Task 1: Set Up Basic Firewall Rules

- **OBJECTIVE**

  Task: Configure firewall settings on a personal computer.
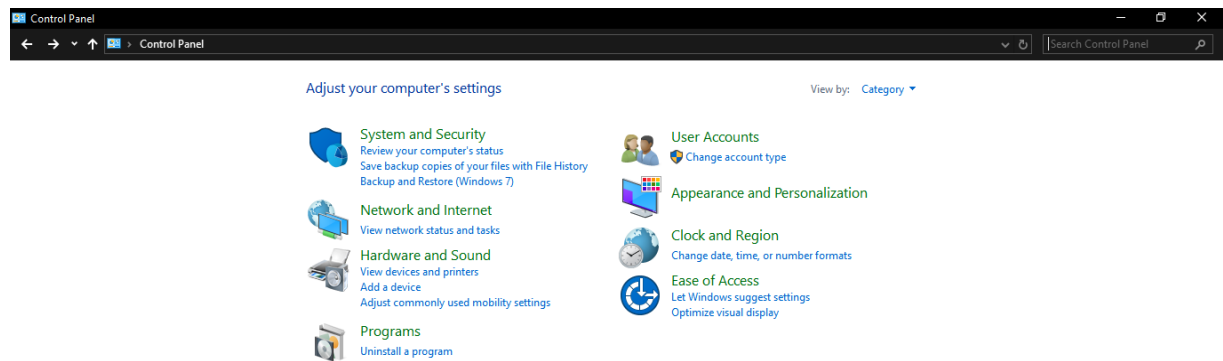
  Details:

  Enable and configure Windows Defender Firewall or a similar firewall.

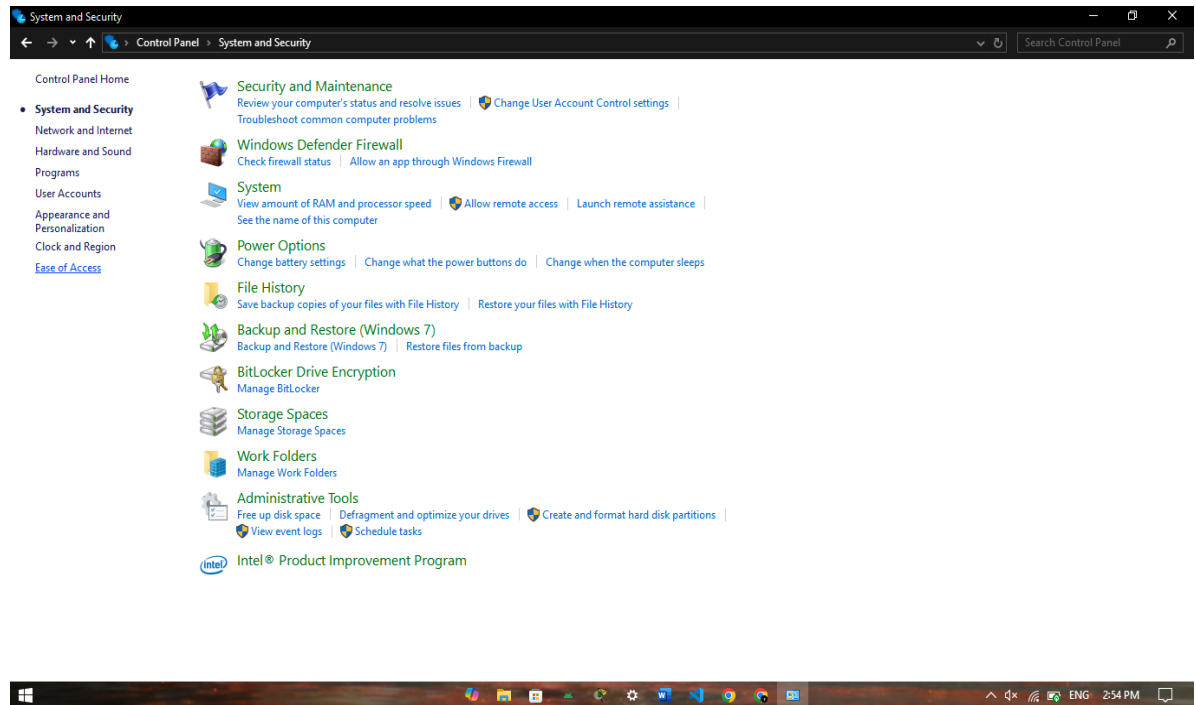 Set rules to block or allow specific applications or ports.

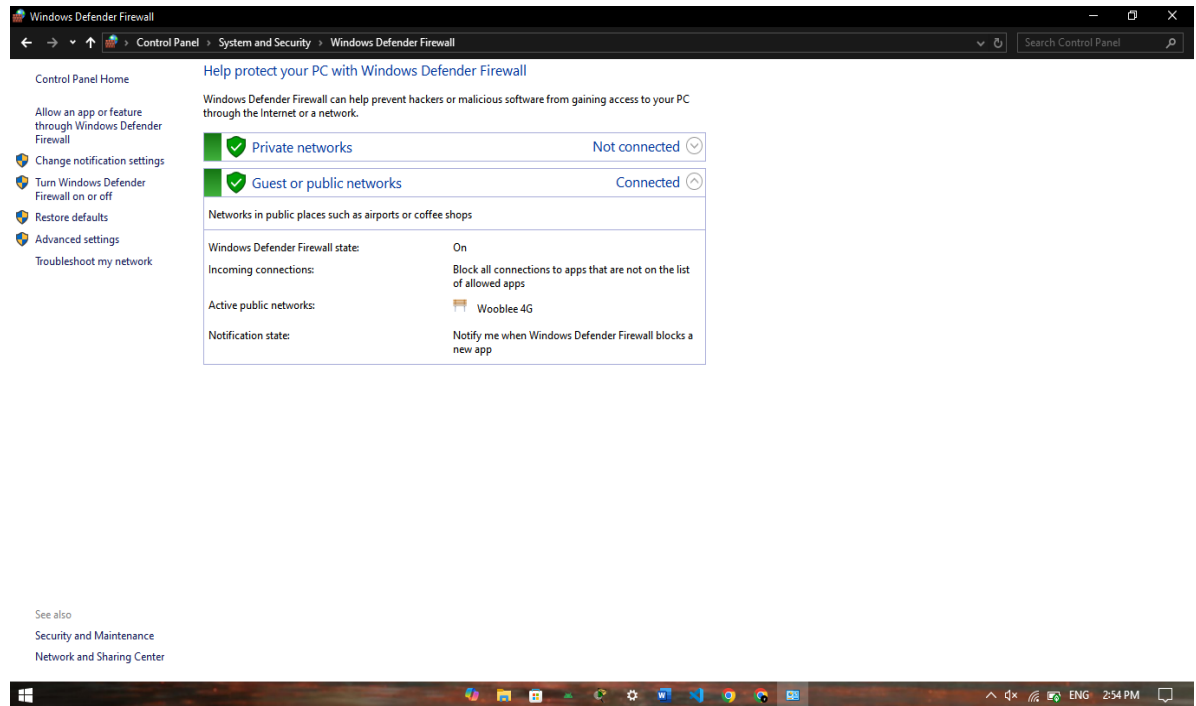- **STEPS**

1. **Open Windows Defender Firewall Settings**:

   o Navigate to the **Control Panel**.

   o

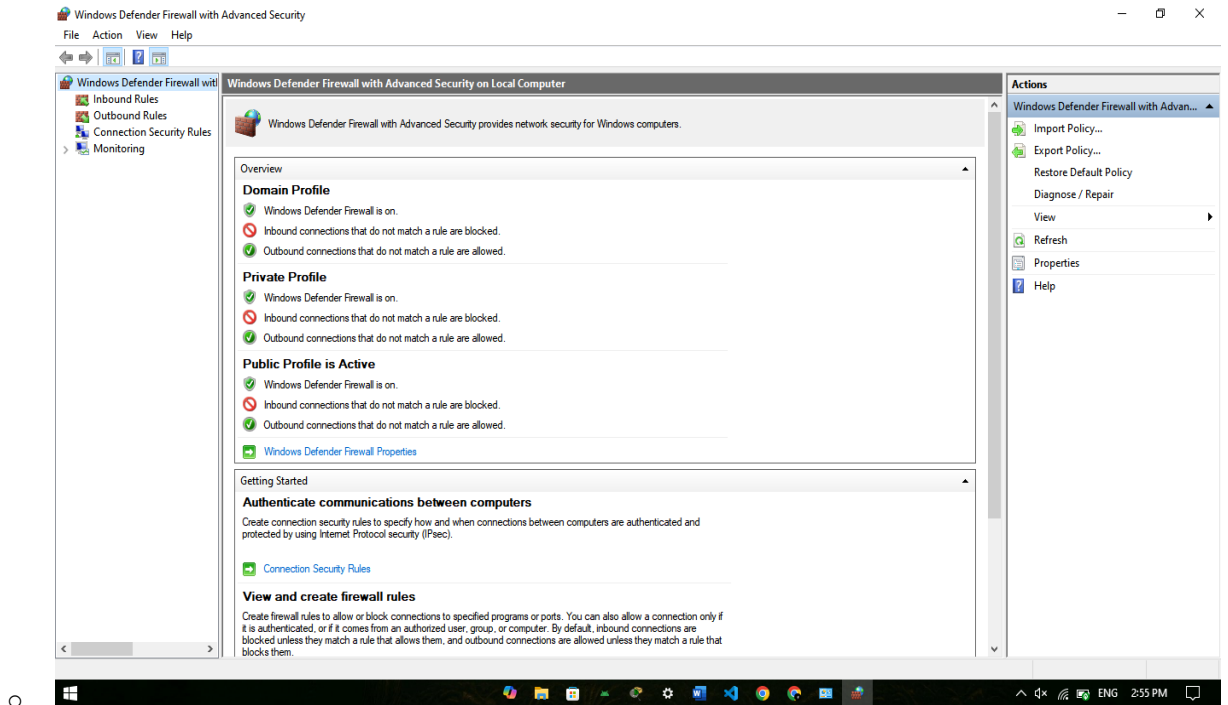   o Select **Security and Maintenance**.

o

o From there, click on **Windows Defender Firewall**.

o

2. **Access Advanced Firewall Settings**:

   o In the Windows Defender Firewall window, click on **Advanced Settings** located on the left-hand side. This will open the **Windows Defender Firewall with Advanced Security** console.

3. **Create a New Inbound Rule**:

   o   In the Advanced Security console, click on **Inbound Rules** in the left-hand panel.

   o   Select **New Rule** from the right-hand panel to begin creating a new inbound rule.

4. **Choose Rule Type**:

   o   You will be prompted to select the type of rule you want to create. Options include:

      ▪   **Program**: Applies the rule to a specific program.

      ▪   **Port**: Applies the rule to a specific port (e.g., TCP or UDP).

      ▪   **Predefined**: Applies a rule to predefined services.

      ▪   **Custom**: Allows you to specify detailed conditions.

   o   Choose the appropriate rule type based on your needs.
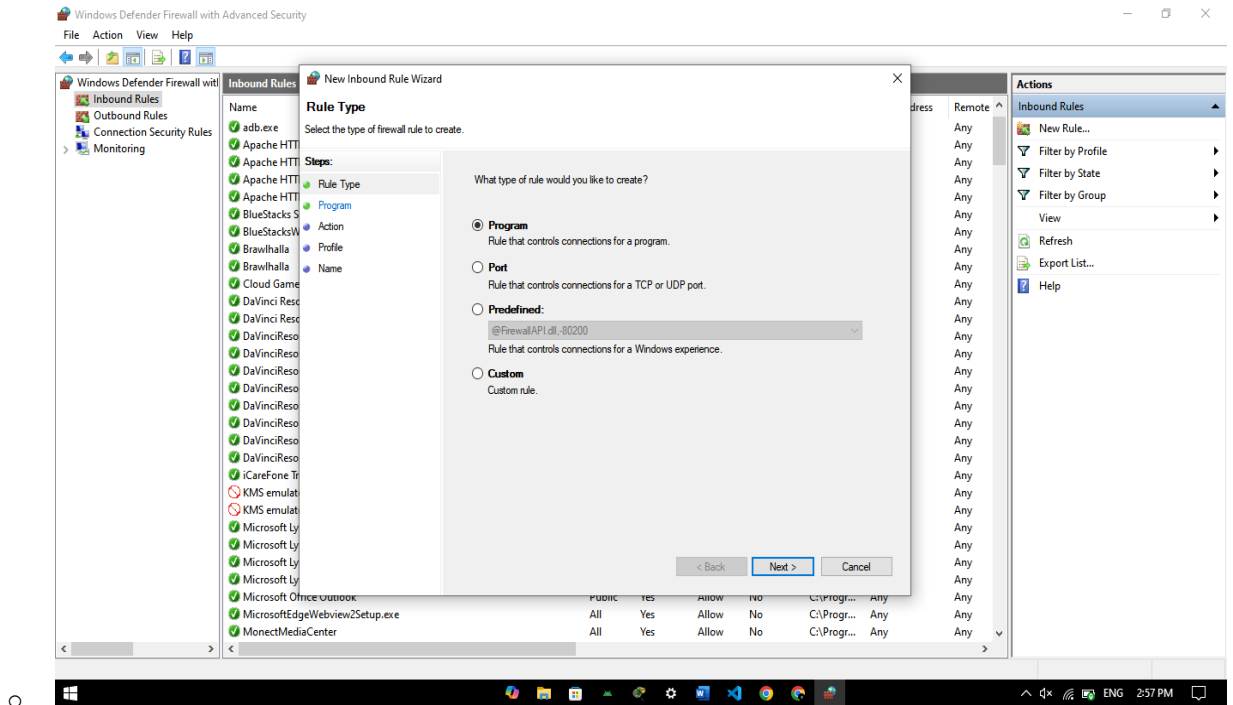
5. **Specify Programs**:

   o If applicable, select whether the rule applies to a **specific program** or **all programs** on the system.
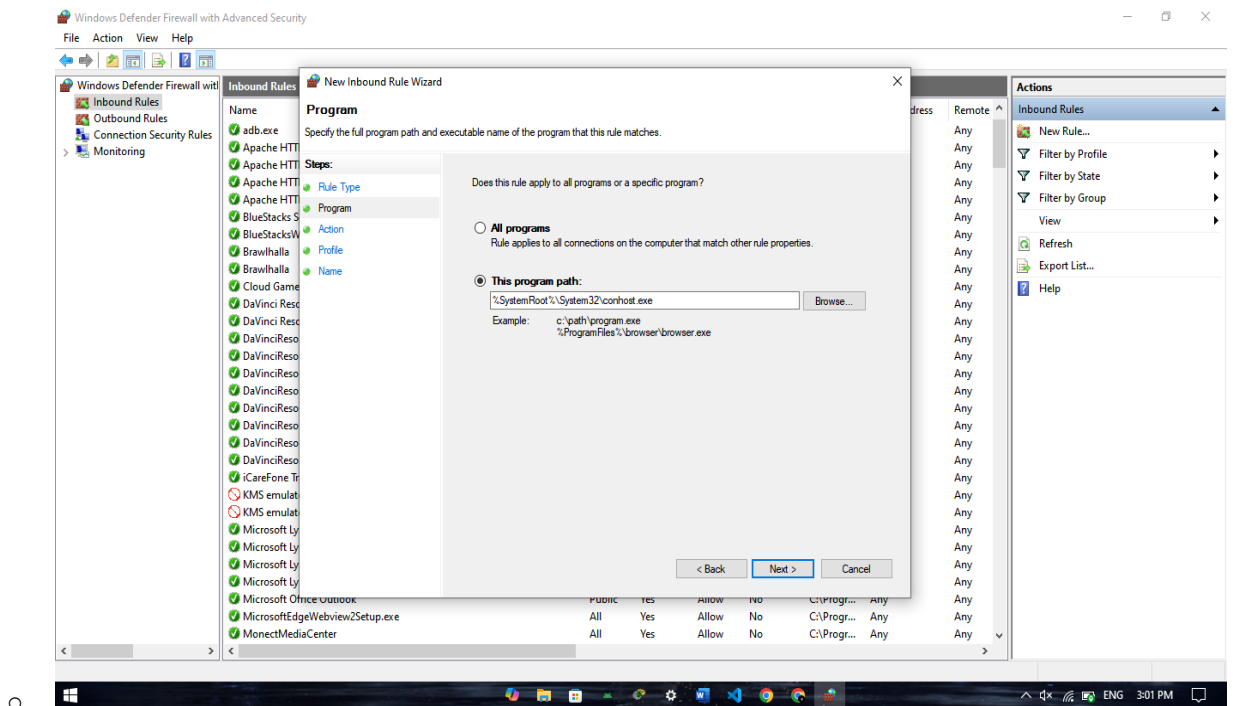

6. **Define Action**:

o Choose the action to be taken when the connection matches the conditions you've set:

- **Allow the connection**.

- **Block the connection**.

- **Allow the connection only if it is secured** (requires that the connection is authenticated and encrypted).
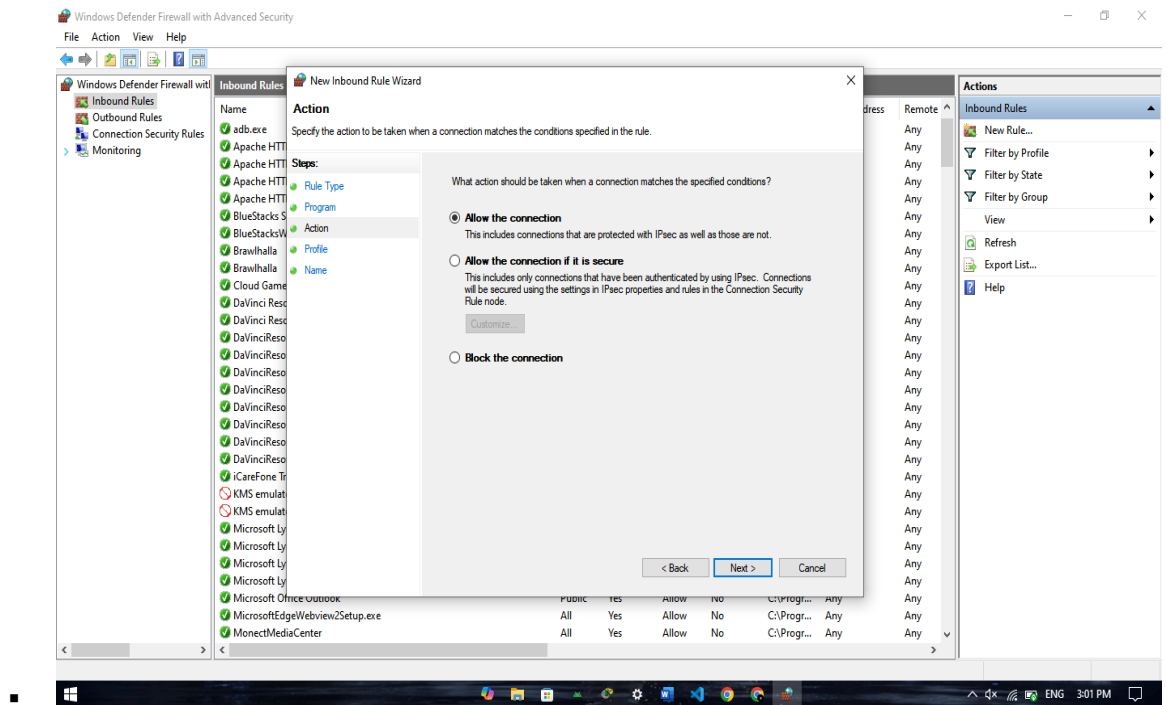
7. **Set Rule Application Conditions**:

o Specify when the rule should be applied:

- **Domain**: Applies when the computer is connected to a domain.

- **Private**: Applies when connected to a private network (e.g., home or work network).

- **Public**: Applies when connected to a public network (e.g., coffee shop Wi-Fi).
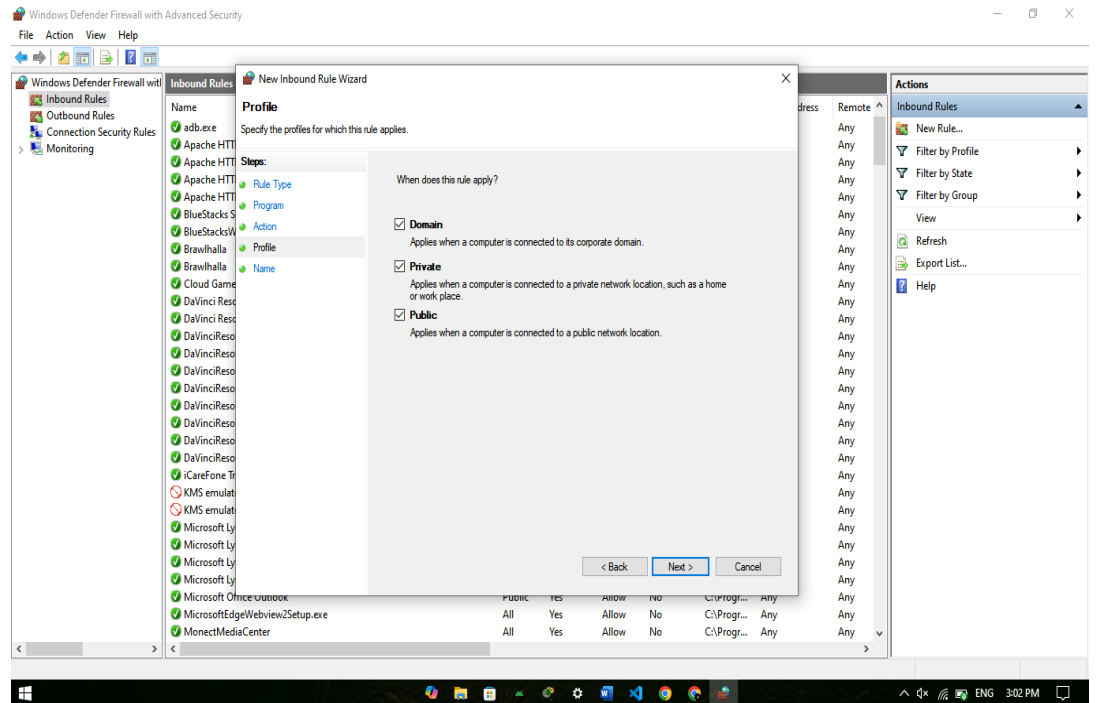
8. **Name and Finalize the Rule**:

   o Give the rule a meaningful name (e.g., "Block Port 445") to identify it easily in the future.

   o Review the settings, and click **Finish** to apply the rule.

   o