



Point to site VPN Set Up

Azure Point-to-Site (P2S) VPN is a secure and flexible way for individual clients to connect to an Azure Virtual Network (VNet) from remote locations. It's particularly useful for users who need to connect from different locations and devices, and it can be set up without the need for a dedicated on-premises VPN gateway. Here's an overview of how Azure P2S VPN works and how to set it up:

How Azure P2S VPN Works

1. Client Initiation: The VPN client on the user's device initiates a connection to the Azure VPN gateway.
2. Authentication: The client uses certificates or Azure Active Directory (Azure AD) to authenticate.
3. VPN Tunnel: Once authenticated, a secure VPN tunnel is established between the client and the Azure VPN gateway.
4. Network Access: Through this tunnel, the client can securely access resources within the Azure VNet.

Features of Azure P2S VPN

1. Secure Communication: Uses SSL/TLS protocols for secure communication.
2. Authentication Options: Supports native Azure AD, RADIUS, or certificate-based authentication.
3. Device Compatibility: Works with Windows, macOS, Linux, iOS, and Android.
4. Scalability: Easily scales to support multiple connections without requiring extensive hardware investments.

Setting Up Azure P2S VPN

Prerequisites

1. An Azure subscription.
2. A configured Azure VNet.
3. A VPN gateway created for the VNet.
4. Steps to Configure Azure P2S VPN

Create a Virtual Network Gateway:

1. In the Azure portal, go to "Create a resource".
2. Search for "Virtual Network Gateway" and click "Create".
3. Configure the settings, such as gateway type (VPN), VPN type (Route-based), and SKU (based on performance requirements).

Configure Point-to-Site VPN:

1. Once the gateway is created, navigate to it in the Azure portal.
2. Under "Settings", select "Point-to-site configuration".

3. Configure the address pool (the range of IP addresses that will be assigned to clients), tunnel type (IKEv2, SSTP, or OpenVPN), and authentication type (Azure AD, RADIUS, or certificates).

Generate VPN Client Configuration Files:

1. After configuring the Point-to-Site settings, generate the VPN client configuration package.
2. This package contains the necessary information for clients to establish a VPN connection.

Distribute VPN Client Configuration:

1. Download the configuration package and distribute it to your users.
2. Users install the VPN client and configuration on their devices.

Connect to the VPN:

- Users open the VPN client and establish a connection to the Azure VPN gateway using their credentials (depending on the authentication method chosen).

Authentication Methods

1. **Azure Certificate Authentication:** Requires generating and uploading a root certificate to Azure. Users are provided with a client certificate derived from the root certificate for authentication.
2. **Azure Active Directory Authentication:** Users authenticate using their Azure AD credentials. This method simplifies management, especially for organizations using Azure AD.
3. **RADIUS Authentication:** Integrates with existing on-premises RADIUS server for authentication. Suitable for organizations that want to leverage their existing RADIUS infrastructure.

Benefits of Azure P2S VPN

1. **Flexibility:** Users can connect from any location with internet access.
2. **Security:** Securely connects remote users to Azure resources.
3. **Scalability:** Easily scales to accommodate more users.
4. **Integration:** Seamless integration with Azure AD and existing infrastructure.
5. Troubleshooting Tips
6. **Connection Issues:** Ensure the VPN client is correctly configured and the address pool is not exhausted.
7. **Authentication Failures:** Verify that certificates are correctly installed and valid, or that Azure AD credentials are correct.
8. **Network Access Problems:** Check network security group (NSG) rules and routing configurations within the VNet.

Azure Point-to-Site VPN is a powerful solution for providing secure remote access to Azure VNets. By following the configuration steps and understanding the features and benefits, organizations can effectively manage remote connectivity for their users.

The end goal is to securely connect a remote client to an Azure Virtual Network using a Point-to-Site VPN, allowing access to resources within the VNet, such as the web server on the VM. This setup demonstrates secure remote connectivity and resource access without needing a public IP address.

To begin with the Lab:

1. First, we are going to launch a virtual machine based on Windows Server 2022 and install a Web Server (IIS) on it. With that, we also want to create a HTML page so that we can identify the VM for ourselves.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Azure Pass - Sponsorship"/>
Resource group *	<input type="text" value="new-grp"/> Create new

Instance details

Virtual machine name *	<input type="text" value="demoVM"/> 
Region *	<input type="text" value="(Europe) North Europe"/>
Availability options	<input type="text" value="No infrastructure redundancy required"/>
Security type	<input type="text" value="Trusted launch virtual machines"/> Configure security features
Image *	<input type="text" value="Windows Server 2022 Datacenter - x64 Gen2"/>  See all images Configure VM generation
VM architecture	<input checked="" type="radio"/> Arm64 <input checked="" type="radio"/> x64  Arm64 is not supported with the selected image.
Run with Azure Spot discount	<input type="checkbox"/>
Size *	<input type="text" value="Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹12,085.69/month)"/>  See all sizes

Administrator account

Username *	demo	✓
Password *	*****	✓
Confirm password *	*****	✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

None
 Allow selected ports

Select inbound ports *

RDP (3389)

- Now in the Networking create a new Virtual Network and choose to public IP so that we can configure our VM by logging in to it.

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more ↗](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

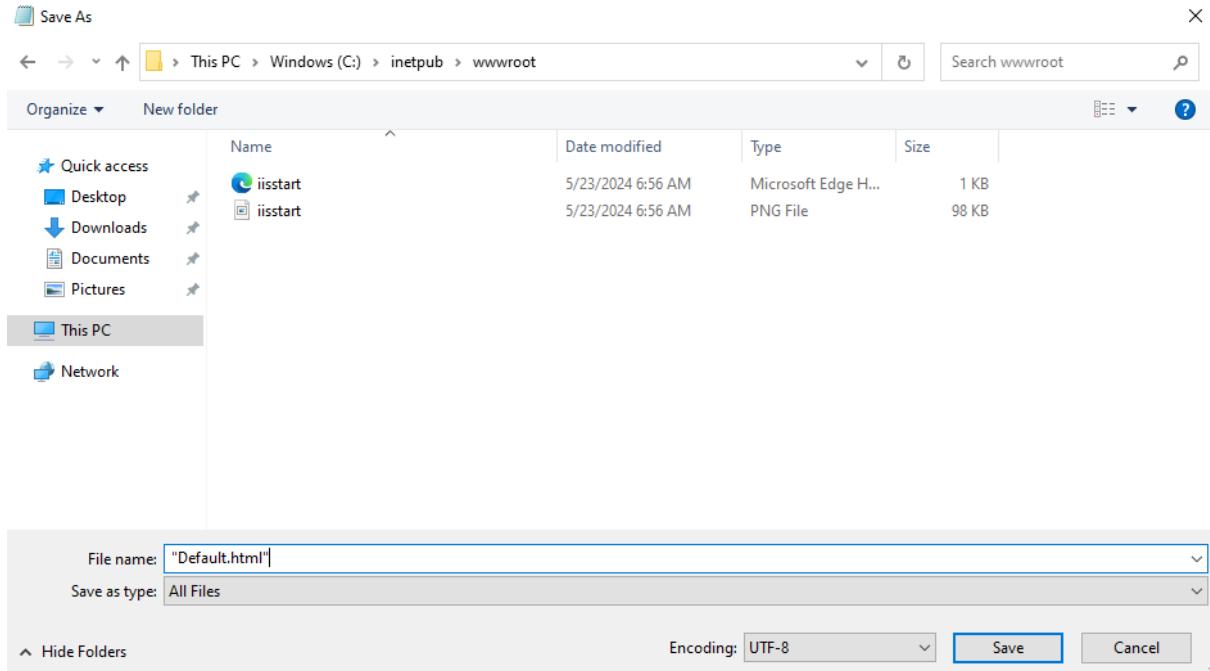
Virtual network *	(new) demo-VN	▼
	Create new	
Subnet *	(new) demoSubnet (10.1.0.0/24)	▼
Public IP	(new) demoVM-ip	▼
	Create new	

- After that move to the Review page and Create your Virtual Machine.
- Once the deployment is complete then you need to login to your VM and install Web Server on it.
- Once the web server is installed then you need to create a default.html page at this location shown below.

*Untitled - Notepad

File Edit Format View Help

```
<h1>This is DemoVM Server</h1>
```



6. Once you have done this now you are going to remove the Public IP address from this demo VM and delete the Public IP address from your resources.
7. For that go to Network Interface of Demo VM and then go to IP configuration and disassociate the Public IP address. After that go to resources and delete the Public IP.



Setting Up the Gateway

1. In this lab, we are going to deploy our VPN gateway. This will be the entry point for the clients onto the virtual network.
2. To have the VPN gateway in place we need to have an empty subnet. This is known as the gateway subnet.
3. Go to the virtual network and then go to subnets, there is a direct option to create Gateway subnet. Click on it.

Home > new-grp > demo-VN

demo-VN | Subnets Virtual network

Subnet Gateway subnet Refresh Manage users Delete

Address space Connected devices Subnets Bastion DDoS protection

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
demoSubnet	10.1.0.0/24	-	250

4. Then while creating it you need to change the size to /26.

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more ↗](#)

Subnet purpose ⓘ Virtual Network Gateway

Name * ⓘ GatewaySubnet

IPv4

Include an IPv4 address space

IPv4 address range * ⓘ 10.1.0.0/16
10.1.0.0 - 10.1.255.255

Starting address * ⓘ 10.1.1.0

Size ⓘ /26 (64 addresses)

Subnet address range ⓘ 10.1.1.0 - 10.1.1.63

5. After that you have to go to the marketplace and search for virtual network gateway and choose this service accordingly.

Virtual network gateway Microsoft

 **Virtual network gateway** Microsoft | Azure Service Add to Favorites

3.9 (27 ratings)

Plan Virtual network gateway Create

6. Then you must follow the snapshots below to create your gateway.

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more ↗](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources. 

Subscription *

Azure Pass - Sponsorship 

Resource group 

new-grp (derived from virtual network's resource group)

Instance details

Name *

demo-network-gateway 

Region *

North Europe 

[Deploy to an edge zone ↗](#)

Gateway type * 

VPN ExpressRoute

SKU * 

VpnGw2AZ 

Generation 

Generation2 

Virtual network * 

demo-VN 

[Create virtual network](#)

Subnet 

GatewaySubnet (10.1.1.0/26) 

 Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address * 

Create new Use existing

Public IP address name *

gateway-IP 

Public IP address SKU

Standard

Assignment

Dynamic Static

Availability zone *

Zone-redundant 

Enable active-active mode * 

Enabled Disabled

Configure BGP * 

Enabled Disabled

7. After that move to the review page and create your gateway. Now this will take time at least 30-40 minutes.
8. Below you can see that the deployment is completed.

Microsoft.VirtualNetworkGateway-20240523141549 | Overview

Deployment

Search X < Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

Your deployment is complete

Deployment name : Microsoft.VirtualNetworkGateway-20240523141549
Subscription : Azure Pass - Sponsorship
Resource group : new-grp
Start time : 23/5/2024, 2:18:34 pm
Correlation ID : 20d5c7be-5ad9-4e21-b241-83189643f739

> Deployment details

Next steps

Go to resource

Certificate for Authentication

1. Now you need to go to Virtual Network Gateway and then go to Point to site configuration then click on configure now.

demo-network-gateway | Point-to-site configuration

Virtual network gateway

Search Save Discard Delete Download VPN client

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Configuration Connections

Point-to-site configuration

Point-to-site is not configured
Configure now

2. Now here you have to write a private address pool as shown below and choose the tunnel type as IKEv2, then you have to choose the authentication type as Azure certificate.

Save Discard Delete Download VPN client

Address pool *

 ✓

Tunnel type

 ▼

IPsec / IKE policy

Default Custom

Authentication type

 ▼

Root certificates

Name	Public certificate data
<input type="text"/>	<input type="text"/>

3. Now we need to create a certificate on our local machine or say our laptop. For that, you need to visit the site mentioned below, copy the script, and paste it into your PowerShell.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

4. First, from this website you are going to copy the certificate for root and then the certificate for the child.
5. Below you can see the snapshot of how it will look when you will paste the script.

```

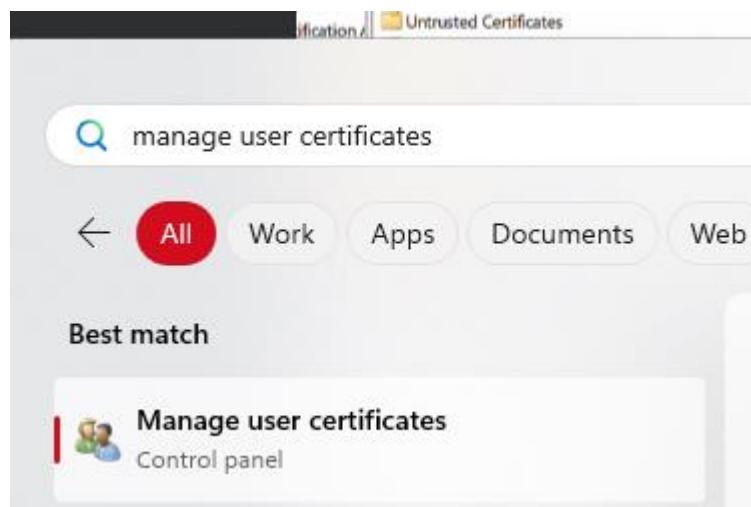
PS C:\Users\PULKIT> $params = @{
>>     Type = 'Custom'
>>     Subject = 'CN=P2SRootCert'
>>    KeySpec = 'Signature'
>>     KeyExportPolicy = 'Exportable'
>>     KeyUsage = 'CertSign'
>>     KeyUsageProperty = 'Sign'
>>     KeyLength = 2048
>>     HashAlgorithm = 'sha256'
>>     NotAfter = (Get-Date).AddMonths(24)
>>     CertStoreLocation = 'Cert:\CurrentUser\My'
>> }
PS C:\Users\PULKIT> $cert = New-SelfSignedCertificate @params
PS C:\Users\PULKIT> $params = @{
>>     Type = 'Custom'
>>     Subject = 'CN=P2SChildCert'
>>     DnsName = 'P2SChildCert'
>>    KeySpec = 'Signature'
>>     KeyExportPolicy = 'Exportable'
>>     KeyLength = 2048
>>     HashAlgorithm = 'sha256'
>>     NotAfter = (Get-Date).AddMonths(18)
>>     CertStoreLocation = 'Cert:\CurrentUser\My'
>>     Signer = $cert
>>     TextExtension = @(
>>         '2.5.29.37={text}1.3.6.1.5.5.7.3.2')
>> )
PS C:\Users\PULKIT>     New-SelfSignedCertificate @params

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

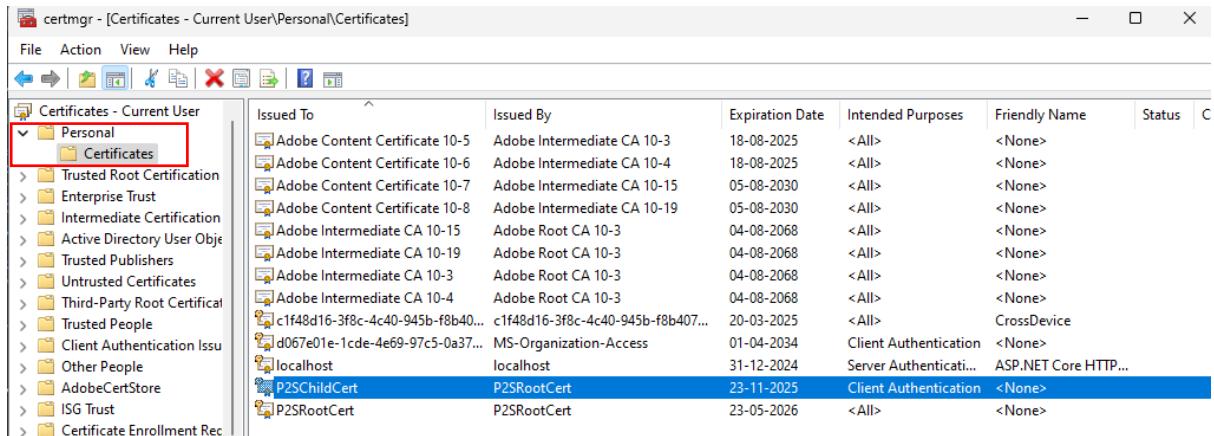
Thumbprint                                Subject
-----                                 -----
CCFB694159E08B8B28696A42A0F463848F0A0A98  CN=P2SChildCert

```

6. If you want to see these certificates then you need to search for manage user certificates on your local machine and open it.



7. There you need to expand personal and then click on certificates. You will see your certificates.



8. We now need to export this root certificate so that we can paste its contents onto our point-to-site VPN connection. I will right-click on the root certificate, choose all tasks, and choose the export option.
9. Follow the below steps to export the root certificate.
- 10. I will right-click on the root certificate, choose all tasks, and choose the export option. In the Wizard I'll click on next. I'll say not to export the private key. Click on next. I'll choose Base64 encoded. Click on Next. I'll just browse, so I'll just save this.**
11. Now we need to copy the data from our root certificate and paste it in Point to site configuration. For that right click on your certificate and choose to open it in notepad.
12. Then you just need to copy the highlighted text as shown below and paste it in point to site configuration.

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIQIS0SAFTQyq10/J6k173ZYDANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDAtQM1NSb290Q2VydDAeFw0yNDA1MjMwOTIwNDlaFw0yNjA1MjMw
OTMwNDdaMBYxFDASBgNVBAMMC1AyU1Jvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQE
AAOCAQ8AMIIBCgKCAQEArA0YOWG2INpwwX1zuQPfdqTk4ZKnKdN5rBnbuHYfBu5uW
3sZFoAT5Ckj1tGVcNkANYARXd8vHNaqNXX0kHyzQ8nuCoroSpN8iYUa6TjJ3XvI8
YDAZ/1k4t4K8WB8apRiJkiuZmuUtBpVz1GJKL/QVkJH311SK3Zms4effwf58oogo
pFCRABRsKC2y0Xzr4Lodp6Zugj2yEdnPXxbj0W/z5zSVmgZ5fH14RNRR6b/R6sLv
COSCKD9tqSuQ204+xcQzjHIwT8XEJeBuVmRz3NHUG40bCJgs1TxDtT3uVssJxsPc
A0ppS/rh0MV50QTXXLa2JzDs1xMGsIHdGAE2MJAAQIDAQABzEwLzA0BgNVHQ8B
Af8EBAMCAgQwHQYDVR00BBYEFheZJiar0I+oYJiV7PmhFU8Q+SJMA0GCSqGSIb3
DQEBCwUA4IBAQAGID1evsZ22QXkgqiN4YnMw4/0MTMxS1010ko0W90r8oZq+C2U
ZC042JKmJX19X/00Je5NGia1Wgo3e1DrL+Vph31Tw3SFqvCStqf4uvN+5HiS4PVX
6gpxjNGajwSpKgmmjrS35ExyYxtu/FTgYLZkEOe1PH44DA+cqZ8psbLkjie0WZr
e/kA5w8WIISTYQEZZJ7xDuLRd1SWSKcacqNT9vic+rDCiBQDA0bhDbGboXCL+A
CtYjLZ/1hbFYwAjR87uV6qkwL30WZUtJi44epEVwccbS8hI2zgUsTRVMAROUro4o
CH9rjex2cRCxKLnvvmfybS01YUg0udBNbrzX/
-----END CERTIFICATE-----
```

13. after that just click on save.

The screenshot shows the 'Root certificates' section of the Azure portal. Under 'Name', there is a field containing 'rootcertificate' with a green checkmark icon. To its right is a 'Public certificate data' field containing a long string of characters: 'MIIC5zCCAc+gAwIBAgIQIS0SAFTQyqI0/J6kl73ZYDANBgkqhkiG9w0B...'. Below these fields are two empty text input boxes. At the bottom right of the certificate row are three icons: a trash can, a three-dot ellipsis, and a copy symbol.

14. Once your connection is saved you will get the option to download the VPN client.
You will see that a zip file has been downloaded and you have to extract it.

The screenshot shows the 'Point-to-site configuration' page for a 'demo-network-gateway'. The top navigation bar includes 'Save', 'Discard', 'Delete', and 'Download VPN client'. The 'Address pool' field contains '172.16.0.0/16' with a green checkmark icon. The left sidebar lists 'Overview', 'Activity log', and 'Access control (IAM)'. The main content area displays the configuration settings.

15. You will see that there are different installers in place here we have to choose Windows AMD 64.

📁 Generic	23-05-2024 15:22	File folder
📁 WindowsAmd64	23-05-2024 15:22	File folder
📁 WindowsPowershell	23-05-2024 15:22	File folder
📁 WindowsX86	23-05-2024 15:22	File folder

16. Then you have to install it. After that you have to search for VPN settings.

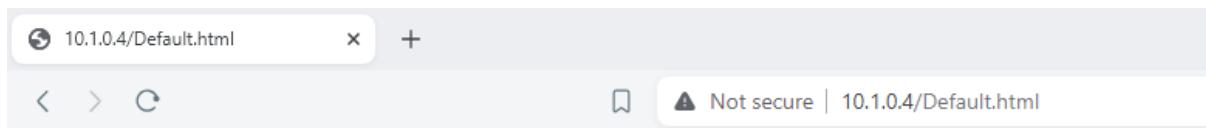
The screenshot shows the Windows Start menu search results for 'vpn settings'. The search bar at the top contains 'vpn settings'. Below it, a list of results is shown under 'Best match'. The first result is 'VPN settings' with a shield icon, followed by 'System settings'. The 'All' button in the search interface is highlighted with a red circle.

17. Here you will see that you have the option to connect with it. Click on connect.

Network & internet > VPN

The screenshot shows the Windows Control Panel under 'Network & internet'. In the 'VPN' section, there is a list of connections. One connection is named 'demo-VN' and is currently 'Not connected'. To its right is a 'Connect' button and a dropdown arrow. At the top right of the list area is a red 'Add VPN' button.

18. Then you have to go to your VM and copy the Private IP address because we don't have the public IP.
19. You will see that your Web Server is running as expected.



This is DemoVM Server

20. You are connecting via the private IP address of the machine, and this is all being done. The traffic is all being routed via the virtual network Gateway.
21. Once you are done with this lab do not delete the resources.