R&D Report on VPN Connectivity in Azure: Point-to-Site (P2S) and Site-to-Site (S2S) using Hyper-V

Prepared by:
Virat Pandey

Celebal Technology
Cloud Infrastructure & Security Internship

Research & Development Document

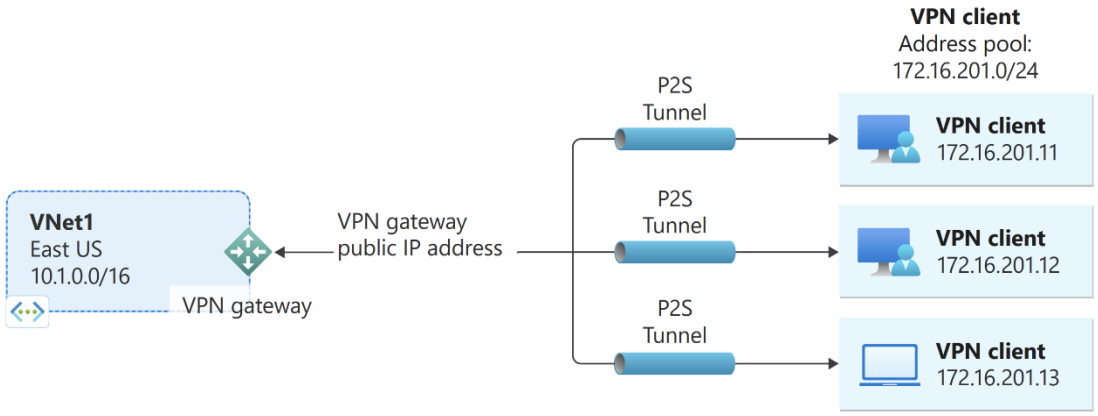
July, 2025

Table of Contents

Introduction

A Point-to-Site (P2S) VPN allows individual devices such as laptops or desktops to securely connect to an Azure Virtual Network from a remote location. Unlike Site-to-Site VPNs, which connect entire networks, P2S is ideal for single-user connectivity—typically used by developers or admins who need secure remote access to Azure resources without setting up entire network infrastructure.

Point-to-Site VPNs are easy to configure, require no on-premises hardware, and provide encryption to ensure secure communication over the internet.



Common Use Cases:

- **Remote Workforce:** Allowing employees working from home or traveling to securely access internal applications and data.
- **Small Branch Offices:** Providing a simple, low-cost solution for a few users in a satellite office to connect to the main corporate network.
- **Secure Management:** Enabling administrators to securely manage cloud resources without exposing management ports to the public internet.

Prerequisites

Before setting up a Point-to-Site VPN, certain Azure components and settings must be in place to ensure successful configuration. Below are the essential prerequisites:

1. **Azure Subscription**
   – A valid and active Azure subscription to provision and manage resources.
2. **Virtual Network (VNet)**
   – Create a Virtual Network (VNet) where the VPN gateway will be associated.
   – Ensure at least one subnet is available for communication.
3. **Gateway Subnet**
   – A special subnet named Gateway Subnet must be created within your VNet.
   – It is required for the VPN Gateway to function properly.
4. **Virtual Network Gateway**
   – A VPN gateway must be created.
   – Type: VPN
   – VPN type: Route-based (required for Point-to-Site).
5. **Public IP Address**
   – Required for the VPN Gateway to allow external clients to connect.
6. **Client Address Pool**
   – A set of IP addresses (e.g., 172.16.201.0/24) that will be assigned to VPN clients when they connect.
7. **Authentication Type**
   – Azure certificate authentication (upload client certificate)
   – OR Azure Active Directory authentication (for enterprise setup)
8. **Root Certificate (for cert-based auth)**
   – A root certificate must be generated and uploaded to Azure.
   – Client certificates are derived from the root for individual device connections.

Step-by-Step Setup Guide to Configure Point-to-Site VPN in Azure