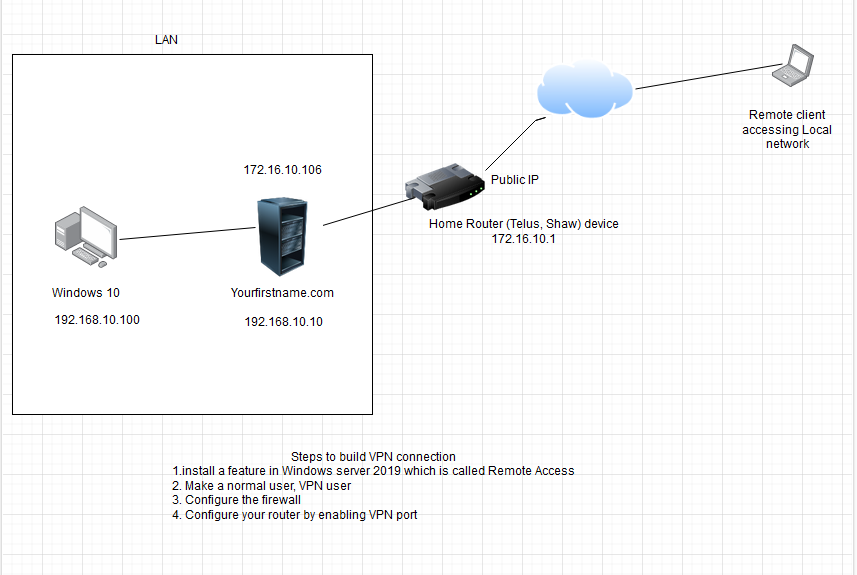
# PART 1 Setup a VPN for your home network with Windows server 2019

The objective of this task is to enable access to an organization network from a remote client machine using a VPN (Virtual Private Network).

Note: Ensure Windows server 2019 has a network adapter connected to the internet.



1. Install Remote Access

* Server Manager--- ‘Add roles and features’
* Select ‘Role based or feature based installation’ ----Select ‘Remote Access’
* From ‘Role Services’ select ‘Direct Access and VPN (RAS)’
* In ‘Configuration’ window click ‘install’
  + Then an additional item will appear at the dashboard of Server Manager named ‘Remote Access’
* Click ‘Remote Access’
* Click ‘More.’ option link in ‘Configuration required for Direct Access and VPN (RAS) at SERVER’
* Click ‘Open the getting started wizard’
  + Click ‘Deploy VPN only’
  + Select ‘Routing and Remote Access (MMC)’
  + Right click on the ‘SERVER’ option on the dashboard of ‘Server Manager’
  + Select ‘Configure and Enable Routing and Remote Access’
  + Select ‘Custom Configuration’
  + Select ‘VPN Access’
  + Again right click on ‘SERVER’
  + Click ‘Properties’
  + Select ‘IPV4’ tab---Select ‘DHCP’

1. Add a VPN user

* Click ‘Active Directory Users and Computers’
* Select the users who are going to use the VPN (any user)
* Right Click on the user
* Click ‘Properties’
* Click on ‘Dial- in’ tab
* Select ‘Allow Access’
* Click ‘Apply’

1. Configuration of Windows Server Firewall

* Access Control Panel, go to Windows Firewall settings, and select 'Allow an app or feature through Windows Firewall.'
* Enable 'Routing and Remote Access' by marking it for both 'Private' and 'Public' networks.

1. Configure you home router

Find the gateway (router) IP address and access it through the internet browser.

Enable 'PPTP' in the port forwarding or application and gaming section with the following information:

* + Service Name: PPTP
  + Start Port: 1723
  + End Port: 1723

**Verify that remote client can connect the LAN network**

Use the website [https://www.yougetsignal.com/what-is-my-ip-address/](https://www.yougetsignal.com/what-is-my-ip-address/" \t "_new)

To o obtain your public IP address and provide it to your classmate, along with the VPN username and password, for connecting to your network, follow these steps:

1. On the Windows 10 client machine Search, look for “VPN Settings”.
2. Under VPN, click on "Add a VPN connection." and enter the following details:
   1. VPN Provider: Windows (built-in)
   2. Connection Name: [Choose a name for the VPN connection, e.g., My VPN]
   3. Server Name or Address: [Enter the public IP address of the VPN server]
3. For VPN type, choose PPTP from the list
4. In the "Type of sign-in info" section, enter the credentials of the user who was allowed access
5. Click "Save" to add the VPN connection.
6. Click on the VPN connection you just created (e.g., My VPN) and click "Connect."
7. Enter the user's credentials (username and password) when prompted.
8. The VPN connection should now establish, and you will be connected to the remote network

**To verify that VPN connection is working, try to ping Windows Server 2016 or Windows 10 Client**

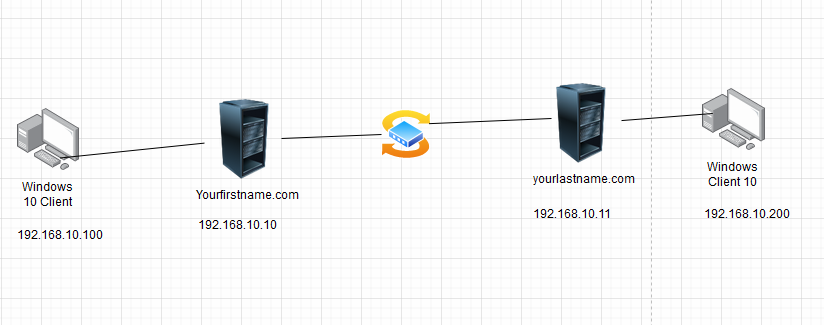
|  |  |
| --- | --- |
| Go to add roles and features and chose remote access and click next |  |
| Chose direct access and VPN |  |
| Click on install to install the feature |  |
| After install deploy only VPN |  |
| After deploy go to routing and remote access for setup |  |
| Click next |  |
| Chose custom configuration |  |
| Click on next |  |
| Chose DHCP and click next |  |
| Completing initialization |  |
| Go to AD users and groups chose a user to allow access in this example will chose mr Khaled jabbari |  |
| Allow access |  |
| Access the user account in windows 10 then create a VPN put the server ip , and chose a protocol ( in this VPN will chose PPTP ) , optional to use user name and password then save |  |
| Go to router and create a new rule for PPTP using port 1723 for internal and external to allow user access the server buy using VPN |  |
| Verify that user connected to VPN network |  |
| Mr Khaled Jabbari connected to VPN and Connected with the server |  |
| Verify from windows server , mr Khaled Jabbari access the server |  |
| If I need to put it public I should to create a new rule with my ips erver in my router |  |
| Connecting by Jordan with my public ip |  |
| Ping from Jordan |  |
| This the public ip for elizabeth connected with my VPN another example |  |
| And here I can see a client connected to my server |  |

# PART2. Creating a Two-Way Forest Trust between two different domains

The objective of this task is to demonstrate your understanding of Active Directory trusts by creating a two-way forest trust between two Windows Server 2019 forests (YourFirstname.com and YourLastname.com). After establishing the trust, you should ensure that clients from YourFirstName.com can connect to server in YourLastName.com without any issues.

Requirements:

1. Two Windows Server 2019 machines. One for each forest (Yourfirstname.com and YourLastname.com).
2. One client machine (Windows 10 or later) for each forest
3. Network connectivity between all servers and clients.



Steps to configure t a two-way forest trust:

Steps are explained in details in the following link

<https://www.youtube.com/watch?v=Cud41sE2KHI>

1. **Configure DNS for Trust Resolution**

Configure DNS forwarders or conditional forwarders on each forest's DNS servers to allow name resolution between the forests.

1. **Create the Forest Trust**

Create a two-way forest trust between YourFirstname.com and Yourlastname.com using the following settings:

* Forest Trust Type: Two-way
* Transitive: Yes
* SID Filtering: No
* Authentication: Forest-wide authentication

1. **Validate Trust Relationship**

Verify the trust relationship by ensuring that you can access resources between the forests:

* From Windows 10 client which is connected to yourfirstname.com, try to login to yourlastname.com domain
* From Windows 10 client which is connected to yourlastname.com, try to login to yourfirstname.com domain

|  |  |
| --- | --- |
| New server with my last name alimoe.com go to dns manager to add a conditional |  |
| Add the moeali.com domain and the ip server for moeali domain 192.168.2.49 |  |
| Move to moeali.com domain and add the conditional fro alimoe.com by adding dns and ip |  |
| As we look in this picture we have 2 conditional |  |
| In this picture we test the access between two domain alimoe.com and moeali.com |  |
| Create trust between server will start with moeali and click in newtrust |  |
| Starting new trust by adding the domain should be trust it with moeali.com (in this example alimoe.com ) |  |
| Chose the forest trust and click next |  |
| Trust in two way and next |  |
| Chose this domain only and click next |  |
| Chose forest wide authentication and click next |  |
| Chose the password trust between domain and this step should be the same in 2 domain |  |
| Show the settings created it between 2 domain |  |
| Trust created it successfully |  |
| Chose the first option bcz we need to create the same settings in second server to confirm |  |
| Same for this part |  |
| Finish the configuration |  |
| Same process in the second server but this time I chose moeali.com as a trust domain for alimoe.com |  |
| Put the same password , used in the first configuration |  |
| And here confirm the outgoing trust |  |
| After create trust between server in both domain , know we need to validate so will go to properties |  |
| Click in validate then ok |  |
| And as we see we validate the outgoing between 2 domain now will go to another server and will do the same steps to validate |  |
| And this the second validation |  |
| And this the user from moeali domain ping the alimoe domain by ping 192.168.2.61 ip for alimoe domain |  |
| Verification |  |
| NOTE | I don’t have enough memory to trun 3 system together , so my apologies to not showing more verification |