R&D Document: VPN Connectivity - Point-to-Site and Site-to-Site Setup on Azure

Name: Sanskar Vishnoi
Batch: Celebal Summer Internship Batch 2
Date: 22nd July 2025

---

1. Overview

Secure site-to-site and point-to-site VPN connections allow organizations to connect Azure virtual networks with on-premises infrastructure or individual remote clients. This document explains detailed procedures and configurations for:

- Point-to-Site (P2S) VPN setup
- Site-to-Site (S2S) VPN setup using Hyper-V

---

2. Point-to-Site VPN (P2S)

Point-to-Site connections are useful for developers or individual users needing secure access to Azure VMs from remote locations without setting up a full VPN device.

2.1 Requirements

- Azure Virtual Network (VNet)
- VPN Gateway
- Self-signed or Root certificate (for Windows clients)
- VPN client configuration package

2.2 Step-by-Step Setup

Step 1: Create a Virtual Network (VNet)

- Navigate to Azure Portal → Virtual Networks → Create
- Define address space (e.g., 10.1.0.0/16) and subnet (e.g., 10.1.0.0/24)

Step 2: Create a Gateway Subnet

- Within the VNet, create a new subnet named “GatewaySubnet”.
- Suggested range: 10.1.255.0/27

Step 3: Create VPN Gateway

- Go to Azure Portal → VPN Gateway → Create
- Choose Region, Virtual Network, Public IP, SKU (e.g., VpnGw1)

- Wait 30-45 mins for provisioning

Step 4: Generate a Root Certificate

- Use PowerShell or makecert tool to generate a root certificate
- Upload public key (.cer) in VPN Gateway → Point-to-site configuration

Step 5: Configure Point-to-Site Settings

- Set IP address pool (e.g., 172.16.201.0/24)
- Choose tunnel type (IKEv2, SSTP, or OpenVPN)
- Add authentication type (Azure certificate or Azure AD)

Step 6: Download VPN Client Package

- From VPN Gateway → Point-to-site → Download VPN client
- Install and connect VPN client on user machine

Step 7: Verify Connectivity

- Connect using VPN client
- Ping internal resources (Azure VM private IP)

2.3 Use Cases

- Developers connecting remotely to VMs
- Temporary or low-scale secure access

---

3. Site-to-Site VPN (S2S) with Hyper-V

Site-to-Site VPN allows a secure connection between your on-premises infrastructure and Azure over IPsec/IKE VPN tunnels.

3.1 Requirements

- On-premises VPN device or Windows Server with RRAS (Hyper-V)
- Azure Virtual Network with GatewaySubnet
- Static public IP address for on-premises gateway

3.2 Setup on Azure Side

Step 1: Create Virtual Network and GatewaySubnet

- Same steps as in P2S

Step 2: Create VPN Gateway

- VPN type: Route-based

- SKU: VpnGw1 or higher

Step 3: Create Local Network Gateway

- Define on-premises public IP
- Address space of on-prem network (e.g., 192.168.0.0/16)

Step 4: Create VPN Connection

- Go to Connections → Add
- Select virtual network gateway and local network gateway
- Provide shared key (must match Hyper-V configuration)

3.3 Setup on On-Premises (Hyper-V)

Step 1: Enable RRAS Role

- Use Windows Server Manager → Add Roles → Select Remote Access
- Install Routing and Remote Access Services (RRAS)

Step 2: Configure RRAS

- Open RRAS → Configure and Enable Routing and Remote Access
- Choose "Secure connection between two private networks"

Step 3: Create Demand-Dial Interface

- Name: AzureS2S
- Connection type: VPN → IKEv2/IPSec
- Enter Azure VPN Gateway Public IP
- Use pre-shared key
- Add static routes to Azure network (e.g., 10.1.0.0/16)

Step 4: Add Static Route

```
route add 10.1.0.0 mask 255.255.0.0 <RRAS internal interface IP>
```

Step 5: Enable NAT (if needed)

- Configure NAT for internet-bound traffic from Azure if required

Step 6: Verify Tunnel Status

- Ping Azure VM from on-premises machine
- Use Azure Portal to check tunnel connectivity

3.4 Use Cases

- Permanent hybrid connectivity

- Secure communication between Azure and branch offices

---

4. Key Considerations

Feature	**Point-to-Site (P2S)**	**Site-to-Site (S2S)**
Use case	Developer remote access	Branch-office to Azure
Setup complexity	Low	Medium to High
Hardware required	No	Yes (or Hyper-V RRAS)
Max clients supported	Up to 128 (depends on SKU)	Depends on VPN gateway
Authentication	Certificate/Azure AD	Pre-shared key

---

5. Summary

Both Point-to-Site and Site-to-Site VPN configurations allow secure data flow between Azure and remote entities. While P2S is best suited for developer and remote user scenarios, S2S is ideal for enterprise-wide network integration.