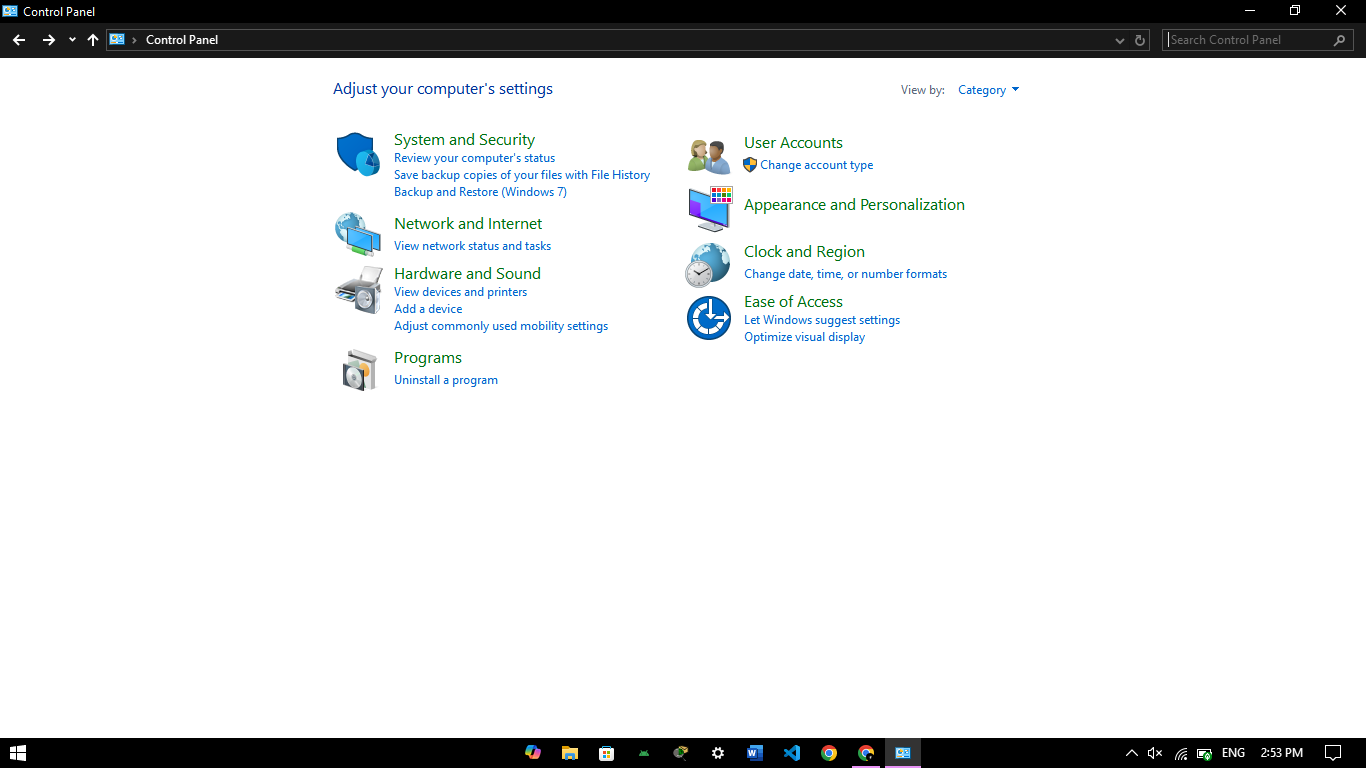
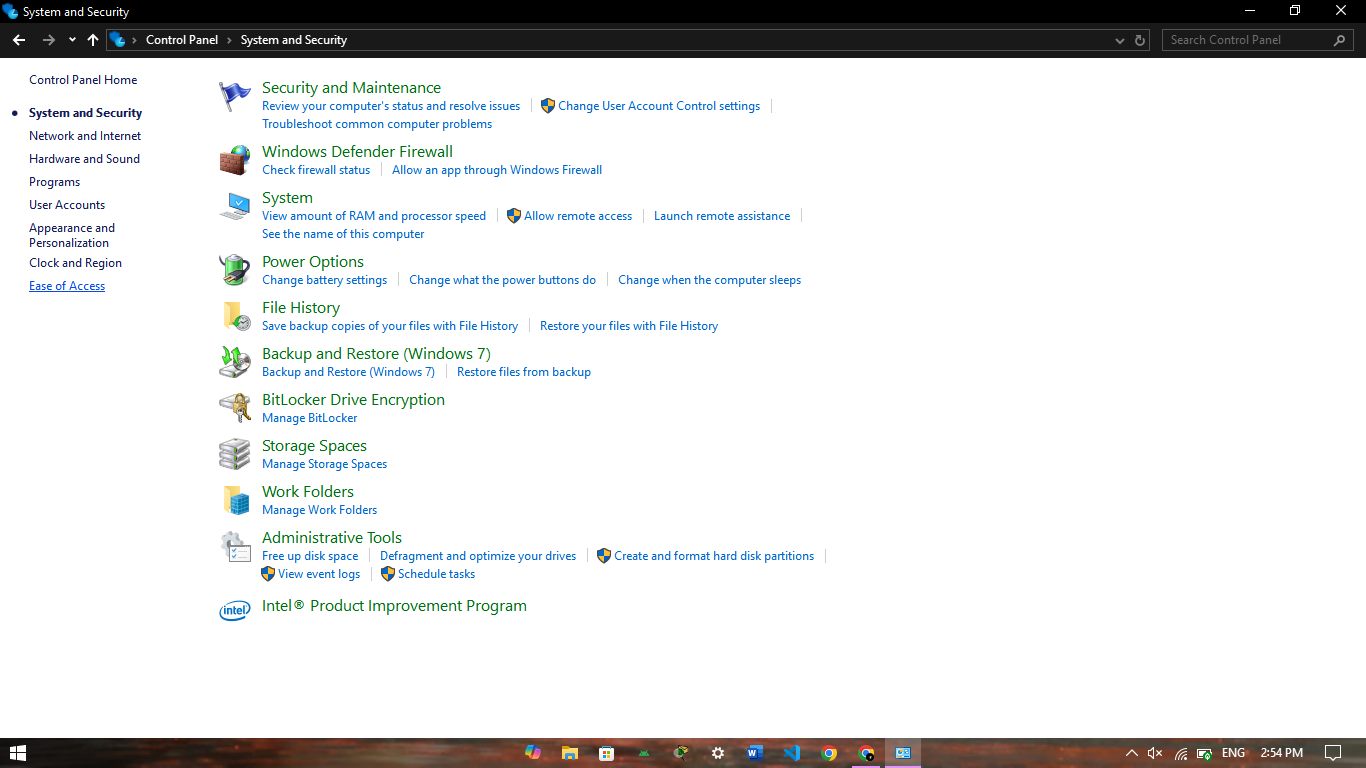
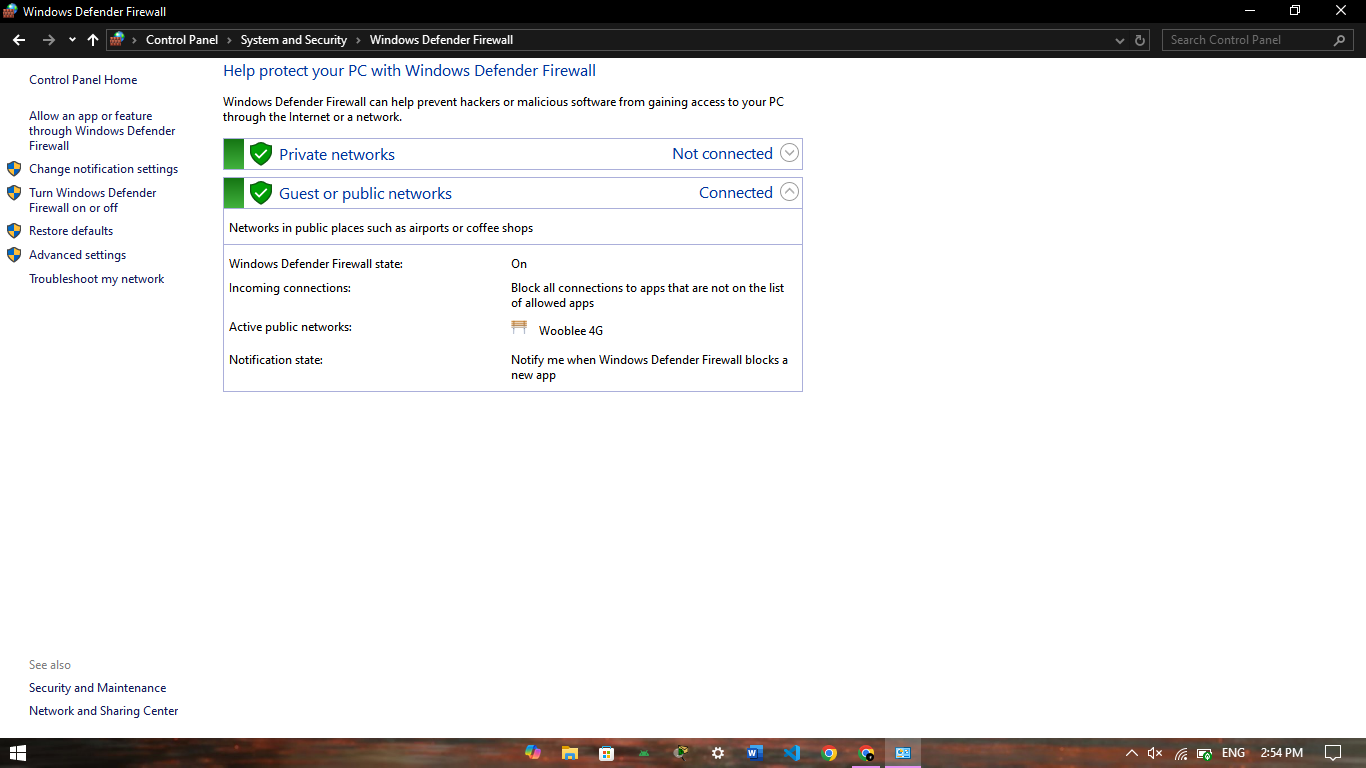
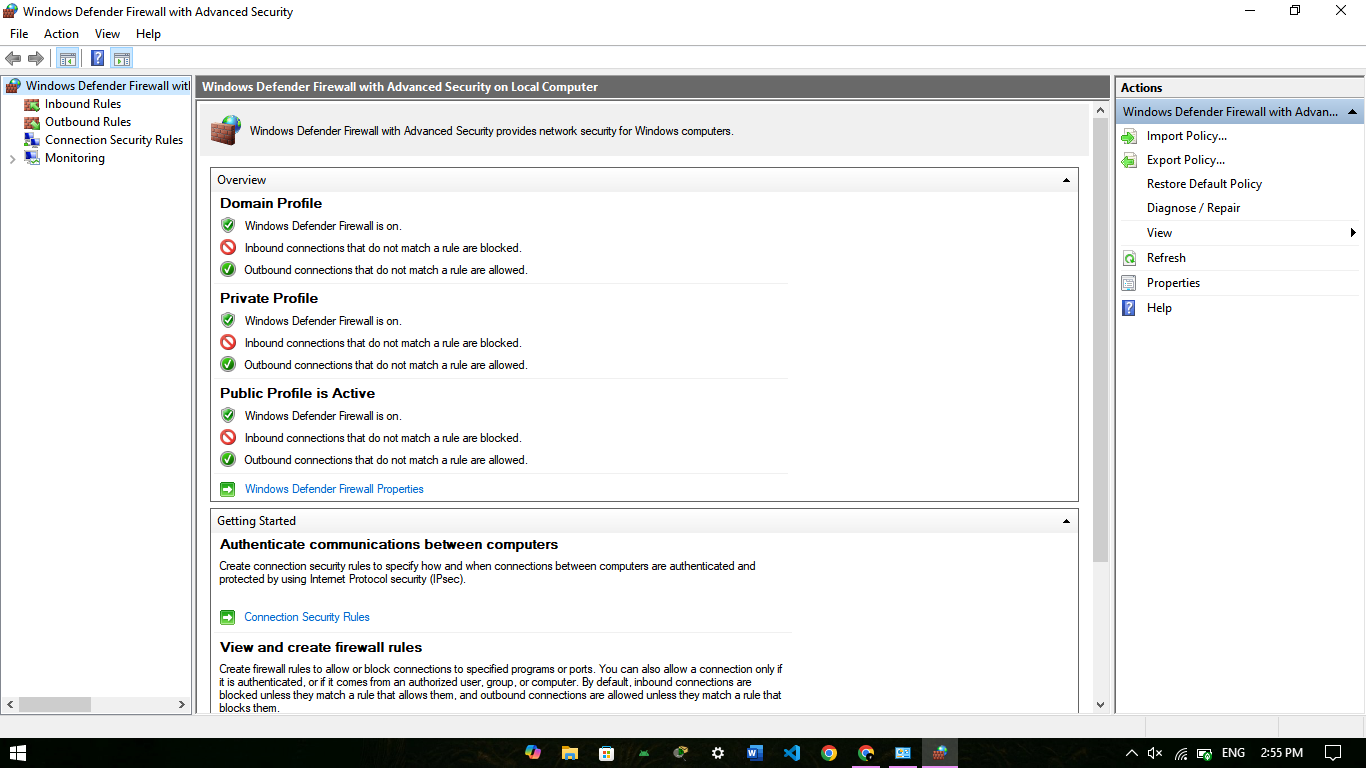
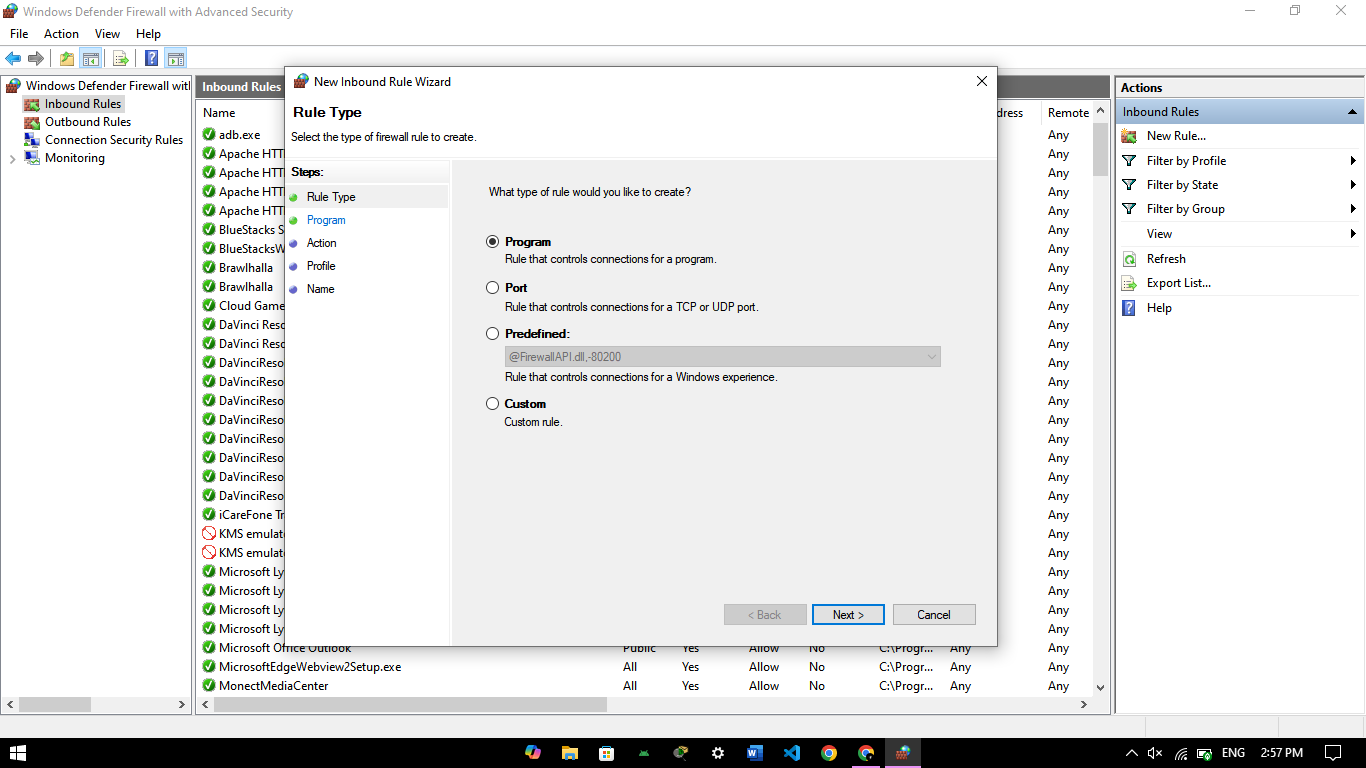
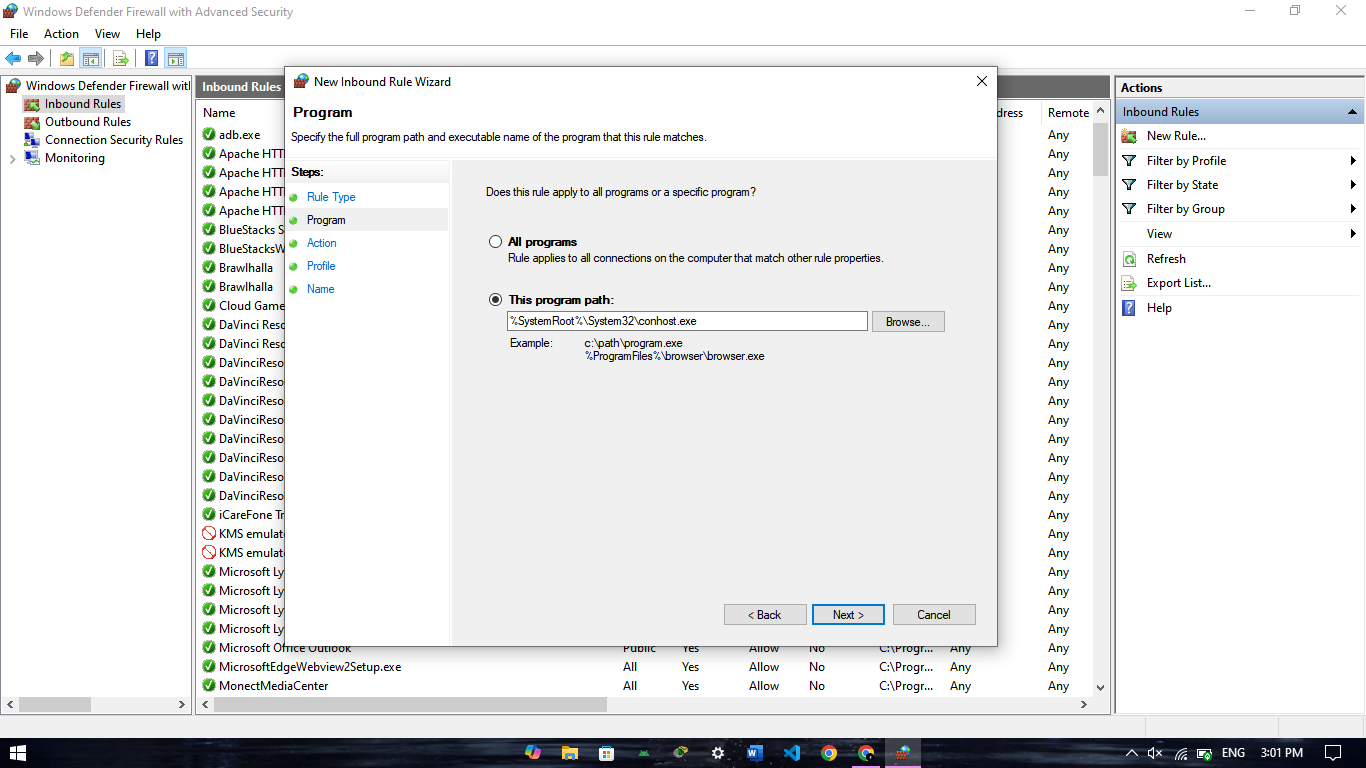
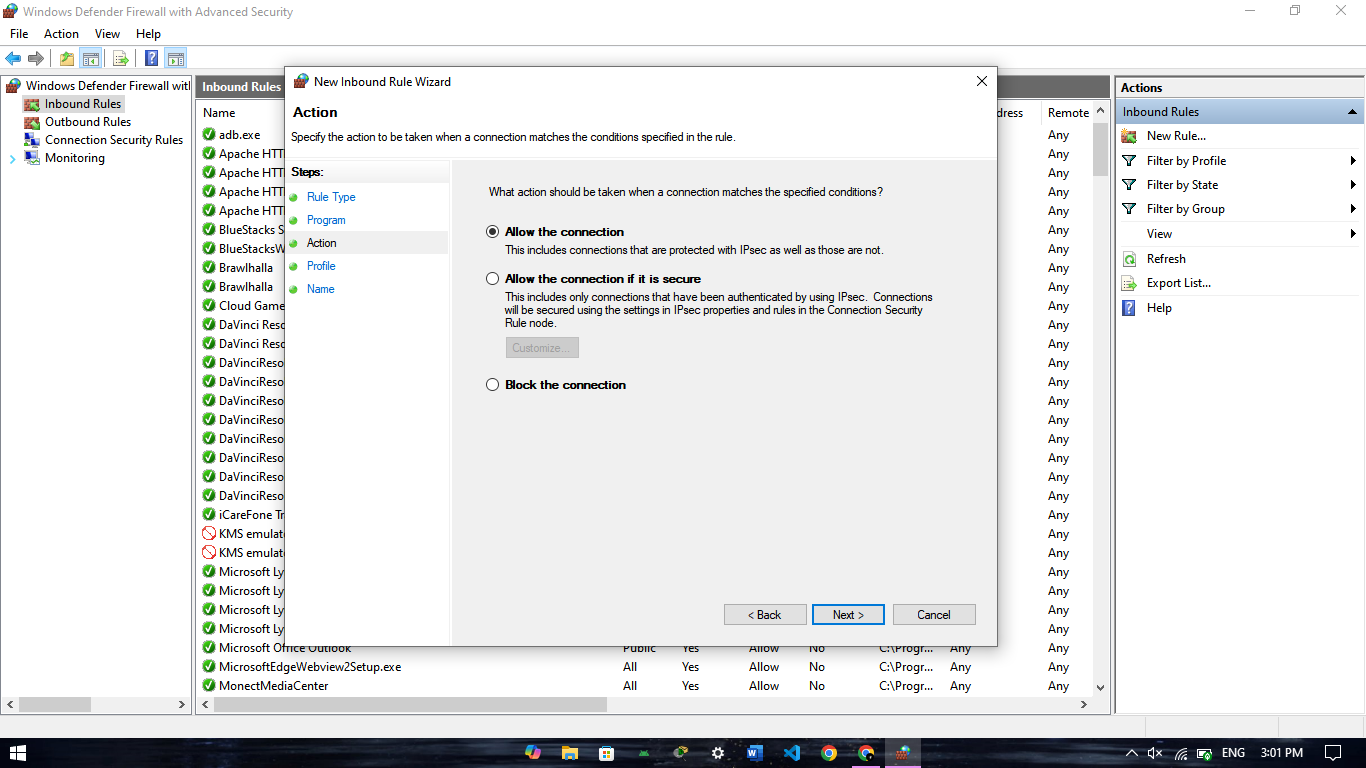
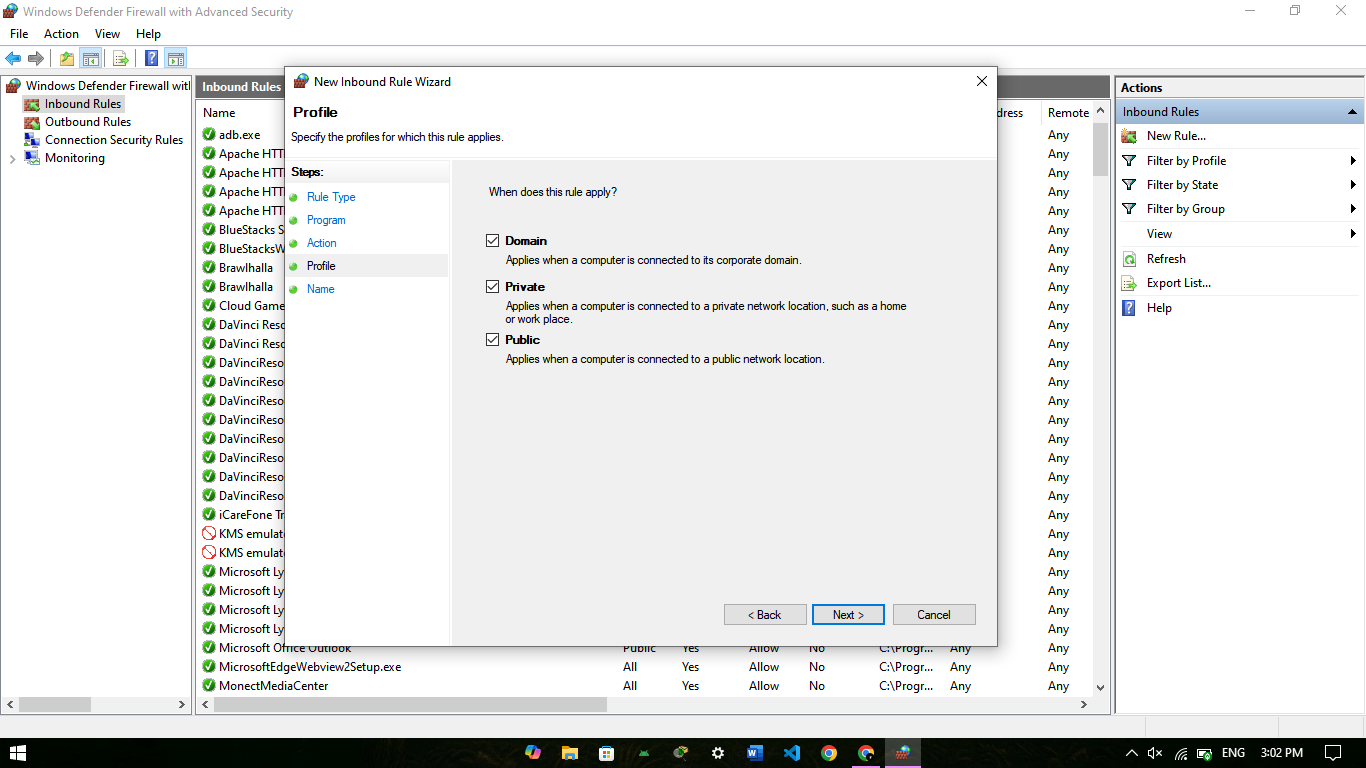
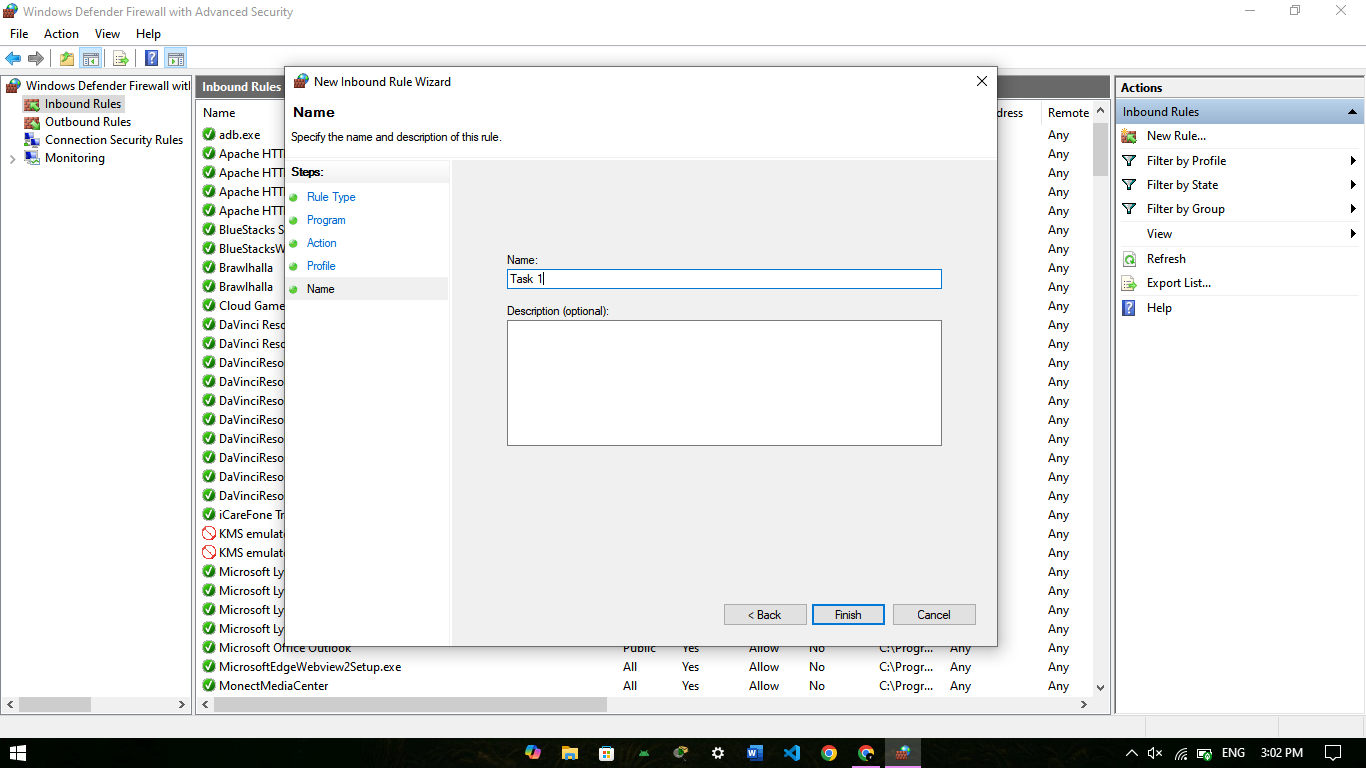
**Task 1: Set Up Basic Firewall Rules**

* **Objective**

To 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**.
   * [](https://private-user-images.githubusercontent.com/181768024/369619136-0ff73789-e6ce-491a-b247-9a47af582546.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjE5MTM2LTBmZjczNzg5LWU2Y2UtNDkxYS1iMjQ3LTlhNDdhZjU4MjU0Ni5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1hOGY5Mzg4OGI4YTdlNWVjNTczOGQ0MmNmNzEzMTk2NzdkYWE4YzZjMDZhYzFmYjI0NzZjODVkYjI5MzBkNDJhJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.eumo45asVbHu1D6HbLEDUr31t9rrpyEepVOTRzWym4Y)
   * Select **Security and Maintenance**.
   * [](https://private-user-images.githubusercontent.com/181768024/369619149-58346356-9e8b-494f-a300-b7f73cc40c39.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjE5MTQ5LTU4MzQ2MzU2LTllOGItNDk0Zi1hMzAwLWI3ZjczY2M0MGMzOS5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1kZjUyY2M4MzkzZjc1NGUxMzg3YjZmOGVlZTY3ODU0ZjUxNzNmMzYwZTI0NThjOGFlMjJkYzJjMjM4YmJiYTNmJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.B6XoRDdr9Ir5aDyeDwWIQVSfKJIJM-GKPdvUkdx3D44)
   * From there, click on **Windows Defender Firewall**.
   * [](https://private-user-images.githubusercontent.com/181768024/369619160-b2a54a97-5d64-4e75-a4e8-dd10f216014c.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjE5MTYwLWIyYTU0YTk3LTVkNjQtNGU3NS1hNGU4LWRkMTBmMjE2MDE0Yy5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1lY2VmNmU3M2M2NDYwYmQ3OWU2ODYyYTg0NzE4OTU1YWE3ZjA4ZDJlZWE5OTA3ZmY2Y2E1ODRkZjliODYzNjdkJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.nS9CapE47G2ipI9LSDb9BA3bEIKsDXUZeYa3rp-01Mw)
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 Advanced Security** console.
   * [](https://private-user-images.githubusercontent.com/181768024/369620579-82889c61-3ed2-4350-8645-947518347e65.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjIwNTc5LTgyODg5YzYxLTNlZDItNDM1MC04NjQ1LTk0NzUxODM0N2U2NS5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1jNmZmOGFkOTY1ZTIwNzg3NGQ4OGUxNDhjNmYzYjMxZWFmZWY4NTZlZjE3MDYyNGNlNmUxNjA0ZjI2ZTM2ZWYzJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.5vCwIL_Zo-jwaqGqJBbllrxbw0iWum7zaL4_8nkoxEk)
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 type based on your needs.
   * [](https://private-user-images.githubusercontent.com/181768024/369621074-6af81343-8acf-4994-a219-de4ed640273e.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjIxMDc0LTZhZjgxMzQzLThhY2YtNDk5NC1hMjE5LWRlNGVkNjQwMjczZS5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT04YWJlMjUwYmUxOWNjZWNjMTY1YTJlMzhiOGU4ODE0Y2RkMWQ3MGM4N2Q5MTY2ZmZjZjNlYzFmNjQ0OTI5MDg2JlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.KYwOyhwhFnvyUA0IWrnakvm7utakmtbf2YM4pvqpKKM)
5. **Specify Programs**:
   * If applicable, select whether the rule applies to a **specific program** or **all programs** on the system.
   * [](https://private-user-images.githubusercontent.com/181768024/369621101-dac4a900-04d2-4afe-b48b-8f3a7cba405a.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjIxMTAxLWRhYzRhOTAwLTA0ZDItNGFmZS1iNDhiLThmM2E3Y2JhNDA1YS5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT04YTljY2ViNzlmYzViYjQ4MDgzMWU5YTU3MzQ1YjFjODAwNmYzOTEyOTIyNmQ1M2IzNWRmYzY2MTA3OTBmM2UyJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.f5OiYVeqXb-PDgoH3MTj9JzLAX-x5C0aiTQo49tB8H0)
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).
     + [](https://private-user-images.githubusercontent.com/181768024/369620960-e1b6294d-af5b-4166-a6f0-3c0e4b988763.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjIwOTYwLWUxYjYyOTRkLWFmNWItNDE2Ni1hNmYwLTNjMGU0Yjk4ODc2My5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT0xZGMxNDA0NjBkYmNlMDM3ZTJmZGYyZTk0ZjU4OTYyNDRhOTc0MGQzNzJmZTE3MGQyNTBmY2IzODRlMTdmOGZhJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.ZTV7FPc55NpRZQ7nyqksS4S99zlqJpOBGBbriw91hZU)
7. **Set Rule Application Conditions**:
   * 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).
     + [](https://private-user-images.githubusercontent.com/181768024/369620985-3b433edb-d896-4716-b3e3-a9a783271834.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjIwOTg1LTNiNDMzZWRiLWQ4OTYtNDcxNi1iM2UzLWE5YTc4MzI3MTgzNC5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1iNTQ0NzgzODZkMGQyODNjZWYyZGYyN2M0NmI0MGYyNTk1YTU2MTM2ZTAzMjliNzRiYTY3NWRhNzQ3NDFlMDNiJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.WioXK9u-MCQsEu3dRS0mPIkBKGrEFNgvNqfkyHdsLxU)
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.
   * [](https://private-user-images.githubusercontent.com/181768024/369621153-3a440e29-3ff7-49c2-8cf5-2f57facf9b8b.PNG?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzI3MDM3ODIsIm5iZiI6MTczMjcwMzQ4MiwicGF0aCI6Ii8xODE3NjgwMjQvMzY5NjIxMTUzLTNhNDQwZTI5LTNmZjctNDljMi04Y2Y1LTJmNTdmYWNmOWI4Yi5QTkc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTI3JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEyN1QxMDMxMjJaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT0xZmYyN2UyN2U4ZWQxNWQ1N2M2YTZlMzdhNzVlZTBmNWU3OGM1ZTBmYWZlMDc2ZmE3ZWYzNzQ5OTUxOTcxMDA3JlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.1uVVqzIX8nuAov2h1fhybNOzydhFtwvybj45p59d7bo)