

CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Harsh Tongariya

College: Arya College of Engineering Information Technology

Domain: Cloud Infra & Security

Student ID: CT\_CSI\_CI\_1160

**Research & Development Document**

Title: How to setup Point to Site

**1. Objective**

The objective of this document is to demonstrate the implementation of a secure, scalable, and cost-effective Point-to-Site (P2S) Virtual Private Network (VPN) in Microsoft Azure. A P2S VPN enables remote client devices to connect to Azure Virtual Networks from any internet-connected location without requiring complex hardware-based solutions.

**2. Overview of Point-to-Site VPN**

A Point-to-Site VPN allows individual clients (like laptops or personal devices) to securely connect to an Azure Virtual Network (VNet) over the internet. It uses secure encryption protocols such as:

* OpenVPN (cross-platform, highly secure)
* SSTP (uses HTTPS for firewall-friendly access)
* IKEv2 (secure, modern, and efficient)

Use Cases

* Secure remote access for developers and administrators
* Connectivity to internal services during work-from-home scenarios
* Remote troubleshooting or testing

**3. Prerequisites**

|  |  |
| --- | --- |
| Requirement | Description |
| Azure Subscription | Required to deploy all resources |
| Virtual Network (VNet) | Logical network to which the VPN will connect |
| VPN Gateway | Handles encrypted VPN traffic |
| Public IP Address | For the VPN Gateway |
| Client Machine | Windows/macOS/Linux with VPN client |
| Certificates (Optional) | Used for authentication in some tunnel types |

**4. Supported Authentication Methods**

Azure supports three authentication types for P2S:

1. Azure Certificate Authentication
   * Upload a trusted root certificate to Azure
   * Generate and install client certificates on remote devices
2. Azure Active Directory (Azure AD)
   * Authenticate clients through Azure AD (supported with OpenVPN protocol only)
3. RADIUS Authentication
   * Uses an on-premises RADIUS server for validation

**5. Implementation: Step-by-Step Setup Using Azure Portal**

Step 1: Create a Virtual Network (VNet)

* Navigate to: Azure Portal → Virtual Networks → + Create
* Input the following:
  + Name: MyVNet
  + Address Space: 10.1.0.0/16
  + Subnet: 10.1.0.0/24

Step 2: Add Gateway Subnet

* Navigate to your created VNet → Subnets → + Gateway Subnet
* Define address prefix: 10.1.1.0/24

Step 3: Create a Public IP Address

* Go to: Public IP Addresses → + Create
* Set:
  + Name: MyVpnPublicIP
  + SKU: Standard
  + Assignment: Static or Dynamic (based on needs)

Step 4: Deploy the VPN Gateway

* Navigate to: VPN Gateways → + Create
* Set:
  + Name: MyVpnGateway
  + Region: Same as VNet
  + Gateway type: VPN
  + VPN type: Route-based
  + SKU: VpnGw1 or higher
  + Virtual Network: Select your MyVNet
  + Public IP: Select MyVpnPublicIP

Note: Deployment may take 30–45 minutes.

Step 5: Configure Point-to-Site VPN on the Gateway

* Navigate to: MyVpnGateway → Point-to-site configuration → Configure now
* Address Pool: 172.16.0.0/24
* Tunnel Type: Choose OpenVPN, IKEv2, or SSTP
* Authentication Type:
  + Upload root certificate (Certificate authentication)
  + OR Configure Azure AD
* Save the configuration

Step 6: Download and Install VPN Client

* After configuration, download the VPN client package for your OS (Windows/macOS/Linux)
* Install and configure using default options

Step 7: Connect to the Azure Network

* Launch the installed VPN client
* Connect using the profile
* Verify connection via:
  + ipconfig to confirm the client IP from the VPN pool
  + Ping internal Azure VMs or services

**6. Validation and Monitoring**

* Use Azure Portal to check active VPN connections (under VPN Gateway → Monitoring)
* Monitor logs and metrics via Azure Monitor or Network Watcher
* Use PowerShell or Azure CLI for script-based verification (optional)

**7. Security Considerations**

* Regularly rotate certificates
* Apply NSGs to limit traffic only to required ports/IPs
* Use Conditional Access with Azure AD for tighter control
* Enable diagnostics logging for audit trails

8**. Troubleshooting Guidelines**

|  |  |
| --- | --- |
| Problem | Resolution |
| VPN connection fails | Ensure public IP is reachable, check ports |
| Certificate not trusted | Verify certificate chain on client device |
| Authentication errors | Revalidate Azure AD or certificate configuration |
| Cannot access VNet resources | Check NSG rules and effective routes |

9. References

* https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-certificate-gateway
* [Azure VPN Gateway: Point-to-Site Overview](https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about)
* [Azure CLI Documentation](https://learn.microsoft.com/en-us/cli/azure/network/vpn-gateway)
* [Certificates for P2S](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site)