Project Title : Active Directory with Remote Access VPN

Microsoft Certified Solutions Associate

Author: Bhavesh Mayekar (linkedin.com/in/bhaveshmayekar)

Course: Microsoft Certified Solutions Associate

Date: 2025-09-11

Objective

The goal of this project is to design and implement a secure enterprise identity and remote access solution.

- Active Directory Domain Services (AD DS) with AD-integrated DNS provide centralized authentication and directory-based management.
- Remote Access VPN (RRAS) using IKEv2 and SSTP allows domain users to connect securely from outside the corporate network.

Why VPN is Important

- **VPN (Virtual Private Network):** Creates a secure encrypted tunnel between remote client and corporate private network over internet.
- **Use Cases:**
  - **Work From Home (WFH):** Employees access company file shares, intranet, and applications securely.
  - **Site-to-Site VPN:** Connects branch offices over the internet to work like a single network.
- **Protocols:**
  - **IKEv2:** Fast, secure, and stable (best for mobile clients).
  - **SSTP:** Uses HTTPS (TCP 443), works even behind firewalls.

Why This Project Matters

- Centralized Identity Management: AD DS gives a single sign-on experience and simplifies IT administration.
- Secure Remote Access: VPN with IKEv2/SSTP allows employees to securely access company resources over the internet.
- Scalability: AD-integrated DNS ensures domain resources scale easily with additional domain controllers.
- Best Practice: Combines directory services with secure remote connectivity critical for modern hybrid workplaces.

Lab Environment Setup

- Server 1 (DC1): Windows Server – Domain Controller (AD DS + DNS)
  VPN Server (RRAS role)
- Client 1: Windows 10/11 domain-joined client

Technologies Used

- Active Directory Domain Services (AD DS)
- AD-integrated DNS
- Remote Access Service (RRAS)
- VPN Protocols: IKEv2, SSTP
- Windows Server 2019/2022/2025
- Authentication: Domain user accounts (Kerberos/NTLM)

Prerequisites Checklist

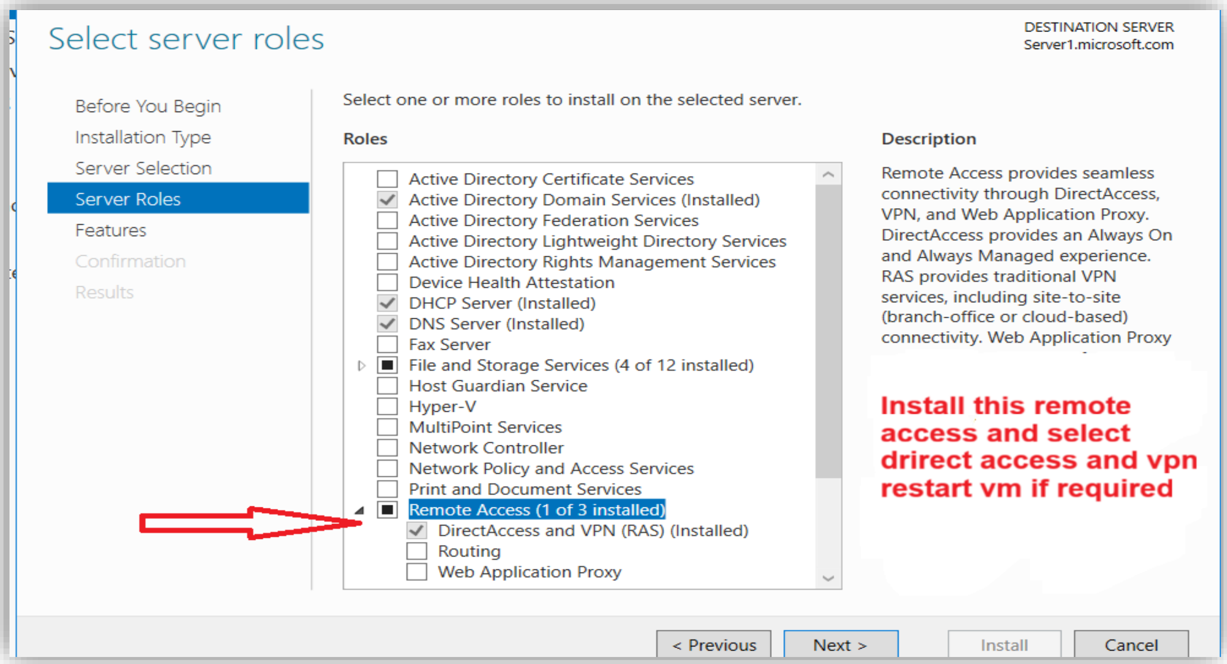
Before configuring VPN with RRAS, ensure the following are in place:

- **Active Directory Domain Services (AD DS):** Domain created (e.g., corp.local).
- **DNS:** AD-integrated DNS configured for secure name resolution.
- **Certificates:** Valid SSL certificate (required for SSTP VPN).
- **Networking:**
  - VPN Server should have proper IP addressing.
  - Firewall ports open for **IKEv2 (UDP 500/4500)** and **SSTP (TCP 443)**.
- **User Accounts:** Domain users created in AD for authentication

Step-by-Step Implementation

Step 1: Install Remote Access Role (VPN) on Server 1

1. Open **Server Manager > Add Roles and Features**.
2. Select **Role-based or feature-based installation**.
3. Choose your **Server 1 (VPN Server)**.
4. Under **Roles**, expand **Remote Access** → select **DirectAccess and VPN (RAS)**.
5. Add required features and complete the wizard.
6. After installation, open **Tools > Routing and Remote Access**.



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

Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (4 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ■ Remote Access (1 of 3 installed)
  - ☑ DirectAccess and VPN (RAS) (Installed)
  - ☐ Routing
  - ☐ Web Application Proxy

Description

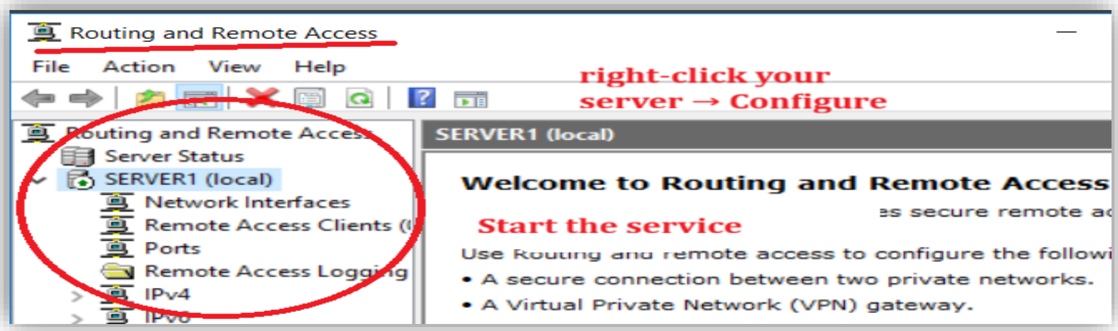
Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy

Install this remote access and select drirect access and vpn restart vm if required

---

Step 2: Configure RRAS for VPN Access (open Tools > Routing and Remote Access.) In the **Routing and Remote Access console**, right-click your server → **Configure and Enable Routing and Remote Access.**

1. Select **Custom Configuration**.
2. Check **VPN Access**.
3. Finish and click **Start Service.**



right-click your server → Configure

SERVER1 (local)

Welcome to Routing and Remote Access

Start the service

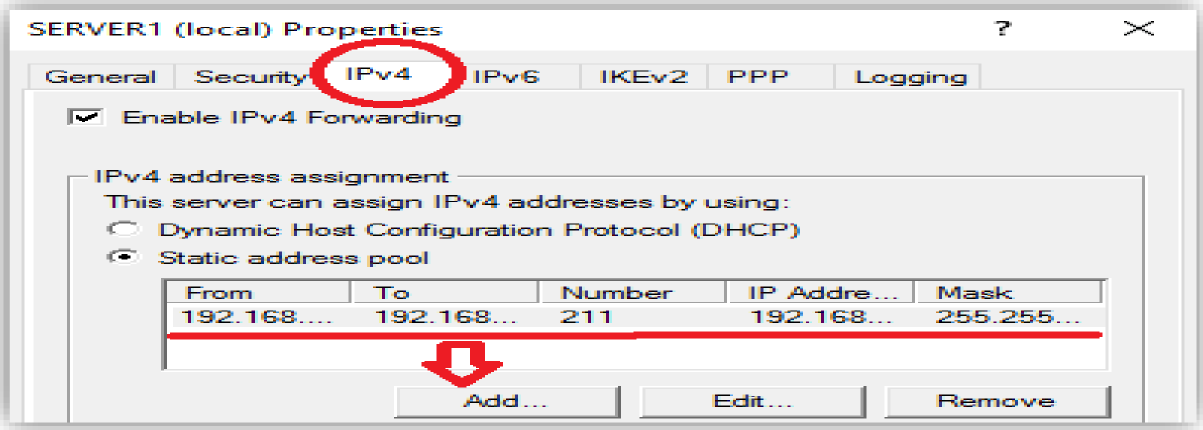
es secure remote ac

Use Routing and remote access to configure the followi

- A secure connection between two private networks.
- A Virtual Private Network (VPN) gateway.

Step 3: Configure IP Address Assignment for VPN Clients

1. In RRAS console, right-click server → **Properties > IPv4 tab**.
2. Select **Static Address Pool**.
3. Add an IP range (e.g., 10.10.10.100 – 10.10.10.200).
   - This will be assigned to VPN clients when they connect.



☑ Enable IPv4 Forwarding

IPv4 address assignment

This server can assign IPv4 addresses by using:

○ Dynamic Host Configuration Protocol (DHCP)

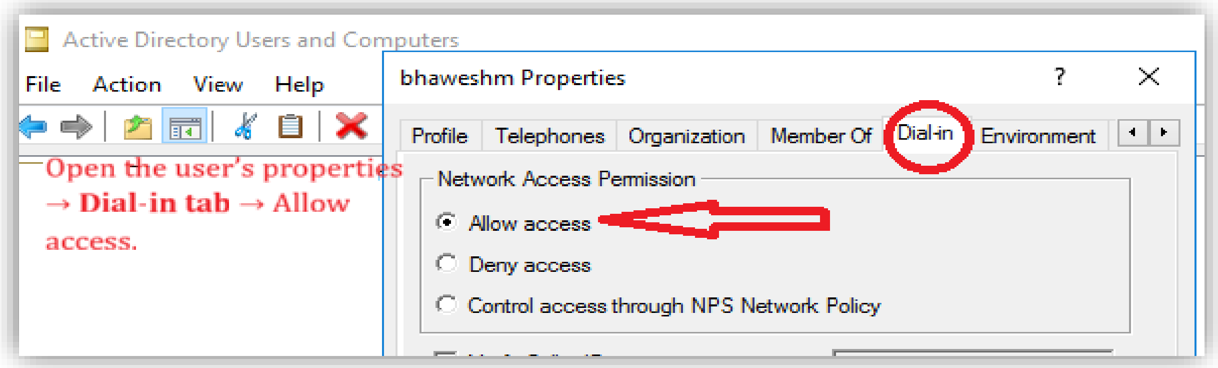
● Static address pool

From	To	Number	IP Addre...	Mask
192.168....	192.168...	211	192.168...	255.255...

Step 4: Configure Authentication with Active Directory

In **Active Directory Users and Computers (ADUC)**:

- Create a test user (e.g., vpnuser1).
- Open the user's properties → **Dial-in tab** → Allow access.



Open the user's properties → **Dial-in tab** → Allow access.

bhaweshm Properties

Network Access Permission

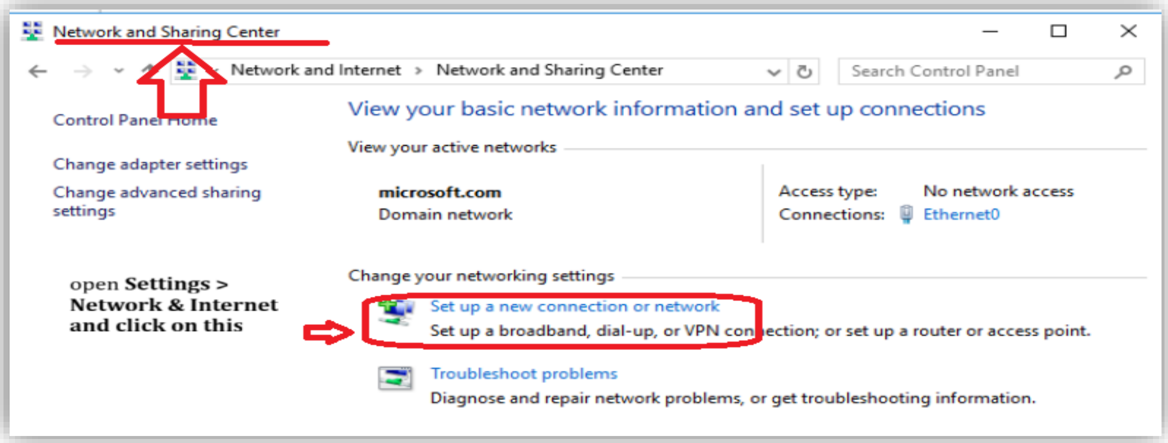
● Allow access

○ Deny access

○ Control access through NPS Network Policy

Step 5: Configure VPN on Client Machine

1. On Windows 10/11 client → open **Settings > Network & Internet > VPN**.
2. Click **Add a VPN Connection**.
3. Enter details:
   - VPN Provider: **Windows (built-in)**
   - Connection Name: *CorpVPN*
   - Server Name or Address: Public IP or FQDN of Server 2
   - VPN Type: Select **IKEv2** or **SSTP**
   - Sign-in Info: Username & password (domain user)
4. Save and click **Connect**.



Network and Sharing Center

Network and Internet > Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

microsoft.com
Domain network

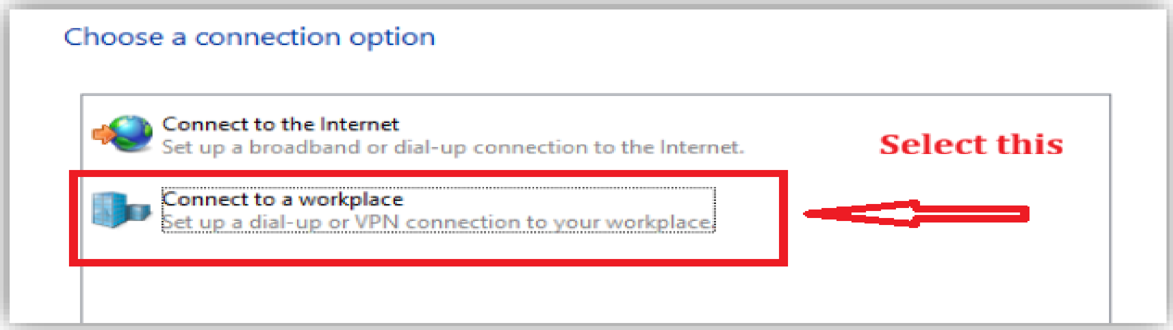
Access type: No network access
Connections: Ethernet0

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

open **Settings > Network & Internet and click on this**

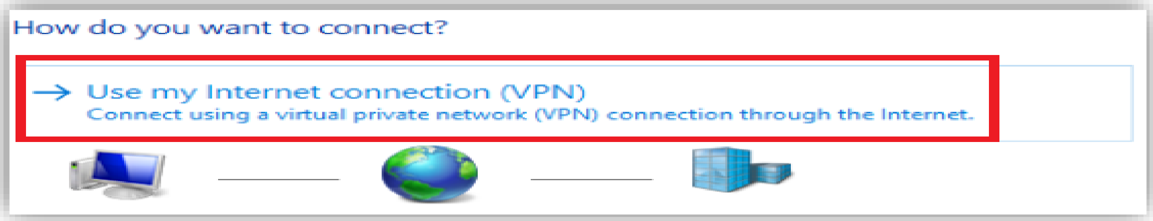


Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

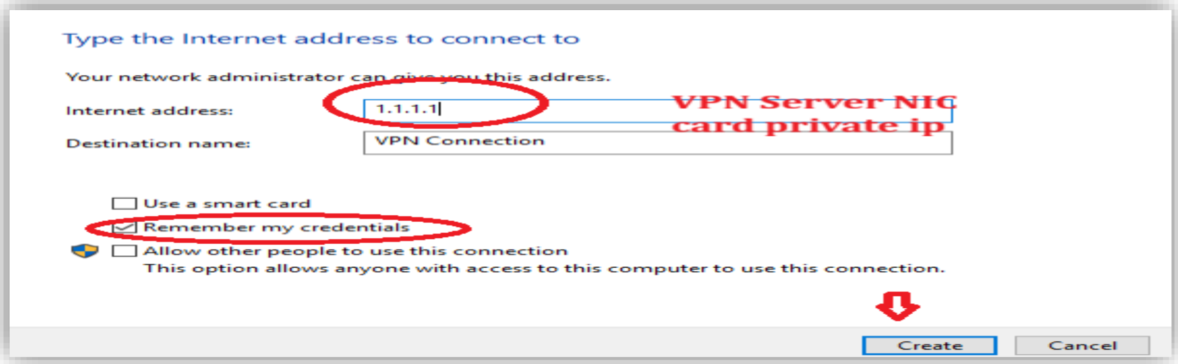
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Select this



How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 1.1.1.1

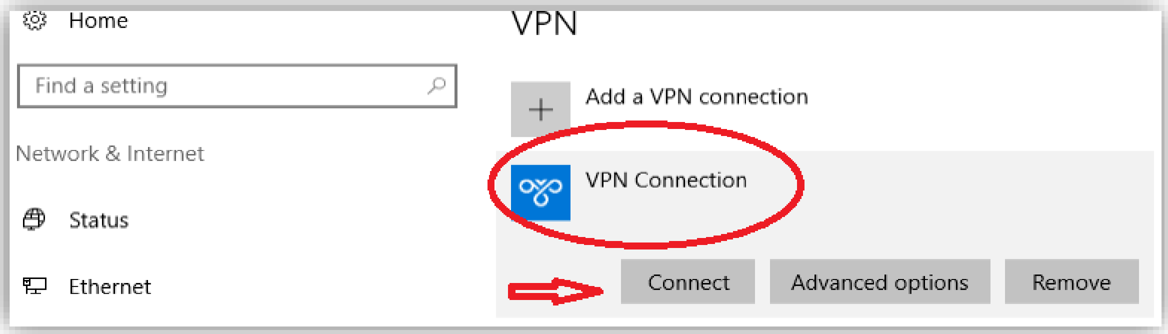
Destination name: VPN Connection

VPN Server NIC card private ip

☐ Use a smart card

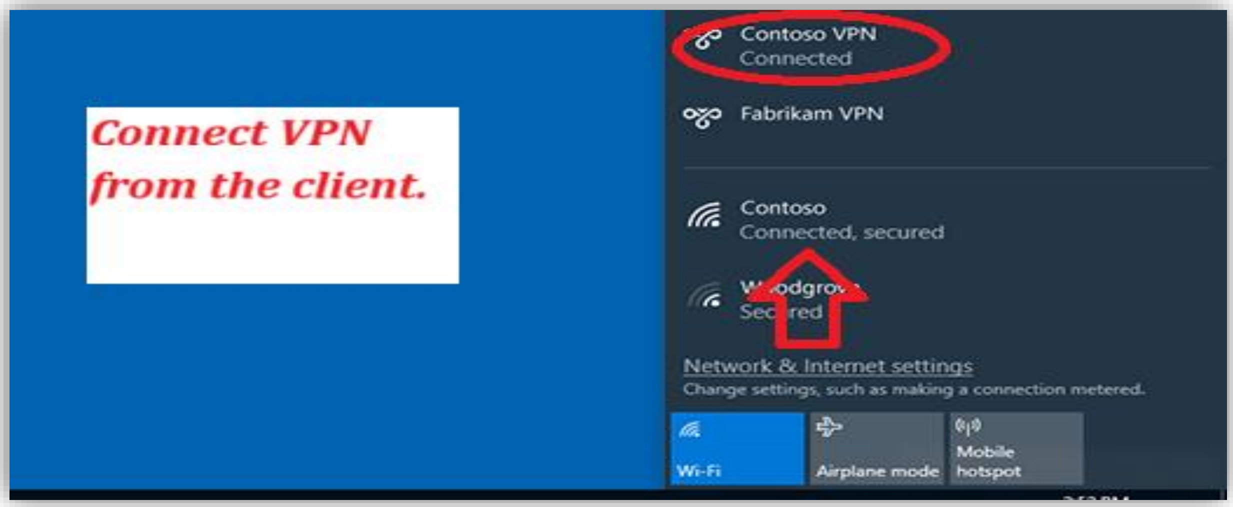
☑ Remember my credentials

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.



Step 6: Test VPN Connectivity

1. Connect VPN from the client.
2. Verify client receives an IP from the VPN pool.



Connect VPN from the client.

Troubleshooting

Even in a lab, VPN setup can face issues. Here are some quick fixes:

- **No internet or VPN not starting?**
  → Check if the server has **two NICs** (one private for LAN, one public for external access). Without proper NIC setup, RRAS may fail.
- **Client cannot connect?**
  → Verify that **PPTP protocol** is enabled in RRAS properties.
  → Ensure firewall allows **TCP 1723** and GRE (protocol 47).
- **User login fails?**
  → In AD, check the user's **Dial-in properties** → Access must be allowed.
- **No IP assigned to client?**
  → Confirm the **static address pool** is configured in RRAS or use DHCP relay.
- **Can't access internal resources after VPN connects?**
  → Check DNS – make sure the client can resolve microsoft.com

---

Conclusion

This project demonstrated how to build a simple but functional **Active Directory with Remote Access VPN** environment. By using **PPTP** (for lab purposes), I was able to:

- Provide remote users secure access into the domain network.
- Centralize authentication with **Active Directory**.
- Assign VPN clients IPs and verify access to internal resources.

In real enterprise setups, IT teams use stronger protocols like **IKEv2/SSTP**, but this lab gave me clear, hands-on understanding of how **VPN, AD DS, DNS, and RRAS** all work together.

Author: Bhavesh Mayekar (linkedin.com/in/bhaveshmayekar)
Course: Microsoft Certified Solutions Associate
Date: 2025-09-11

Developed by: Bhavesh Mayekar