**Research and Development Document**

**ON**

**Point To Site**

****

****

**By**

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

**Under**

**Celebal Summer Internship**

**in**

**Cloud Infra & Security**

**VPN Gateway**

**Azure VPN Gateway service can be used to send encrypted traffic between an Azure virtual network and on-premises locations over the public Internet. You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network**

A diagram of a network

AI-generated content may be incorrect.

**Key Use of VPN Gateway:**

To securely send **encrypted traffic** across public networks between Azure and on-premises or between Azure virtual networks.

**Use cases**

* **Site-to-site connectivity**: Connect on-premises networks to Azure virtual networks using IPsec VPN protocols.
* **Point-to-site connectivity**: Connect individual devices, such as laptops or mobile devices, to Azure virtual networks using VPN protocols.
* **Remote access**: Provide remote access to Azure resources for employees working from home or on the go.
* **Hybrid applications**: Build hybrid applications that require secure connections between on-premises and Azure resources.

**Hybrid Connectivity:**

Hybrid connectivity is a critical component of a cloud architecture, which combines on-premises infrastructure, private cloud services, and public cloud services. Hybrid connectivity enables you to connect and maintain resiliency with your Azure resources.

**Use cases**

* Site-to-site connectivity: Connect on-premises networks to Azure virtual networks using IPsec VPN protocols.
* Point-to-site connectivity: Connect individual devices, such as laptops or mobile devices, to Azure virtual networks using VPN protocols.
* Remote access: Provide remote access to Azure resources for employees working from home or on the go.
* Hybrid applications: Build hybrid applications that require secure connections between on-premises and Azure resources.

A screenshot of a computer

AI-generated content may be incorrect.

**Azure ExpressRoute**

It provides private, dedicated connectivity between on-premises networks and Azure datacenters. It offers higher reliability, faster speeds, and lower latencies compared to connections over the public internet. ExpressRoute connections can be established through an ExpressRoute circuit, which is a dedicated connection between your on-premises network and an Azure datacenter. ExpressRoute is suitable for scenarios requiring low latency connections and high bandwidth requirements.

Use cases

* Hybrid applications: Build hybrid applications that require low latency and high bandwidth connections between on-premises and Azure resources.
* Data transfer: Transfer large amounts of data between on-premises and Azure resources without using the public internet.
* Disaster recovery: Establish a reliable and secure connection for disaster recovery solutions, such as Azure Site Recovery.
* Compliance: Meet regulatory and compliance requirements by using private connections instead of public internet connections.
* Big data analytics: Transfer large datasets to Azure for analysis and processing without using the public internet.
* Backup and archiving: Use ExpressRoute to transfer backup data to Azure Blob Storage or Azure Archive Storage for long-term retention.

**Azure Virtual WAN**

**Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch, branch-to-Azure, and Azure-to-Azure connectivity. It simplifies the deployment and management of branch connectivity by providing a unified hub-and-spoke architecture. Virtual WAN supports multiple connectivity options, including VPN, ExpressRoute, and SD-WAN.**

**Use cases**

* **Branch connectivity: Connect multiple branch offices to Azure resources using a unified hub-and-spoke architecture.**
* **SD-WAN integration: Integrate with third-party SD-WAN solutions to optimize branch connectivity and performance.**
* **Automated branch management: Simplify the deployment and management of branch connectivity with automated provisioning and configuration.**
* **Global connectivity: Connect multiple Azure regions and on-premises networks using a single Virtual WAN hub.**
* **Optimized routing: Use Azure's global backbone network to optimize routing and performance for branch-to-branch and branch-to-Azure connectivity.**
* **Security: Use Azure Firewall and other security services to protect branch connectivity and enforce security policies.**

**Creating a VPN Gateway on Azure :**

**Create a Virtual Network**

* **Resource Group: TestRG1**
* **VNet Name: VNet1**
* **Region: East US**
* **Address Space: 10.1.0.0/16**
* **Subnet: FrontEnd (10.1.0.0/24)**

**Azure Portal > Virtual Network > Create → Fill in required fields → Create**

**Create Gateway Subnet**

* **Name must be GatewaySubnet**
* **Suggested size: /27 or larger (e.g., 10.1.255.0/27)**

**In VNet > Subnets > +Subnet > Select Virtual Network Gateway purpose**

**Do not associate NSGs with GatewaySubnet**

**Create VPN Gateway**

* **Name: VNet1GW**
* **Type: VPN**
* **SKU: VpnGw2AZ (Zone-redundant)**
* **Generation: Gen2**
* **Enable Active-Active: Optional**
* **Public IPs: VNet1GWpip1 (+pip2 if active-active)**

**Azure Portal > VPN Gateway > Create > Fill fields > Create**

**Takes ~45 minutes to deploy**

**View Public IP**

**Go to VPN Gateway > Properties > Click IP link**

**Upgrade Gateway SKU**

**VPN Gateway > Configuration > Select new SKU from dropdown > Save**

**⚠ Not all SKUs are upgradable**

**Reset VPN Gateway**

**VPN Gateway > Help > Reset > Click Reset**

* **Managed Identity Setup**

1. Azure Portal → Search Managed Identities → Create.
2. Input a name (e.g., vpngwy-managed).
3. Choose a Resource Group (can be different from VPN Gateway's).
4. Click Review + create, then Create.

* **Enable Key Vault Access on VPN Gateway**

1. Go to your VPN Gateway in the portal.
2. Navigate to Settings → Configuration.
3. Set:
   * Enable Key Vault Access: Enabled
   * Managed Identity: Select the one you created earlier.
4. Click Save.

* **Create Local Network Gateway**

Used to represent your on-premises VPN device in Azure.

Create Steps:

1. Go to Local network gateways → Create.
2. On Basics tab:
   * Name: Site1
   * Region: e.g., East US
   * Endpoint Type:
     + IP Address: Use if you have a static IP.
     + FQDN: Use if you have a dynamic IP with DNS mapping.
   * Address Space: Enter on-premises address ranges (e.g., 192.168.1.0/24).
3. (Optional) On Advanced tab: Configure BGP if required.
4. Click Review + create → Create.

* FQDN must resolve to one IPv4 address only.
* VPN Gateway DNS cache refreshes every 5 minutes.
* All FQDNs must resolve to unique IPs if using multiple gateways.

**Certificates**

**Site-to-site certificate authentication architecture relies on both inbound and outbound certificates.**

**The inbound and outbound certificates don't need to be generated from the same root certificate.**

**Outbound certificate**

* The outbound certificate is used to verify connections coming from Azure to your on-premises site.
* The certificate is stored in Azure Key Vault. You specify the outbound certificate path identifier when you configure your site-to-site connection.
* You can create a certificate using a certificate authority of your choice, or you can create a self-signed root certificate.

When you generate an outbound certificate, the certificate must adhere to the following guidelines:

* Minimum key length of 2048 bits.
* Must have a private key.
* Must have server and client authentication.
* Must have a subject name.

Inbound certificate

* The inbound certificate is used when connecting from your on-premises location to Azure.
* The subject name value is used when you configure your site-to-site connection.
* The certificate chain public key is specified when you configure your site-to-site connection.

**Configuring Point-to-Site VPN:**

**(MICROSOFT ENTRA ID AUTHENCTICATION)**

* **Add the VPN client address pool**

The client address pool is a range of private IP addresses that you specify. The clients that connect over a point-to-site VPN dynamically receive an IP address from this range. Use a private IP address range that doesn't overlap with the on-premises location that you connect from, or the virtual network that you want to connect to. If you configure multiple protocols and SSTP is one of the protocols, then the configured address pool is split between the configured protocols equally.

1. In the Azure portal, go to your VPN gateway.
2. On the page for your gateway, in the left pane, select Point-to-site configuration.
3. On the Point-to-site configuration page, click Configure now.
4. On the point-to-site configuration page, you'll see the configuration box for Address pool.
5. In the Address pool box, add the private IP address range that you want to use. For example, if you add the address range 172.16.201.0/24, connecting VPN clients receive one of the IP addresses from this range. The minimum subnet mask is 29 bit for active/passive and 28 bit for active/active configuration.
   1. **How to setup Point to Site**

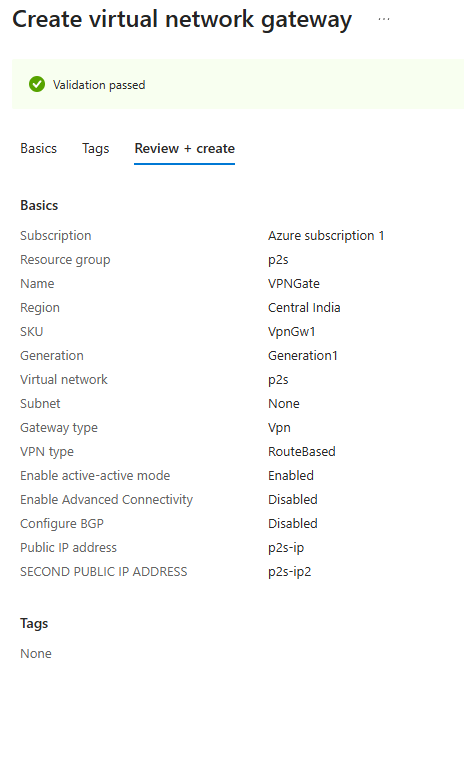
**Step 1 : Create Vnet**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Step 2 : Create VPN GatewayA screenshot of a computer

AI-generated content may be incorrect.**

****

**Step 3 : Create Root Certificate from local system**

Script :

$rootCert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

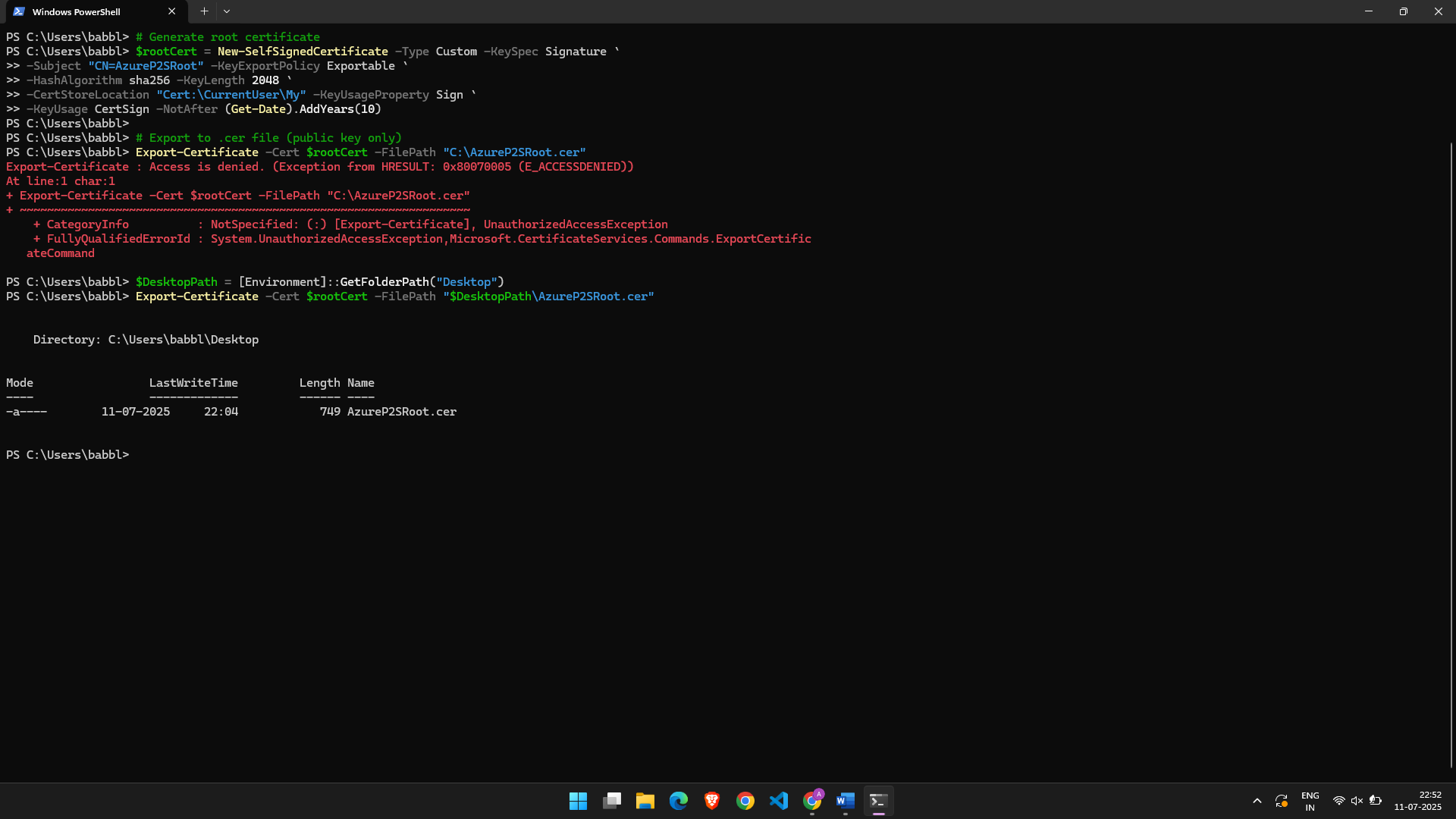
-Subject "CN=AzureP2SRoot" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign `

-KeyUsage CertSign -NotAfter (Get-Date).AddYears(10)

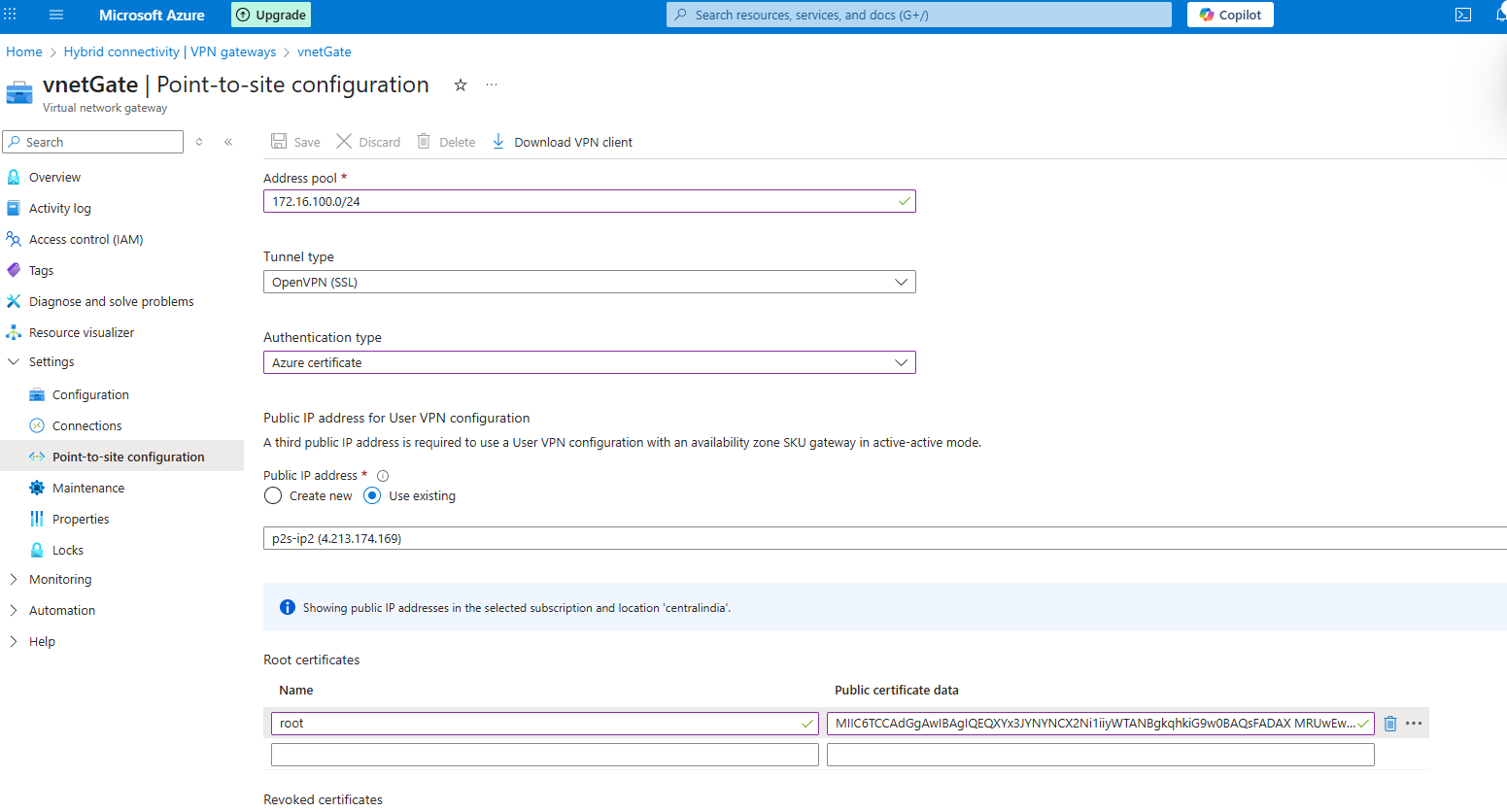
**Export-Certificate -Cert $rootCert -FilePath "C:\AzureP2SRoot.cer"**



**Upload on Azure :**

**A screenshot of a computer

AI-generated content may be incorrect.**

****

**Generating Client Certificate :**

**ON LOCAL SYSTEM POWERSHELL**

Script : $clientCert = New-SelfSignedCertificate -Type Custom -DnsName "P2SClient" `

-KeySpec Signature -Subject "CN=P2SClientCert" `

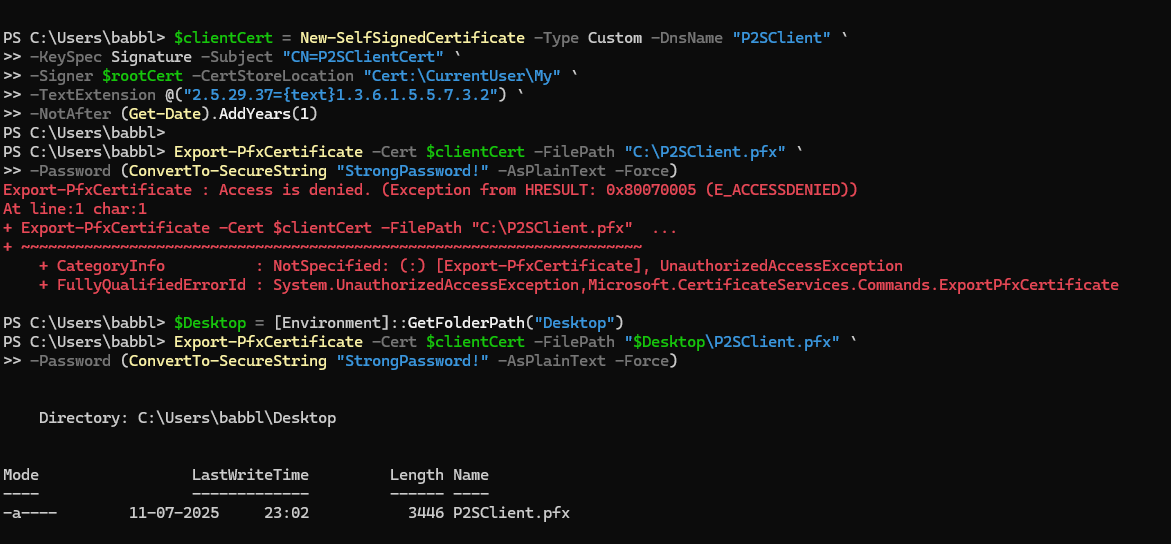
-Signer $rootCert -CertStoreLocation "Cert:\CurrentUser\My" `

-TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2") `

-NotAfter (Get-Date).AddYears(1)

Export-PfxCertificate -Cert $clientCert -FilePath "C:\P2SClient.pfx" `

-Password (ConvertTo-SecureString "StrongPassword!" -AsPlainText -Force)



**Step 5 : Checking VPN Connection**

A screenshot of a computer

AI-generated content may be incorrect.

**2.Setup Site-to-Site (S2S) VPN using Hyper-V and RRAS**

**Step 1:Create Virtual Network & Gateway in Azure :**

**Already Done**

**Step 2: Set Up Hyper-V VM (Your On-Prem VPN Router)**

1. **In Hyper-V Manager, create a VM**
   * **OS: Windows Server (2016 or newer)**
   * **2 NICs: one connected to internal network, one to external (internet)**
   * **Assign static private IP to internal NIC**
2. **Log into the VM**

### **Step 3**: **Install & Configure RRAS (Routing and Remote Access)**

Install-WindowsFeature RemoteAccess -IncludeManagementTools

Install-WindowsFeature Routing

**Step 4:Configure RRAS for VPN**

1. Open Routing and Remote Access (RRAS):
   * Run: rrasmgmt.msc
2. Right-click your server > Configure and Enable Routing and Remote Access
3. Choose:
   * Custom configuration
   * Check VPN Access and NAT
4. Finish wizard > Start the RRAS service

**Step 5 :Add Site-to-Site VPN Interface**

1. In RRAS:
   * Right-click Network Interfaces > New Demand-Dial Interface
2. Name: AzureS2S (or similar)
3. Connect using: VPN
   * VPN type: IKEv2 (select manually if needed)
4. Enter Azure VPN Gateway Public IP
5. Authentication:
   * Leave username blank
   * Use pre-shared key (e.g., P2S2Skey123)
6. Routing:
   * Add route to Azure VNet (e.g., 10.1.0.0/16)

**Step 6: Add Static Route to Azure**

In RRAS > IP Routing > Static Routes:

* Destination: 10.1.0.0
* Mask: 255.255.0.0
* Interface: AzureS2S
* Metric: 1

**Step 7: Allow VPN and NAT in Firewall**

**In PowerShell:**

Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

**References**

* **Microsoft Azure Documentation**
* **Medium.com**
* **NetITGeeks**