Create three subnets : 1. Web tier 2. App tier 3. DB tier DB Tier should not access any tier(Web & App tier) App tier should access the DB tier and Web tier as well, Web tier should acccess only App tier. Only Web tier is allowed to connect to the internet.Deploy two VM's in each tier(One VM should be Linux & another should be Windows). Configure Apache Server on Linux VM's And IIS Server on Windows.

Step 1: Set Up Your Azure Environment

1. **Log in to Azure Portal**:

   - Go to [Azure Portal](https://portal.azure.com).

   - Enter your credentials to log in.

2. **Create a Resource Group**:

   - In the left sidebar, click on "Resource groups".

   - Click "Create".

   - Fill in the details:

     - **Subscription**: Select your subscription.

     - **Resource group**: Enter a name, e.g., `MyResourceGroup`.

     - **Region**: Select your desired region.

   - Click "Review + create" and then "Create".

Step 2: Create a Virtual Network (VNet) and Subnets

1. **Create a Virtual Network**:

   - In the left sidebar, click on "Virtual networks".

   - Click "Create".

   - Fill in the details:

     - **Subscription**: Select your subscription.

     - **Resource group**: Select the resource group you created earlier.

     - **Name**: Enter a name, e.g., `MyVNet`.

     - **Region**: Select the same region as your resource group.

   - Click "Next: IP Addresses".

2. **Add Subnets**:

   - Under the "IP Addresses" tab, click "+ Add subnet".

     - **Subnet name**: `WebSubnet`

     - **Subnet address range**: `10.0.1.0/24`

   - Click "+ Add subnet" again and repeat for:

     - **Subnet name**: `AppSubnet`

     - **Subnet address range**: `10.0.2.0/24`

   - Click "+ Add subnet" again and repeat for:

     - **Subnet name**: `DBSubnet`

     - **Subnet address range**: `10.0.3.0/24`

   - Click "Review + create" and then "Create".

Step 3: Create Network Security Groups (NSGs)

1. **Create NSG for Web Tier**:

   - In the left sidebar, click on "Network security groups".

   - Click "Create".

   - Fill in the details:

     - **Subscription**: Select your subscription.

     - **Resource group**: Select your resource group.

     - **Name**: Enter `WebNSG`.

     - **Region**: Select the same region.

   - Click "Review + create" and then "Create".

2. **Create NSG for App Tier**:

   - Repeat the above steps to create an NSG named `AppNSG`.

3. **Create NSG for DB Tier**:

   - Repeat the above steps to create an NSG named `DBNSG`.

Step 4: Configure Network Security Group Rules

1. **Web Tier NSG Rules**:

   - Navigate to "Network security groups" and select `WebNSG`.

   - Under "Settings", click on "Inbound security rules".

   - Click "Add".

     - **Source**: `Any`

     - **Source port ranges**: `*`

     - **Destination**: `Any`

     - **Destination port ranges**: `80, 443`

     - **Protocol**: `TCP`

     - **Action**: `Allow`

   - Click "Add".

2. **App Tier NSG Rules**:

   - Select `AppNSG`.

   - Under "Settings", click on "Inbound security rules".

   - Click "Add".

     - **Source**: `VirtualNetwork`

     - **Source port ranges**: `*`

     - **Destination**: `Any`

     - **Destination port ranges**: `*`

     - **Protocol**: `TCP`

     - **Action**: `Allow`

   - Click "Add".

3. **DB Tier NSG Rules**:

   - Select `DBNSG`.

   - Under "Settings", click on "Inbound security rules".

   - Click "Add".

     - **Source**: `VirtualNetwork`

- **Source port ranges**: `*`

    - **Destination**: `Any`

    - **Destination port ranges**: `*`

    - **Protocol**: `TCP`

    - **Action**: `Allow`

  - Click "Add".

Step 5: Create Virtual Machines (VMs)

1. **Web Tier VMs**:

  - Create a Linux VM:

    - In the left sidebar, click on "Virtual machines".

    - Click "Create" and select "Azure virtual machine".

    - Fill in the details:

      - **Subscription**: Select your subscription.

      - **Resource group**: Select your resource group.

      - **Virtual machine name**: Enter `WebLinuxVM`.

      - **Region**: Select your region.

      - **Image**: Select `Ubuntu Server`.

      - **Size**: Choose an appropriate size (e.g., `Standard_B1s`).

      - **Authentication type**: Choose `SSH public key` and enter your SSH key.

    - Click "Next: Disks", then "Next: Networking".

      - **Virtual network**: Select `MyVNet`.

      - **Subnet**: Select `WebSubnet`.

      - **Public IP**: Select "Create new" and provide a name.

      - **NIC network security group**: Select `None`.

      - **Configure network security group**: Select `WebNSG`.

    - Click "Review + create" and then "Create".

  - Repeat to create a Windows VM in the `WebSubnet` with similar steps.

2. **App Tier VMs**:

   - Create a Linux VM in the `AppSubnet` following the same steps as above.

   - Create a Windows VM in the `AppSubnet` with similar steps.

3. **DB Tier VMs**:

   - Create a Linux VM in the `DBSubnet` following the same steps as above.

   - Create a Windows VM in the `DBSubnet` with similar steps.

Step 6: Configure Internet Access for Web Tier

1. **Create a Public IP Address**:

   - Navigate to "Public IP addresses".

   - Click "Create".

   - Fill in the details:

     - **Subscription**: Select your subscription.

     - **Resource group**: Select your resource group.

     - **Name**: Enter `WebPublicIP`.

     - **SKU**: Select `Standard`.

     - **Assignment**: Select `Static`.

   - Click "Review + create" and then "Create".

Step 7: Configure Apache and IIS Servers

1. **Install Apache on Linux VMs**:

   - SSH into the Linux VM.

   - Run the following commands:

     ```bash
     sudo apt update
     sudo apt install apache2 -y
     sudo systemctl start apache2
     sudo systemctl enable apache2
     ```

- Verify by accessing the public IP of the Linux VM in a browser.

2. **Install IIS on Windows VMs**:

   - RDP into the Windows VM.

   - Open PowerShell as an Administrator and run:

     ```powershell
     Install-WindowsFeature -name Web-Server -IncludeManagementTools
     ```

   - Verify by accessing the public IP of the Windows VM in a browser.

Step 8: Validate the Setup

- Ensure that the Web tier VMs can access the App tier VMs.

- Ensure that the App tier VMs can access the DB tier VMs.

- Ensure that the DB tier VMs cannot access the Web and App tier VMs.

- Ensure only Web tier VMs have internet access.

By following these steps, you will have created a secure, multi-tier network in Azure with the appropriate access controls and server configurations.