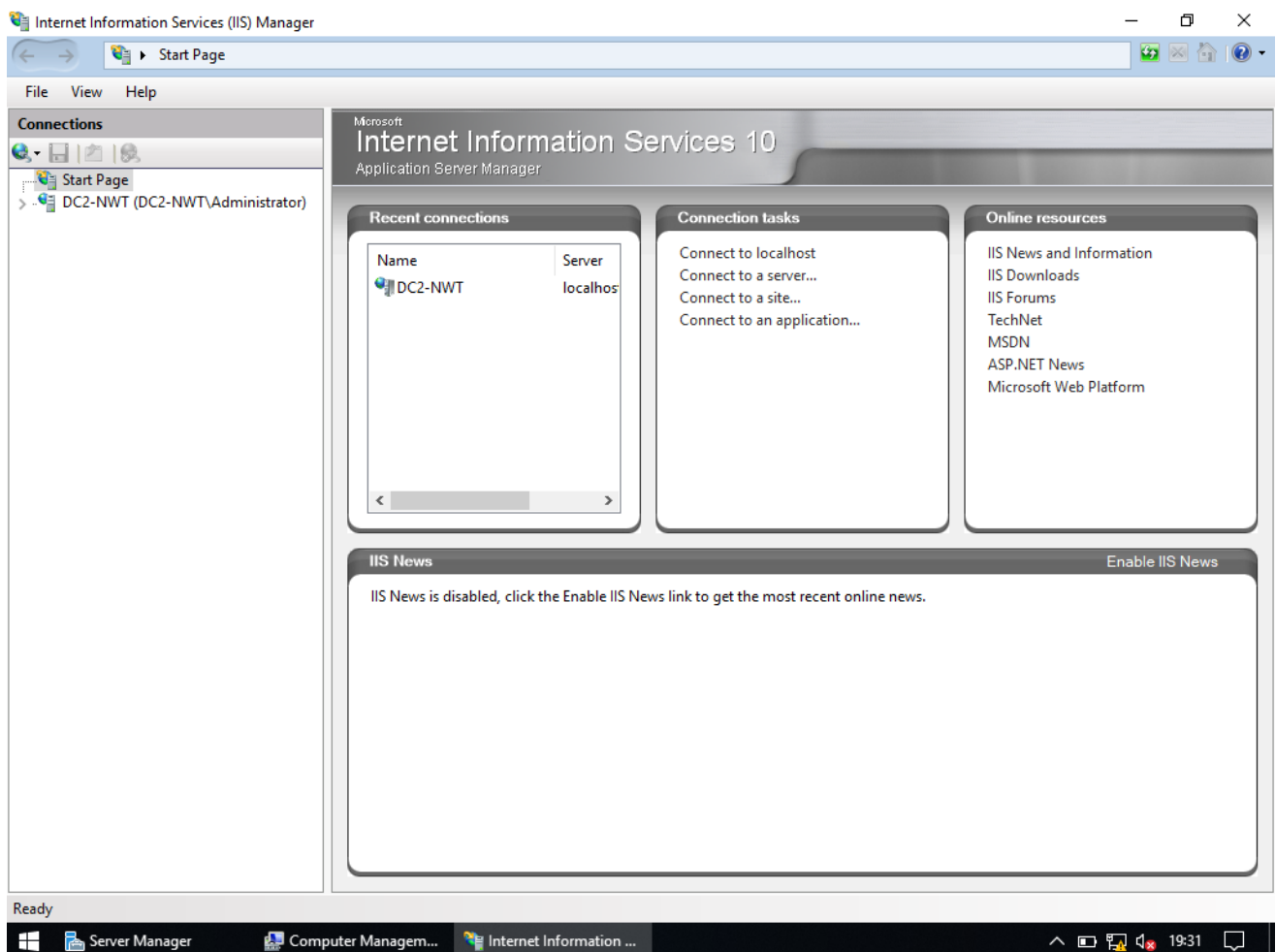
The computer management control panel is opened.



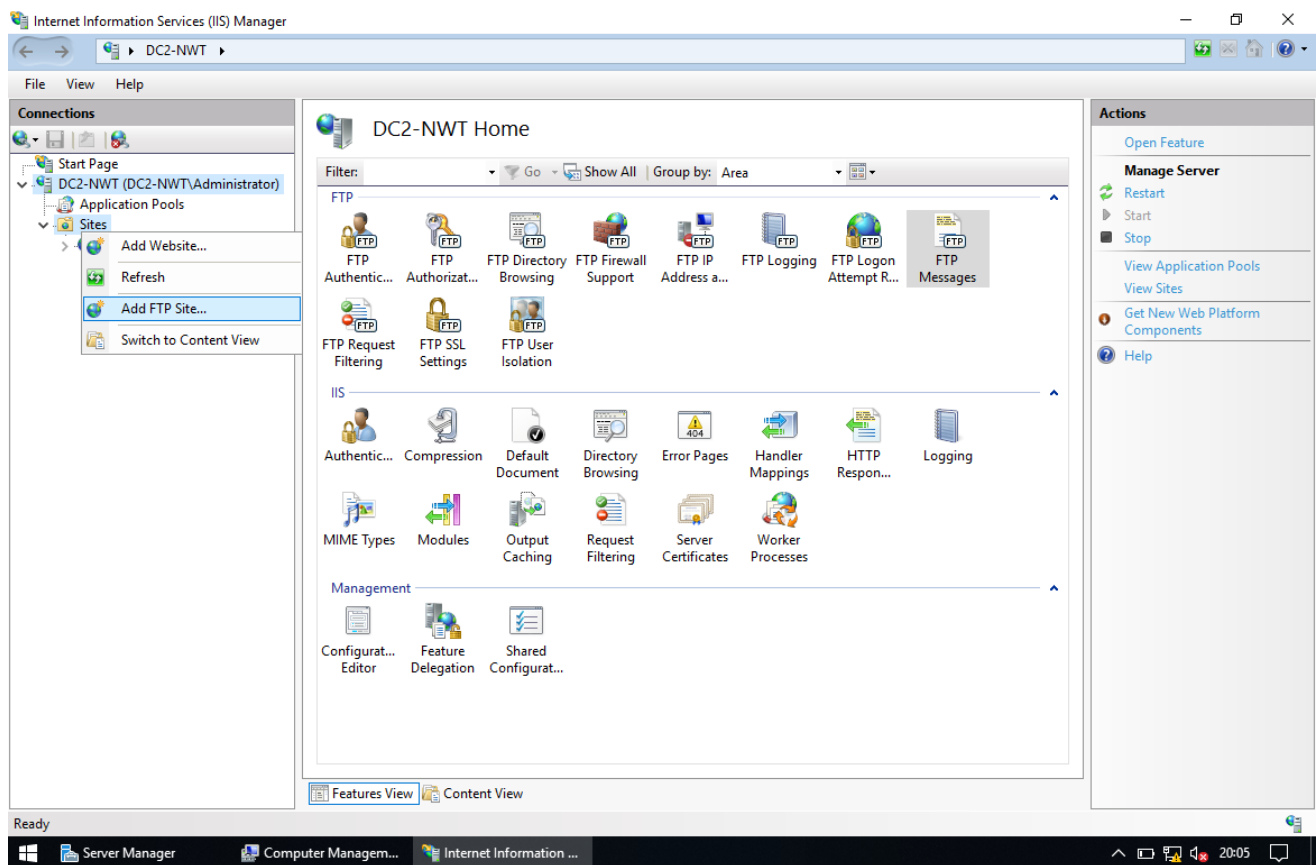
A new user by the name 'ftpuser' with the **P@ssw0rd** passphrase set as their password. The 'User must change password at next logon' checkbox is unchecked.



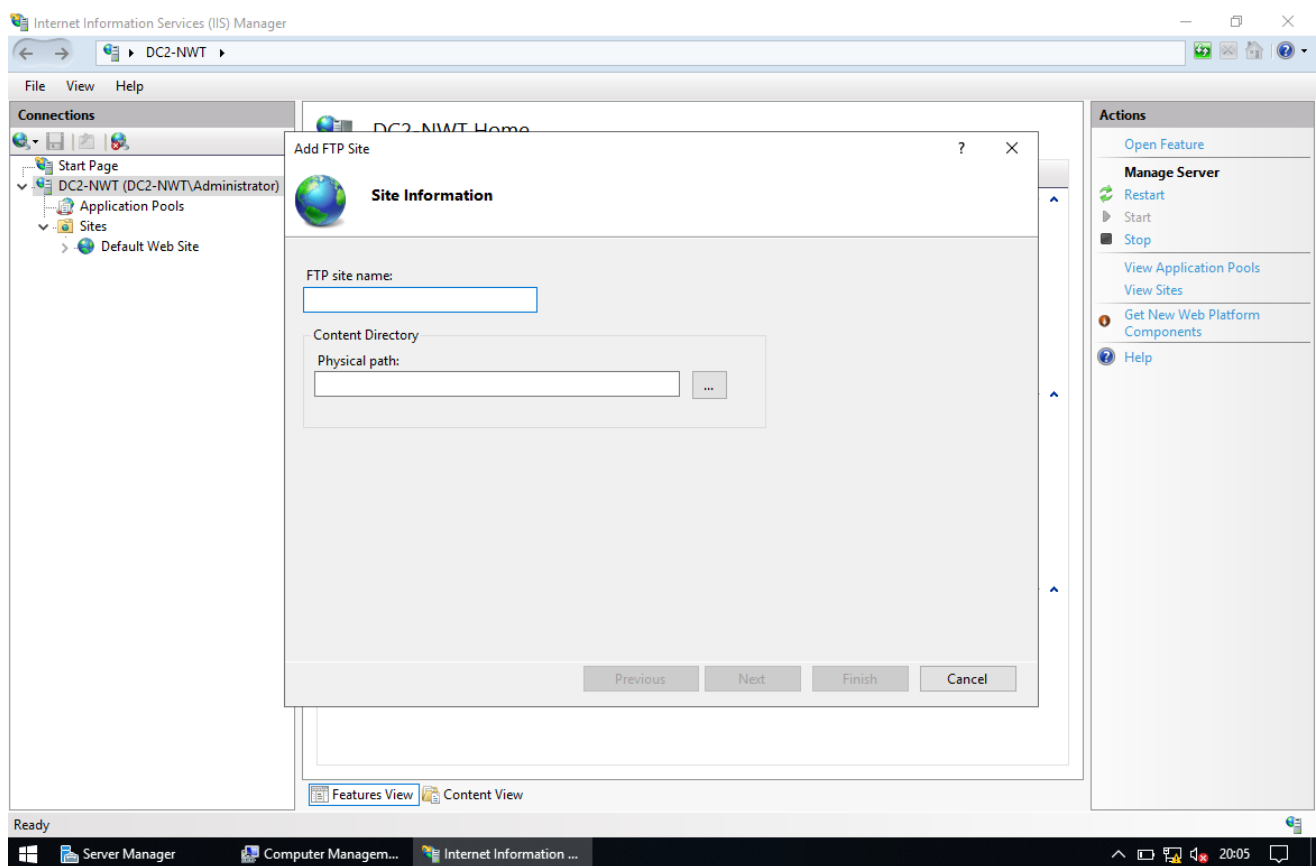
The account is created successfully.



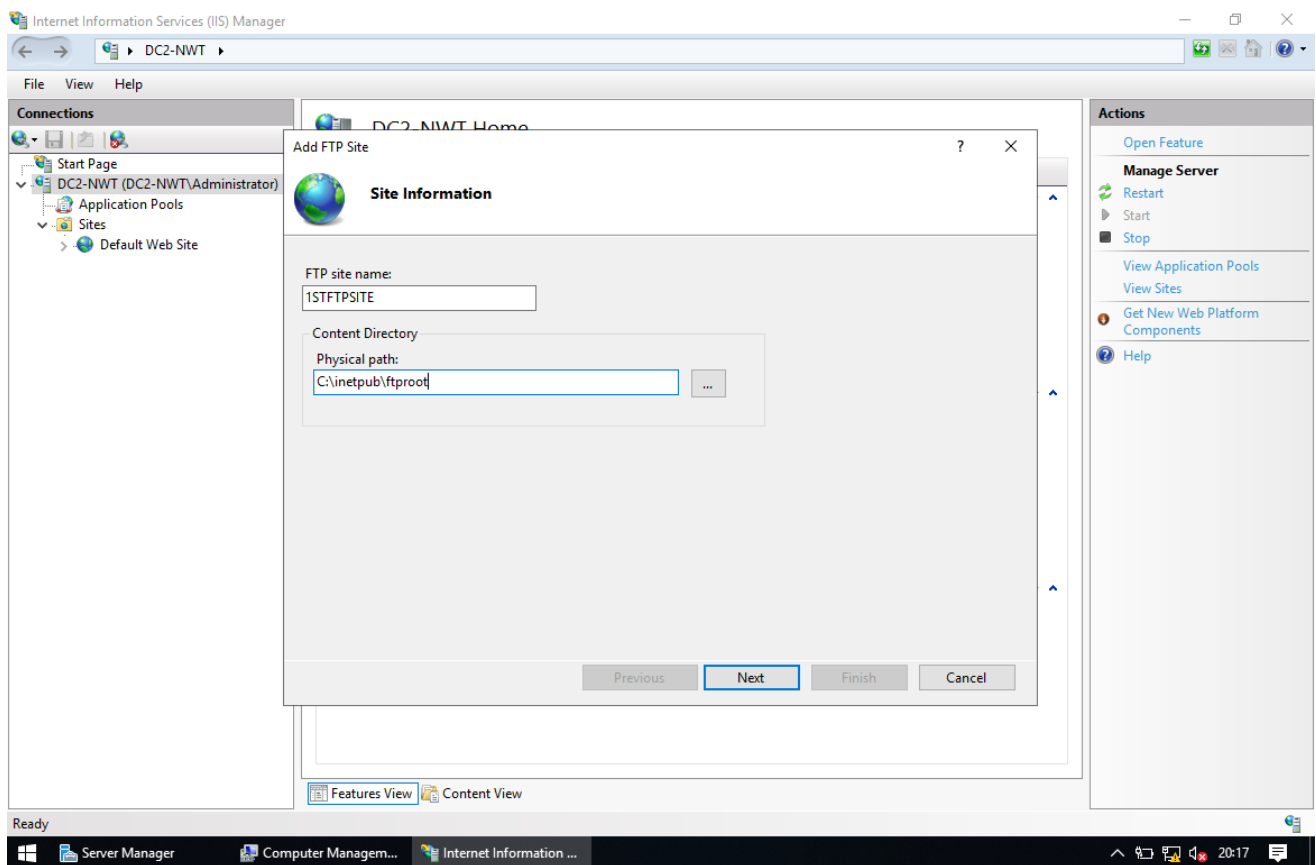
The Internet Information Services (IIS) Manager is opened.



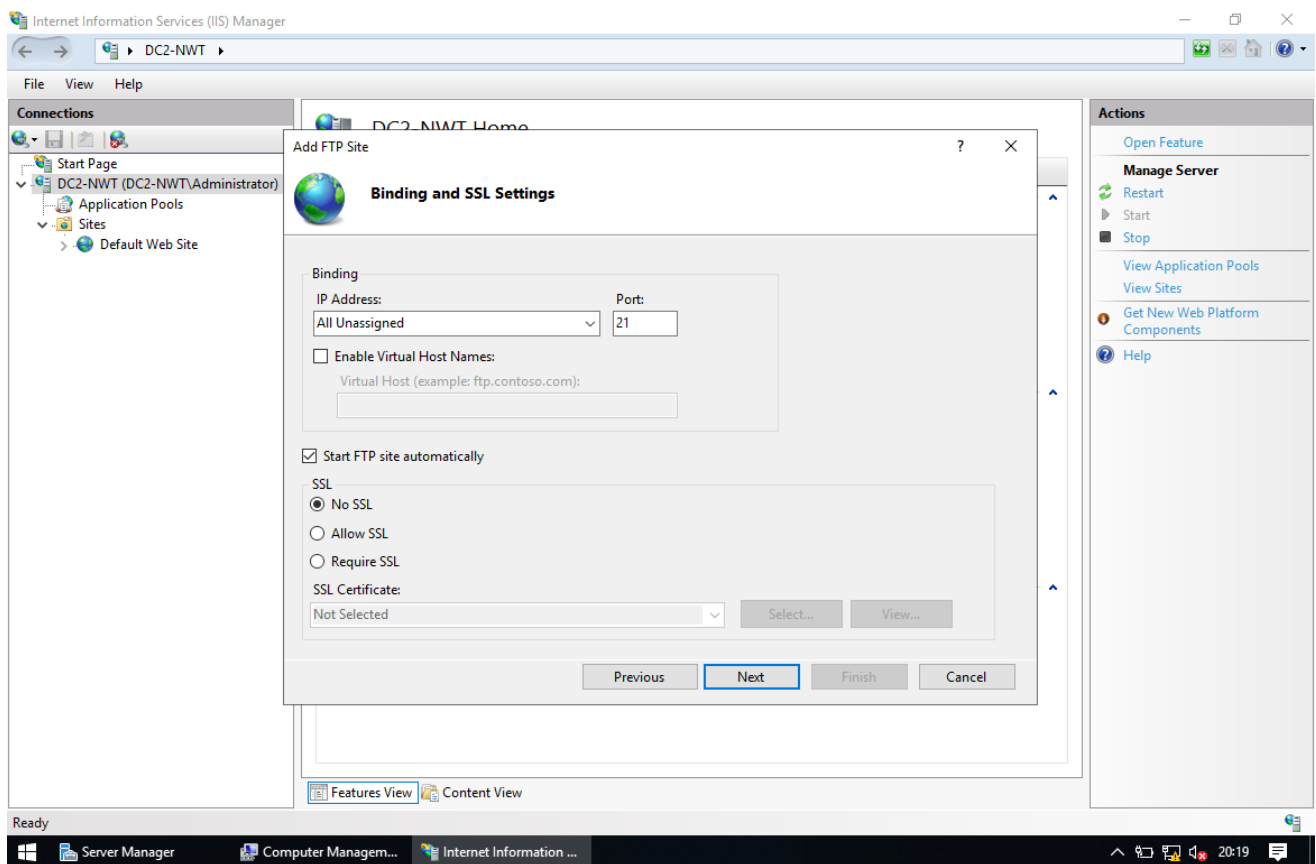
A new FTP site will be created using the 'Add FTP Site...' function.



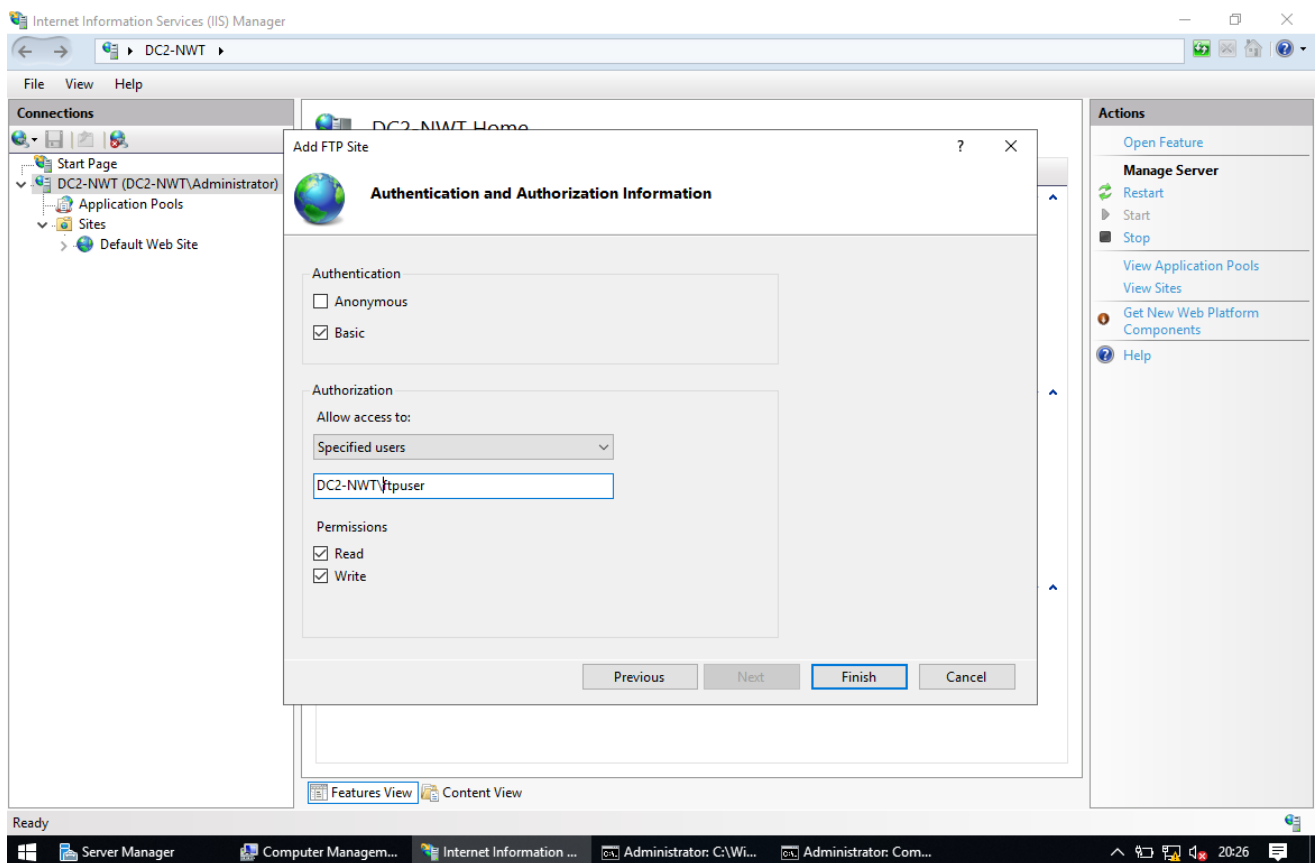
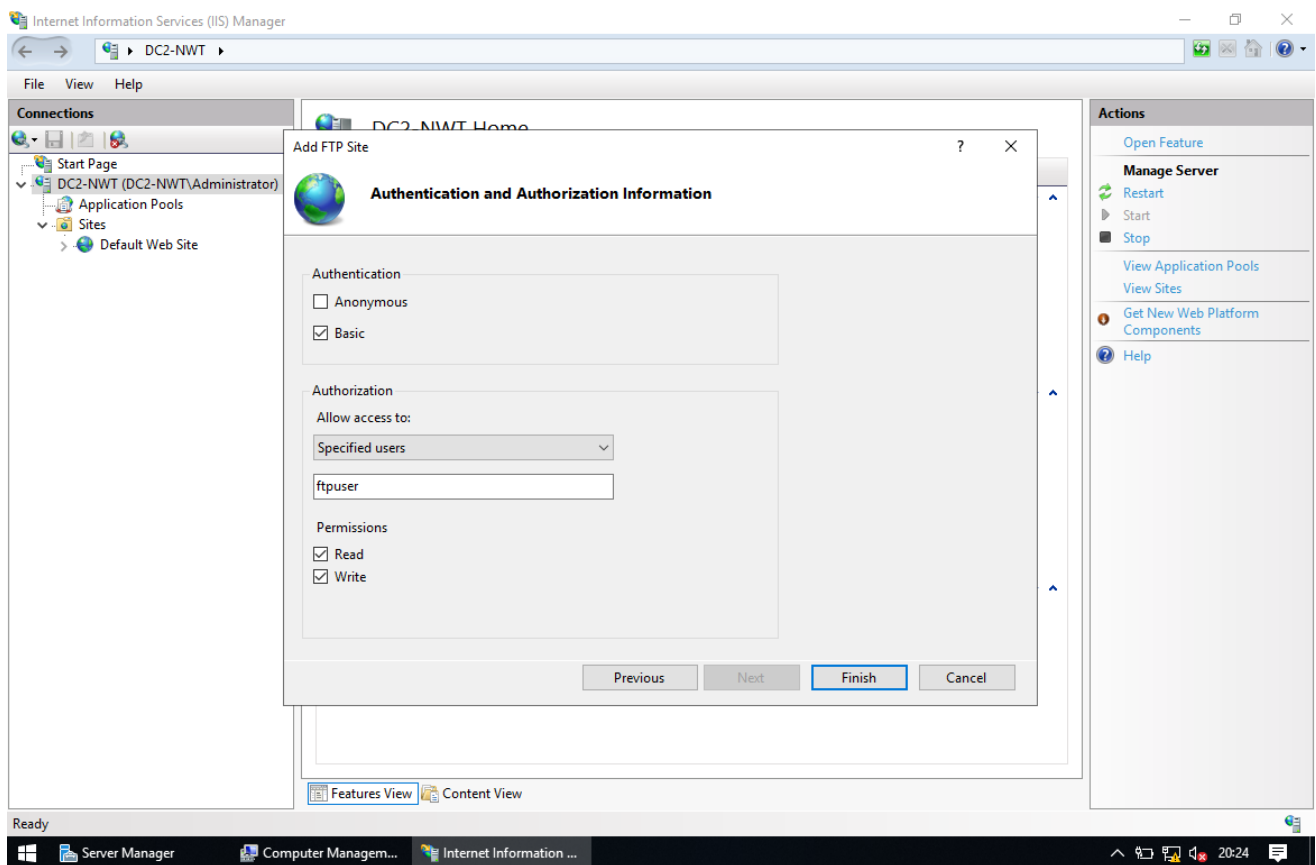
The 'Add FTP Site' wizard appears.



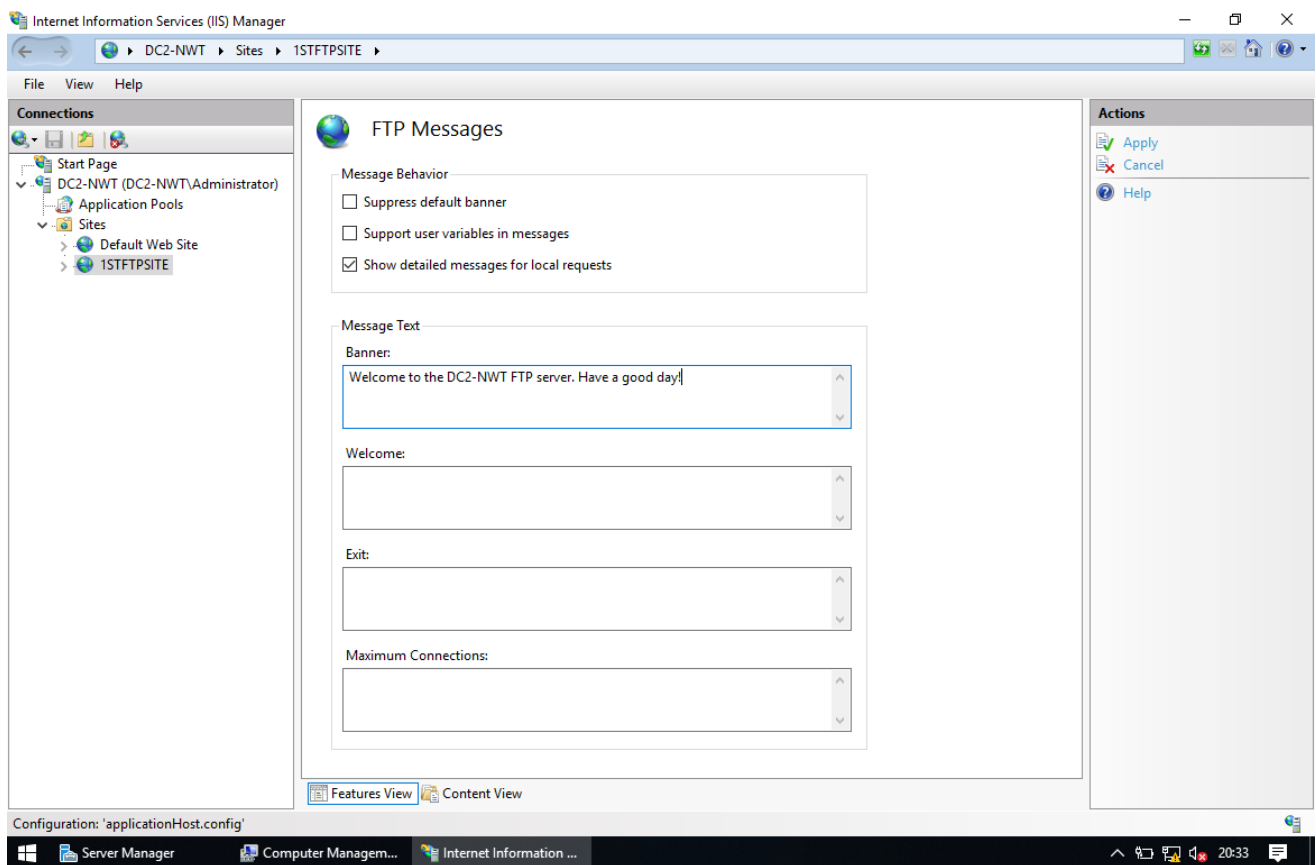
The website information is entered accordingly.



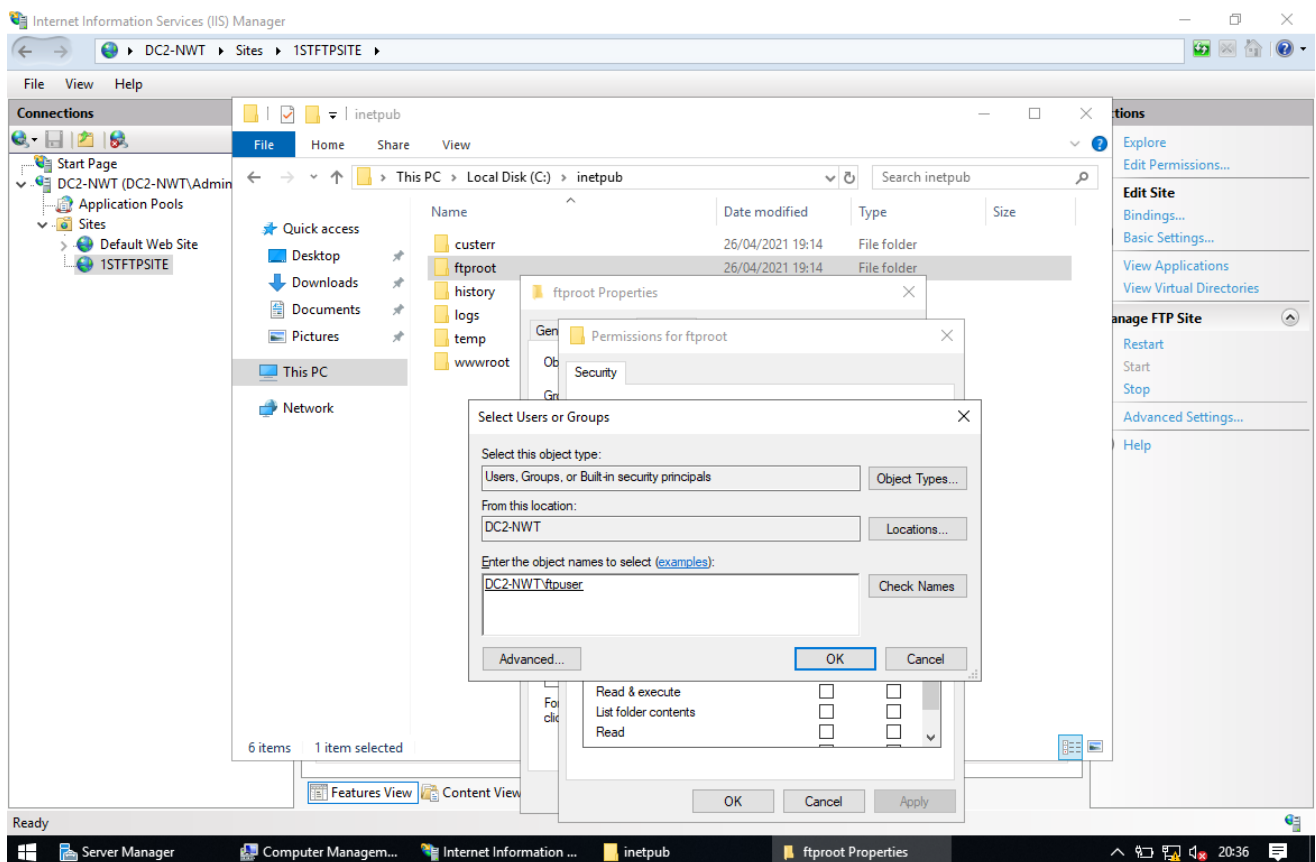
The 'No SSL' option is selected.



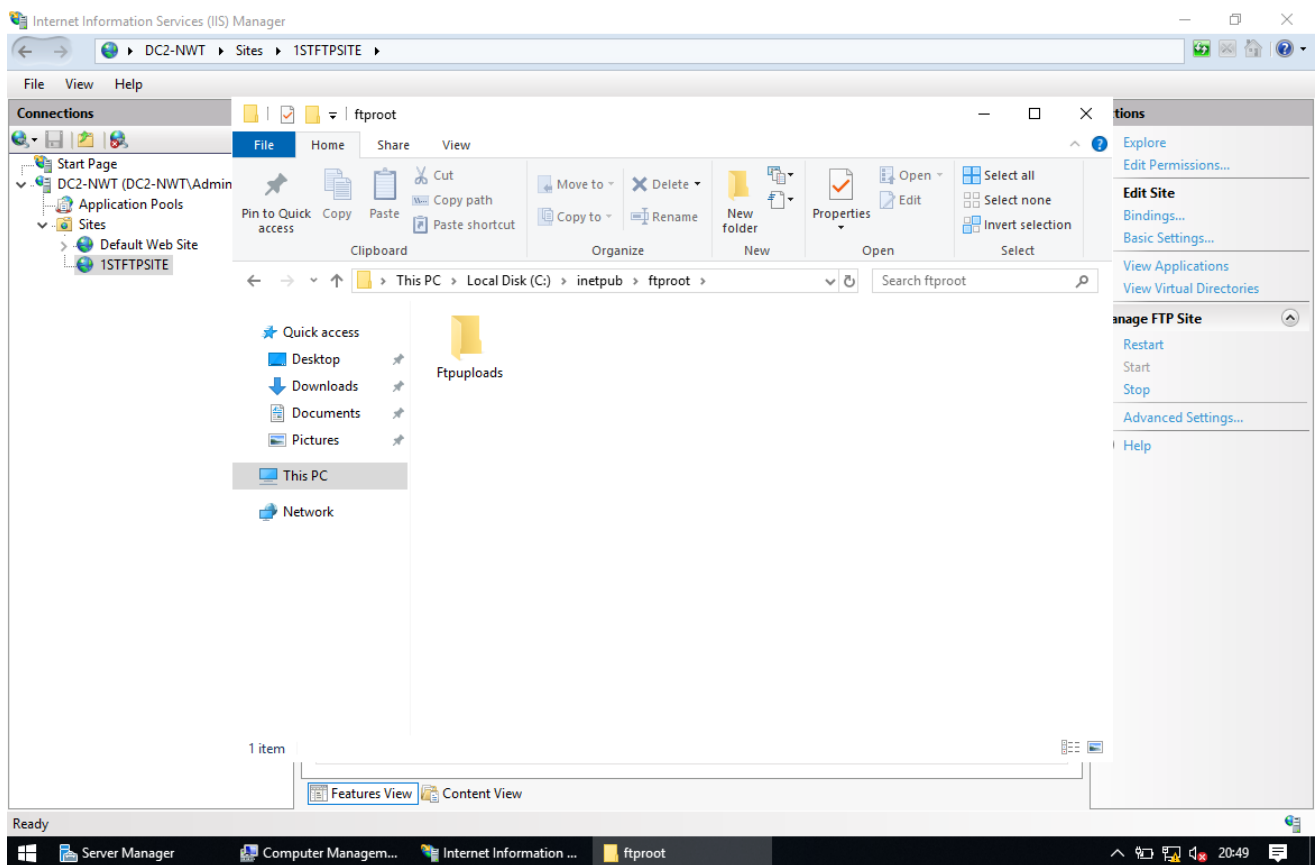
The Authentication is set to 'Basic' and the Authorisation is given to a specific user with the username 'ftpuser' using the 'DC2-NWT' hostname.



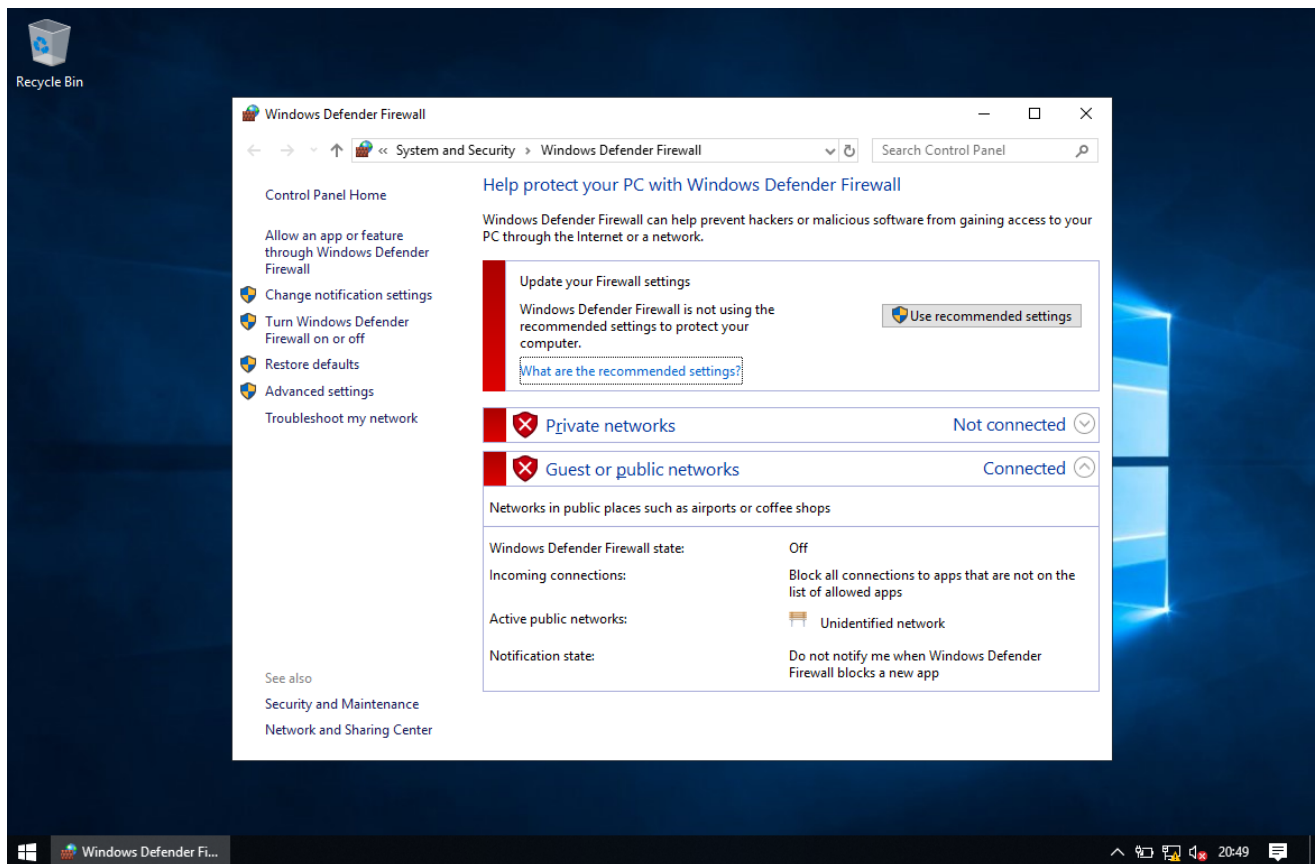
The banner has been set to welcome the user to the FTP server.



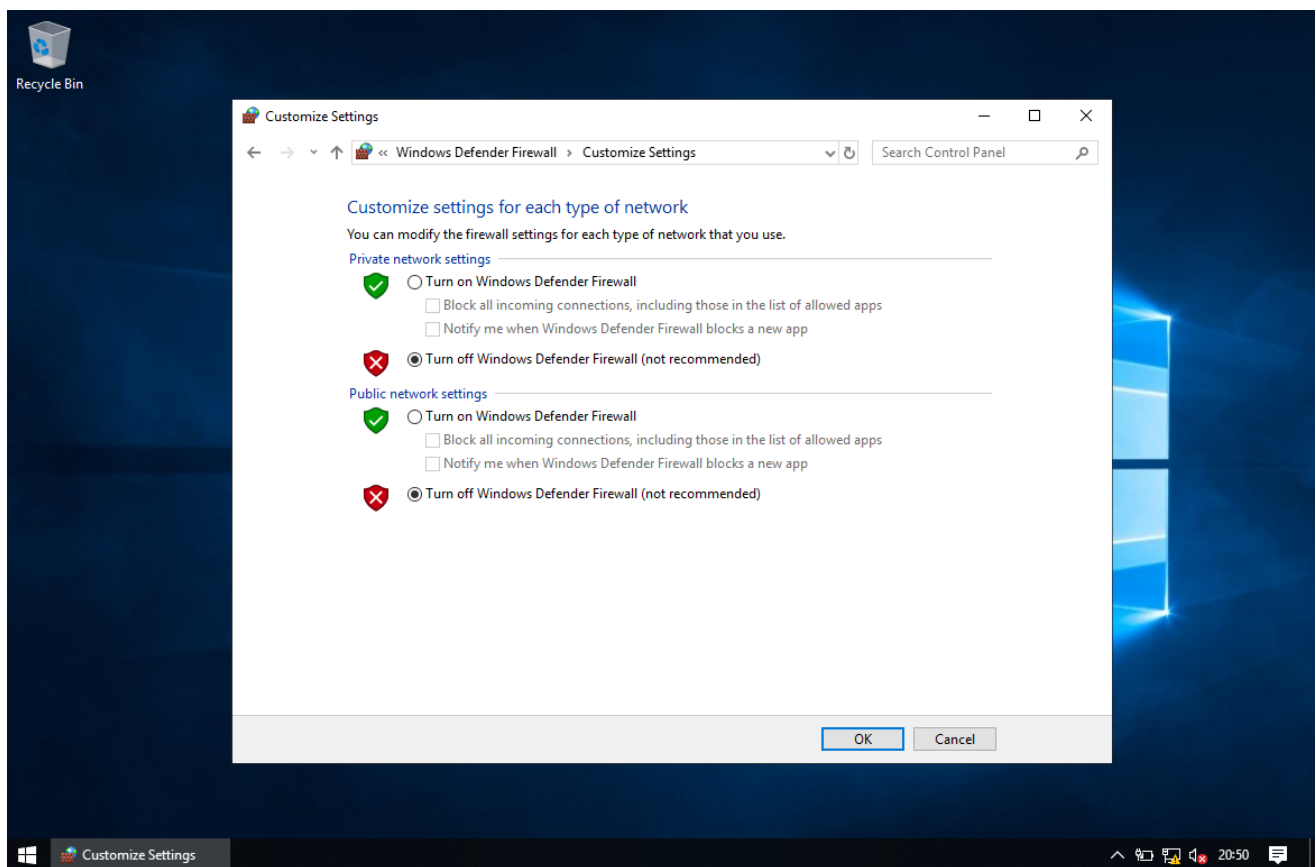
DC2-NWT\ftpuser is added to the security tab for the ftproot folder.



A new folder named 'Ftpuploads' is created in the root ftp folder.

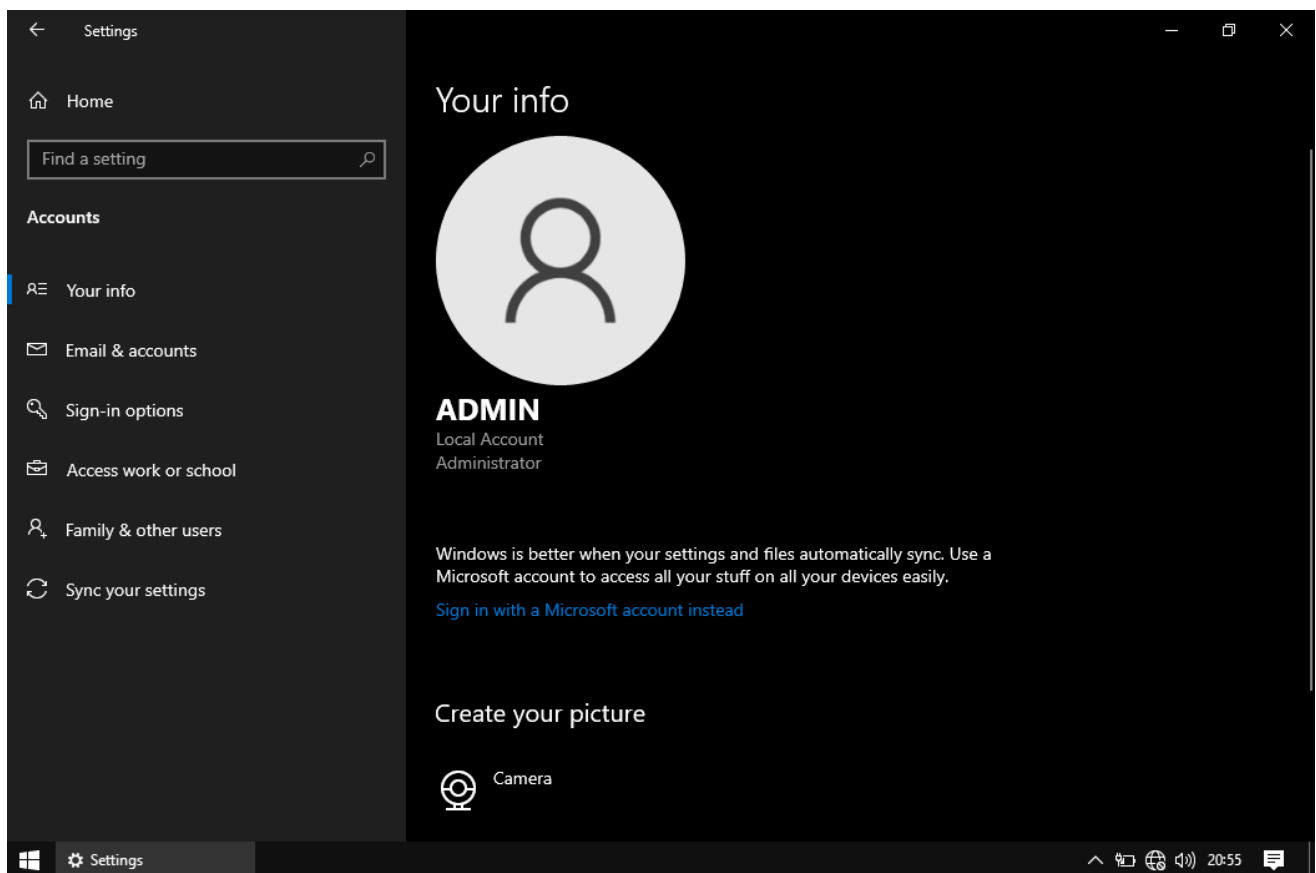


The brief instructs to confirm that no firewalls are installed on the server.

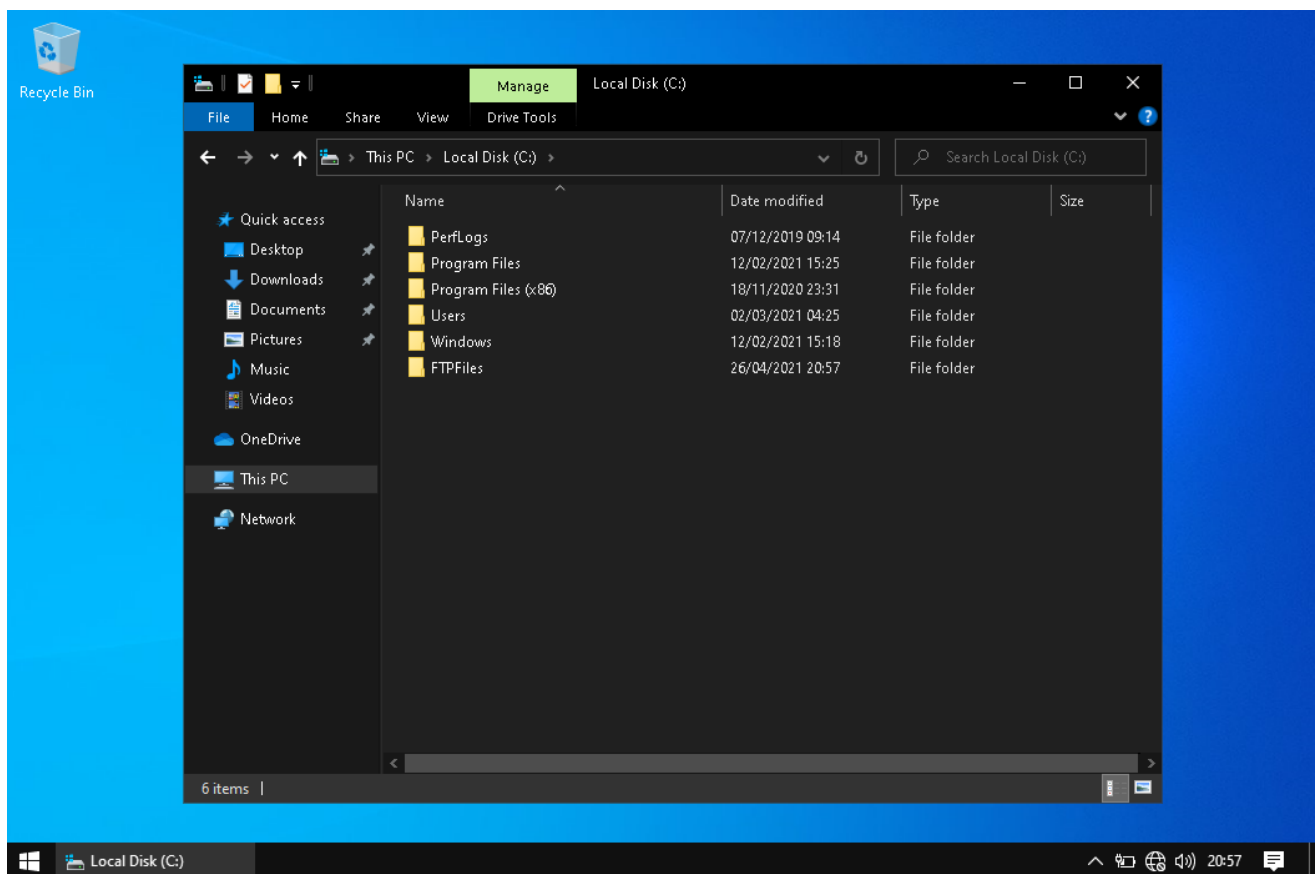


Further confirmation.

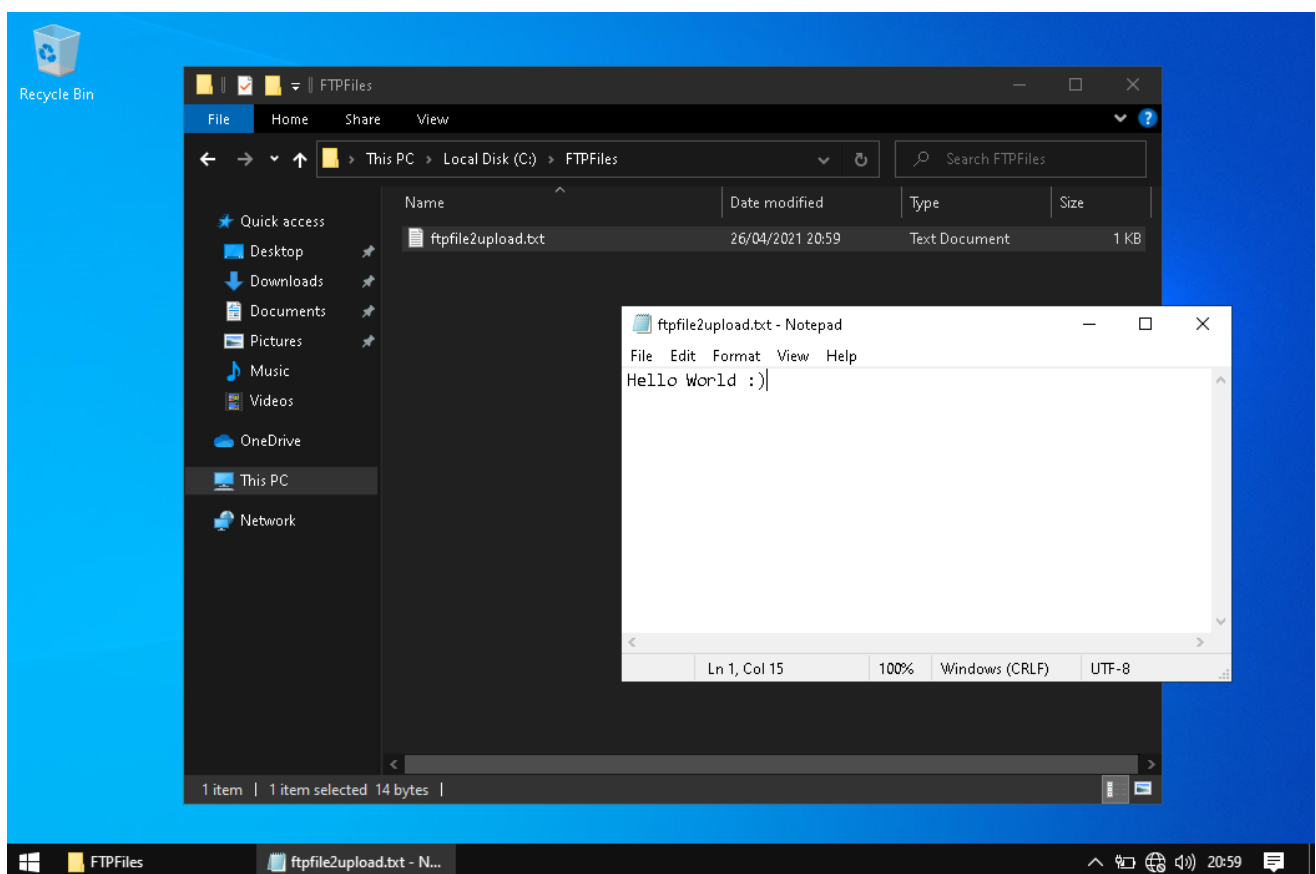
// On Client 2 //



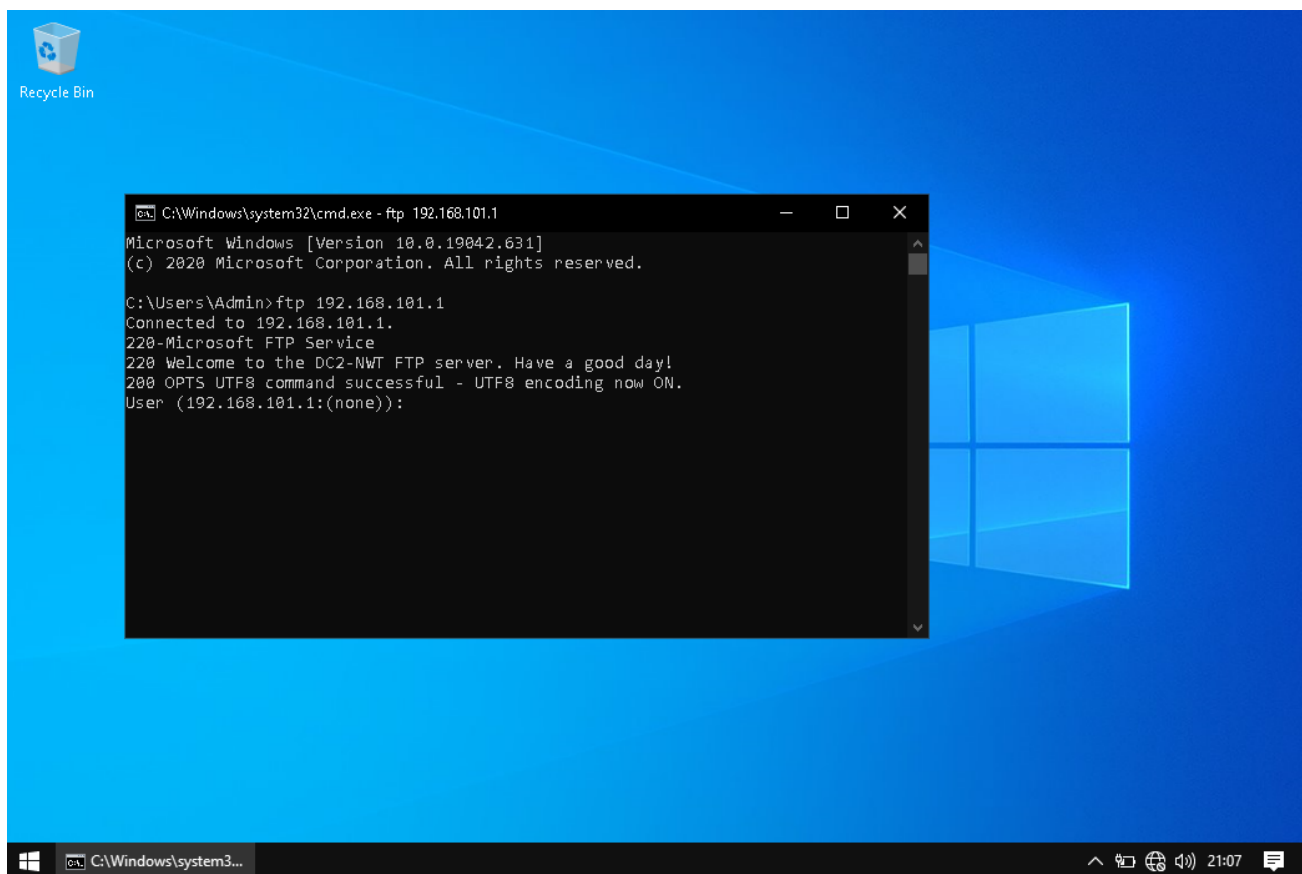
An admin account is logged into to access the command prompt as a policy is set to disallow access to the command prompt for non-admin users.



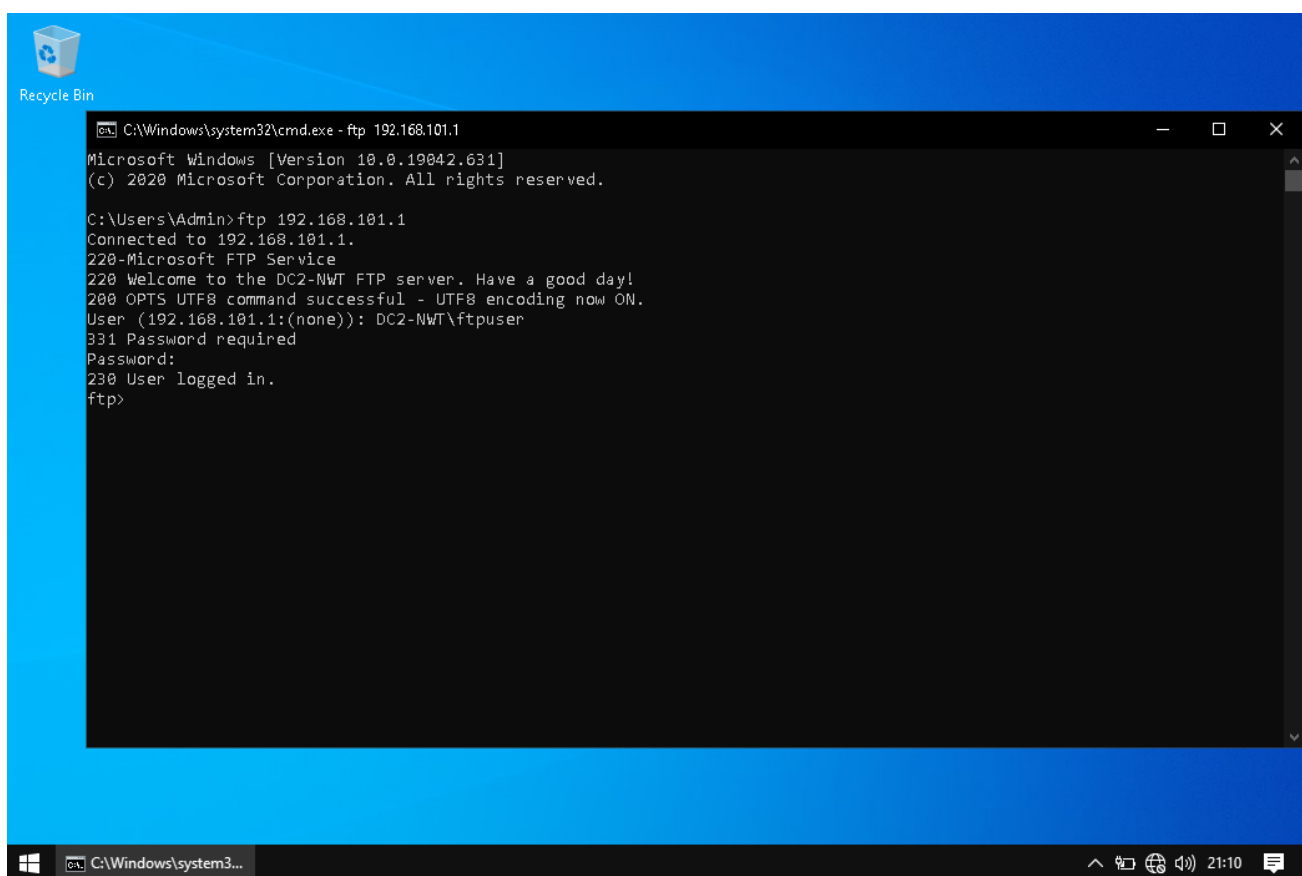
A new folder named 'FTPFiles' is created in the C: directory root folder on Client 2.



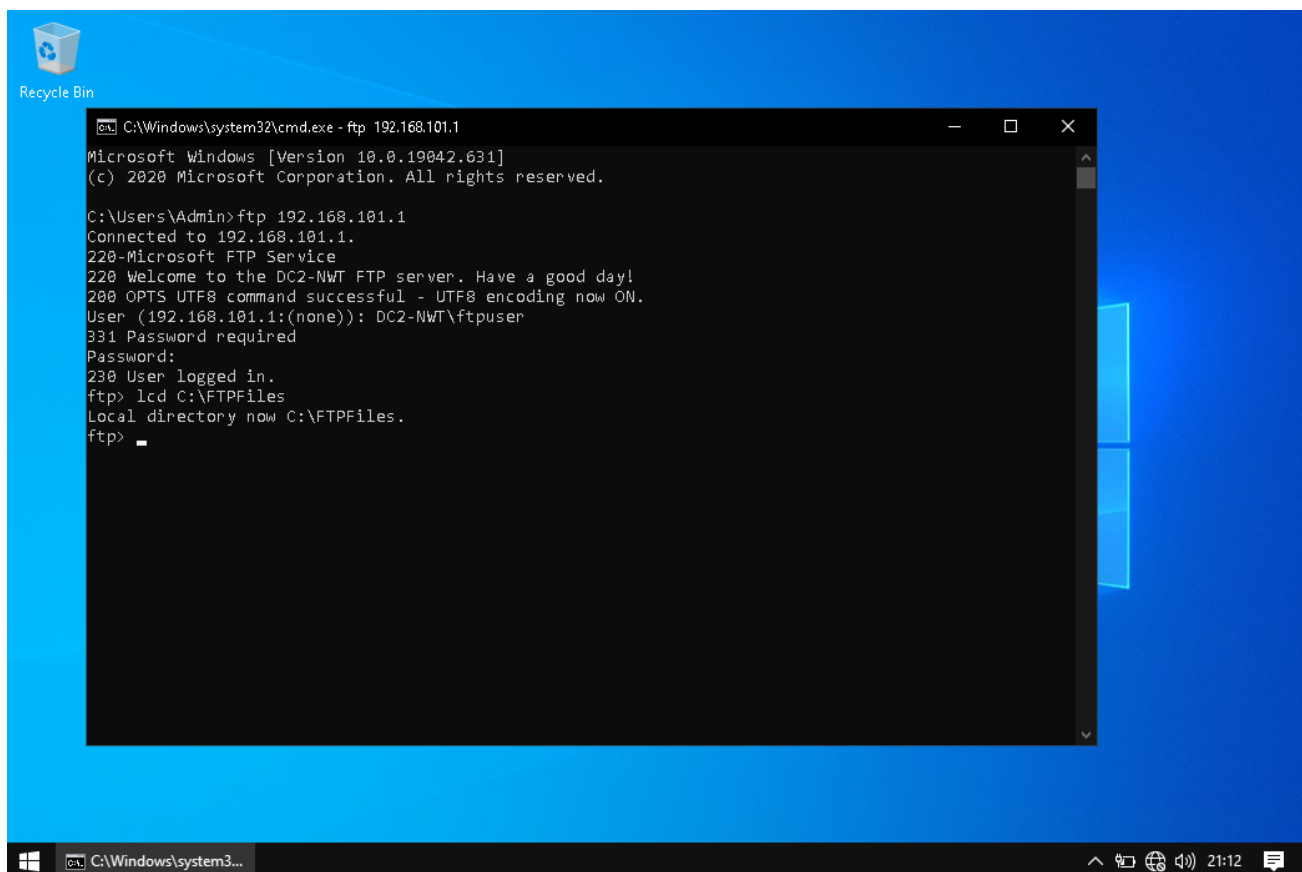
A new file 'ftpfile2upload.txt' is created inside the FTPFiles folder.



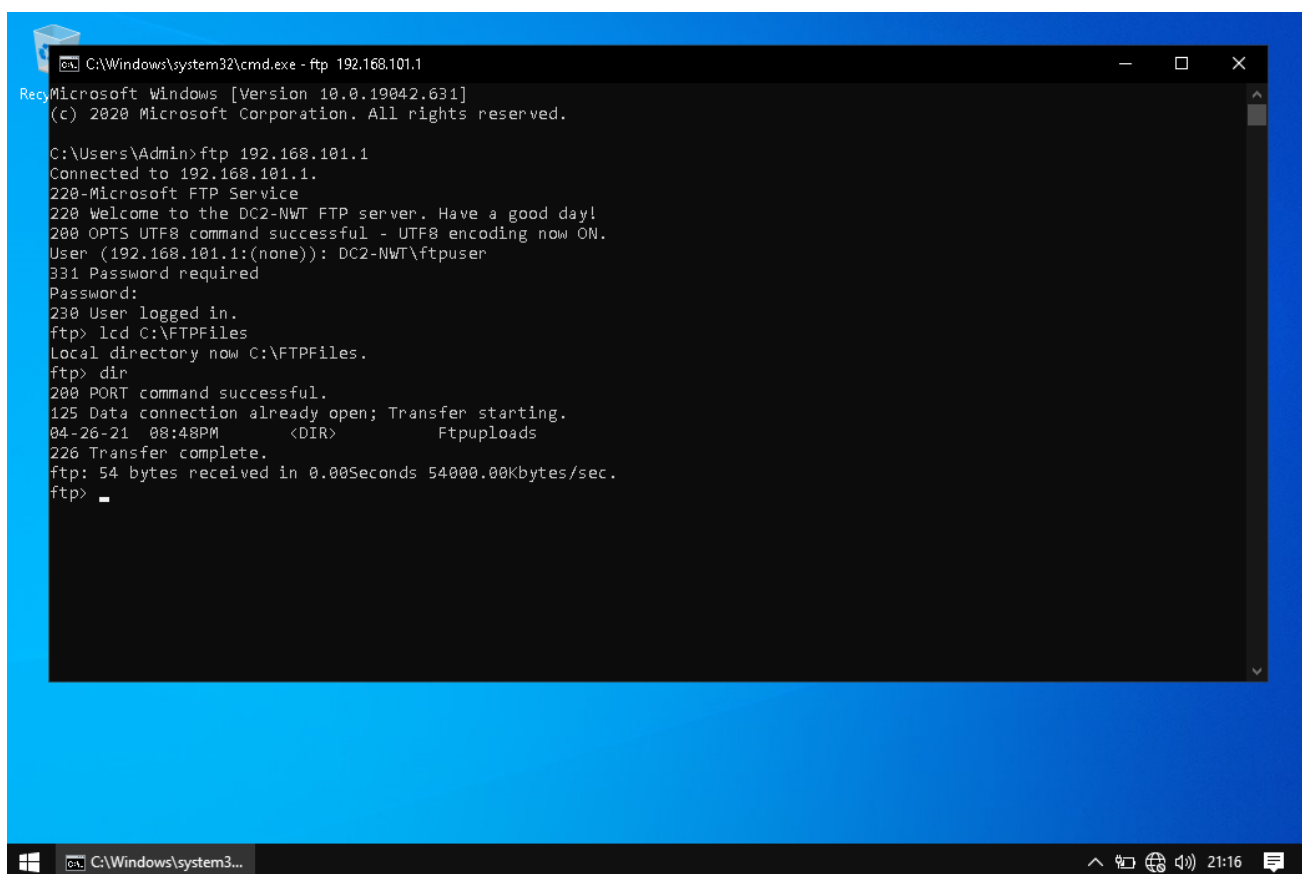
Success! Using CMD to connect to the FTP server, the banner appears correctly. An attempt to log in using the login details provided by the brief will be attempted.



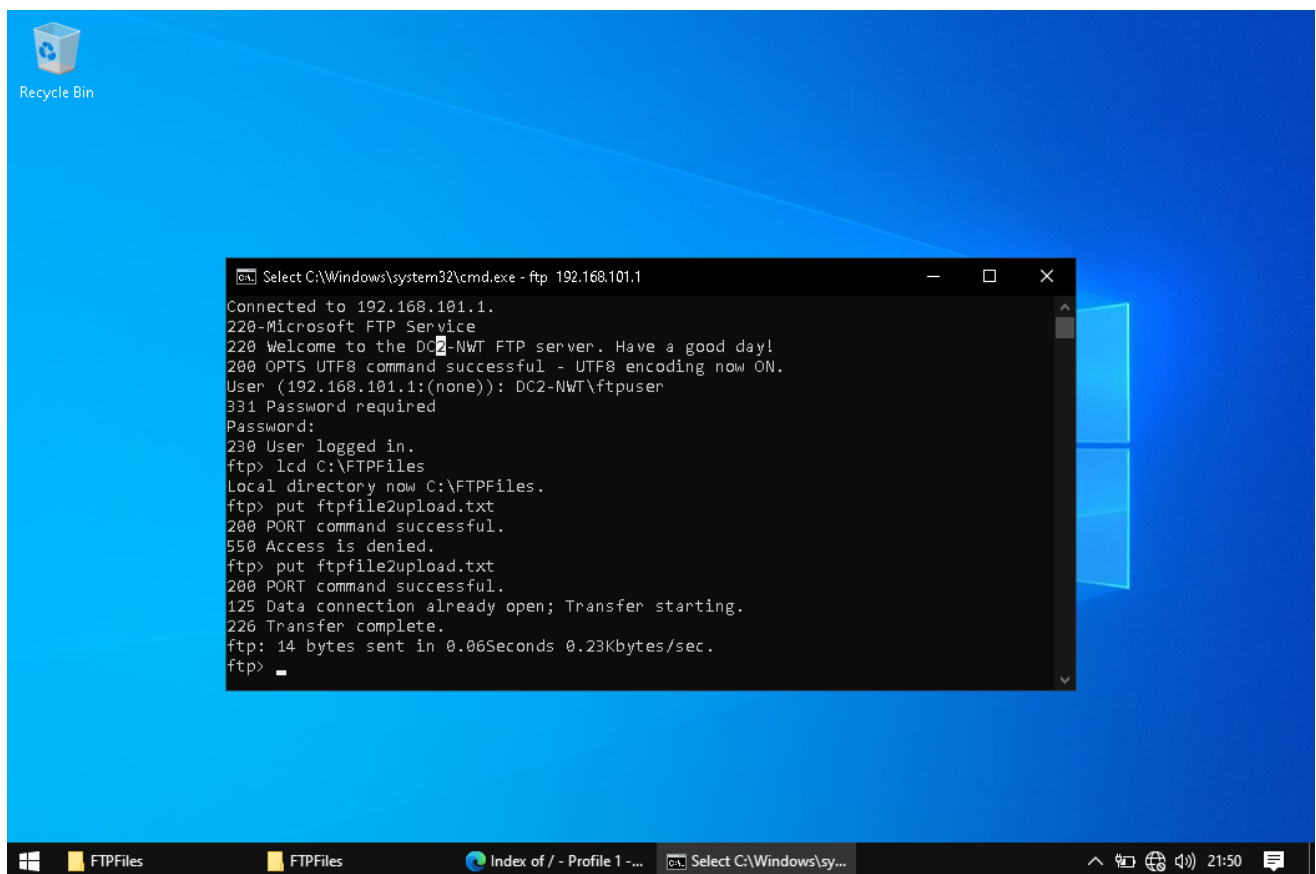
Another success. The server delivers a 230 and the user is successfully logged in.



The directory is changed to C:\FTPFiles using the LCD command.

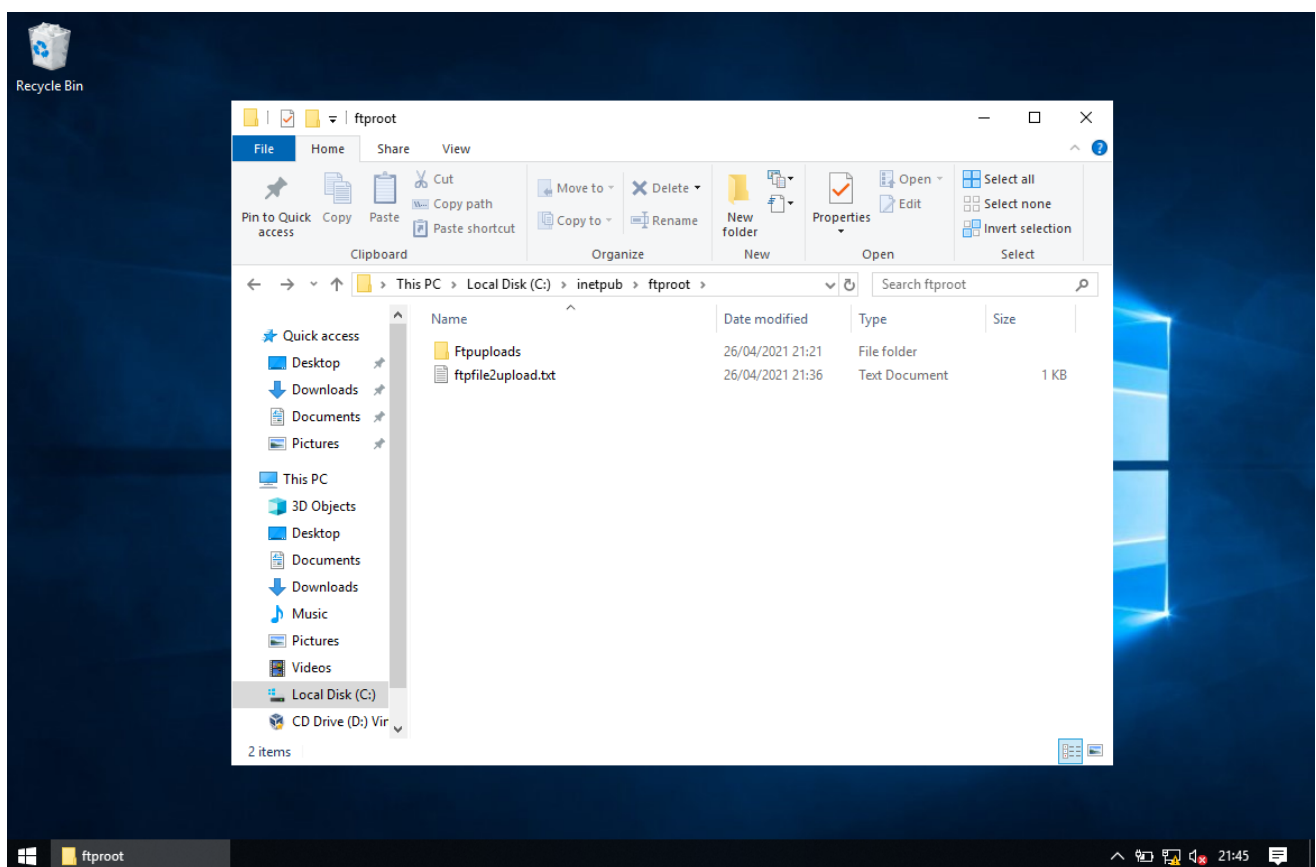


The directory is explored using the dir command.

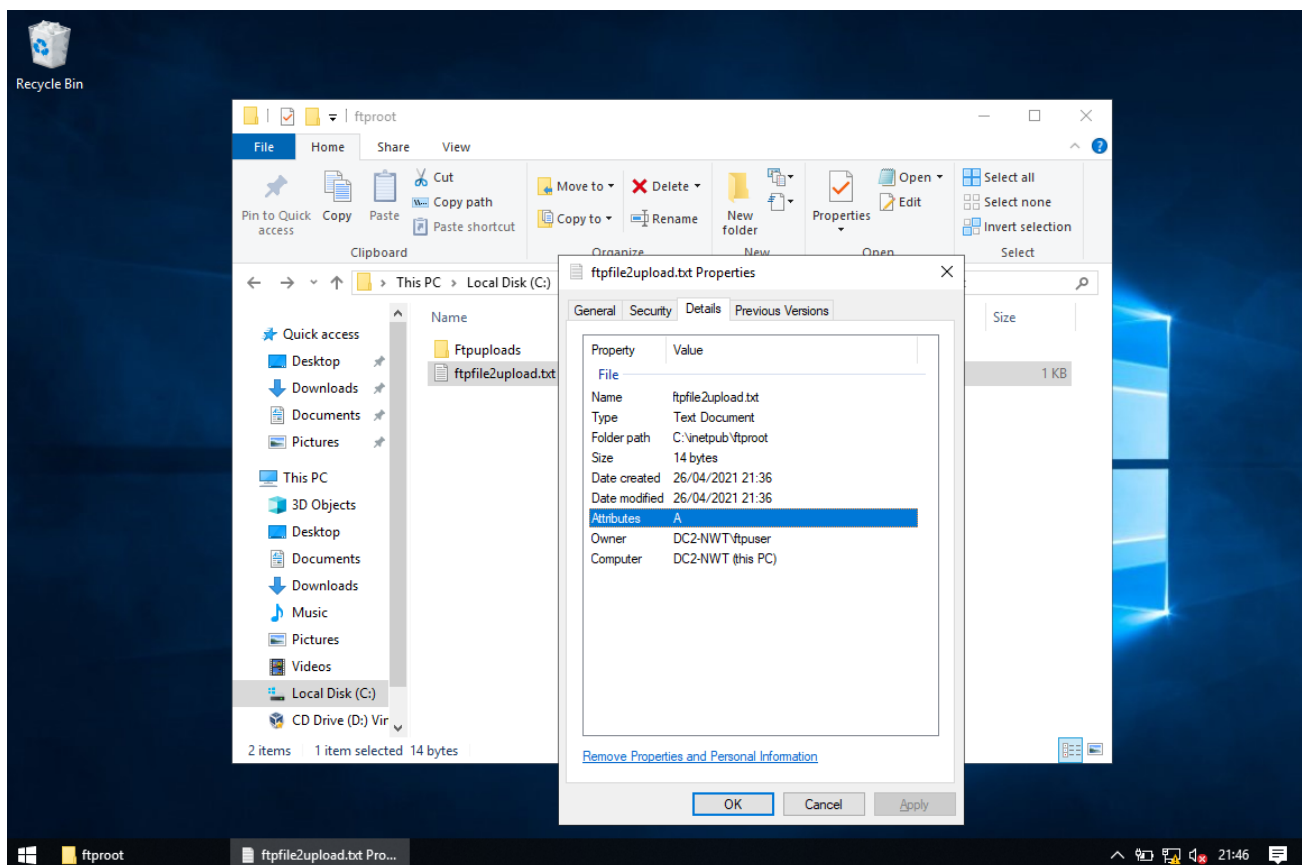


According to the ftp prompt, the file was transferred successfully.

// On Server 2 //



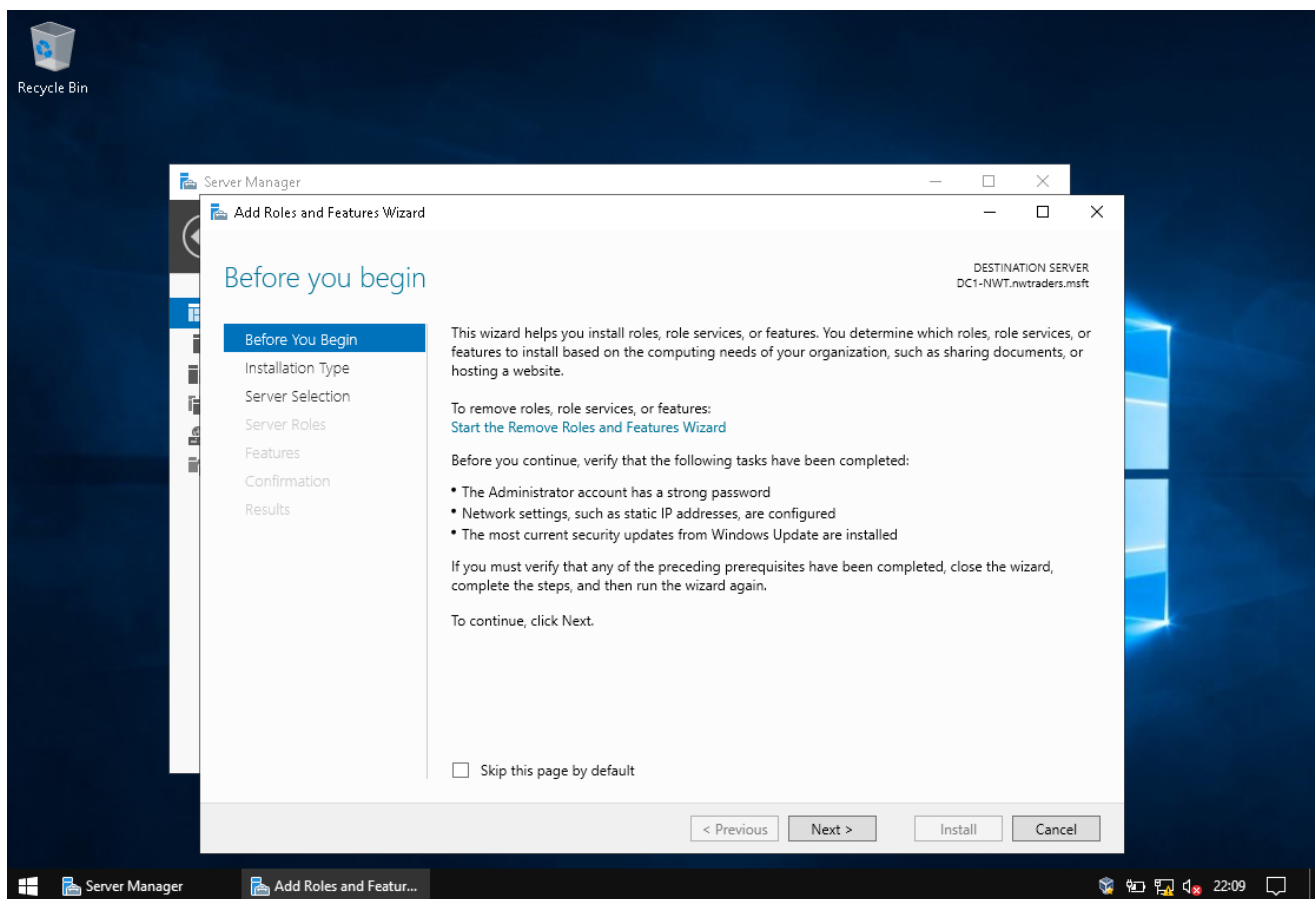
The 'ftpfile2upload.txt' appears successfully.



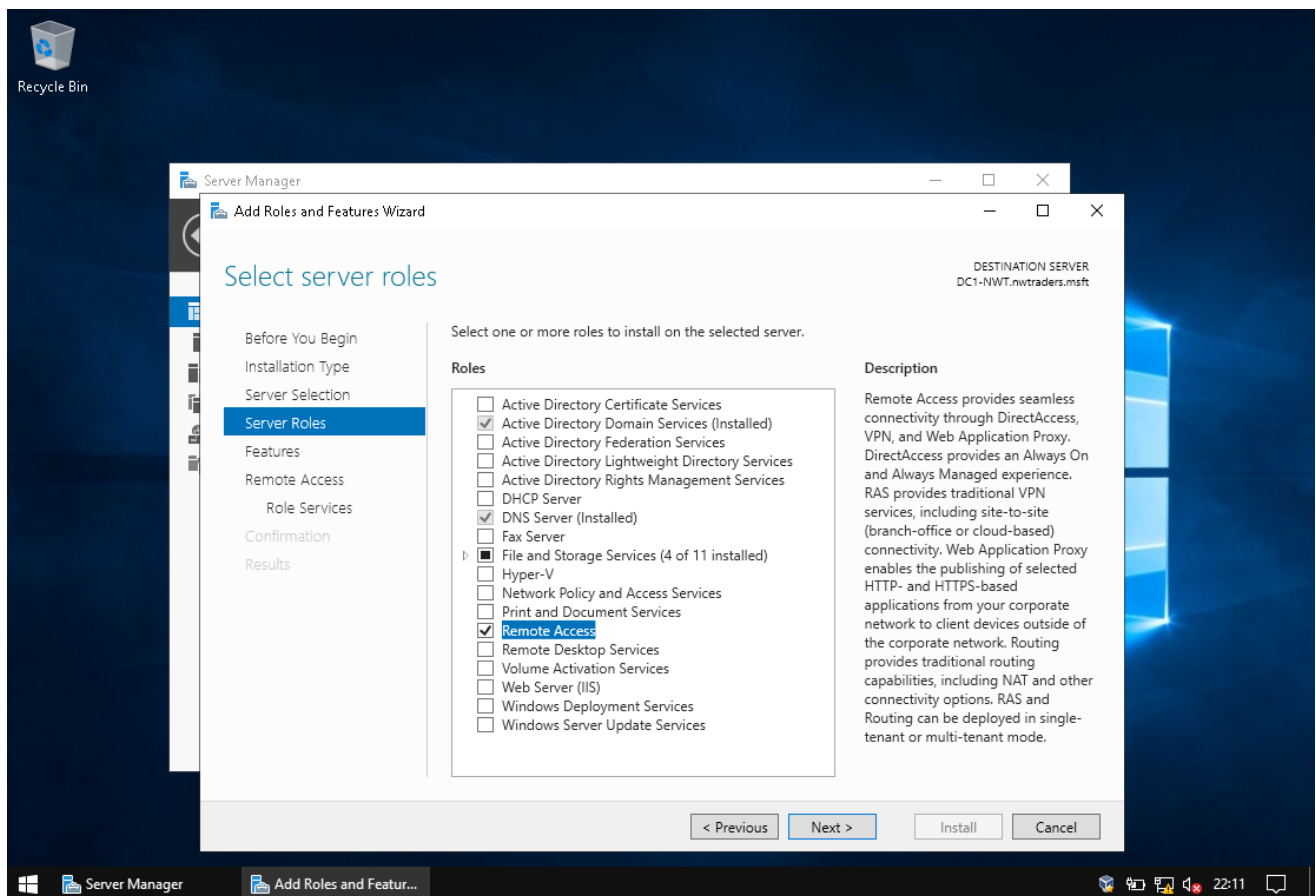
Attached to the meta data, the owner of the file (DC2-NWT\ftpuser) provides evidence that this file was sent by a separate user on another machine.

Task 3: Installing and configuring the Routing and Remote Access Service

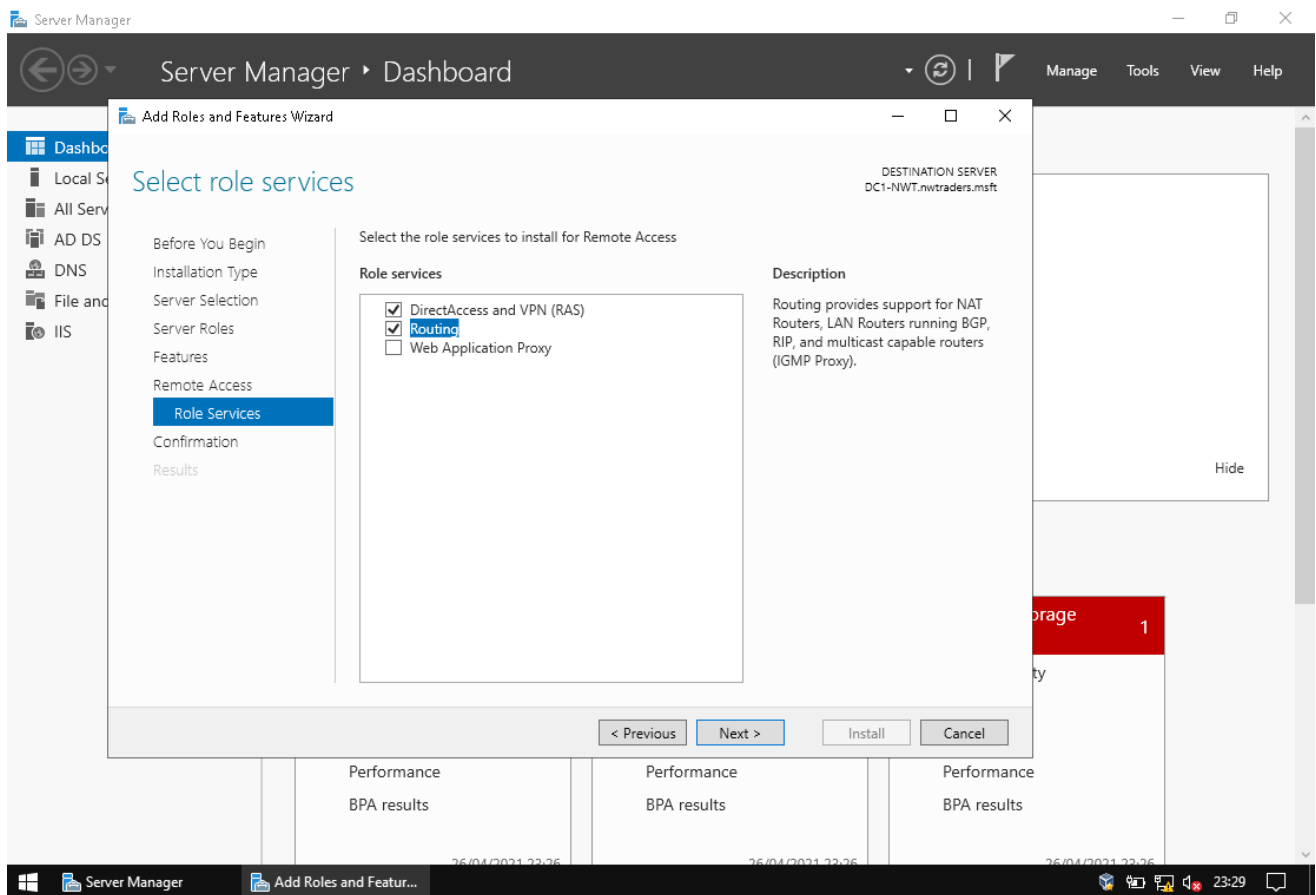
// On Server 1 //



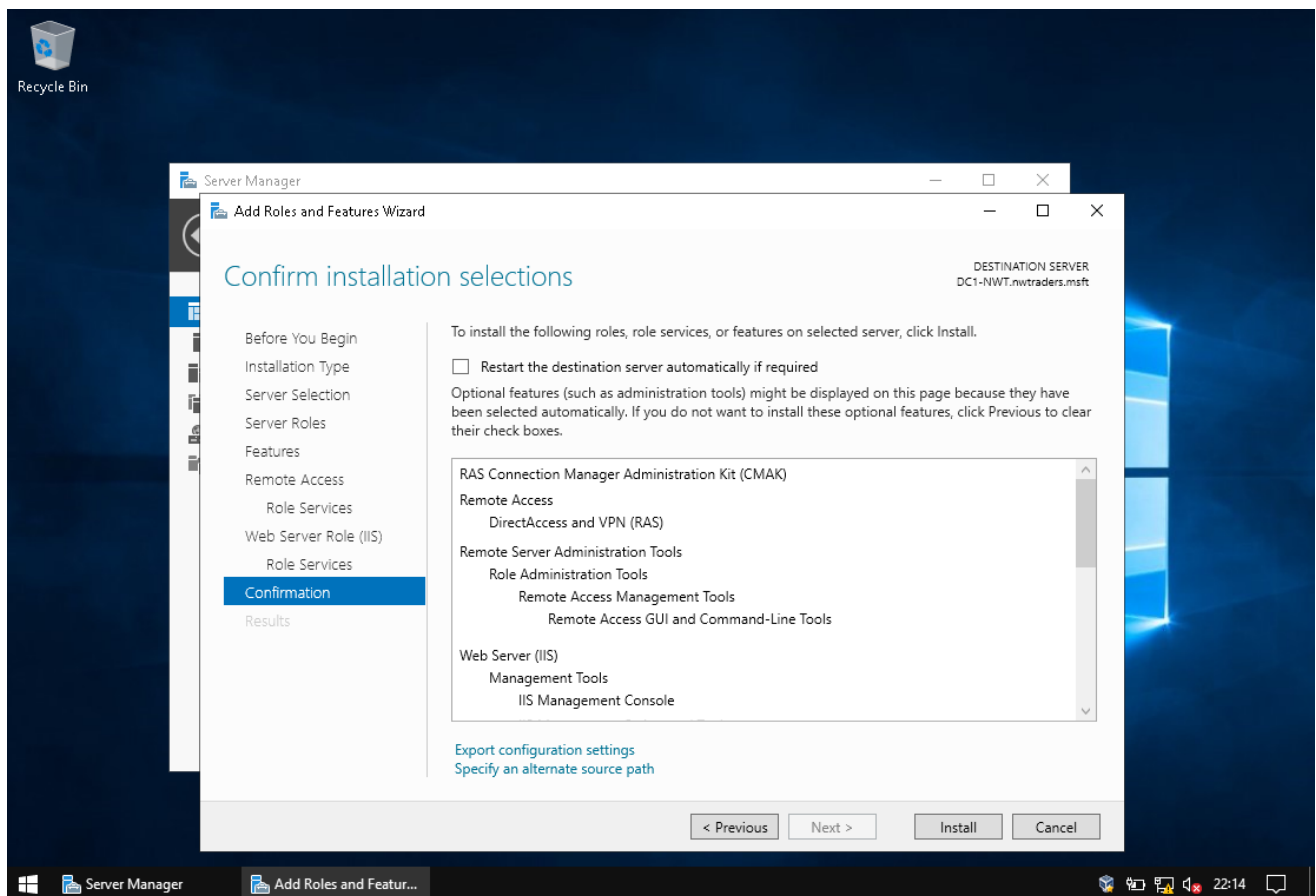
The 'Add Roles and Features Wizard' was opened on the Server 1.



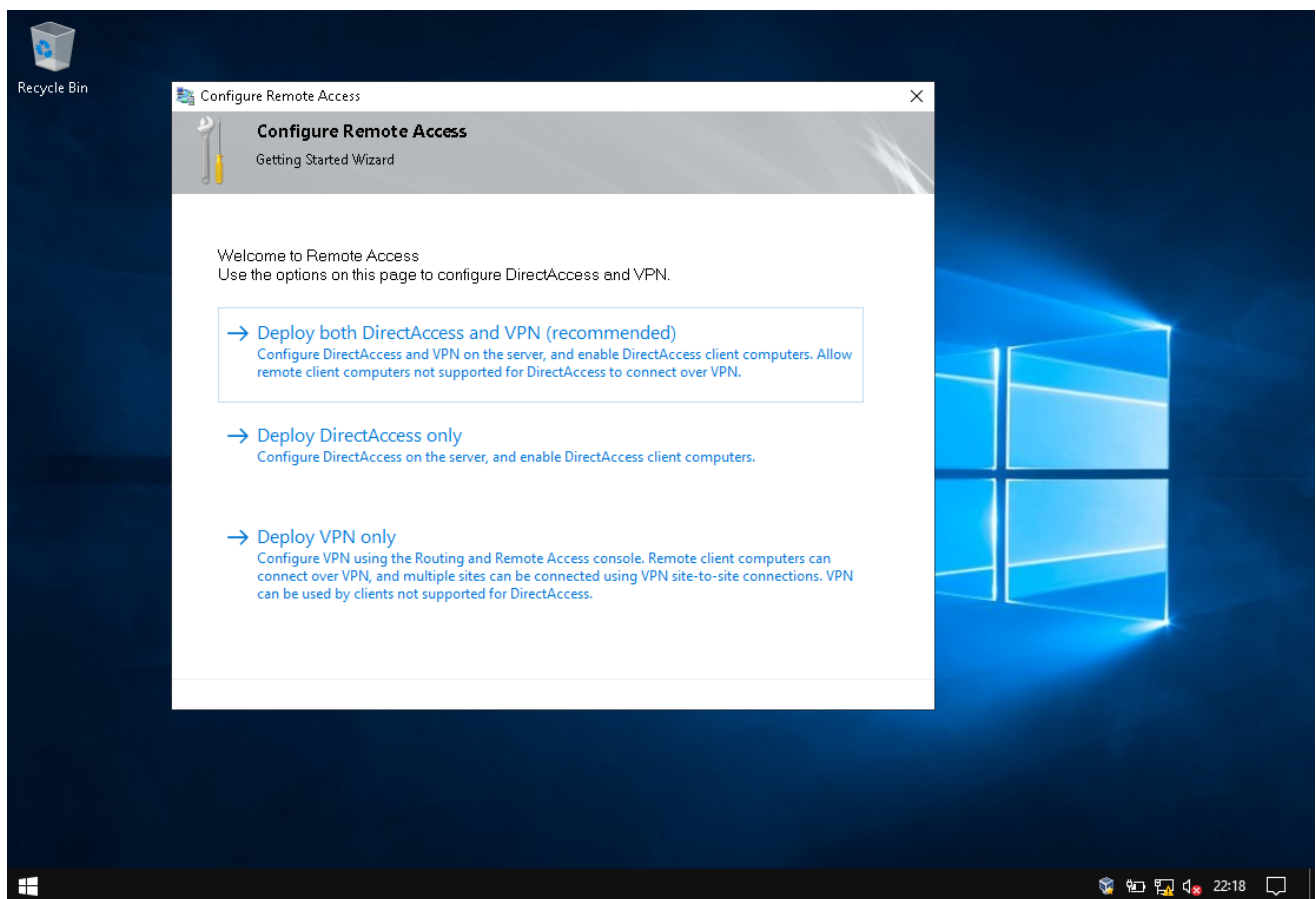
'Remote Access' was selected as a Server Role.



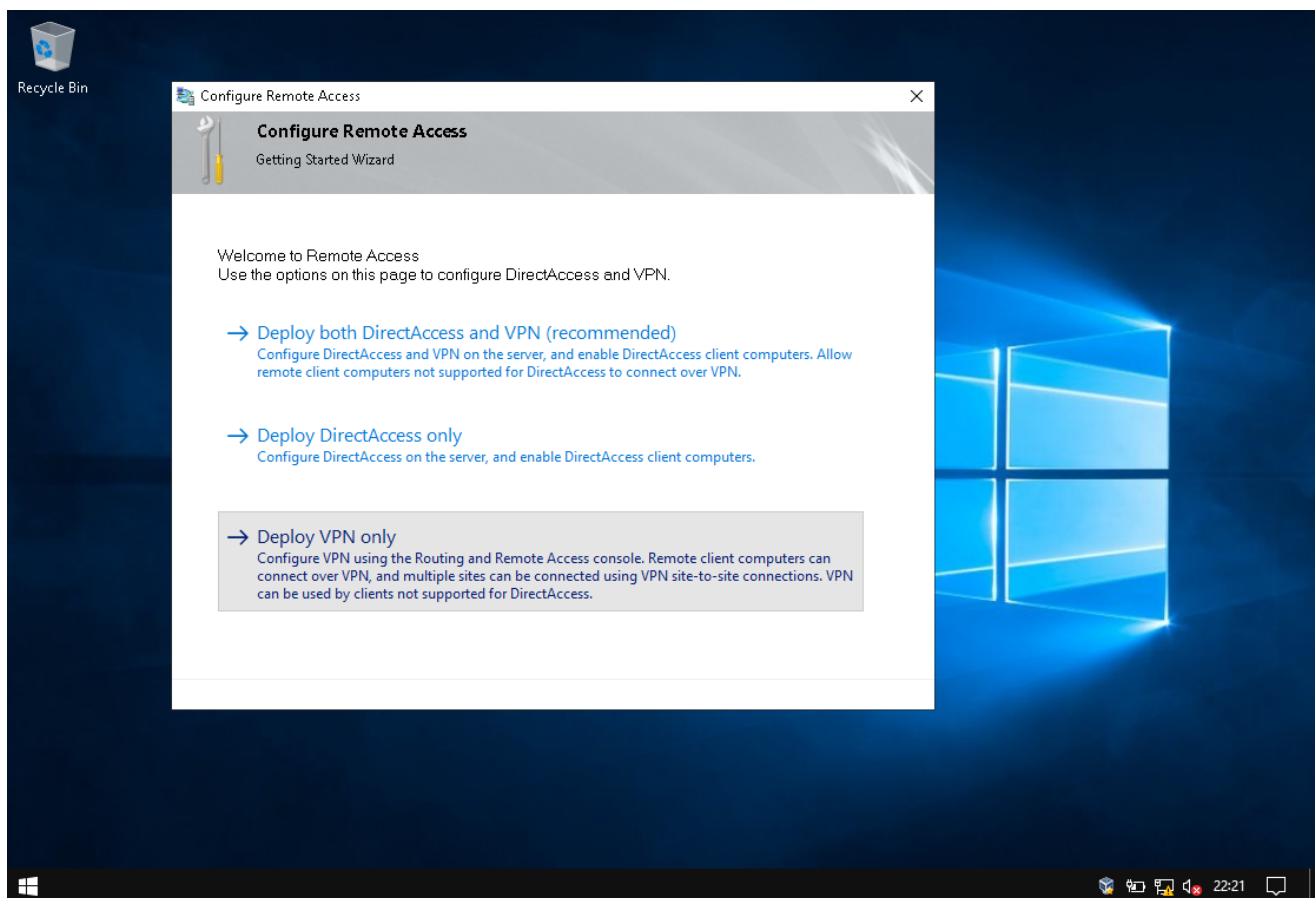
‘DirectAccess and VPN (RAS)’ and ‘Routing’ was checked as instructed by the brief.



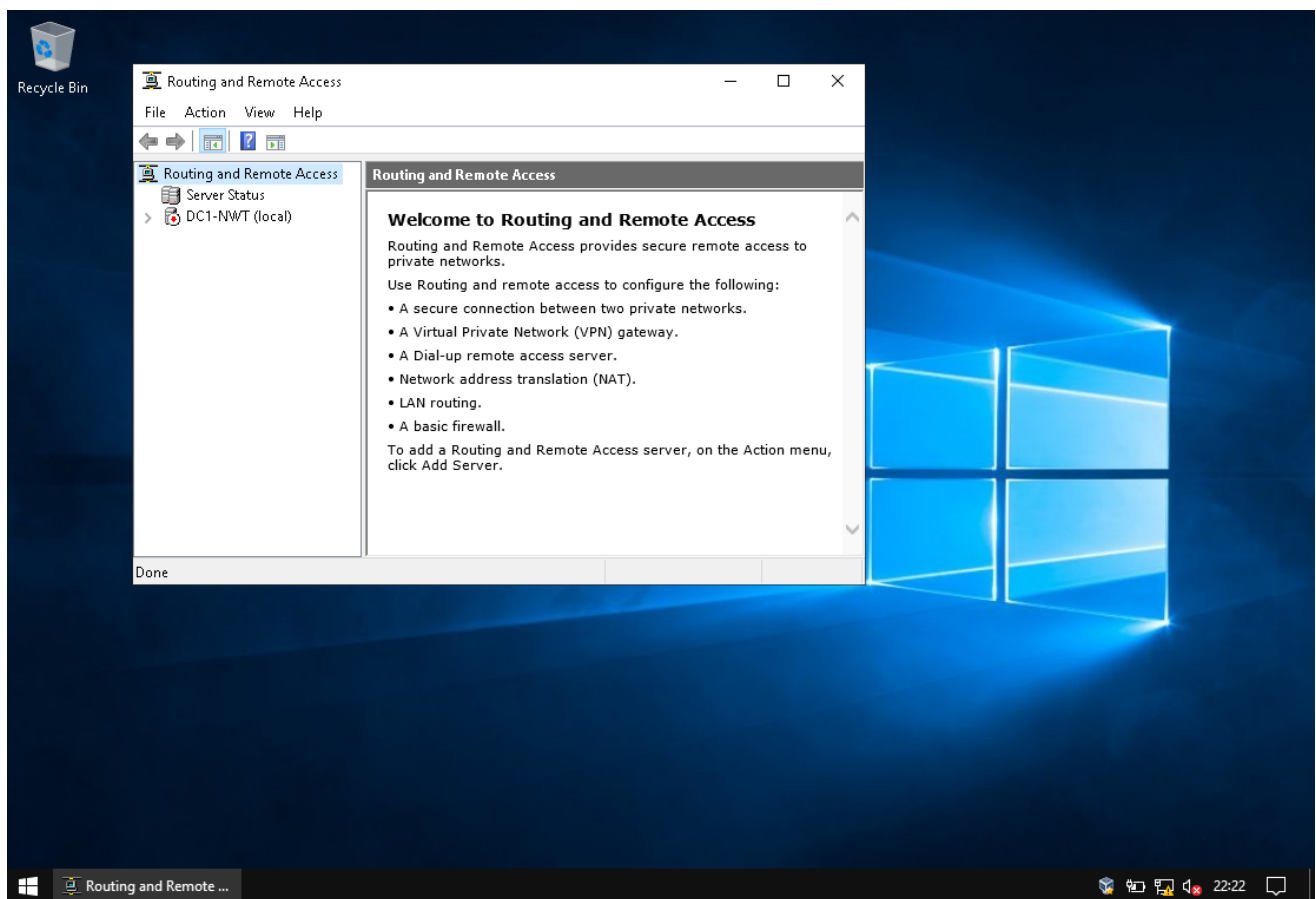
The confirmation screen appeared and the changes were confirmed.



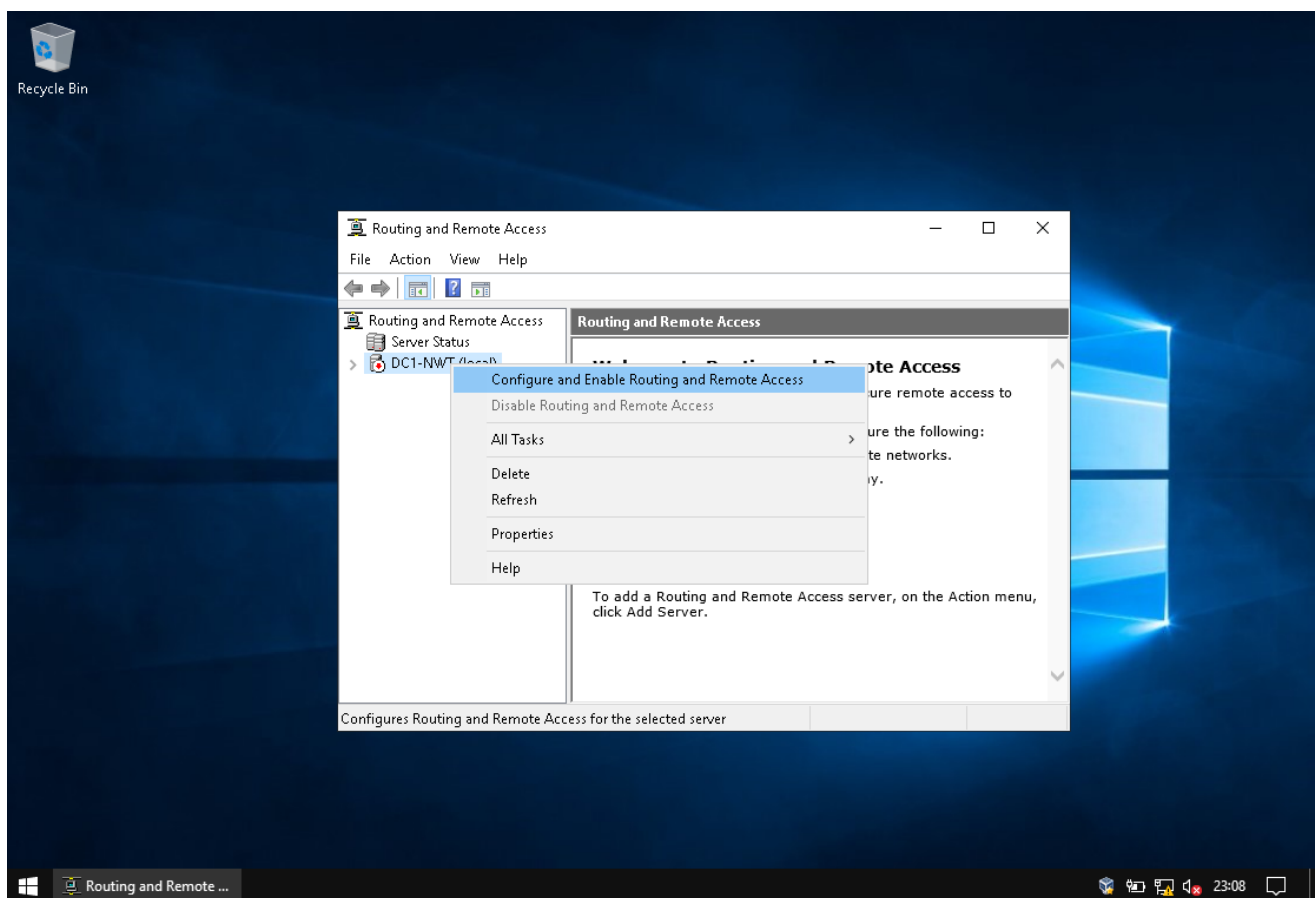
The 'Configure Remote Access' wizard appears (*Although it does not appear on the task bar*).



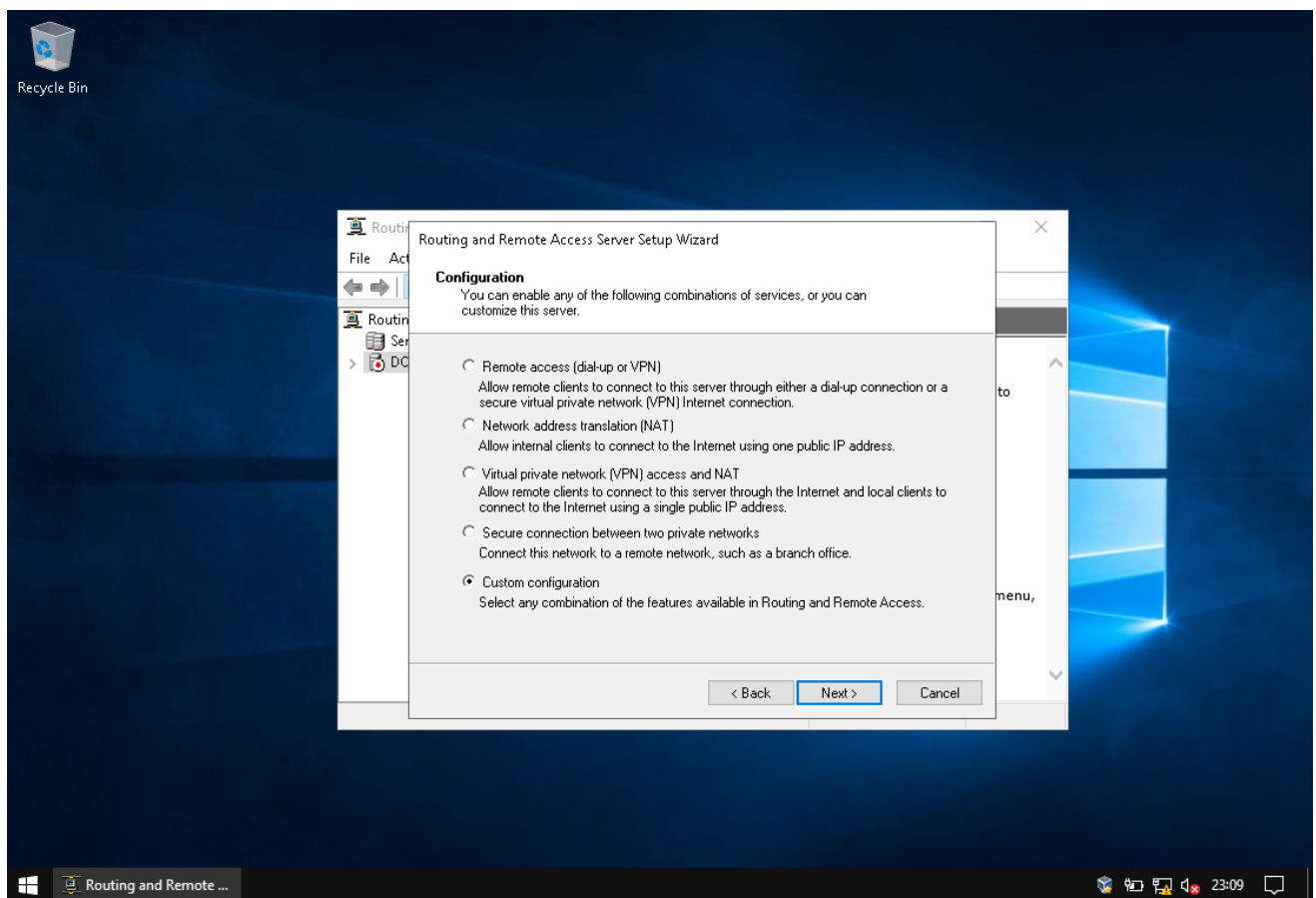
'Deploy VPN only' was selected.



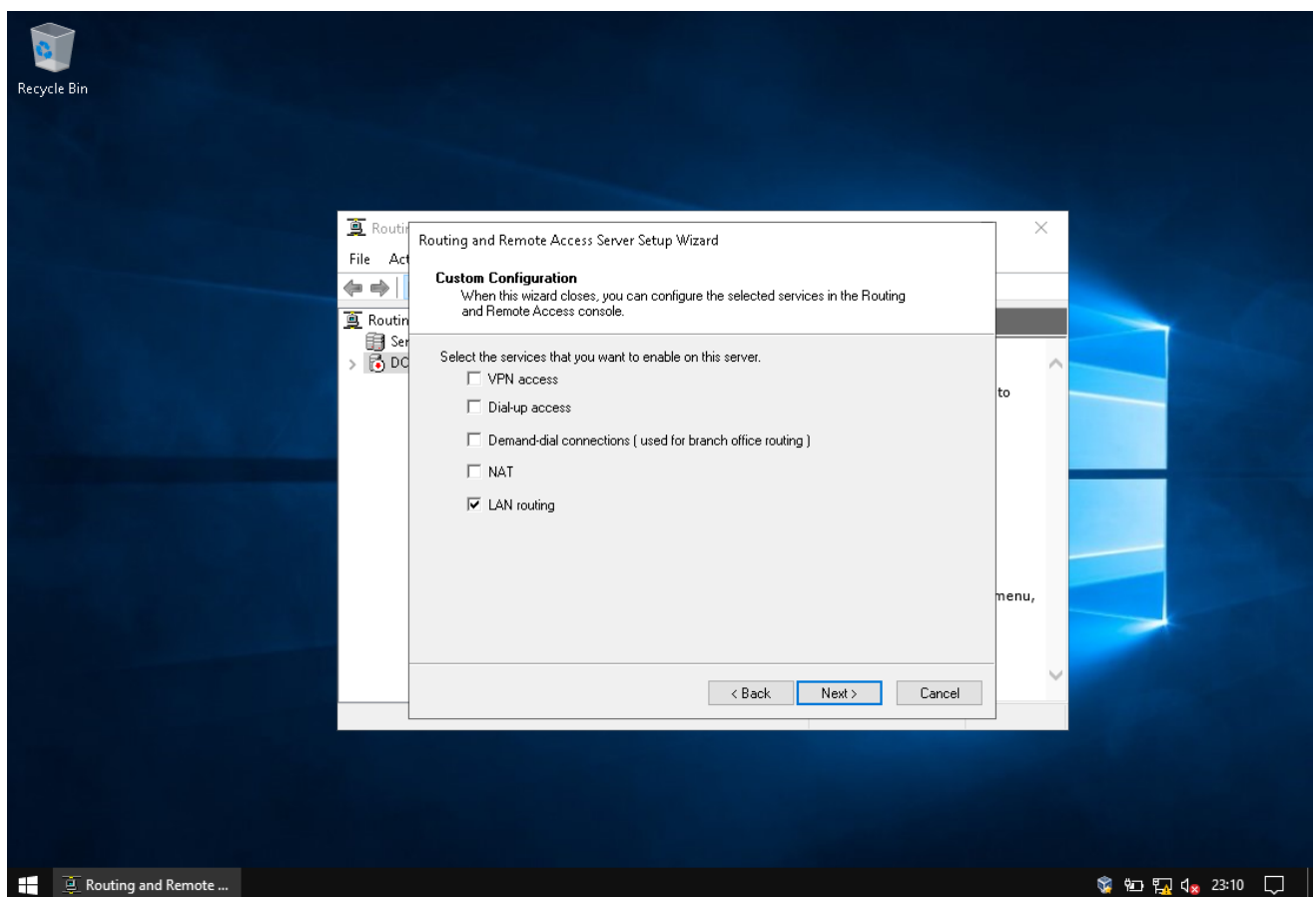
The 'Routing and Remote Access' page appears.



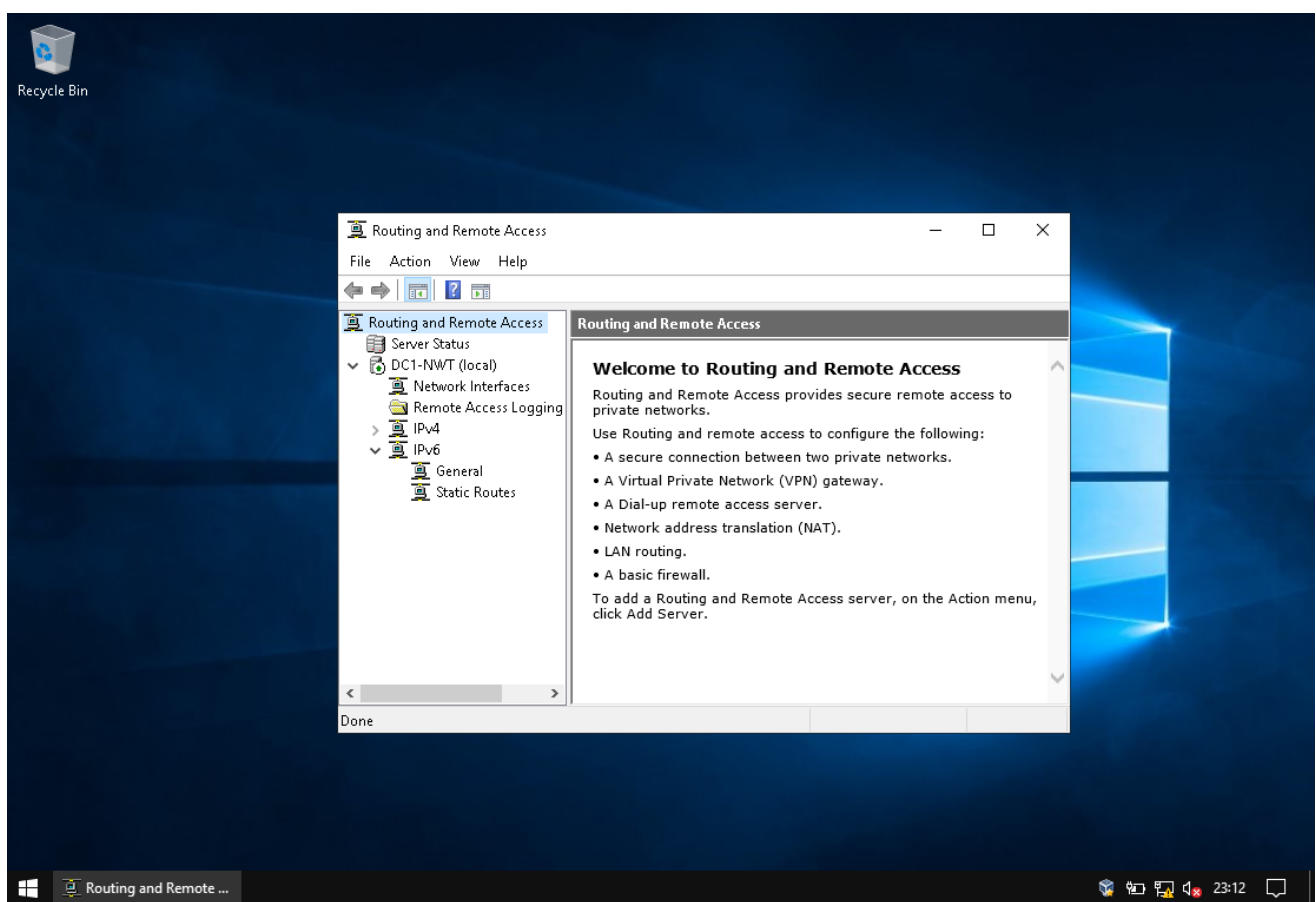
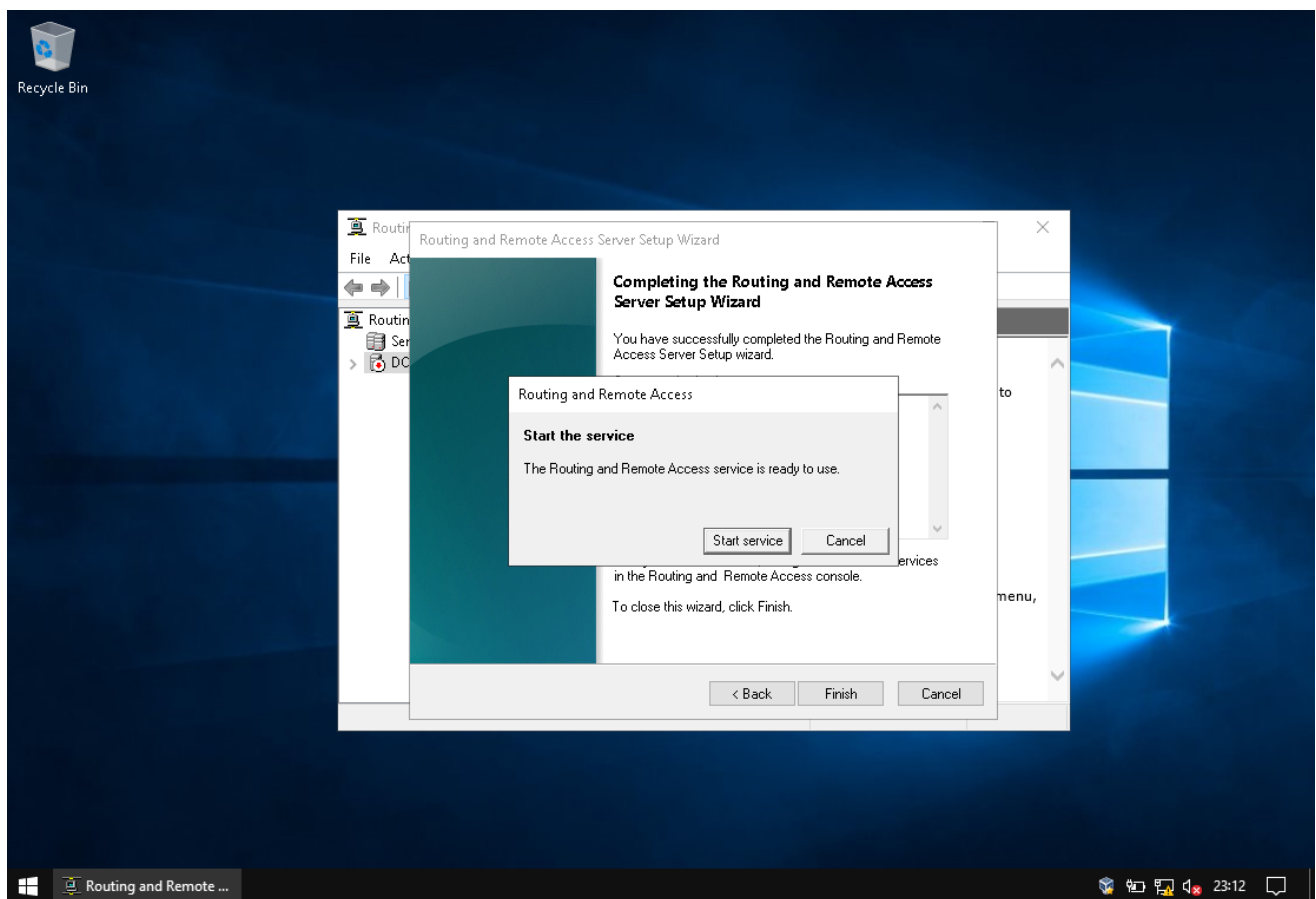
A context menu is opened above the server, and the 'Configure and Enable Routing and Remote Access' option is selected.



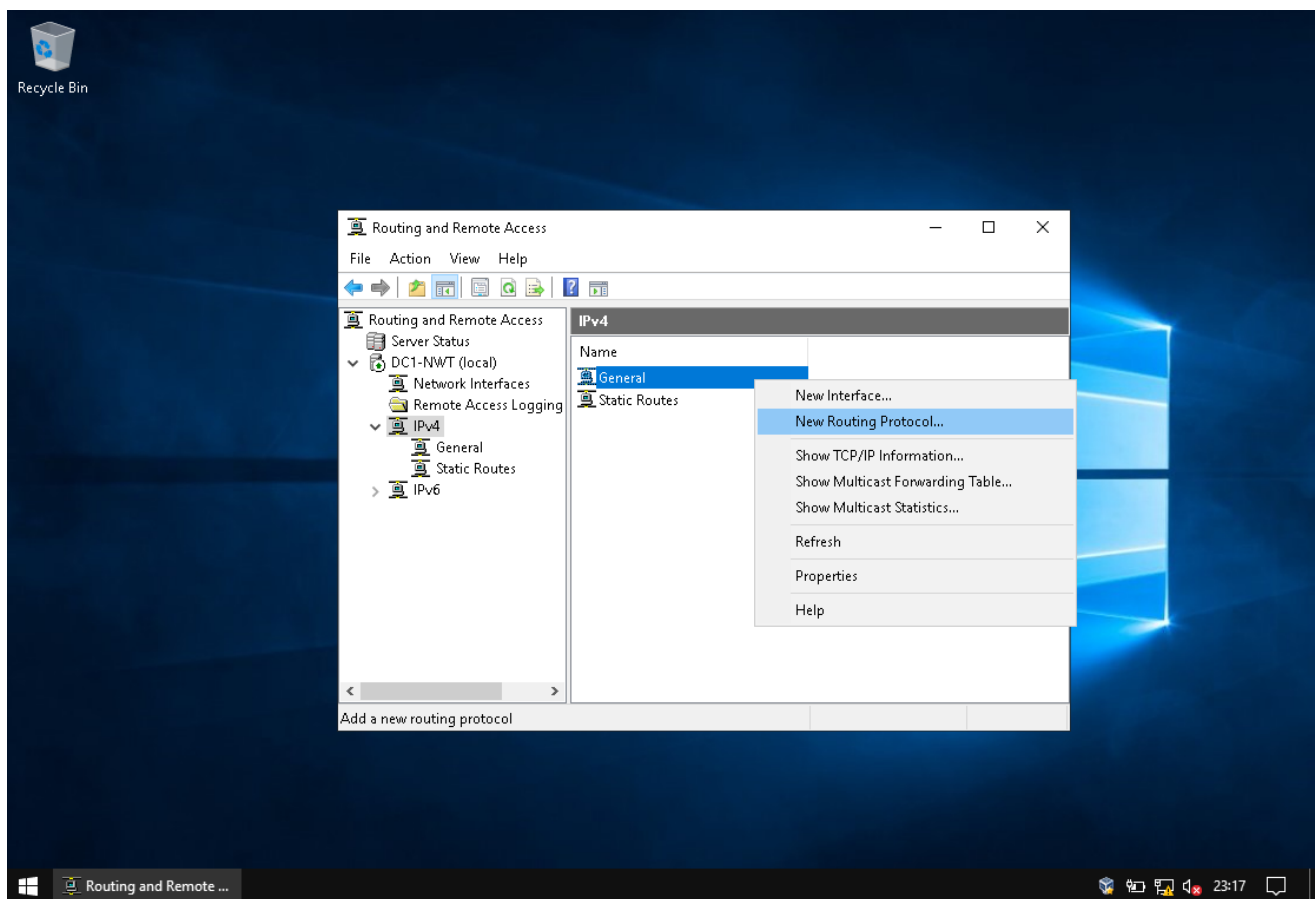
The 'Custom configuration' option is selected.



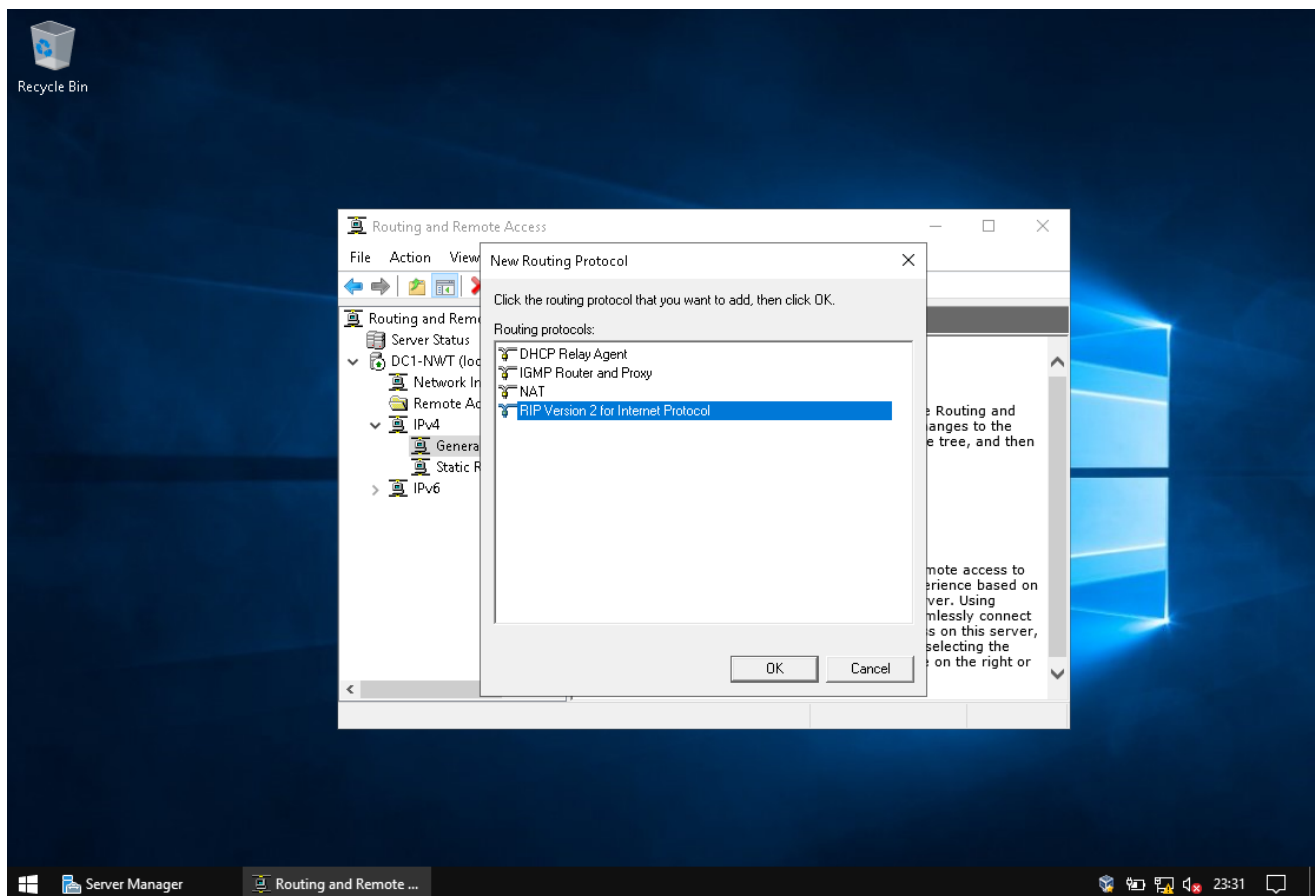
'LAN routing' is checked.



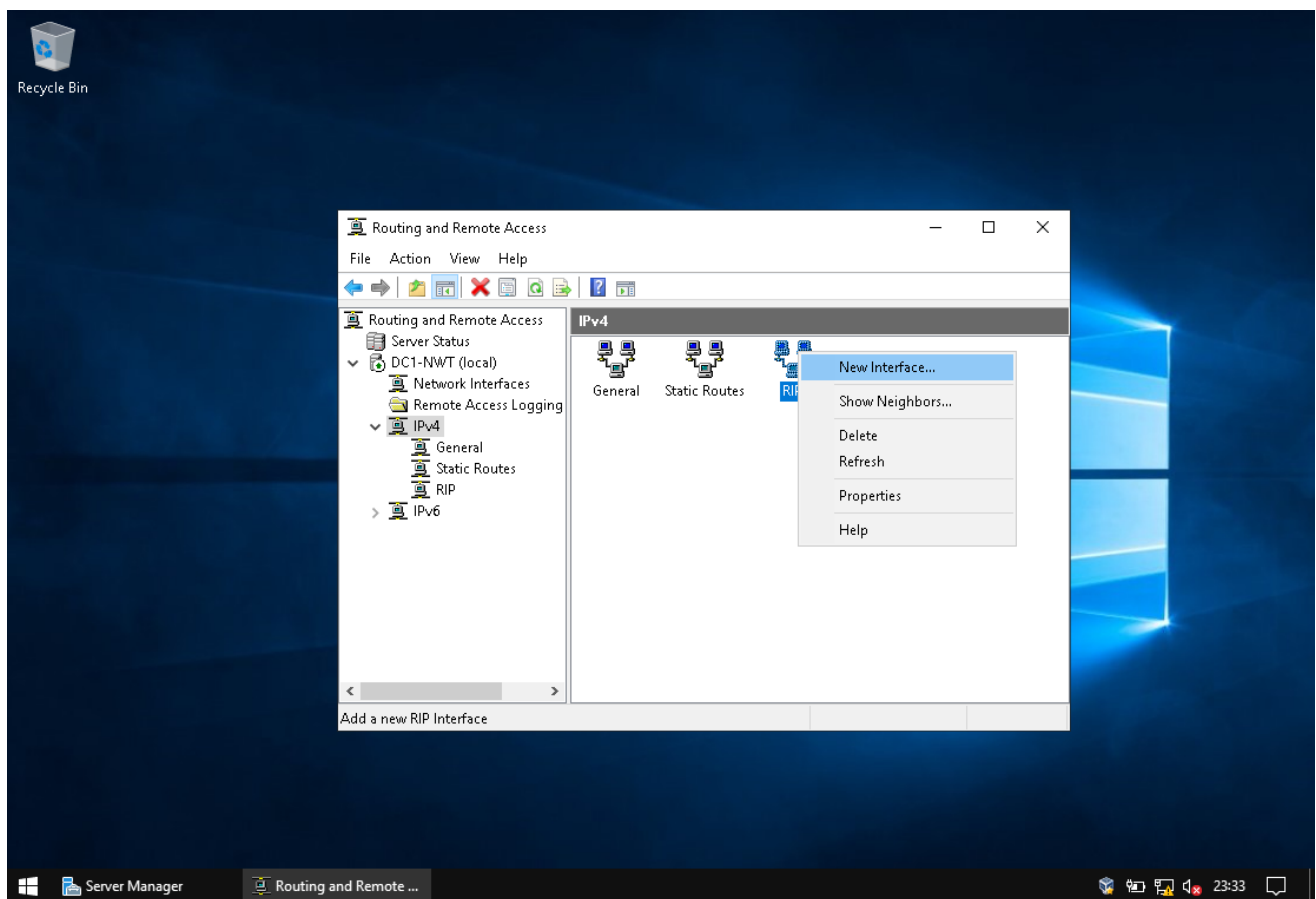
The service has started (indicated by the green up arrow on the server name)



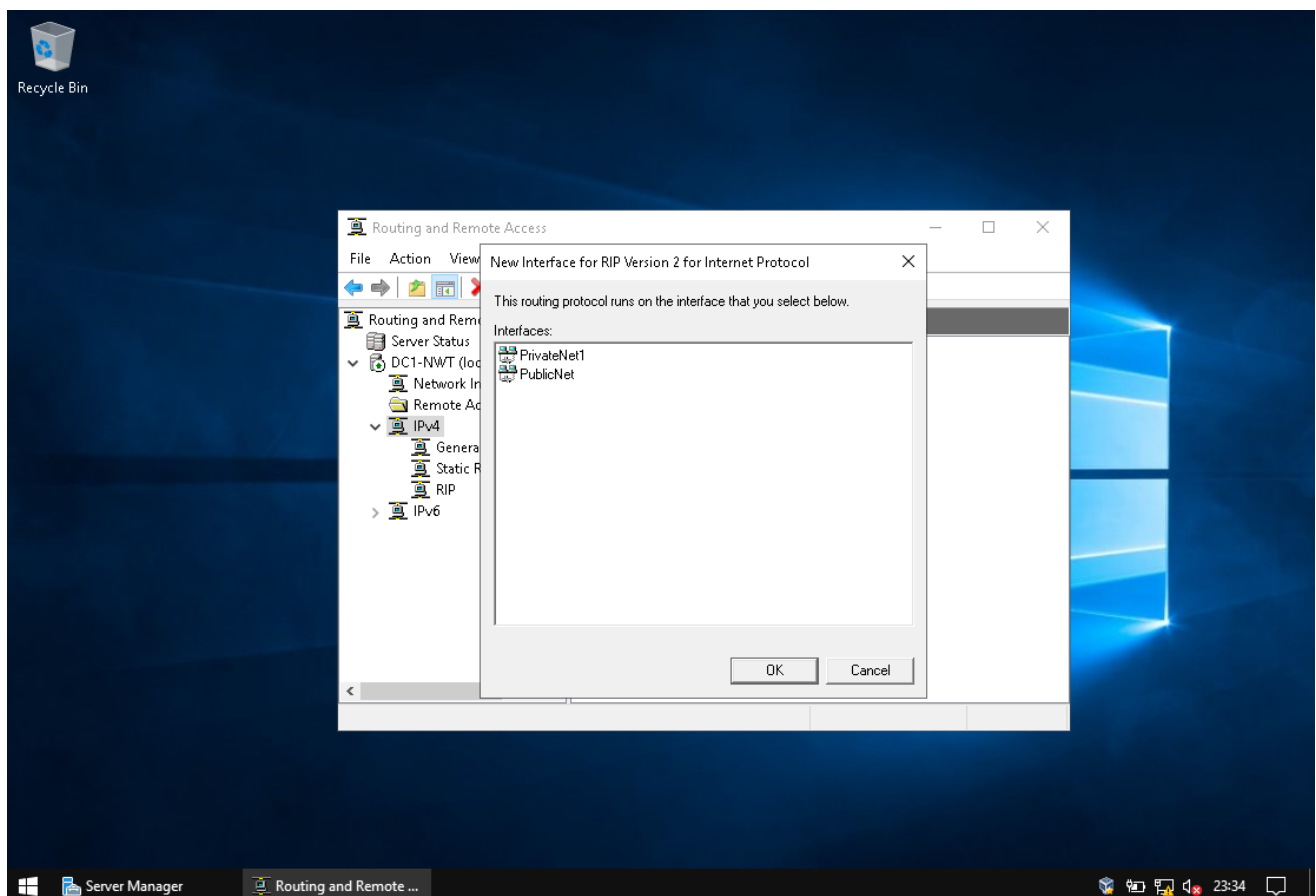
A new Routing Protocol will be created under IPv4 > General.



'RIP Version 2 for IP' is selected as instructed by the brief.

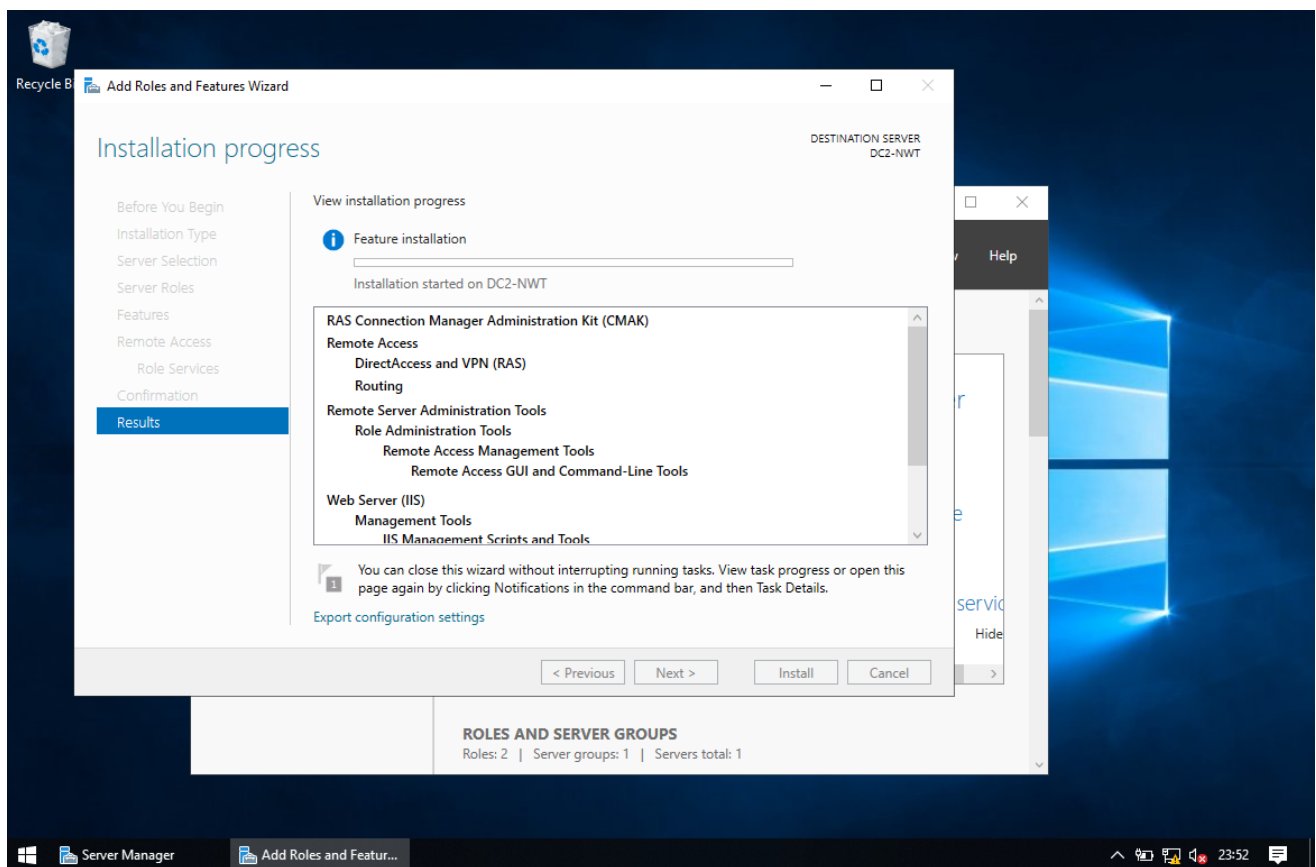


The RIP object is right clicked, and the 'New Interface...' option on the context menu that appears is selected.

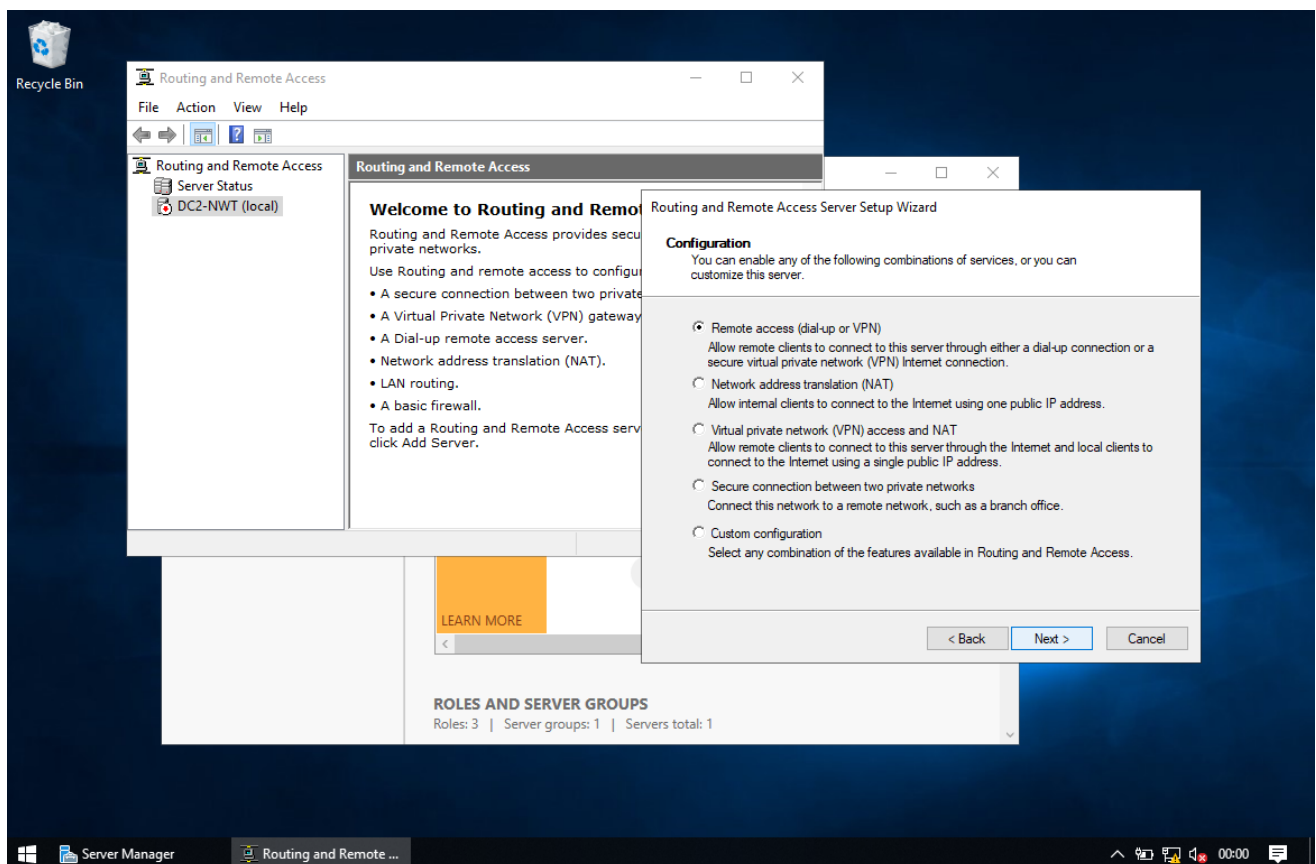


The two interfaces are listed successfully.

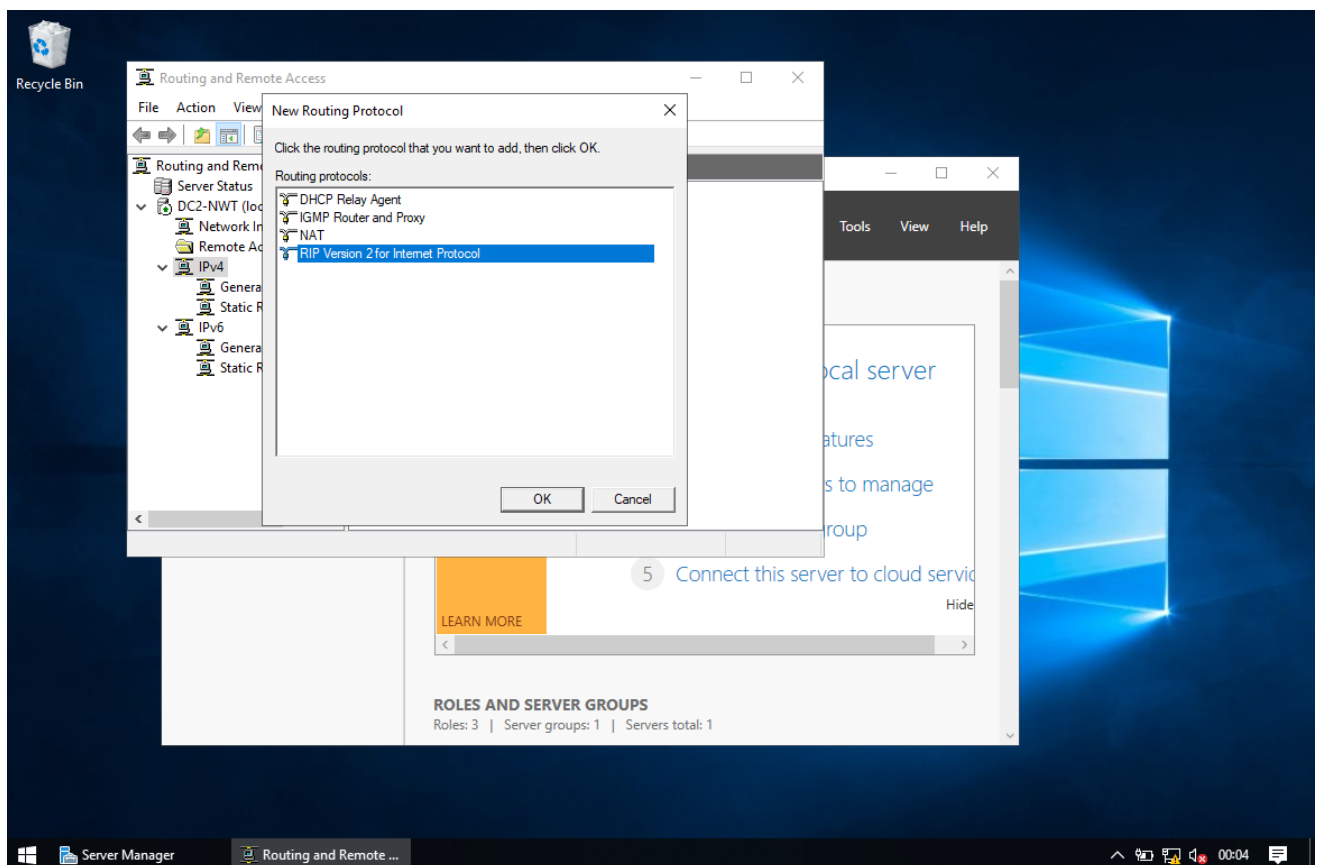
// On Server 2 //



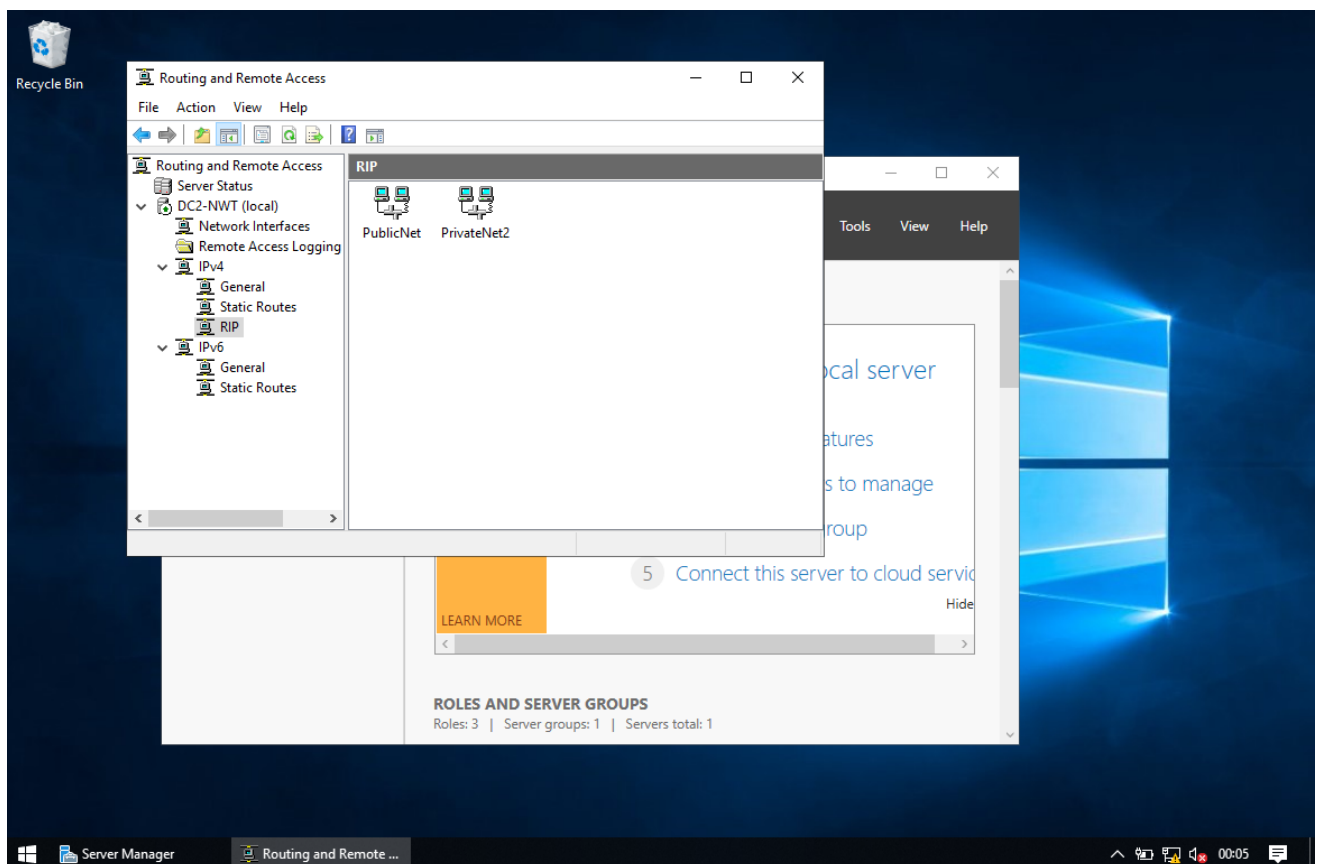
The Remote Access toolkit was installed successfully.



The DC2-NWT was enabled as a Remote Access Service as instructed by the brief (with a custom configuration, configured the same way as Server 1).

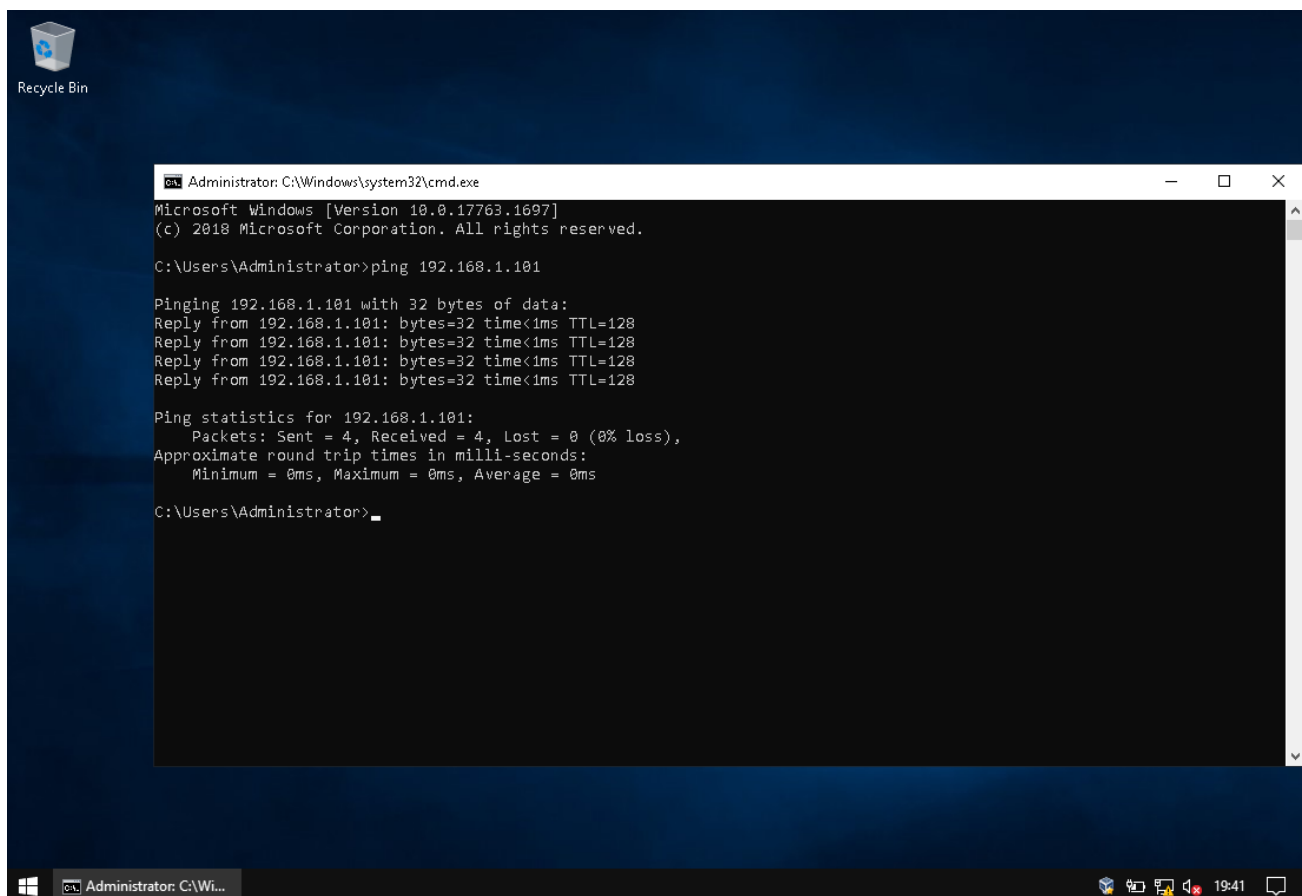


RIP Version 2 for Internet Protocol was selected as a new Routing Protocol.



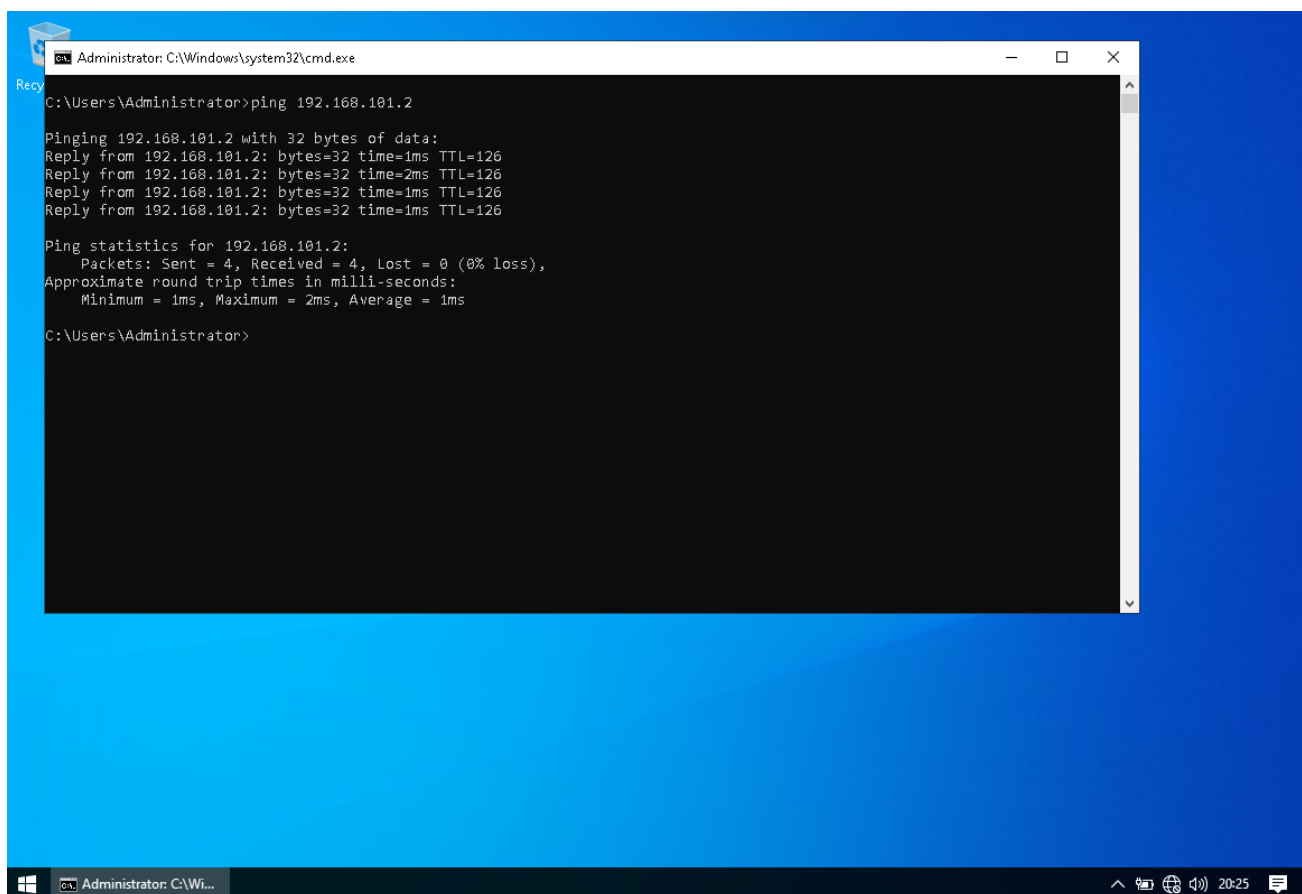
Both interfaces were added to the RIP stack.

// On Server 1 //



A successful connection was established when attempting to ping Server 2 from Server 1.

// On Client 1 //

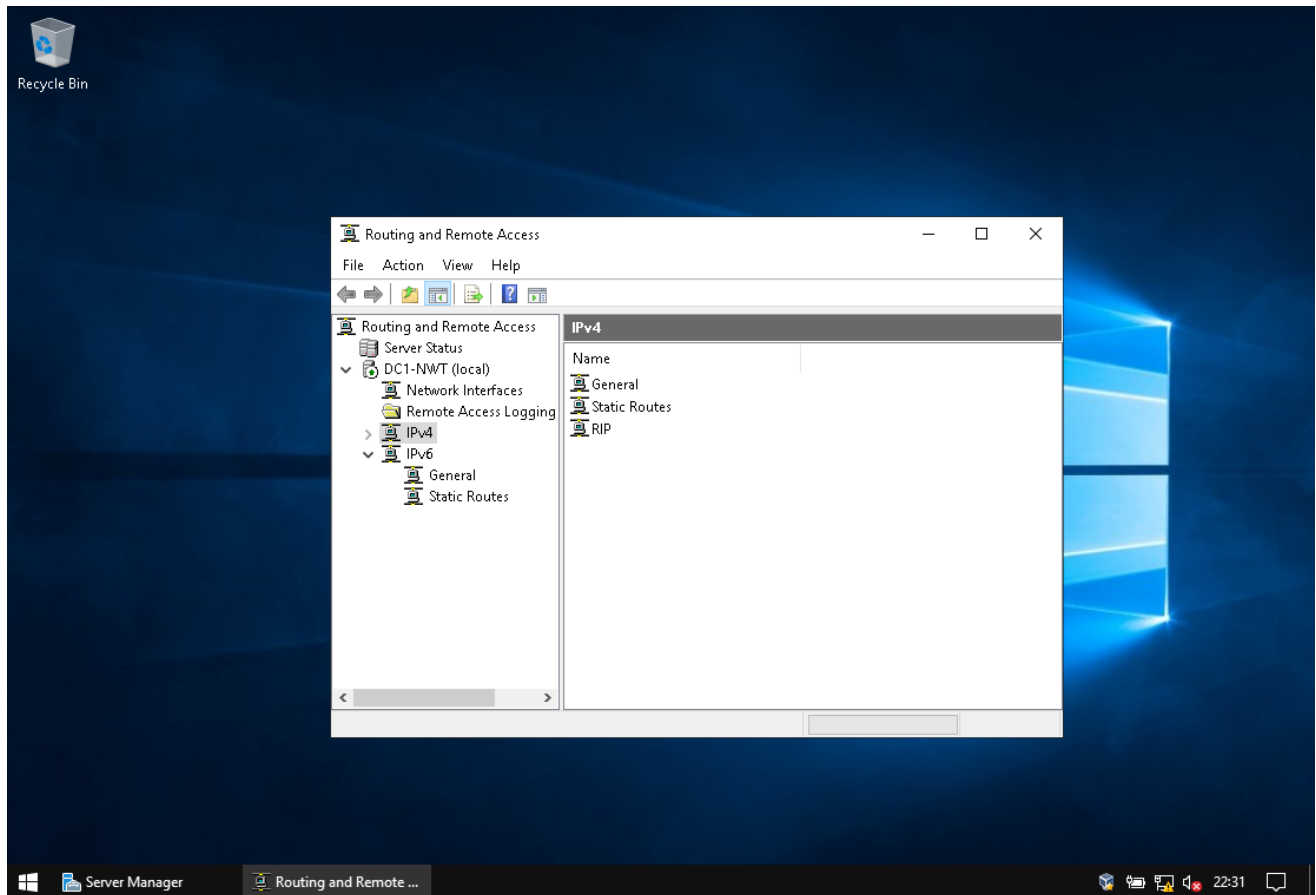


A successful Ping from Client 1 to Client 2 was established.

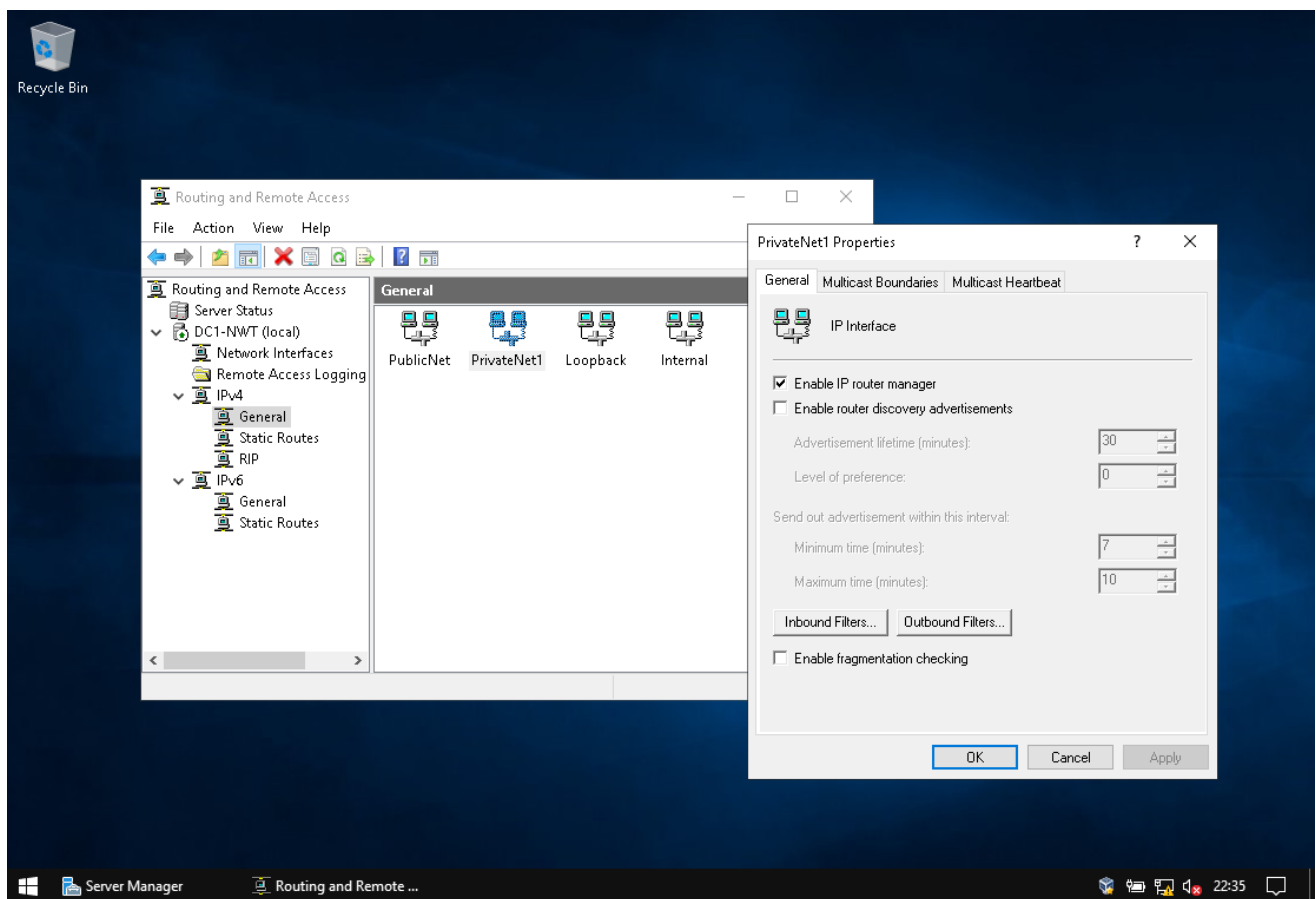
Observation: How Routers reference which networks they are able to connect to

Task 4: IP Packet Filtering

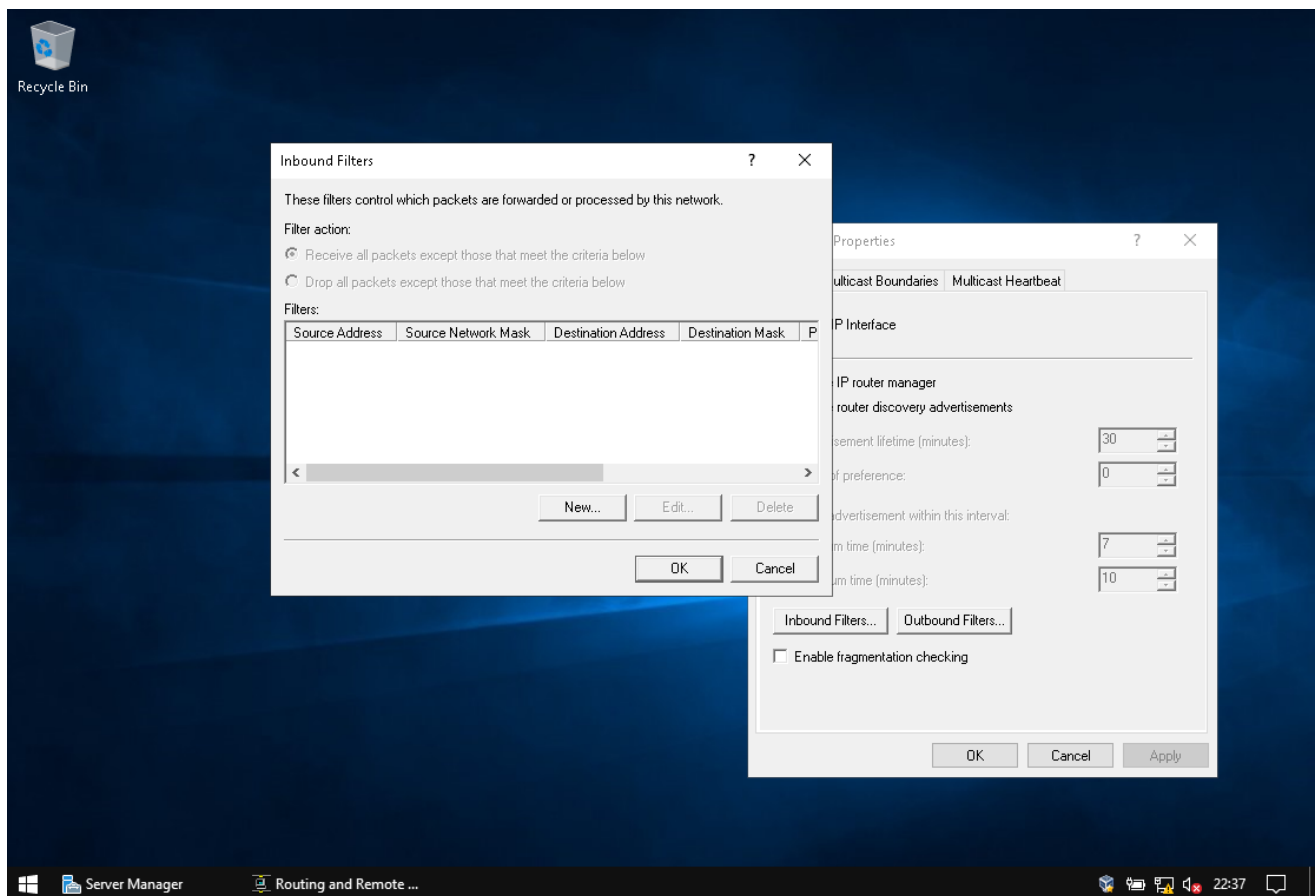
Filter 1



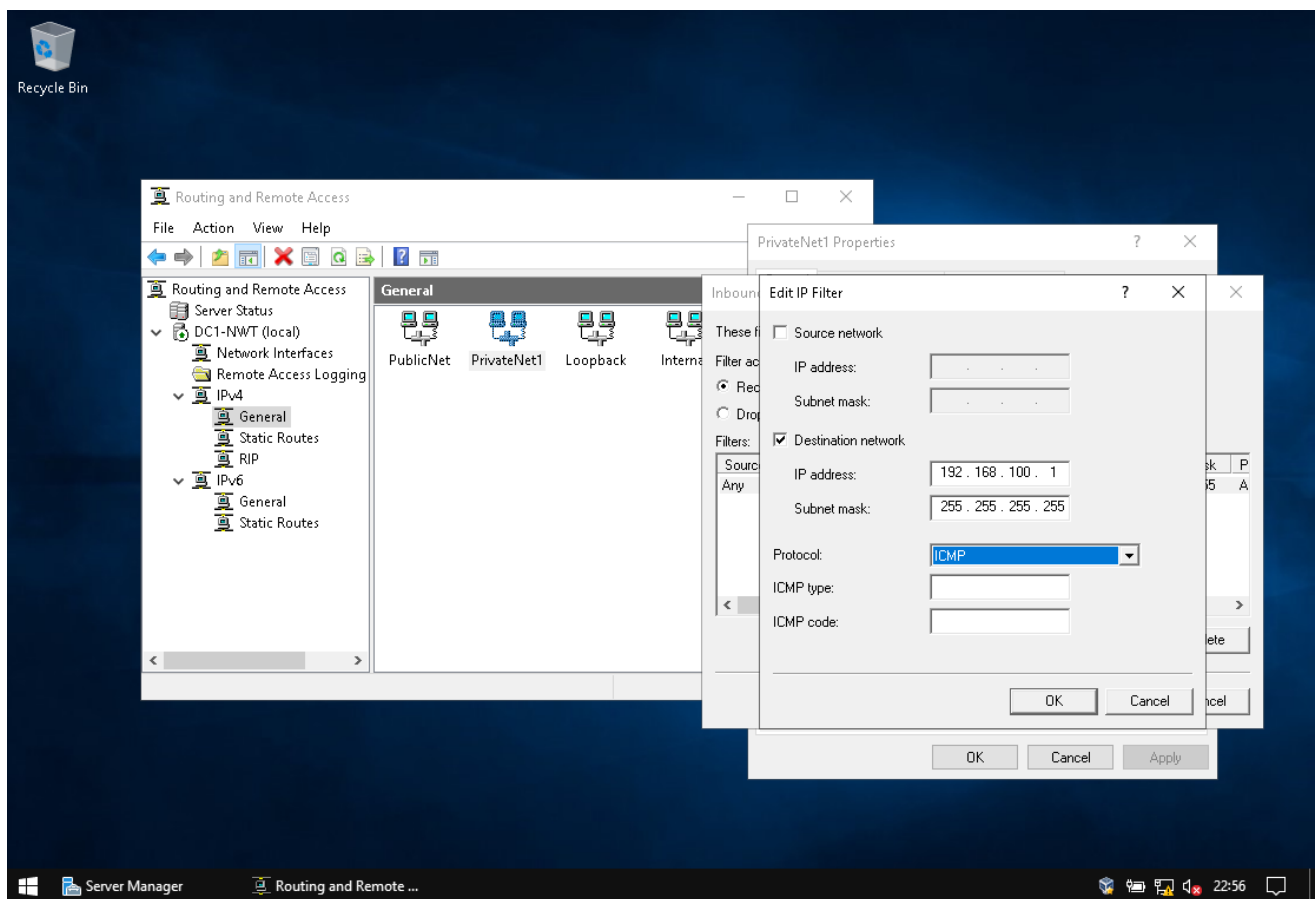
The 'Routing and Remote Access' control panel was opened on Server 1.



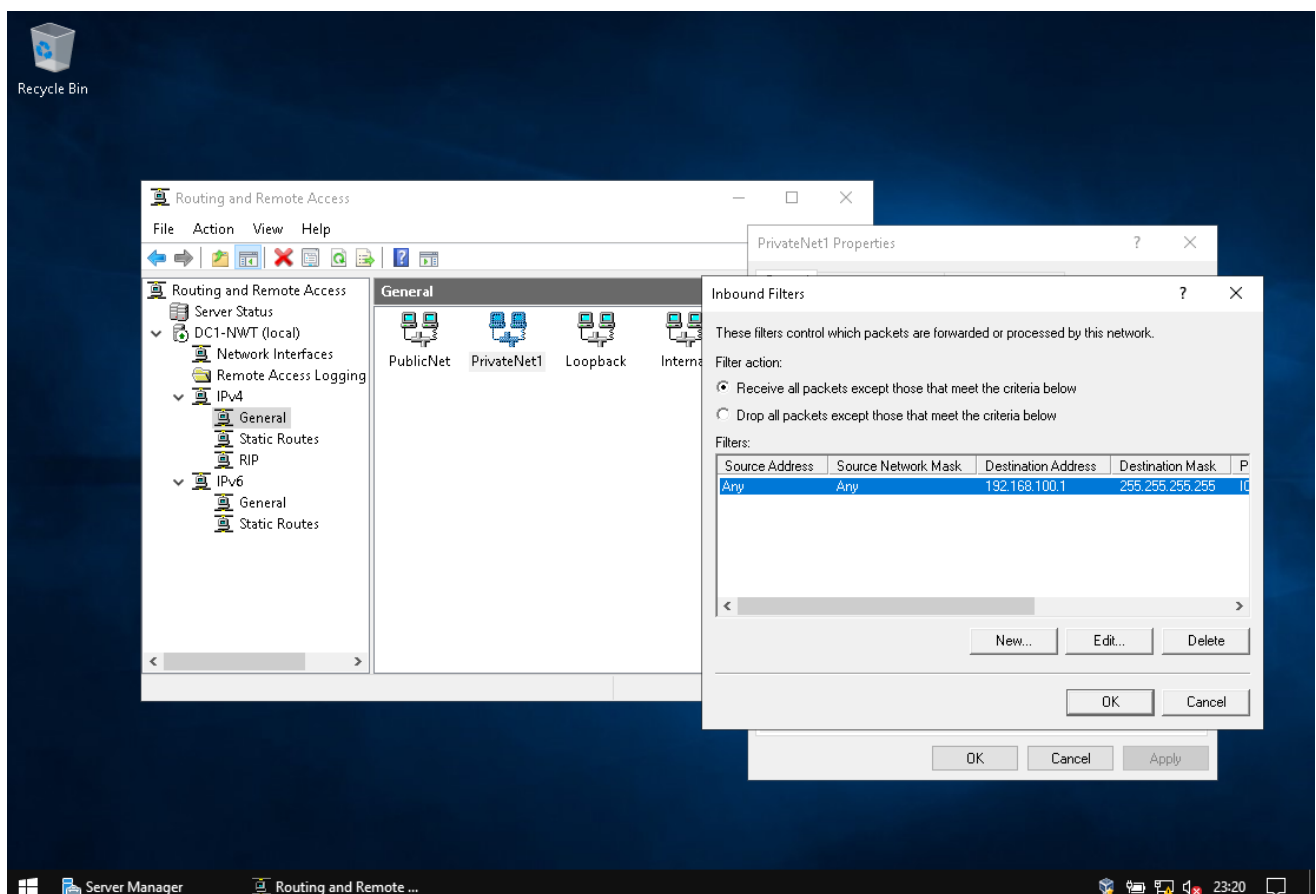
PrivateNet1's property window was opened.



The inbound filter was opened.

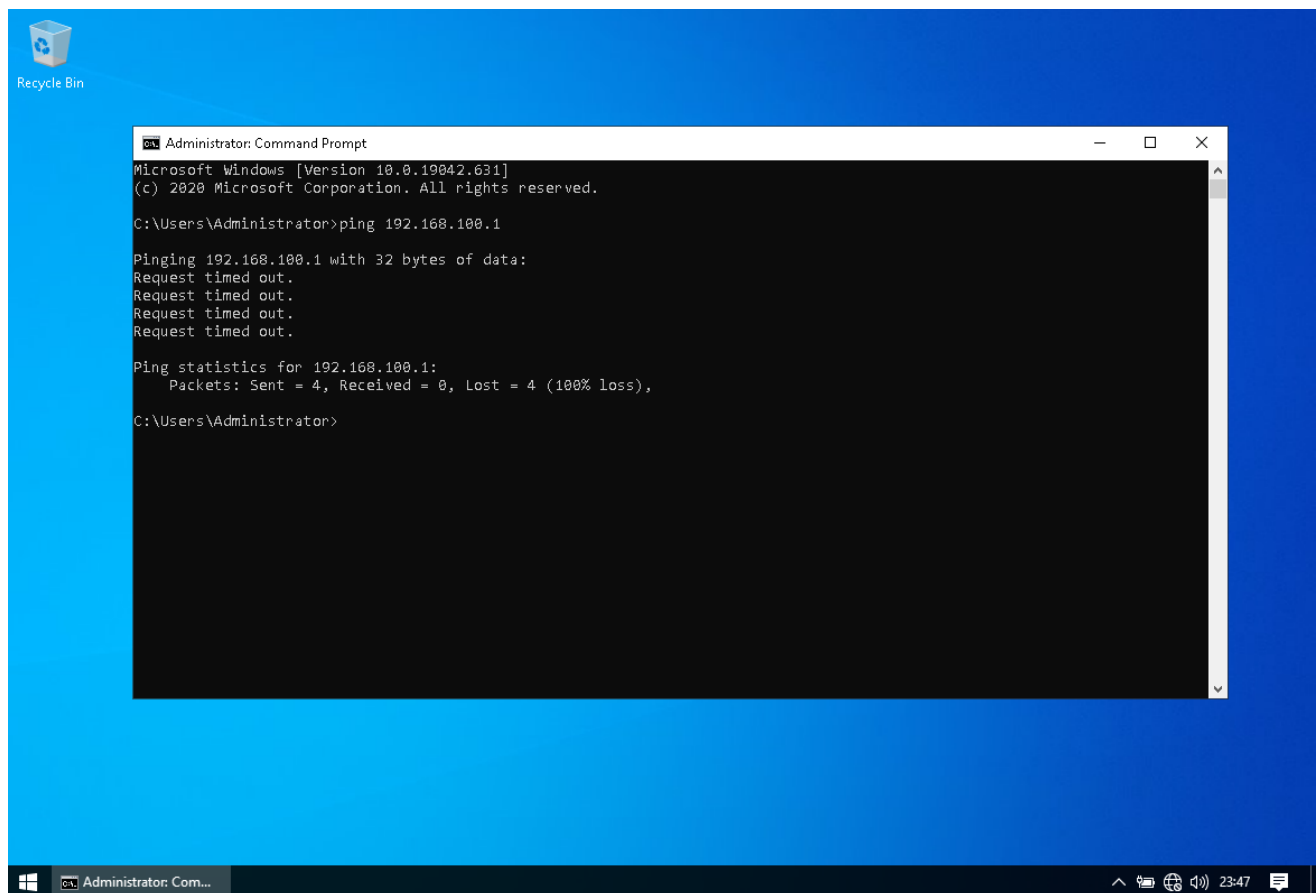


A new inbound IP filter was added, set as a destination network, with the IP address 192.168.100.1 as directed by the brief. The subnet mask was set to 255.255.255.255 and the protocol was set to 'ICMP'.

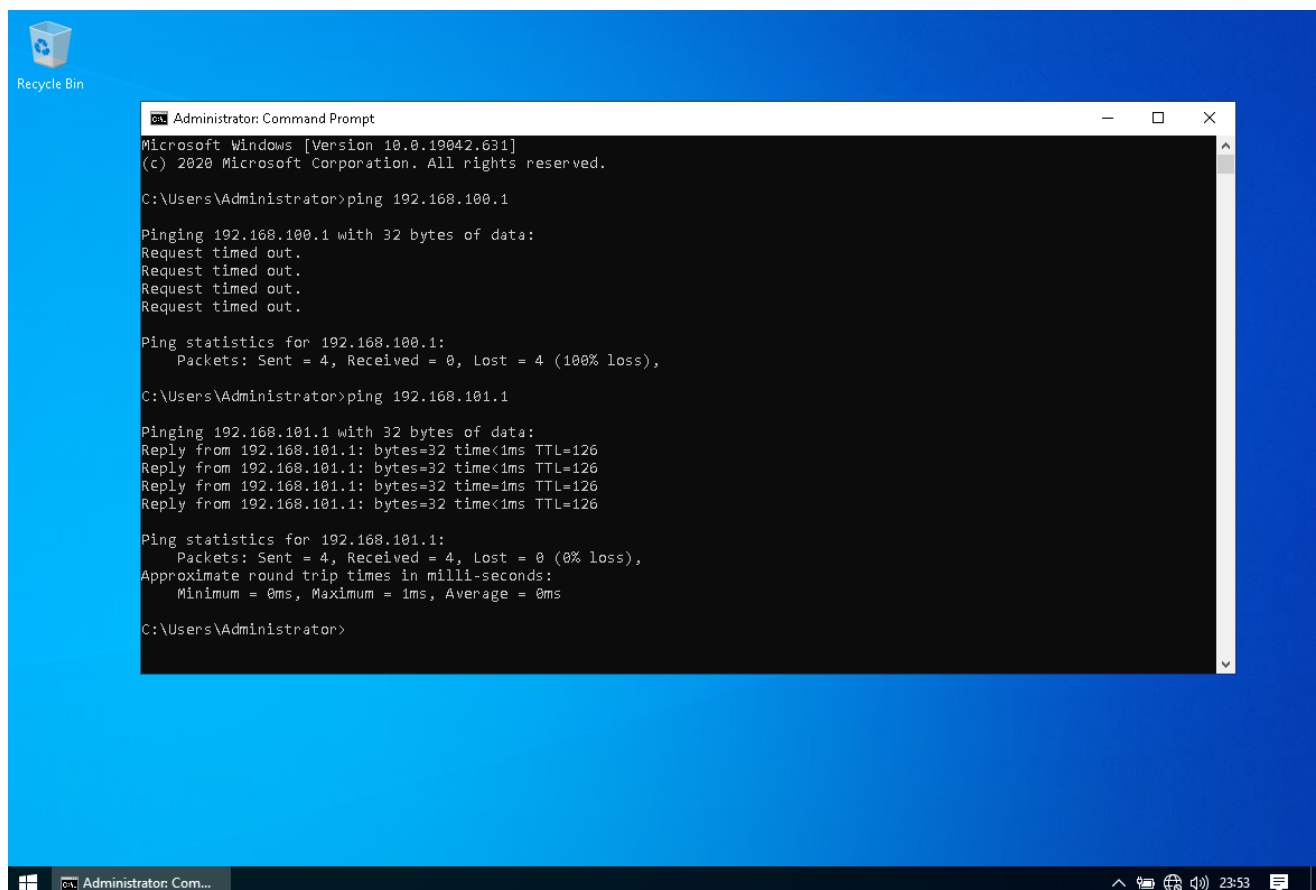


'Receive all packets except those that meet the criteria below' was checked by default.

// On Client 1 //

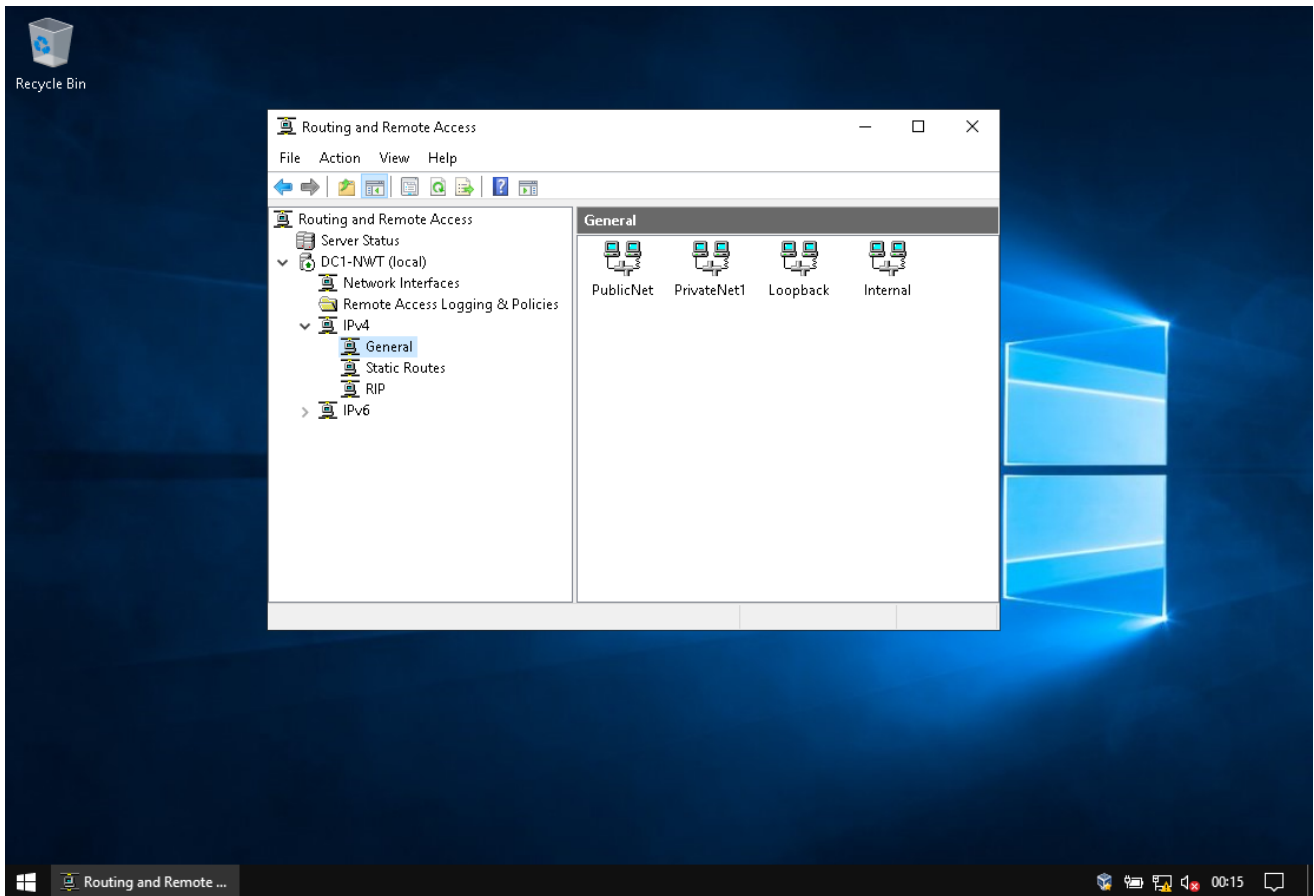


The request timed out, as expected, as the router is denying our ping access.

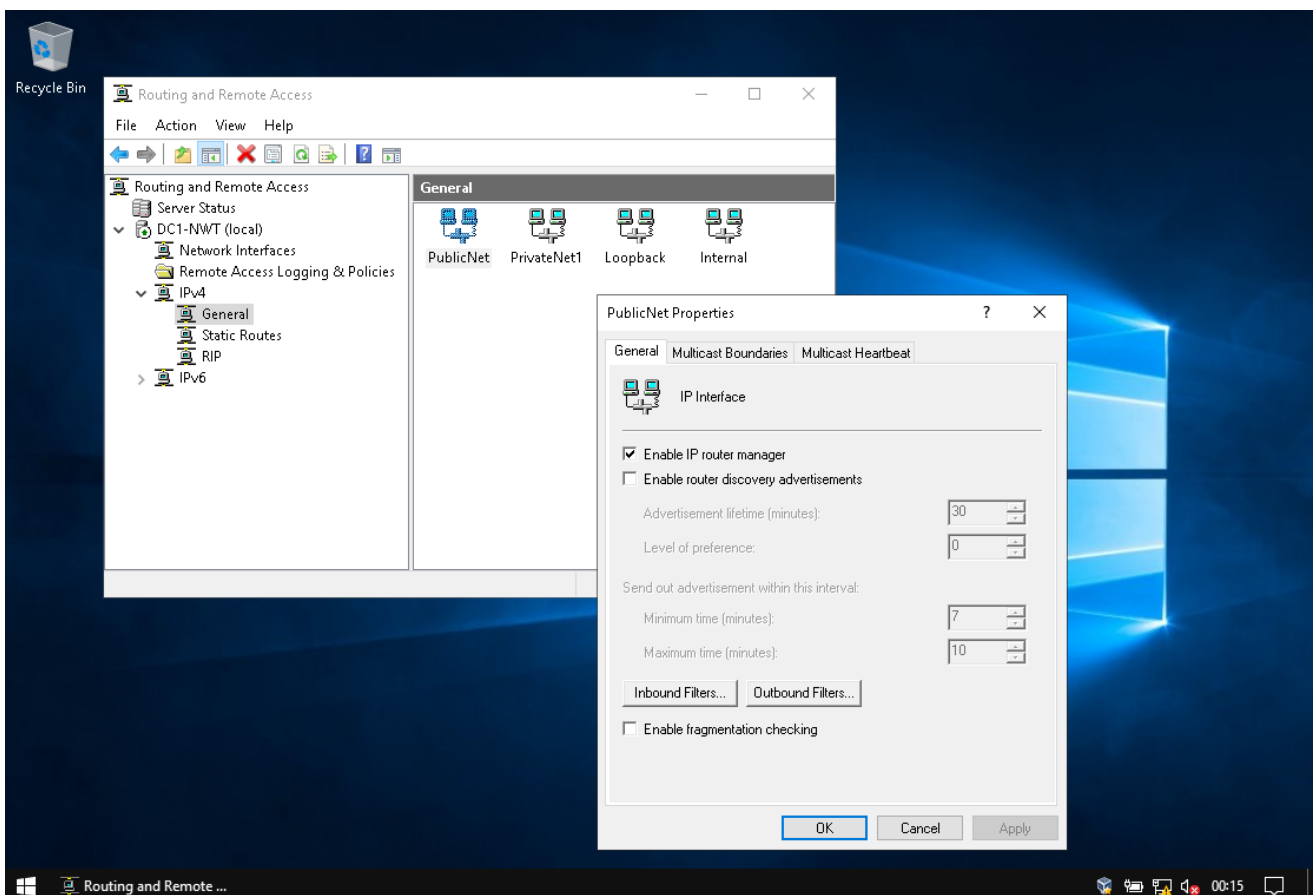


Pinging another host (this time Client 2) is successful. Which showcases the connection is denying the ping access to Server 1 exclusively.

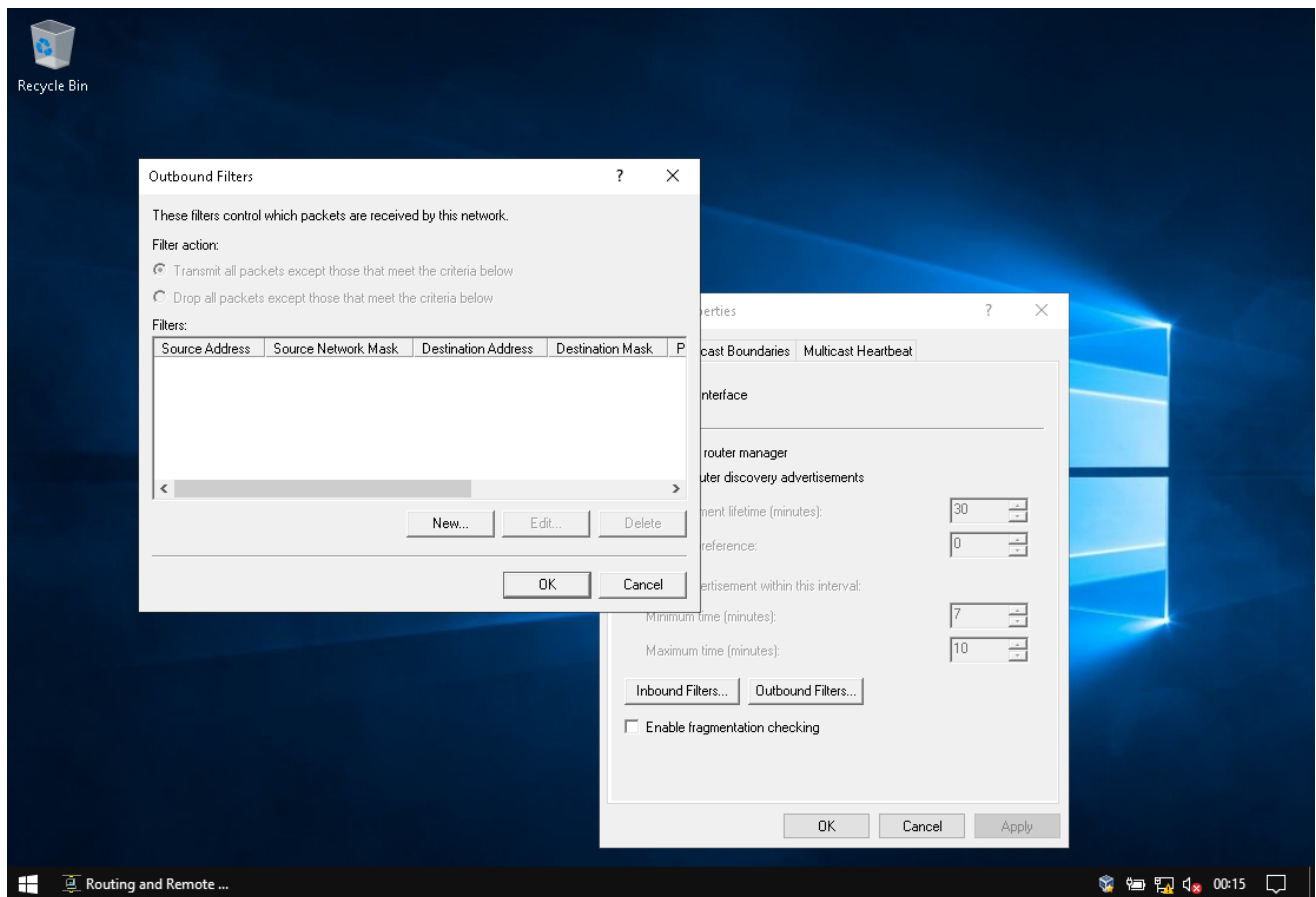
Filter 2



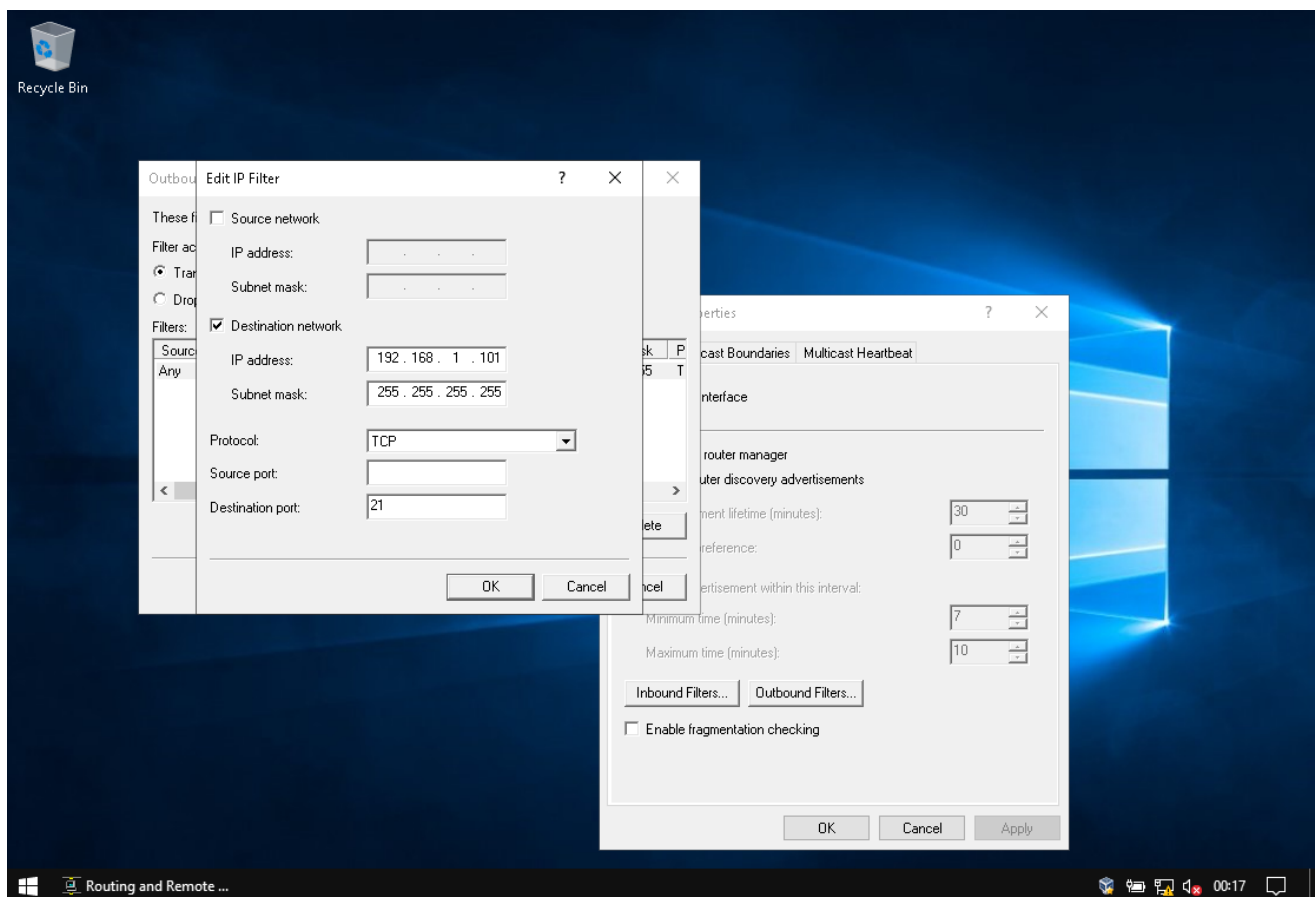
The 'Routing and Remote access' control panel is opened.



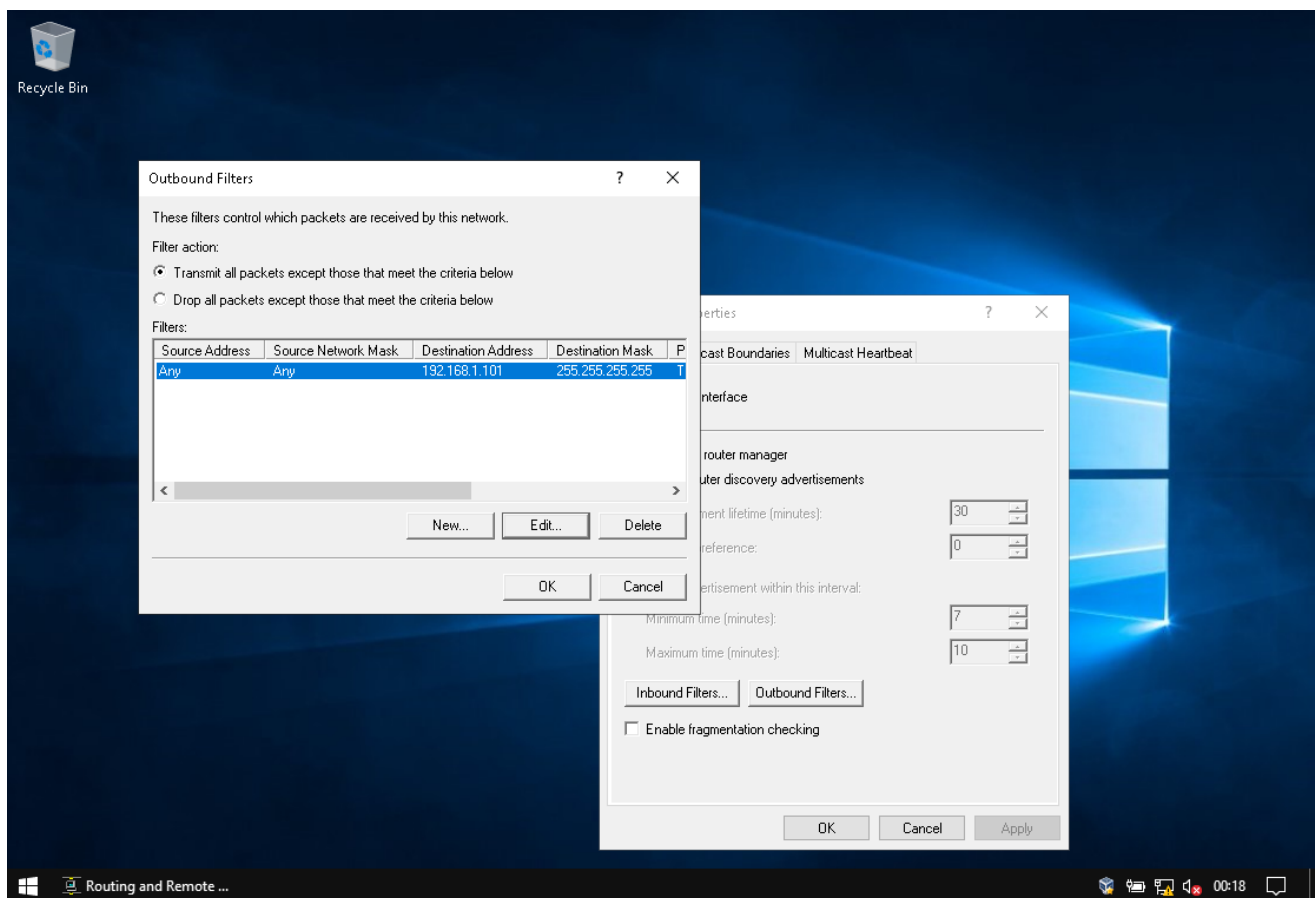
The properties window for 'PublicNet' is opened.



The 'Outbound Filters' control panel is opened.

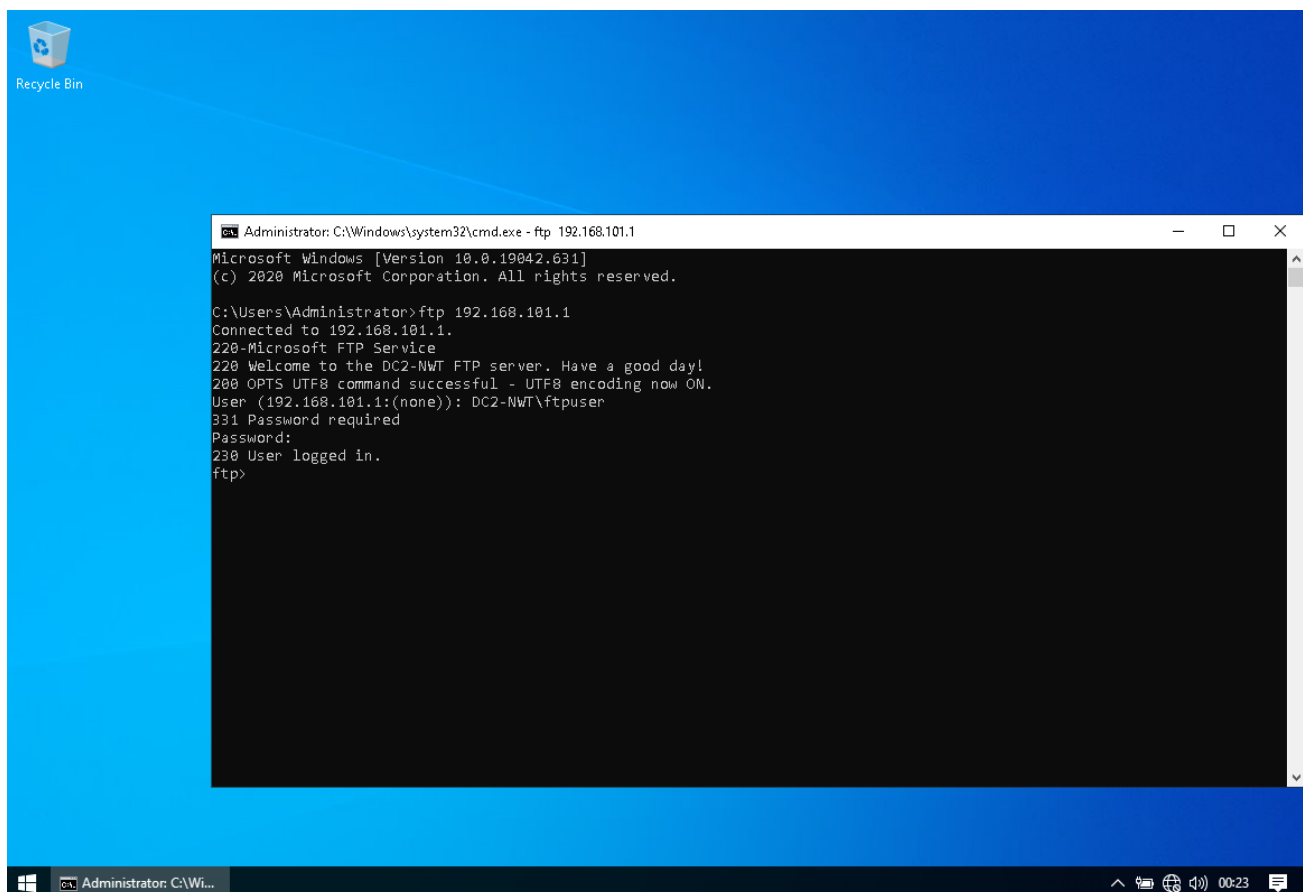


A new destination network with an IP address of **192.168.1.101** is added with a subnet mask of **255.255.255.255** with the TCP protocol and a destination port of 21. As instructed by the brief.



'Transmit all packets except those that meet the criteria below' is checked automatically by default.

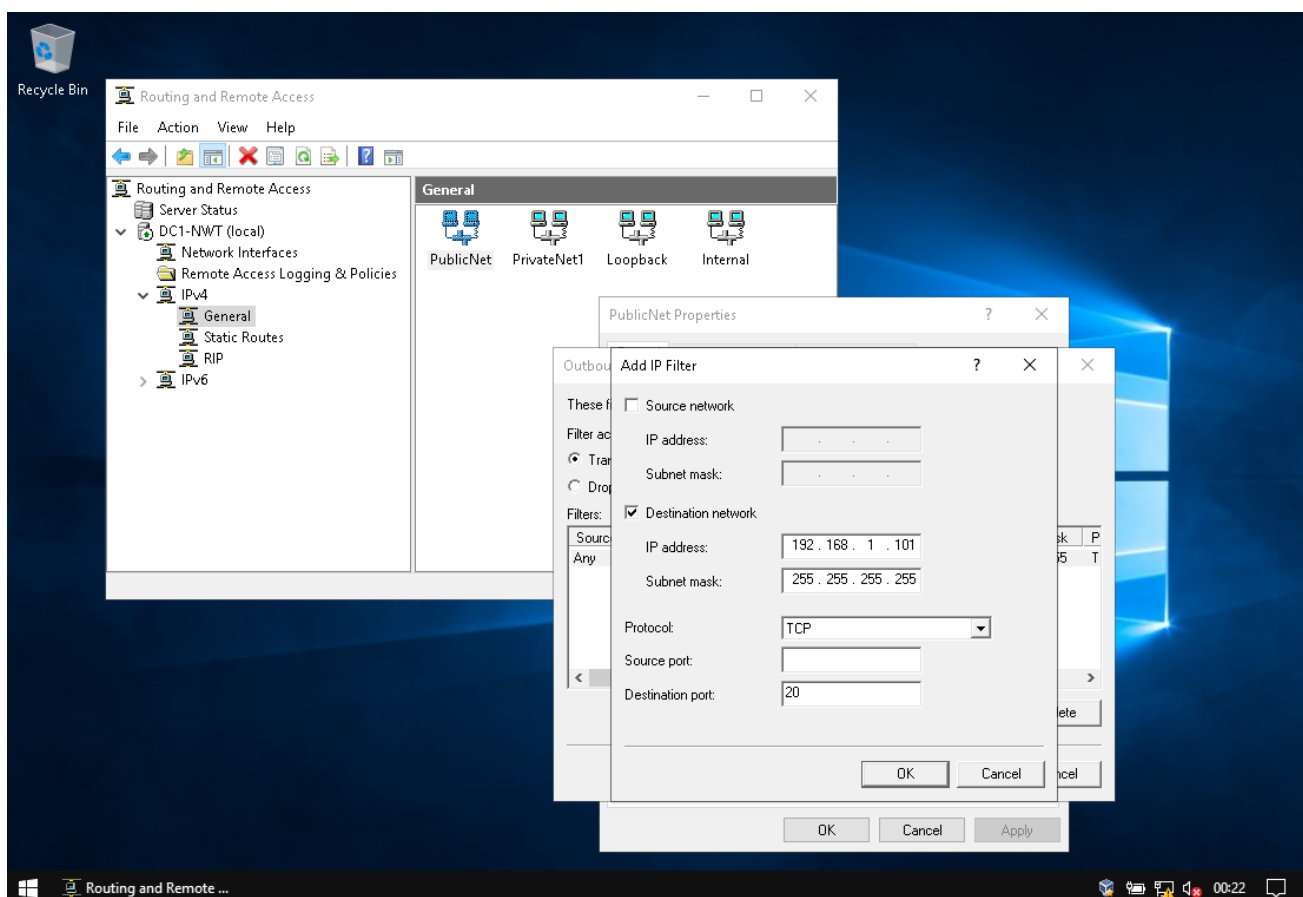
// On Client 1 //



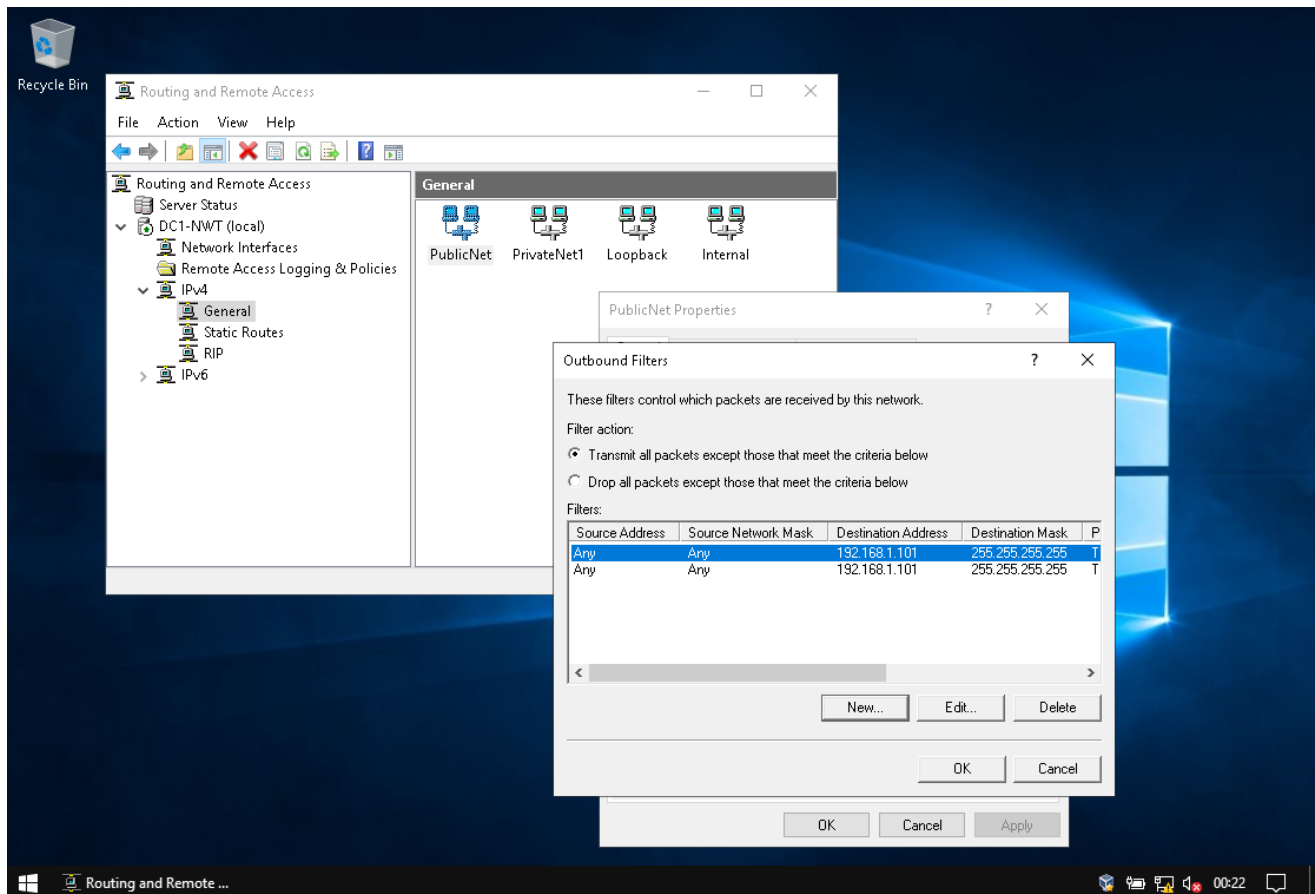
Unfortunately, Client 1 was able to access the FTP server using the FTP command.

// On Server 1 //

2nd attempt: To add a new outbound filter using port 20, as FTP can run on 2 bounding ports.

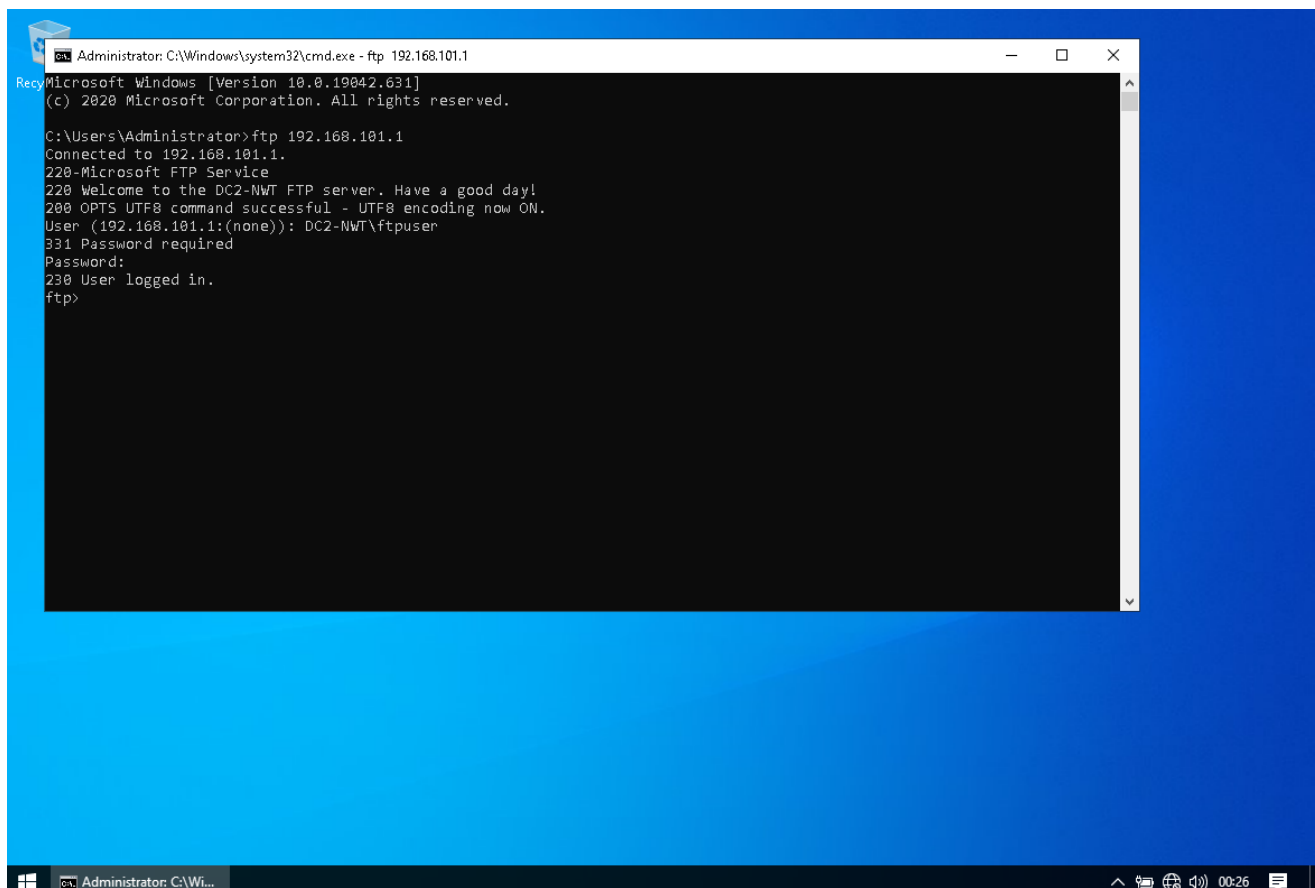


A new filter was added, using port 20 as opposed to port 21. The other filter isn't removed.



Outbound filters now contain two filters, one for port 21, and the other for port 20.

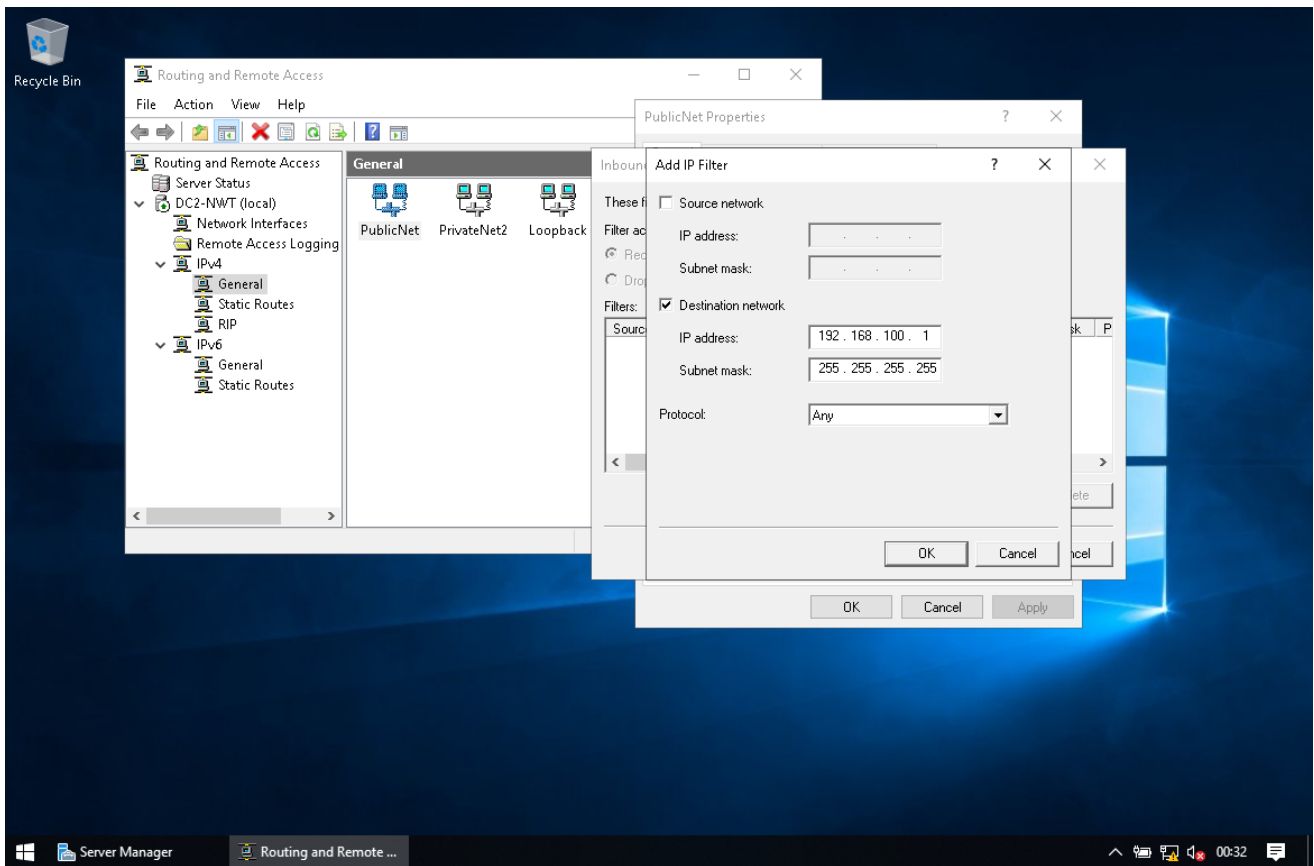
// On Client 1 //



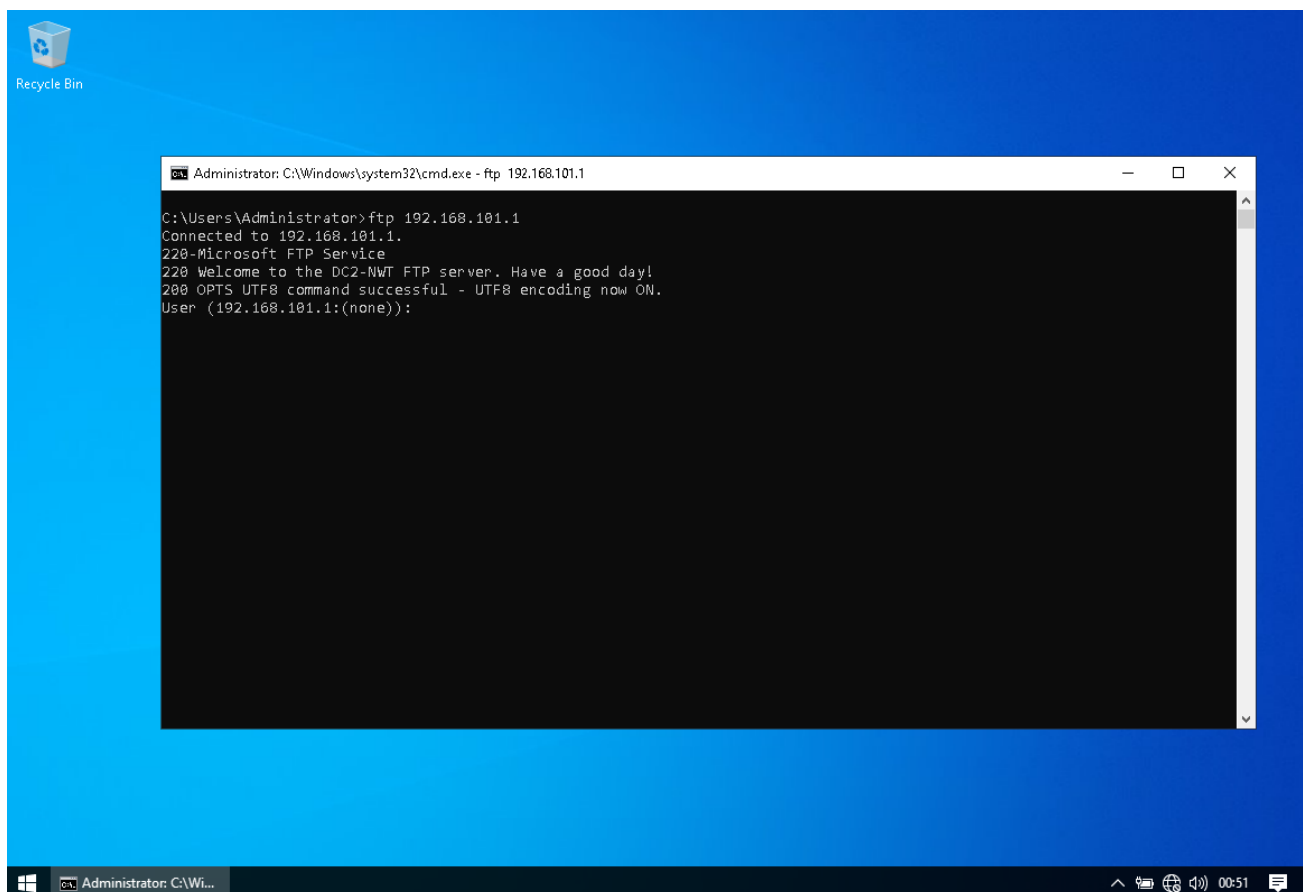
Despite the new filter, a connection was still established to the FTP server.

3rd attempt: Add an inbound filter to the server where the FTP server itself is hosted instead.

// On Server 2 //

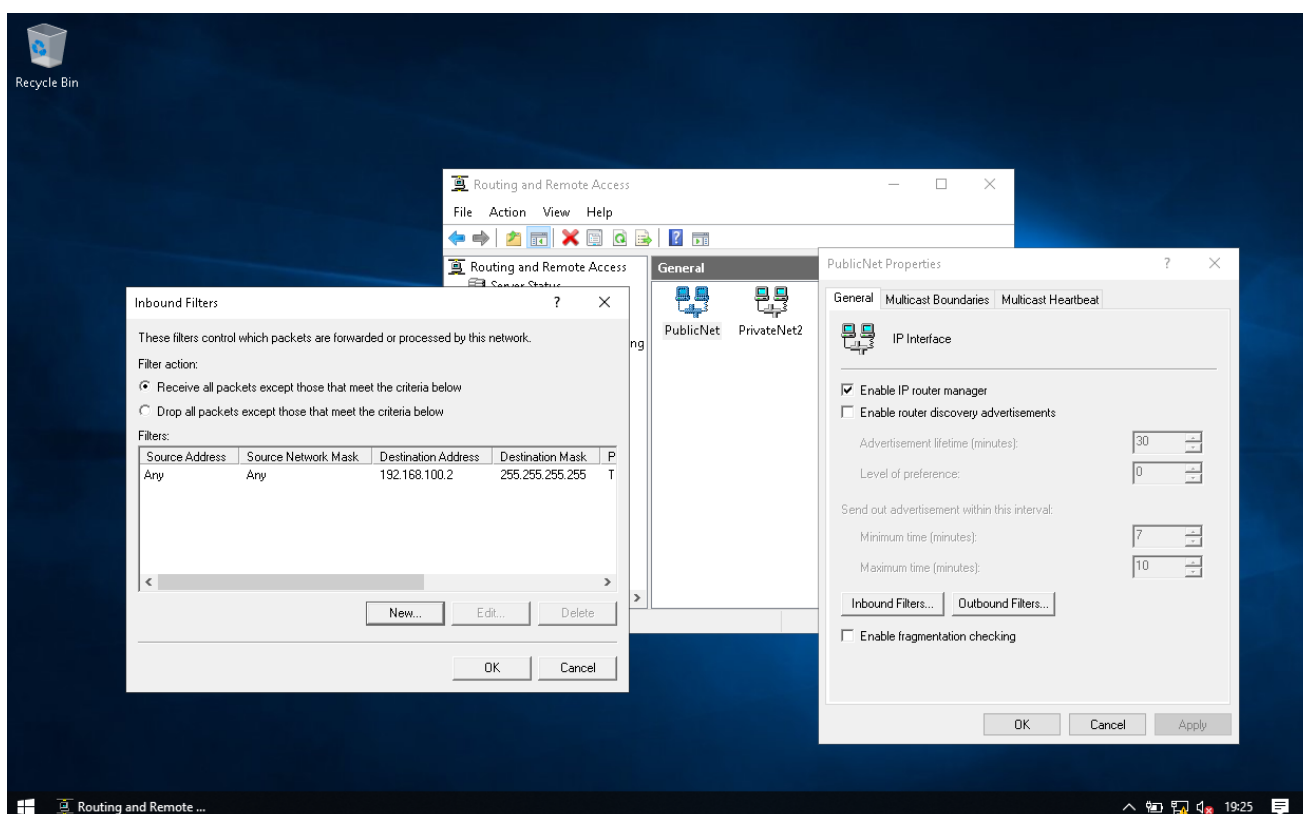


Adding the literal IP address of the PrivateNet1 interface to the inbound filters on Server 2 **should** prevent access to the FTP server on Server 2.



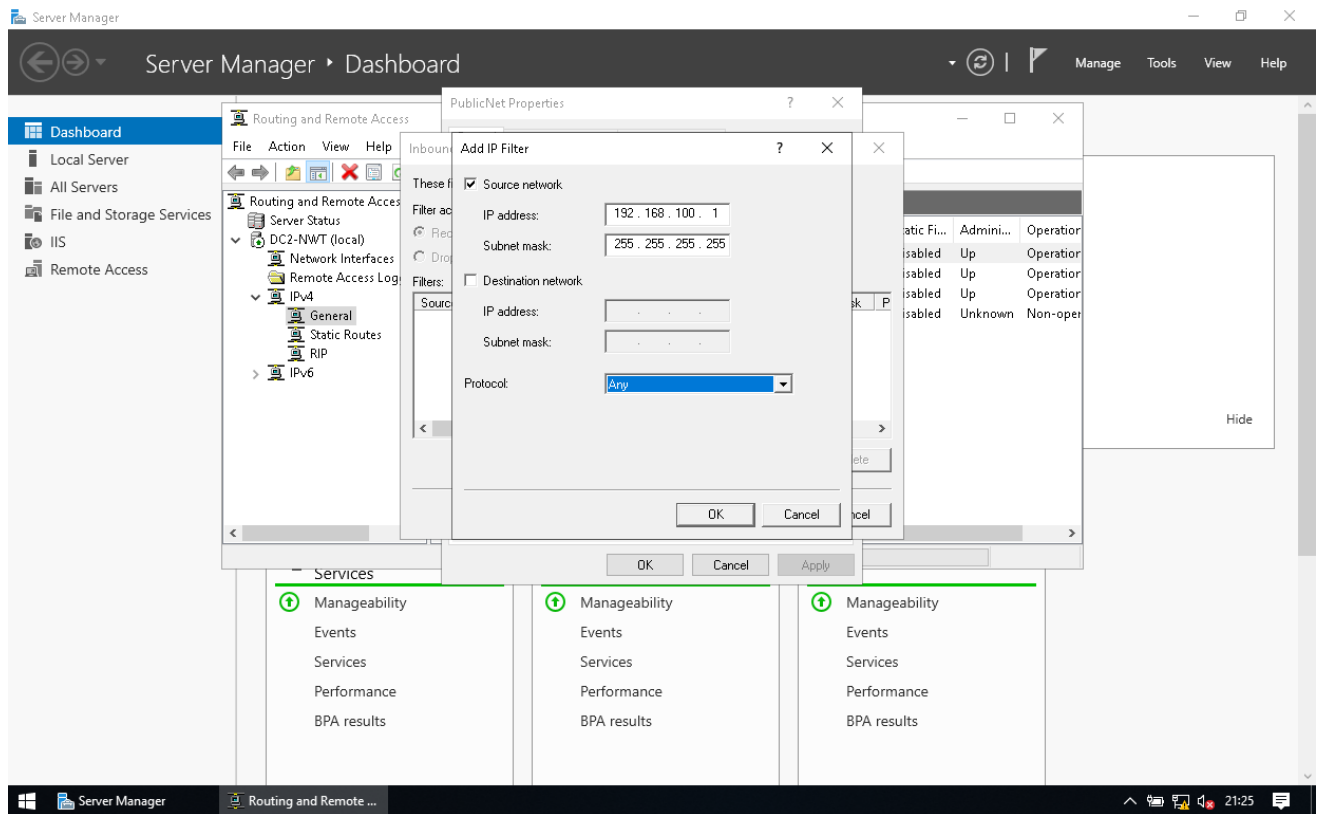
Despite adding 192.168.100.1 & 192.168.100.2 to the inbound filter list, with both the protocol set as 'any' and 'TCP' and the port set as both 21 and 20 for both of them, the ability to restrict Client 1 from connecting to Server 2 was unsuccessful; and the author is uncertain as to why.

Filter 3



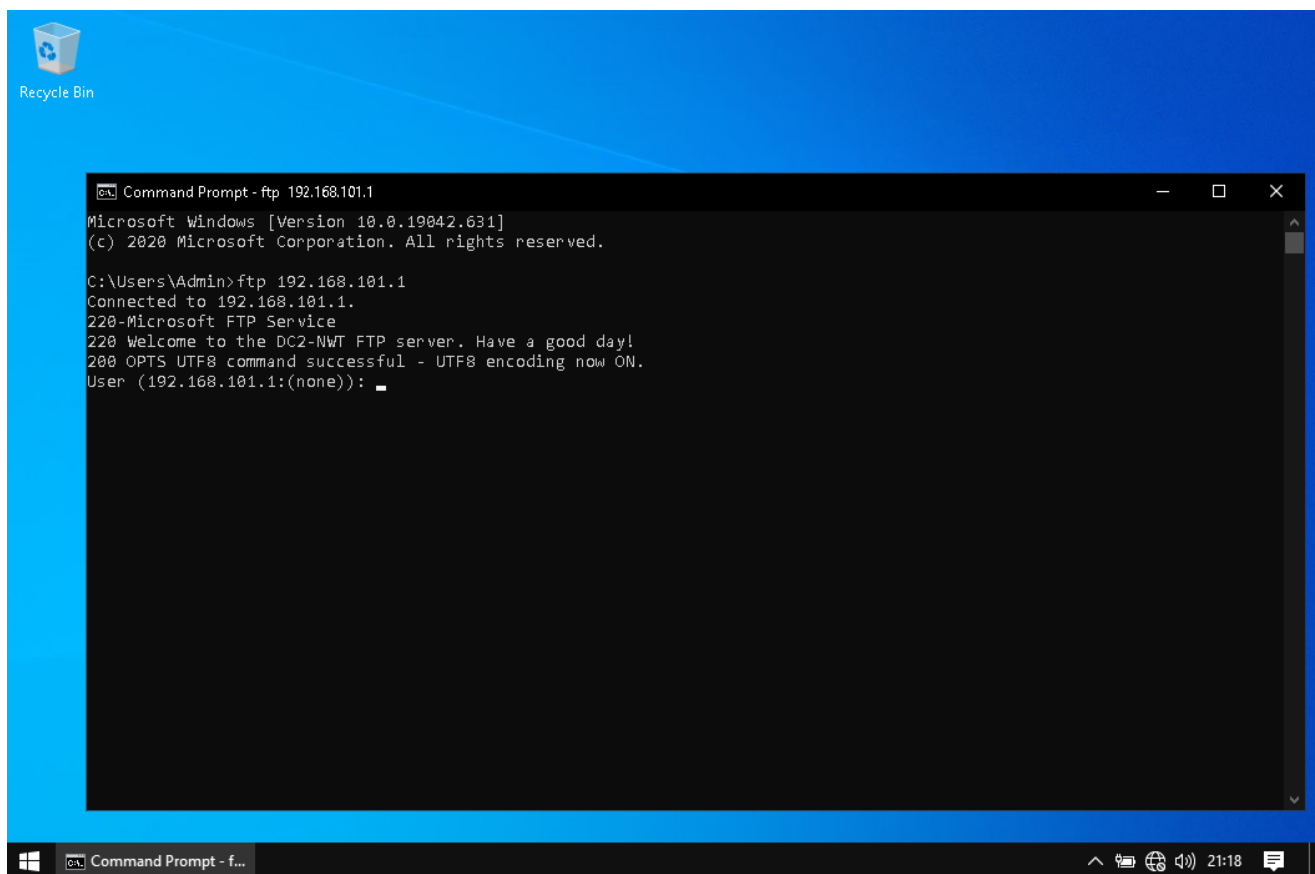
// On Server 1 //

These are the inbound packets currently set on server 1, the filter itself is currently set to 'Receive all packets except those that meet the criteria below'. As we cant to restrict all traffic to any device except for Client 1, we switch the toggle to 'Drop all packets except those that meet the criteria below' and add Client 1 as a source address.



The **source** network is set to Client 1. Client 1's IP address according to the brief is 192.168.100.1

// On Client 1 //

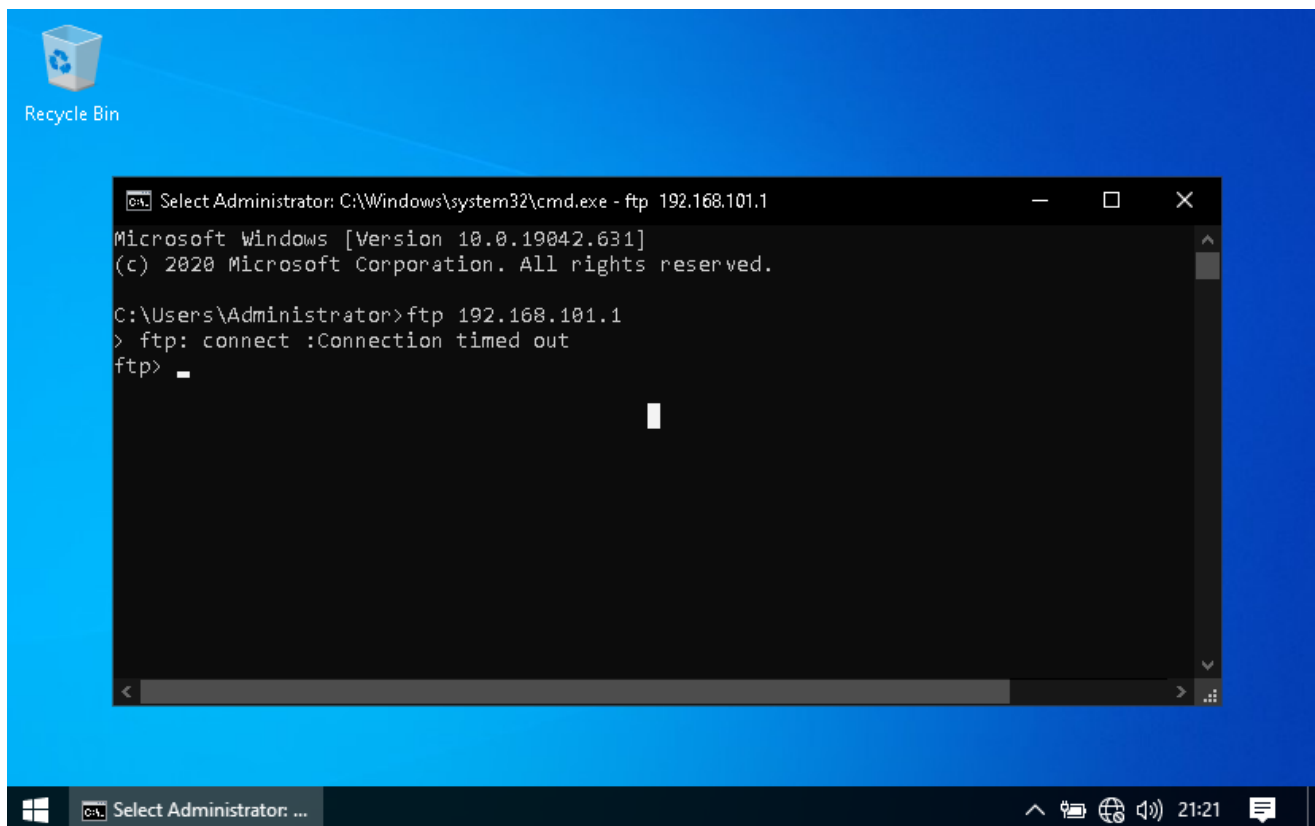


```
Command Prompt - ftp 192.168.101.1
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ftp 192.168.101.1
Connected to 192.168.101.1.
220-Microsoft FTP Service
220 Welcome to the DC2-NWT FTP server. Have a good day!
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.101.1:(none)): 
```

Client 1 was able to connect using FTP to 192.168.101.1 successfully.

// On Client 2 //



```
Select Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.101.1
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 192.168.101.1
> ftp: connect :Connection timed out
ftp> 
```

Client 2 was unable to connect, instead sending a 'connection timed out' response.

Packets have 2 major elements on their header: a source IP and a destination IP that can be read like an address on an envelope. A filter reads the header of the packet and filters connections based on the header, a lot like a firewall. The configuration we're using is set to deny access to any connection that doesn't have its source IP address set to Client 1.

An issue with rule sets like these is that packets can be edited and source addresses can be changed. These inbound/outbound filters are best used for managing networks such as these.

Task 5: Failover Clustering for high availability systems/services

Concept 1: Understanding the difference between a hot, warm or cold server

A cold server

A cold server is a server that sits in a network and is usually almost always in a shut down state. A cold server is only used in the event of a disaster, as a backup server for operation when the main server is either busy, interrupted or has failed. Many organisations prefer a cold server, as they are cost effective due to their nature of being mostly unused and therefore, consume less electricity. – However, as they sit in a shut down state, they take a lot of processing power when turning on, and are often susceptible to mandatory software and firmware updates before they can be used, so the time it takes for a cold server to start up is much longer than any other failover server type. [1]

A warm server

A warm server is a server that is periodically booted to receive updates and is the middleman between a cold server and a hot server. It still remains off most of the time, much like a cold server, but is periodically booted to install software and firmware updates. Microsoft doesn't offer a free license for disaster recovery for warm or hot servers, so this type of server isn't as cost effective as a cold server [2]

A hot server

A hot server is a more costly failover server type that remains on at all times as a backup server, ready to take over for when the main server is down or busy. A hot server is on at all times, which means it is constantly using electricity, and will need to be maintained regularly, as its computational components are always in use. This is the most effective disaster recovery method, and is often the preferred method of backup by large organisations [3]

We'd have to make a decision based on our financial position. A hot server is the most reliable form of failover, best for business where every second of server downtime can financially impact a company. For a small organisation or institute, such as a university, a warm server would be the best option. The software itself isn't free but the cost of running a warm server is minimised compared to a hot server. As hot servers are booted every once in a while, they receive adequate updates.

Concept 2: Prerequisites

According to Microsoft docs; verification of various prerequisites must be confirmed before setting up failover clustering. One major prerequisite is that all the nodes **must** run the exact same version of Windows Server (and they must run Windows Server in the first place). [4] This may be an issue, especially considering:

- **Windows Server Edition costs**

Although it may not cost a terrific amount, it still costs a company or organisation to run Windows Server Edition.

- **You cannot use a node running other operating systems**

If your organisation has a node running Linux for example, they won't be able to utilise Microsoft's failover cluster features if the main server goes down, as they run a different infrastructure with a different feature set.

Other prerequisites to take into consideration may include:

- You'll need to ensure all servers are connected to the same active directory domain
- You'll need to ensure that the account the cluster is created on has administrative rights on all servers that are going to be added as a cluster node [6]

Task 6: Observational Tasks

Architecture

- **Section 1-A: The use (including installation) of a personally owned network interface, including but not limited to: switches, routers, WAP and servers is strictly prohibited at all times.**

This policy would need to be enforced to ensure the best security and performance. This policy also ensures that the security is dependent on the company itself, access is guaranteed for the company, complete transparency of how all devices are being used, decisions that impact the performance of the device being 100% company dependent and complete ownership and access of the device not being dependent on the employee but rather administrated by the company itself (or whoever leases the network interface). [7]

- **Section 1-B: One DHCP server is required to assign IP addresses, it cannot be done manually or automatically by the Operating System**

Section 1-B is enforced to ensure complications that arise when IP addresses

are either assigned automatically or manually by the administrator never occur and that IP addresses are always assigned by one single DHCP server to minimise complications and errors. Without this policy, a lazy administrator is bound to manually set IP addresses or forget to set an IP, in this case, the Operating System will assign the IP address automatically and issues will occur. [8]

Topology

It's extremely important that we choose the best network topology for the best performance and to ensure we reach the 99% uptime threshold. There are several different types of network topology, each with their own set of advantages and disadvantages; these usually fall into a convention of 'the better the performance, the higher the price'. The best topology is one that can offer the best reliability and performance without being too costly.

- **Section 2-A: The main network must operate on a hybrid topology at all times, such as a tree topology.**

Although a tree topology is expensive, according to the brief, we are an enterprise network who operate in multiple locations worldwide, so an assumption that said enterprise should be able to cover the higher costs, as they are not a small business, and should rely on better networking performance and infrastructure as an essential element of their IT infrastructure.

- **Section 2-B: The inner topologies of the main network must use the best and most efficient topology for that particular sub-network. The topology must be as efficient as possible, but a less efficient topology can be used if the added efficiency of a better topology isn't necessary, and the cost can be cut.**

This policy ensures that network engineers evaluate each sub-network in the hybrid tree topology to ensure it suits the network's uses efficiently, but also ensures that network engineers take cost into consideration. For example, if a sub-network of 7 devices (5 PCs and 2 printers) is used at the reception of the facility, a mesh topology, for example, would be unnecessarily expensive. [9]

References

[1] "What is Cold Server? - Definition from Techopedia", *Techopedia.com*. [Online]. Available: <https://www.techopedia.com/definition/14302/cold-server>.

[2] "What is cold/warm/hot server? - Definition from WhatIs.com", *SearchWindowsServer*. [Online]. Available: <https://searchwindowsserver.techtarget.com/definition/cold-warm-hot-server>.

[3] "What is a Hot Server? - Definition from Techopedia", *Techopedia.com*. [Online]. Available: <https://www.techopedia.com/definition/25247/hot-server>.

[4] "Create a failover cluster", *Docs.microsoft.com*, 2019. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster#verify-the-prerequisites>.

- [5] M. Lahn, "How Much Does a Windows Server License Cost?", *Servermania.com*, 2021. [Online]. Available: <https://www.servermania.com/kb/articles/how-much-does-a-windows-server-cost/>.
- [6] "Create a failover cluster", *Docs.microsoft.com*, 2019. [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster#verify-the-prerequisites>. [Accessed: 30- Apr- 2021]
- [7] "Network Architecture", *Its.unl.edu*. [Online]. Available: <https://its.unl.edu/bestpractices/network-architecture>. [Accessed: 30- Apr- 2021]
- [8] Z. Kerravala, "DHCP defined and how it works", *Network World*, 2018. [Online]. Available: <https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html>.
- [9] S. Mudrakola, "Network topology guide: Why it's crucial you build the right structure", *TechGenix*, 2018. [Online]. Available: <https://techgenix.com/network-topology/>.