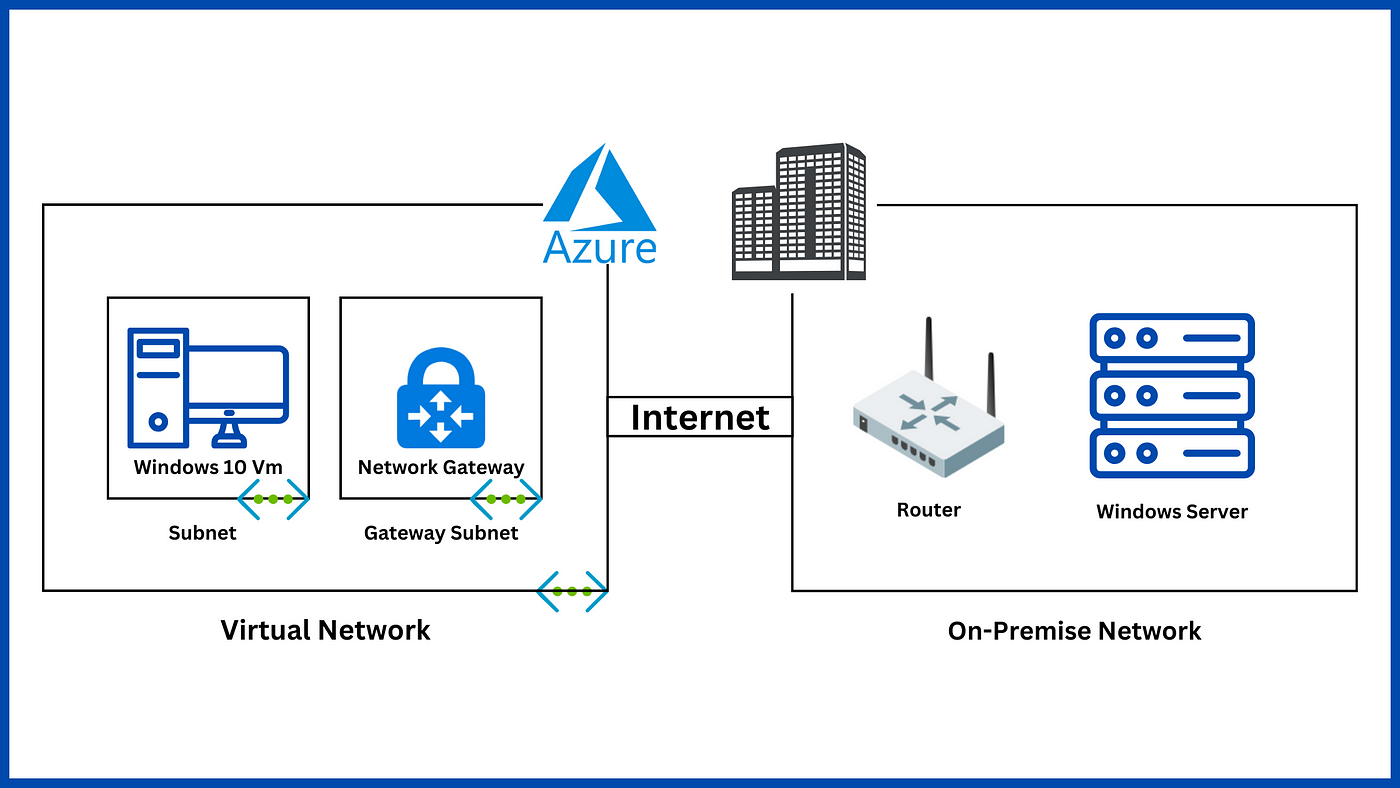
**Question 1: Your organization needs to set up a secure site-to-site VPN connection between the on-premises network and Azure. Explain the steps to achieve this using RRAS on the on-premises side and an Azure VPN gateway.**

ANS: **Step 1: Configure Azure Virtual Network and VPN Gateway**

1. Log in to the Azure portal.
2. Go to "Create a resource" > "Networking" > "Virtual Network".
3. Enter the necessary details like name, address space, resource group, and region.
4. Click "Create".
5. Create a Virtual Network Gateway:
6. In the Azure portal, go to "Create a resource" > "Networking" > "Virtual Network Gateway".
7. Enter details:
8. Name: Choose a name for the gateway.
9. Gateway type: Select "VPN".
10. VPN type: Select "Route-based".
11. SKU: Select an appropriate SKU (e.g., VpnGw1).
12. Virtual network: Select the virtual network created earlier.
13. Public IP address: Create a new public IP address.
14. Click "Review + create" and then "Create". Note that this process can take up to 45 minutes.

**Step 2: Configure On-Premises RRAS Server**

1. Install and Configure RRAS:
2. On your on-premises server, open Server Manager.
3. Go to "Add roles and features" and install the "Remote Access" role.
4. After installation, open the "Routing and Remote Access" console.
5. Right-click the server name and select "Configure and Enable Routing and Remote Access".
6. Choose "Custom configuration", then select "VPN access and NAT", and complete the wizard.
7. Configure VPN in RRAS:
8. In the "Routing and Remote Access" console, right-click the server name and select "Properties".
9. Go to the "Security" tab and configure the preshared key for IPsec (must match the shared key you will set in Azure).
10. Set Up Demand-Dial Interface:
11. In the "Routing and Remote Access" console, expand the server name, right-click "Network Interfaces", and select "New Demand-Dial Interface".
12. Follow the wizard, entering the name for the interface, the public IP address of the Azure VPN gateway, and other relevant details.

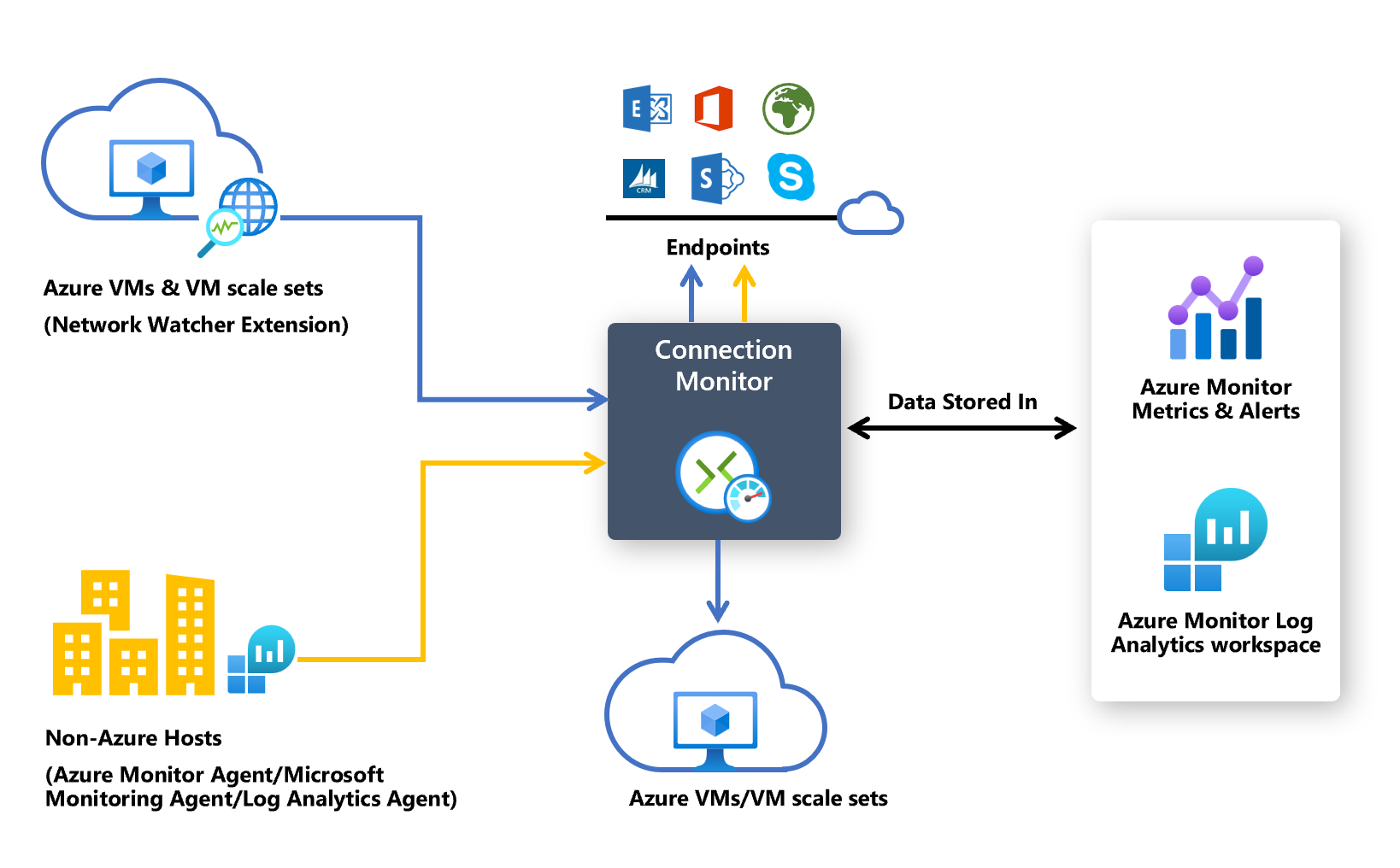


**Step 3: Create Local Network Gateway in Azure**

1. Create a Local Network Gateway:
2. In the Azure portal, go to "Create a resource" > "Networking" > "Local Network Gateway".
3. Enter details:
4. Name: Choose a name for the local network gateway.
5. IP address: Enter the public IP address of the on-premises RRAS server.
6. Address space: Enter the address space of the on-premises network.
7. Click "Create".

**Step 4: Create Site-to-Site VPN Connection**

1. Create the Connection:
2. In the Azure portal, navigate to the Virtual Network Gateway created earlier.
3. Click on "Connections" and then "Add".
4. Enter details:
5. Name: Enter a name for the connection.
6. Connection type: Select "Site-to-site (IPSec)".
7. Virtual network gateway: Select your Azure virtual network gateway.
8. Local network gateway: Select the local network gateway created earlier.
9. Shared key (PSK): Enter the preshared key (must match the key set in RRAS).
10. Click "OK" to create the connection.



**Step 5: Configure Firewall and Routing**

1. Configure Firewalls:
2. Ensure that firewalls on both sides (Azure and on-premises) allow VPN traffic (UDP ports 500 and 4500 for IPsec).
3. Add Static Routes:
4. On the RRAS server, add static routes to route traffic to the Azure network via the VPN connection.
5. In the "Routing and Remote Access" console, right-click "Static Routes" under "IPv4" and add routes to the Azure address space.

**Step 6: Verify and Test the VPN Connection**

1. Verify Connection in Azure:
2. In the Azure portal, go to the Virtual Network Gateway and check the status of the VPN connection. It should show as "Connected".
3. Test Connectivity:
4. From an on-premises machine, ping a resource in the Azure virtual network to ensure connectivity.
5. Verify that resources on both sides of the VPN can communicate as expected.

**Troubleshooting**

**Common Issues:**

1. Verify IP addresses and preshared key.
2. Check firewall rules and ensure that necessary ports are open.
3. Ensure correct network routing on both the Azure and on-premises sides.

**Logs and Diagnostics:**

1. Use Azure Network Watcher for diagnostic tools to check VPN connection status and troubleshoot issues.
2. Check the RRAS logs and event viewer on the on-premises server for errors.