**R&D Document on How to Set Up Point-to-Site (P2S) VPN in Azure**

**Introduction**

This document provides a detailed guide on setting up a Point-to-Site (P2S) VPN in Azure. P2S VPN allows individual clients to connect to your Azure Virtual Network (VNet) from anywhere.

**Objective**

To enable secure, encrypted communication between individual clients and the Azure Virtual Network.

**Prerequisites**

* An Azure subscription
* A Virtual Network (VNet) already created in Azure
* A Virtual Network Gateway

**Steps to Set Up Point-to-Site VPN**

**Step 1: Create a Virtual Network Gateway**

1. **Navigate to the Azure Portal**.
2. **Create a Virtual Network Gateway**:
   * Go to "Create a resource" and search for "Virtual Network Gateway".
   * Click "Create".
   * Configure the settings:
     + Name: VNetGateway
     + Region: Same as your VNet
     + Gateway type: VPN
     + VPN type: Route-based
     + SKU: Select appropriate SKU (e.g., VpnGw1)
     + Virtual network: Select your VNet
     + Public IP address: Create a new public IP address
   * Click "Review + create" and then "Create".

**Step 2: Configure Point-to-Site VPN**

1. **Navigate to the Virtual Network Gateway**:
   * Go to your newly created Virtual Network Gateway.
   * In the settings, select "Point-to-site configuration".
2. **Add Configuration**:
   * Address pool: Define an address range (e.g., 10.2.0.0/24).
   * Tunnel type: Select SSTP (SSL) or OpenVPN (SSL).
   * Authentication type: Azure certificate or RADIUS.
   * Root certificates: If using Azure certificate, upload the root certificate.
   * Click "Save".

**Step 3: Generate and Download VPN Client Configuration**

1. **Generate VPN Client**:
   * In the Point-to-site configuration blade, click "Download VPN client".
   * Select your operating system and download the VPN client package.
2. **Install VPN Client**:
   * Distribute the client package to users.
   * Users install the VPN client on their devices and connect to the VNet.

**Best Practices**

* Use strong, complex passwords for VPN connections.
* Regularly update the root certificates and distribute them to users.
* Monitor VPN connections for unusual activity.

**Troubleshooting**

* **Connection Issues**: Check the VPN client configuration and ensure the address pool does not overlap with other network ranges.
* **Authentication Issues**: Ensure that certificates are correctly installed and not expired.

**Conclusion**

Setting up a Point-to-Site VPN in Azure enables secure connections for remote users to access resources within a VNet. Following the steps and best practices outlined ensures a robust and secure configuration.

**R&D Document on How to Set Up Site-to-Site VPN using Hyper-V**

**Introduction**

This document provides a detailed guide on setting up a Site-to-Site (S2S) VPN using Hyper-V. S2S VPN allows entire networks to connect securely over the internet.

**Objective**

To establish a secure, encrypted connection between an on-premises network and an Azure Virtual Network (VNet) using Hyper-V.

**Prerequisites**

* An Azure subscription
* A Virtual Network (VNet) already created in Azure
* A Virtual Network Gateway
* Hyper-V installed on your on-premises server
* Public IP address for on-premises VPN device

**Steps to Set Up Site-to-Site VPN using Hyper-V**

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

1. **Navigate to the Azure Portal**.
2. **Create a Virtual Network Gateway**:
   * Go to "Create a resource" and search for "Virtual Network Gateway".
   * Click "Create".
   * Configure the settings:
     + Name: VNetGateway
     + Region: Same as your VNet
     + Gateway type: VPN
     + VPN type: Route-based
     + SKU: Select appropriate SKU (e.g., VpnGw1)
     + Virtual network: Select your VNet
     + Public IP address: Create a new public IP address
   * Click "Review + create" and then "Create".

**Step 2: Configure Local Network Gateway**

1. **Create Local Network Gateway**:
   * Go to "Create a resource" and search for "Local Network Gateway".
   * Click "Create".
   * Configure the settings:
     + Name: OnPremGateway
     + IP address: Public IP address of your on-premises VPN device
     + Address space: On-premises network range (e.g., 192.168.1.0/24)
   * Click "Create".

**Step 3: Create a VPN Connection**

1. **Create VPN Connection**:
   * Navigate to your Virtual Network Gateway.
   * Click on "Connections" and then "Add".
   * Configure the settings:
     + Name: S2SConnection
     + Connection type: Site-to-site (IPSec)
     + Virtual network gateway: Select your VNet gateway
     + Local network gateway: Select your on-premises gateway
     + Shared key: Enter a shared key (must match the key on the on-premises VPN device)
   * Click "OK".

**Step 4: Configure Hyper-V for VPN**

1. **Set Up Hyper-V Server**:
   * Ensure Hyper-V is installed and configured on your on-premises server.
2. **Install Routing and Remote Access Role**:
   * Open Server Manager and add the Routing and Remote Access role.
   * Configure Routing and Remote Access:
     + Open Routing and Remote Access Management Console.
     + Right-click the server and select "Configure and Enable Routing and Remote Access".
     + Choose "Custom configuration" and select "VPN access" and "NAT".
     + Complete the wizard and start the service.

**Step 5: Configure VPN Connection in Hyper-V**

1. **Configure VPN Device**:
   * Open the Hyper-V Manager.
   * Connect to your virtual machine (VPN server).
   * Open Routing and Remote Access Management Console.
   * Right-click on your server and select "Properties".
   * Go to the "Security" tab and configure VPN settings to match Azure's configuration.
   * Go to the "IP" tab and configure the IP range for VPN clients.
2. **Establish Connection**:
   * Ensure the shared key matches the one configured in Azure.
   * Configure firewall rules to allow VPN traffic.

**Best Practices**

* Use strong encryption methods and complex keys.
* Regularly monitor VPN connections and logs.
* Keep Hyper-V and VPN device software up to date.

**Troubleshooting**

* **Connection Issues**: Verify the shared key and ensure the public IP addresses are correctly configured.
* **Performance Issues**: Check the network bandwidth and ensure the Hyper-V server has sufficient resources.

**Conclusion**

Setting up a Site-to-Site VPN using Hyper-V enables secure, encrypted communication between an on-premises network and an Azure VNet. Following the detailed steps ensures a reliable and secure connection.