Task 1

Set up Basic Firewall Rules

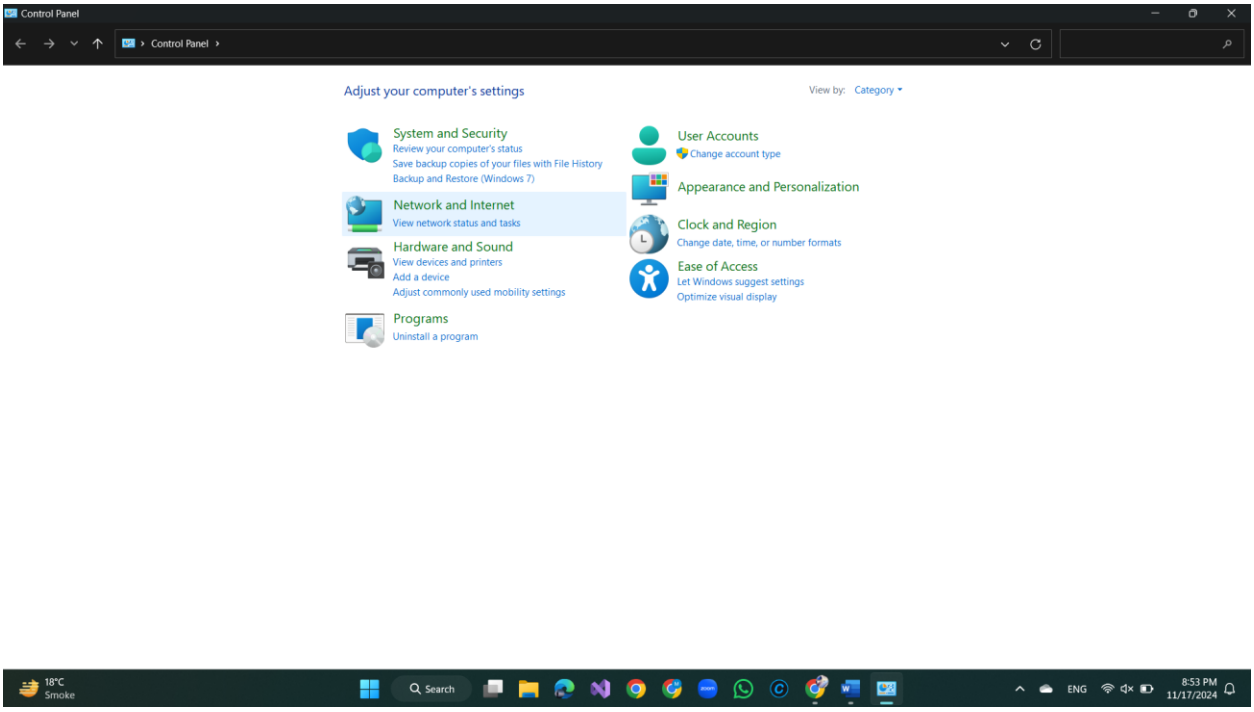
➢ Objective:

Configure and create custom firewall rules using Windows Defender Firewall to control incoming connections on the system.

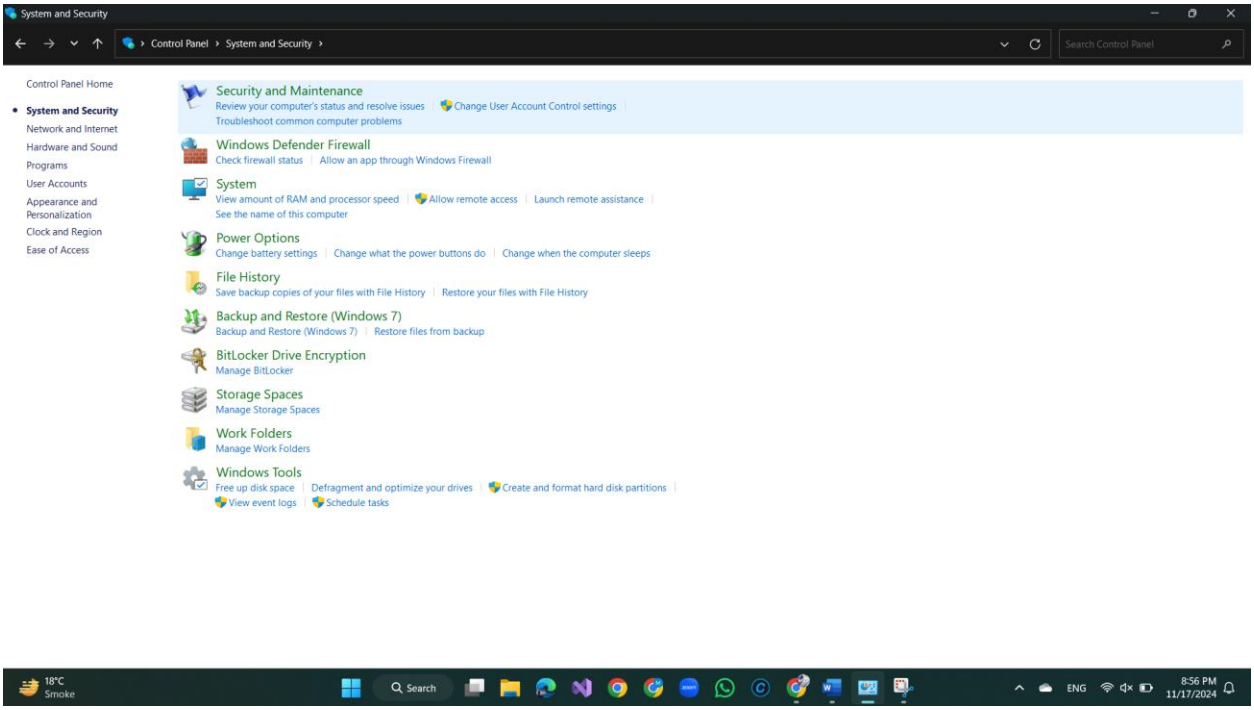
➢ Steps:

1: Open Windows Defender Firewall Settings:

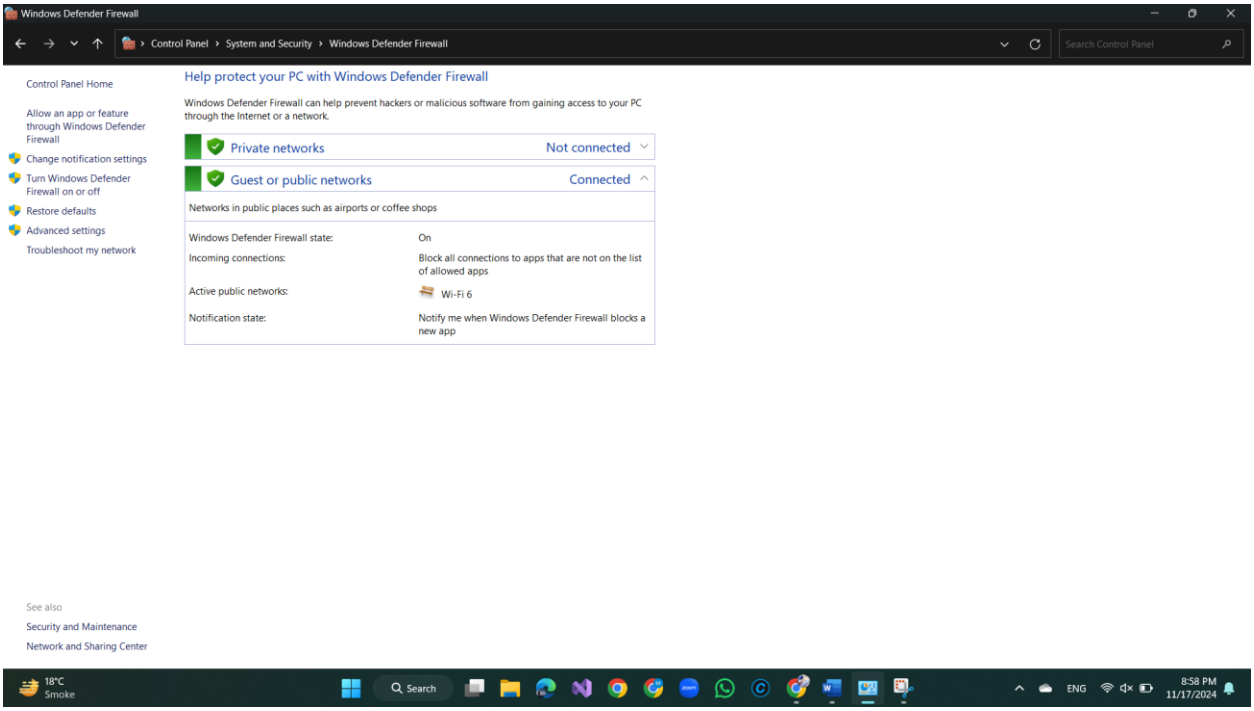
- Navigate to the **Control Panel**



- Select **Security and Maintenance**.

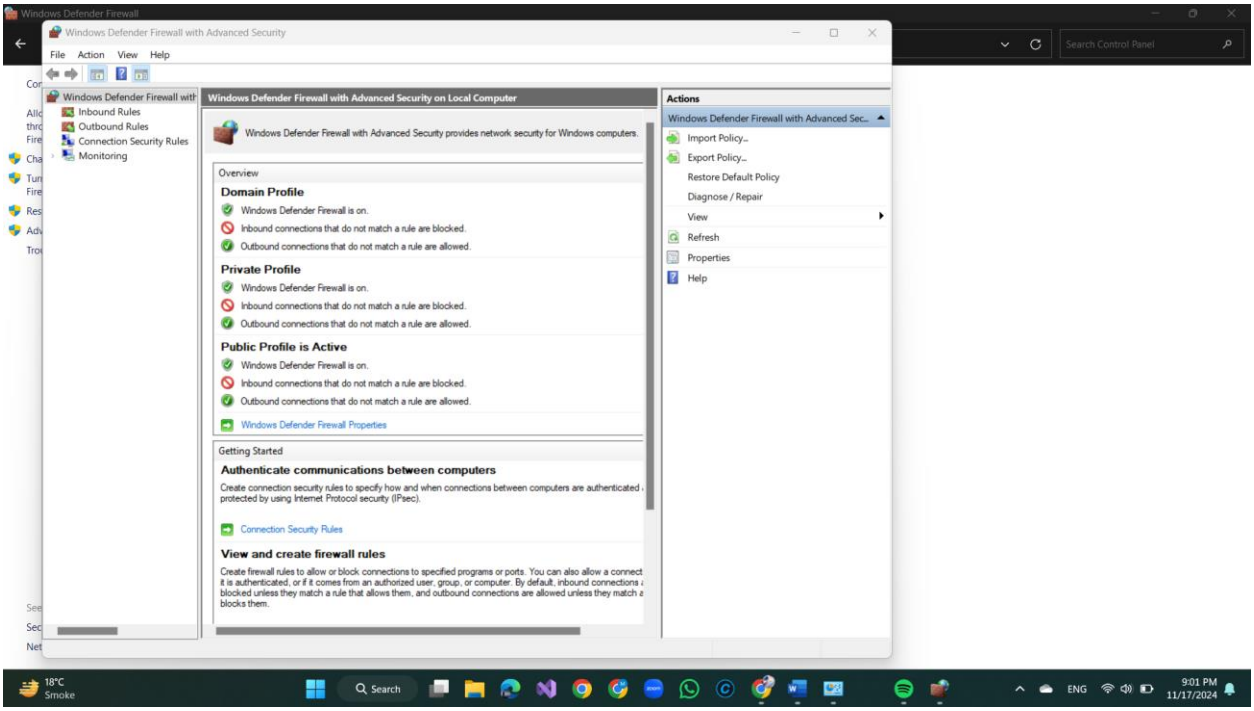


- From there, click on **Windows Defender Firewall**



2: Access Advanced Firewall Settings:

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

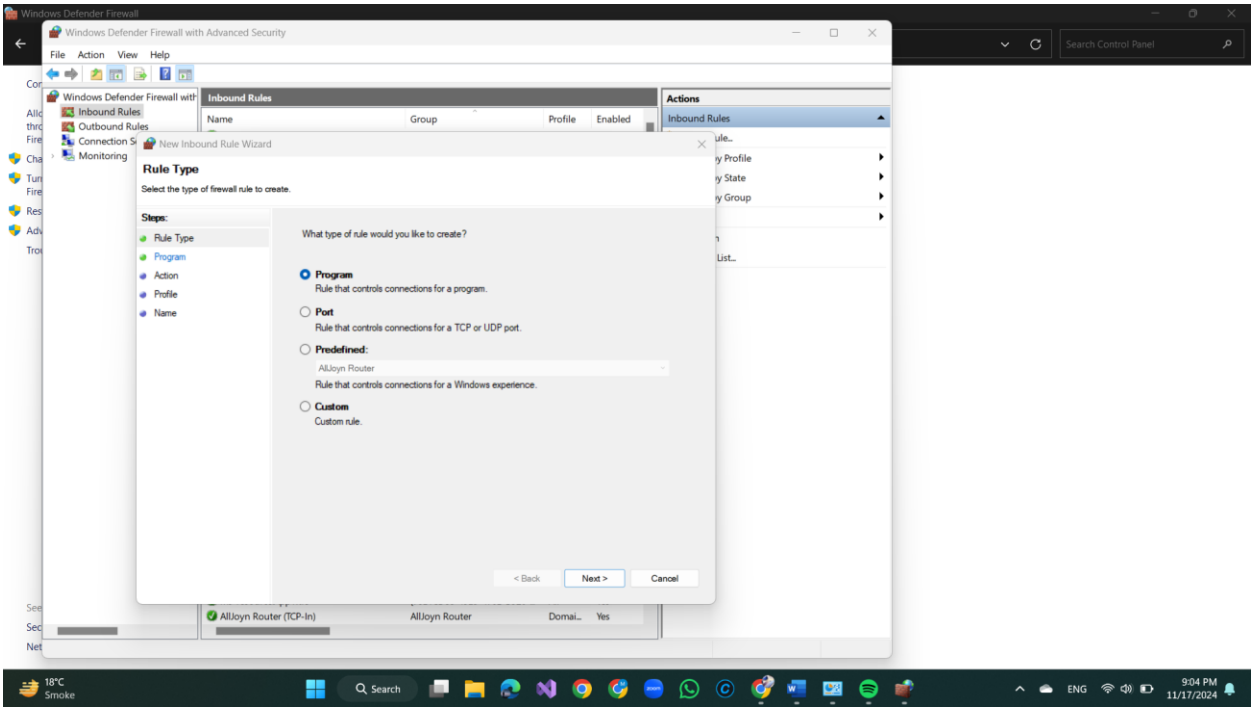


3: Create a New Inbound Rule:

- In the Advanced Security console, click on **Inbound Rules** in the left-hand panel.
- Select **New Rule** from the right-hand panel to begin creating a new inbound rule.

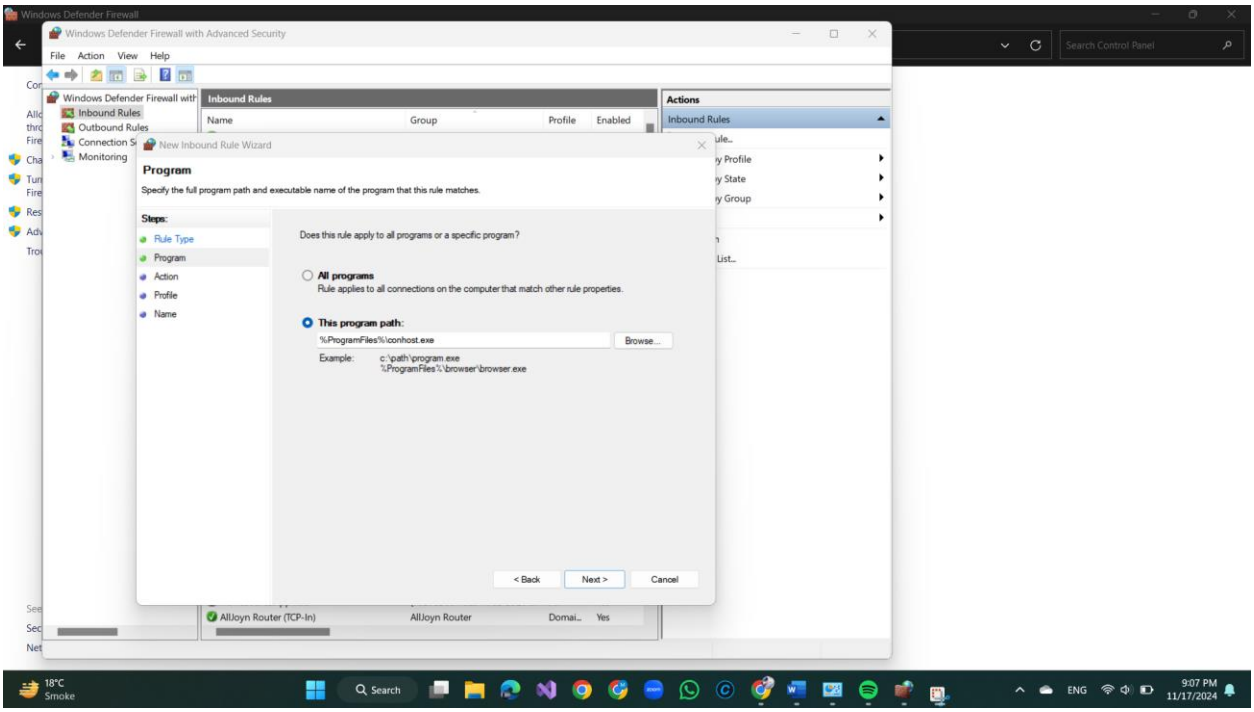
4: Choose Rule Type:

- 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.
- Choose the appropriate rule based on your needs.



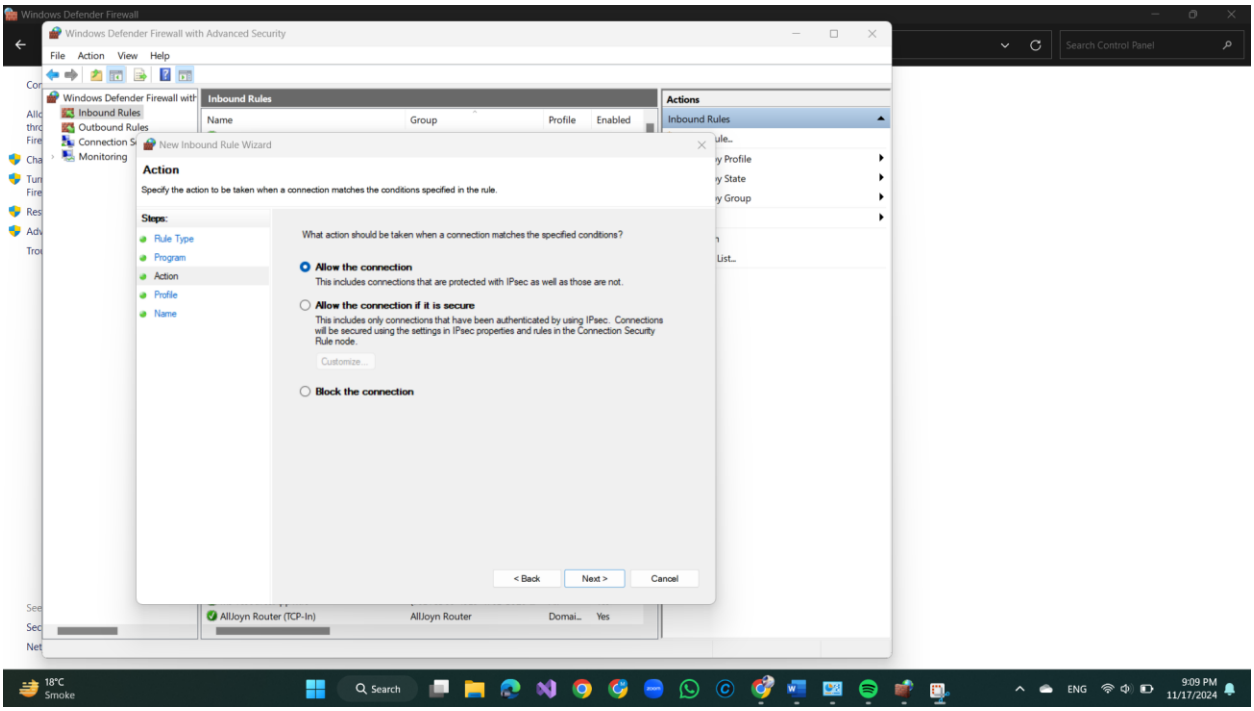
5: Specify Programs:

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



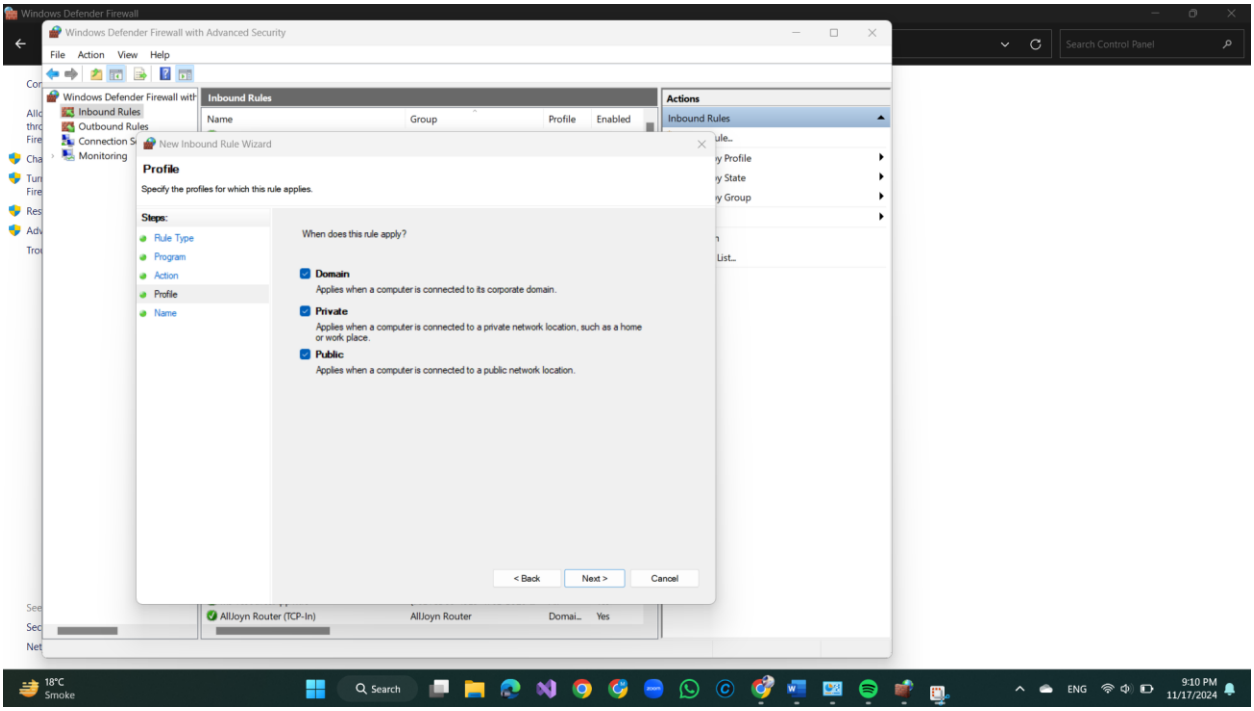
6: Define Action:

- 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:

- Specify when the rule should be applied:
    - **Domain**: This 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:

- Give the rule a meaningful name (e.g., "Block Port 445") to identify it easily in the future.
- Review the settings and click **Finish** to apply the rule.