1. **Prepare R&D Document on How to setup Site to Site using Hyper-V**

**Ans:**

* **Introduction**

A Site-to-Site VPN allows offices in multiple fixed locations to establish secure connections with each other over the Internet. This document provides a step-by-step guide to setting up a Site-to-Site VPN using Hyper-V, a virtualization platform by Microsoft.

* **Prerequisites**

1. An active Azure subscription.
2. - Administrative access to Azure and on-premises networks.
3. - Public IP addresses for each site.
4. - VPN-compatible routers or firewalls at each site.
5. - Basic understanding of networking concepts.

* **Setting Up Virtual Network in Azure**

**Log in to Azure Portal:**

1. Go to the [Azure Portal] .
2. Create a Virtual Network:
3. Navigate to "Create a resource" > "Networking" > "Virtual Network".
4. Fill in the required details: name, address space, resource group, and location.
5. Click "Create".

* **Add Subnets:**

1. After the Virtual Network is created, go to "Subnets".
2. Click "Add Subnet" and define the subnet name and address range.

* **Setting Up Virtual Network Gateway**
* Creating the Gateway
  1. Create a Virtual Network Gateway:
  2. Navigate to "Create a resource" > "Networking" > "Virtual Network Gateway".
  3. Fill in the required details:
  4. Name: Enter a name for the gateway.
  5. Gateway type: Select "VPN".
  6. VPN type: Select "Route-based".
  7. SKU: Choose the appropriate SKU based on your needs.
  8. Virtual network: Select the virtual network created earlier.
  9. Public IP address: Create a new public IP address for the gateway.
* **Configuring On-Premises VPN Device**

1. Supported Devices
2. Ensure that your on-premises VPN device is compatible with Azure VPN Gateway. Refer to the [list of supported VPN devices and IPsec/IKE parameters].
3. Download Configuration Script:
4. After the gateway is created, download the configuration script for your specific VPN device from the Azure portal.

* **Configure the VPN Device:**

1. Use the downloaded script to configure your on-premises VPN device.
2. Ensure that the device has the correct public IP and is set to connect to the Azure VPN gateway.

* **Creating Local Network Gateway**

1. Create a Local Network Gateway:
2. Navigate to "Create a resource" > "Networking" > "Local Network Gateway".
3. Fill in the required details:
4. Name: Enter a name for the local network gateway.
5. IP address: Enter the public IP address of the on-premises VPN device.
6. Address space: Enter the address space of the on-premises network.

**Create the Local Network Gateway:**

1. Click "Review + create".
2. Click "Create".

* **Connecting the VPN Gateways**
  1. Create a VPN Connection: Navigate to the Virtual Network Gateway.
     1. Navigate to the Virtual Network Gateway.
     2. Fill in the required details:
     3. Name: Enter a name for the connection.
     4. Connection type: Select "Site-to-site (IPSec)".
     5. Virtual network gateway: Select your virtual network gateway.
     6. Local network gateway: Select the local network gateway created earlier.
     7. Shared key (PSK): Enter a shared key for the connection (must match the key configured on the on-premises VPN device).

**2. Create the Connection:**

1. Click "OK" to create the connection.

* **Verifying the Connection**

1. Verify Connection Status:

* + 1. In the Azure portal, navigate to the Virtual Network Gateway.
    2. Click "Connections" to view the status of the VPN connection.
    3. Ensure that the connection status is "Connected".
* Testing the VPN Connection

1. Ping Test:

From an on-premises machine, use the ping command to test connectivity to a resource in the Azure virtual network.

2. Access Resources:

Verify that you can access resources in the Azure virtual network from the on-premises network and vice versa.

* **Troubleshooting**
  1. Common Issues:

1. Incorrect IP addresses or shared key.
2. Firewall settings blocking VPN traffic.
3. Misconfiguration of network settings.

2. Logs and Diagnostics:

* + 1. Use Azure Network Watcher for diagnostic tools.
    2. Check logs on the on-premises VPN device for errors.
* **Conclusion**

Setting up a Site-to-Site VPN using Azure involves configuring virtual network gateways, local network gateways, and VPN connections. This document provides a comprehensive guide to achieving a secure and reliable connection between Azure and on-premises networks.