PRACTICAL NO: 5

AIM: To implement and understand Windows security features using the firewall and other security measures, ensuring network protection and safe data usage.

OBJECTIVE: To learn the configuration of the Windows Firewall to control inbound and outbound traffic and configure additional security measures like Windows Defender, network policies, and access controls.

REQUIREMENTS:

- A computer with Windows OS (Windows 10 or later preferred).
- Administrator privileges for making system-level changes.
- Internet connectivity for updates.
- Access to Windows Defender and firewall configuration settings.

THEORY:

Firewalls

A firewall is a critical security system that acts as a barrier between a trusted internal network and untrusted external networks like the Internet. Firewalls monitor and control incoming and outgoing network traffic based on security policies.

Importance of Firewalls:

- Prevent unauthorized access to a network or system.
- Protect sensitive data from being accessed or stolen.
- Mitigate risks from malware and other malicious activities.

Types of Firewalls:

- **Packet-Filtering Firewall:** Filters packets based on source/destination IP, port, and protocol.
- **Stateful Inspection Firewall:** Tracks the state of active connections and makes decisions based on the connection's context.

- **Application Layer Firewall:** Operates at the application layer and filters traffic based on specific applications.

Features of Firewalls:

- Logging and reporting capabilities to monitor security events.
- Intrusion prevention by blocking known malicious activities.
- Network Address Translation (NAT) for hiding internal network details.

Windows Firewall

Windows Firewall is a built-in security feature in the Microsoft Windows operating system. It is a host-based firewall designed to filter incoming and outgoing traffic and protect the system from potential threats.

Key Features of Windows Firewall:

- **Profiles:** Configures separate rules for domain, private, and public network profiles.
- **Inbound and Outbound Rules:** Allows users to define which types of traffic are permitted or blocked.
- **Logging:** Maintains a log of dropped packets and successful connections for auditing purposes.
- **Application Control:** Lets users specify which applications are allowed or blocked from accessing the network.

Advantages:

- Integrated with the Windows OS, providing seamless operation.
- User-friendly graphical interface for rule configuration.
- Supports advanced configurations via PowerShell and Group Policy.

Limitations:

- Does not replace a network-level firewall for enterprise environments.
- May require additional configuration for complex setups.

Windows Defender: Windows Defender is Microsoft's built-in antivirus and anti-malware solution, designed to protect the system from threats such as viruses, ransomware, spyware, and phishing attacks. It provides real-time protection and regularly updated threat definitions to address new vulnerabilities.

Key Features of Windows Defender:

- **Real-Time Protection:** Continuously monitors the system for suspicious activities and threats.
- **Periodic Scanning:** Provides quick, full, and custom scan options to detect and remove malware.
- **Cloud-Based Protection:** Utilizes Microsoft's vast database to identify emerging threats quickly.
- **Exploit Protection:** Safeguards against attacks targeting software vulnerabilities.
- **Firewall Integration:** Works in conjunction with Windows Firewall for a holistic security approach.

Advantages:

- Built into the Windows OS, ensuring no additional installation is required.
- Lightweight and does not consume excessive system resources.
- Free for all Windows users with regular updates.

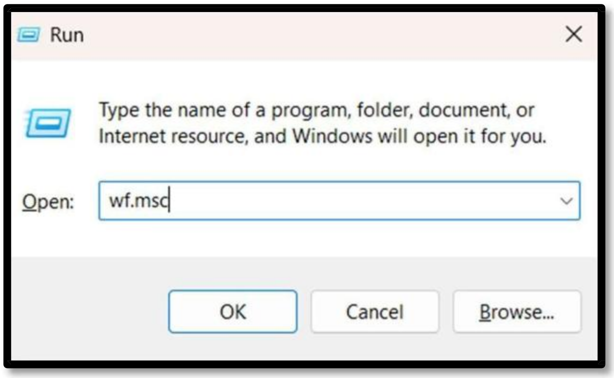
PROCEDURE:

1. **Open Run Dialog**:

   Press Win + R to open the **Run** dialog box.

2. **Access Advanced Firewall Settings**:

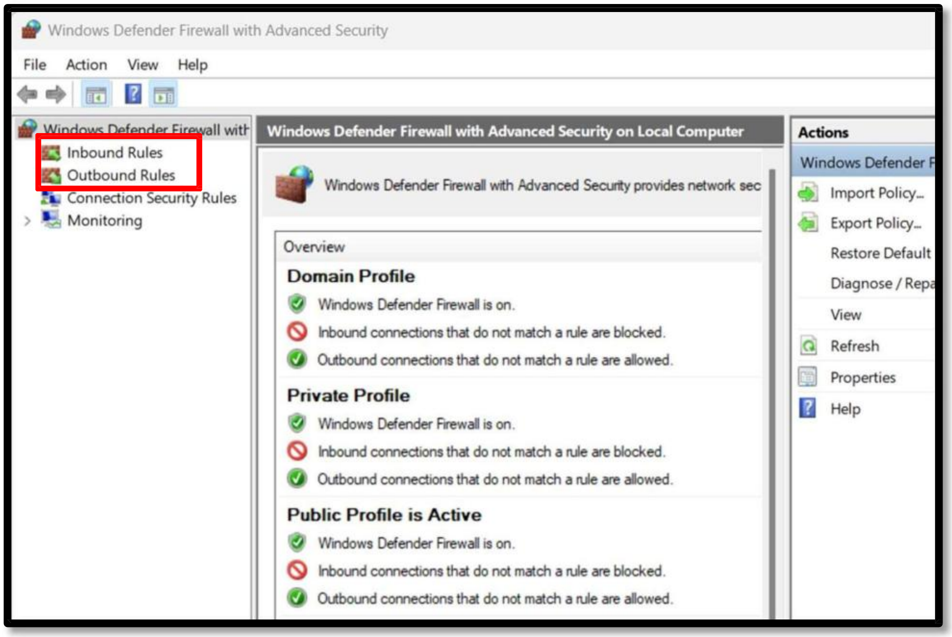
   Type wf.msc in the **Run** dialog and pressing **Enter**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

3. **View Existing Rules**:
   - Click on **Inbound Rules** or **Outbound Rules** in the left pane.



Windows Defender Firewall with Advanced Security provides network sec

Overview

Domain Profile

✓ Windows Defender Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

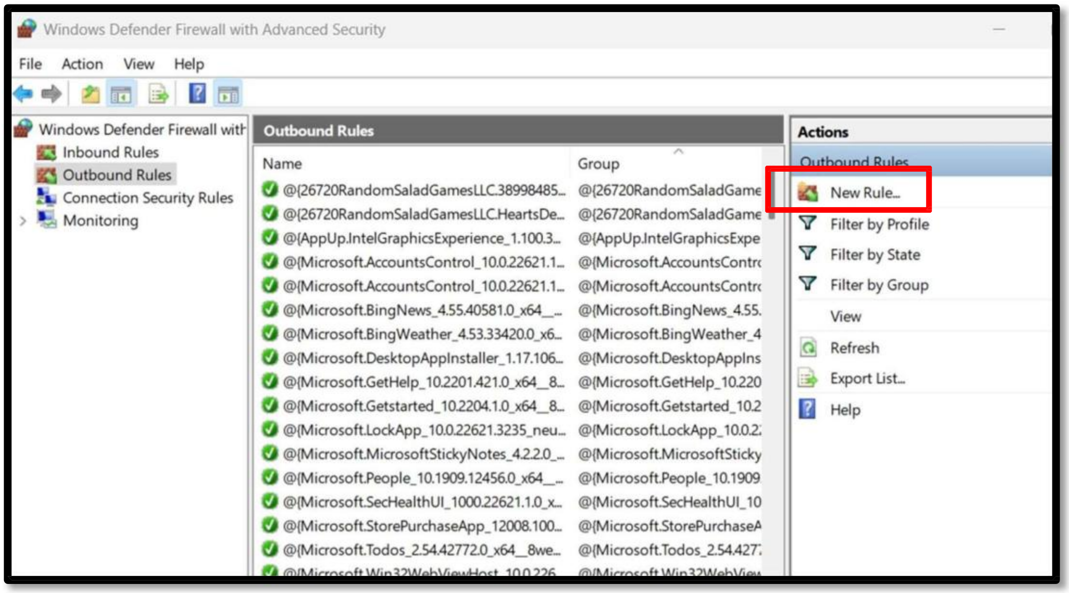
✓ Windows Defender Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

   - Scroll through the list to see existing rules.

4. **Create a New Inbound/Outbound Rule**:
   - Select **Inbound Rules** (for incoming connections) or **Outbound Rules** (for outgoing connections) from the left pane.

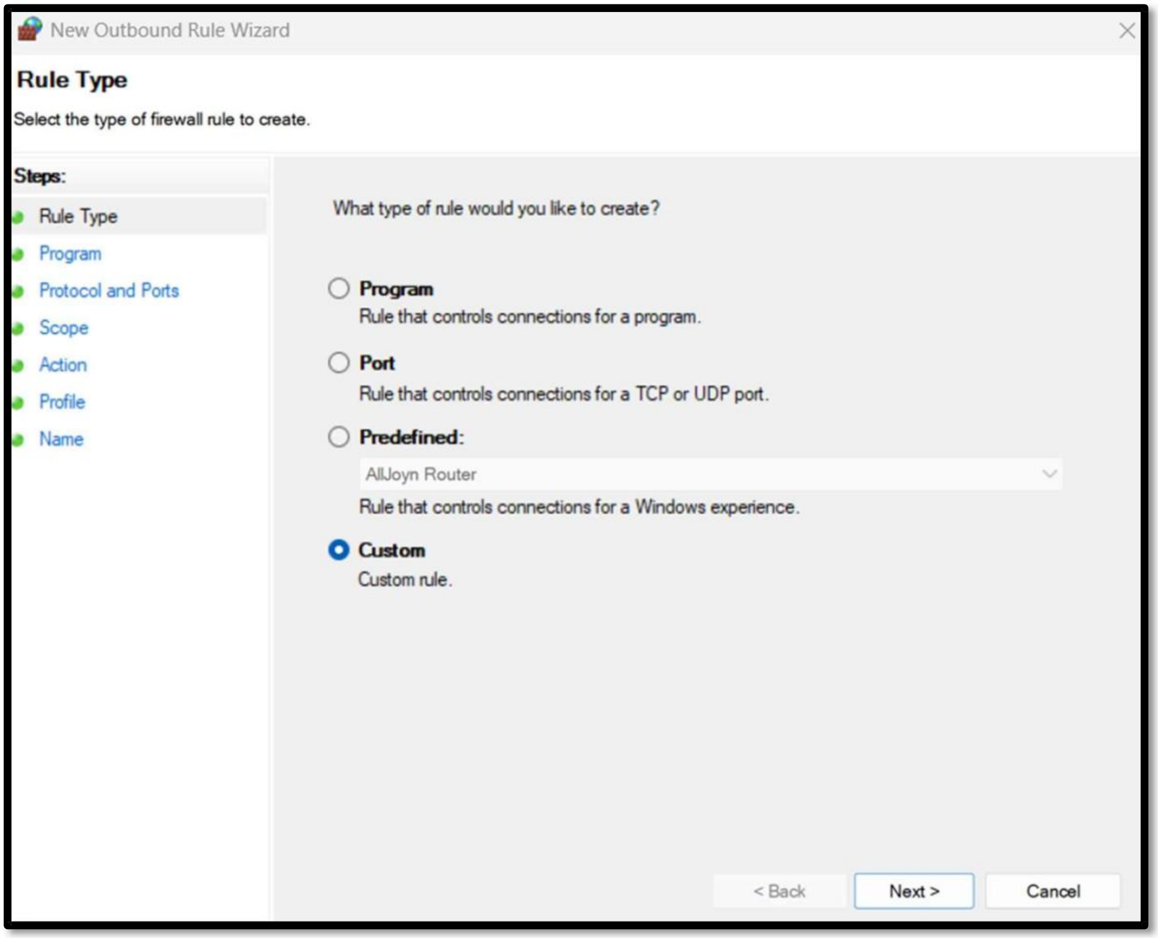


Outbound Rules

Name	Group
✓ @{26720RandomSaladGamesLLC.38998485...	@{26720RandomSaladGame
✓ @{26720RandomSaladGamesLLC.HeartsDe...	@{26720RandomSaladGame
✓ @{AppUp.IntelGraphicsExperience_1.100.3...	@{AppUp.IntelGraphicsExpe
✓ @{Microsoft.AccountsControl_10.0.22621.1...	@{Microsoft.AccountsContrc
✓ @{Microsoft.AccountsControl_10.0.22621.1...	@{Microsoft.AccountsContrc
✓ @{Microsoft.BingNews_4.55.40581.0_x64__...	@{Microsoft.BingNews_4.55.
✓ @{Microsoft.BingWeather_4.53.33420.0_x6...	@{Microsoft.BingWeather_4
✓ @{Microsoft.DesktopAppInstaller_1.17.106...	@{Microsoft.DesktopAppIns
✓ @{Microsoft.GetHelp_10.2201.421.0_x64__8...	@{Microsoft.GetHelp_10.220
✓ @{Microsoft.Getstarted_10.2204.1.0_x64__8...	@{Microsoft.Getstarted_10.2
✓ @{Microsoft.LockApp_10.0.22621.3235_neu...	@{Microsoft.LockApp_10.0.2:
✓ @{Microsoft.MicrosoftStickyNotes_4.2.2.0_...	@{Microsoft.MicrosoftSticky
✓ @{Microsoft.People_10.1909.12456.0_x64__...	@{Microsoft.People_10.1909
✓ @{Microsoft.SecHealthUI_1000.22621.1.0_x...	@{Microsoft.SecHealthUI_10
✓ @{Microsoft.StorePurchaseApp_12008.100...	@{Microsoft.StorePurchaseA
✓ @{Microsoft.Todos_2.54.42772.0_x64__8we...	@{Microsoft.Todos_2.54.427:
✓ @{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebView

- In the right pane, click **New Rule...**.

5. **Select Rule Type**:
   - Choose the type of rule you want to create. For example:
     - **Program**: Block or allow a specific program.
     - **Port**: Restrict or allow specific ports.
     - **Predefined**: Use pre-configured rules.
     - **Custom**: Set advanced parameters for your rule.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

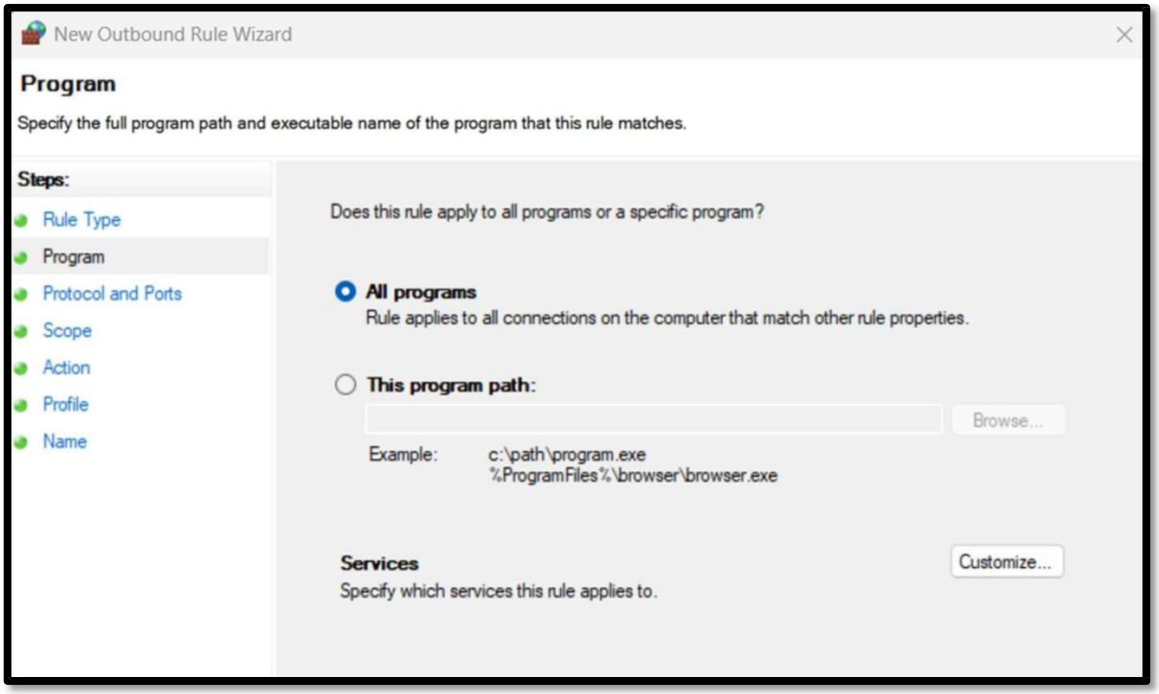
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined**:
AllJoyn Router
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

- Click **Next**.

6. **Specify Program or Port**:
   - For **Program**: Browse and select the program .exe file.



New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

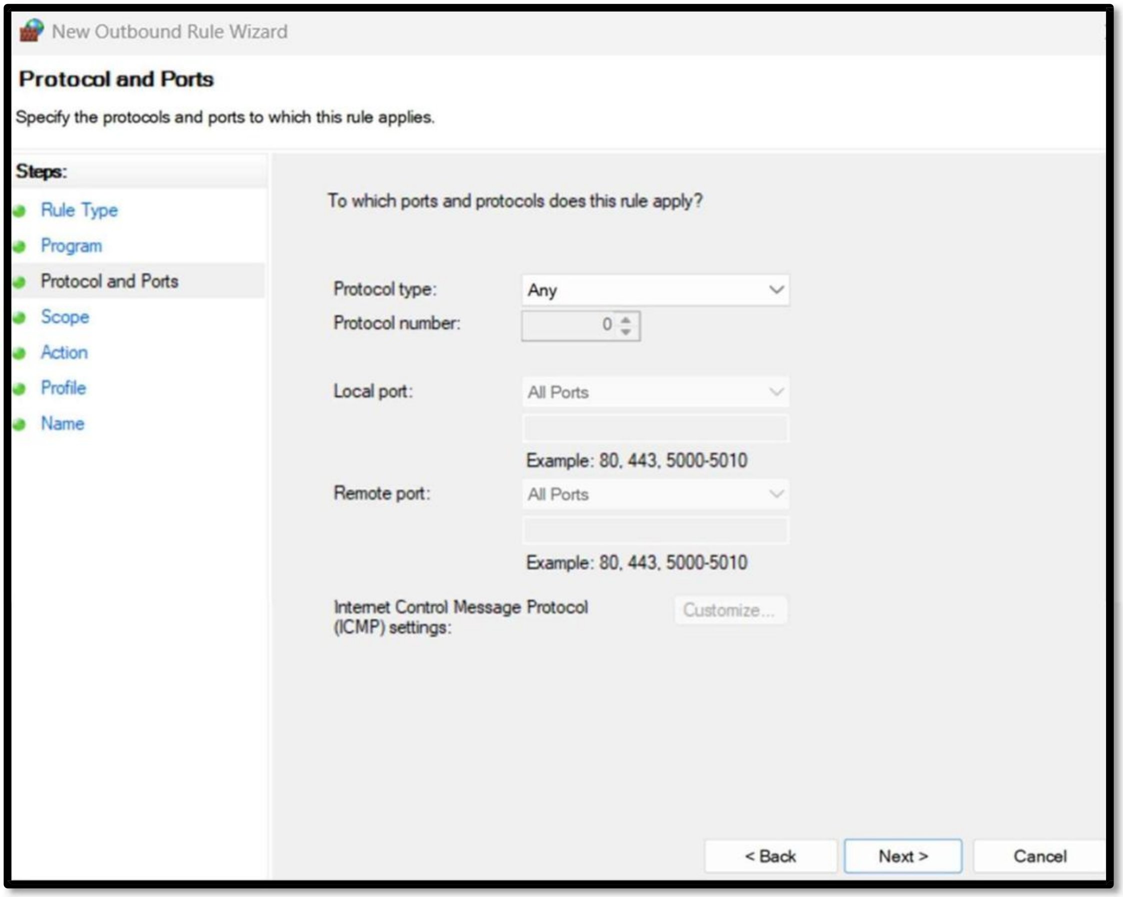
Browse...

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

Customize...

- For **Port**: Select **TCP** or **UDP**, then specify the port number(s).



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: Any
Protocol number: 0

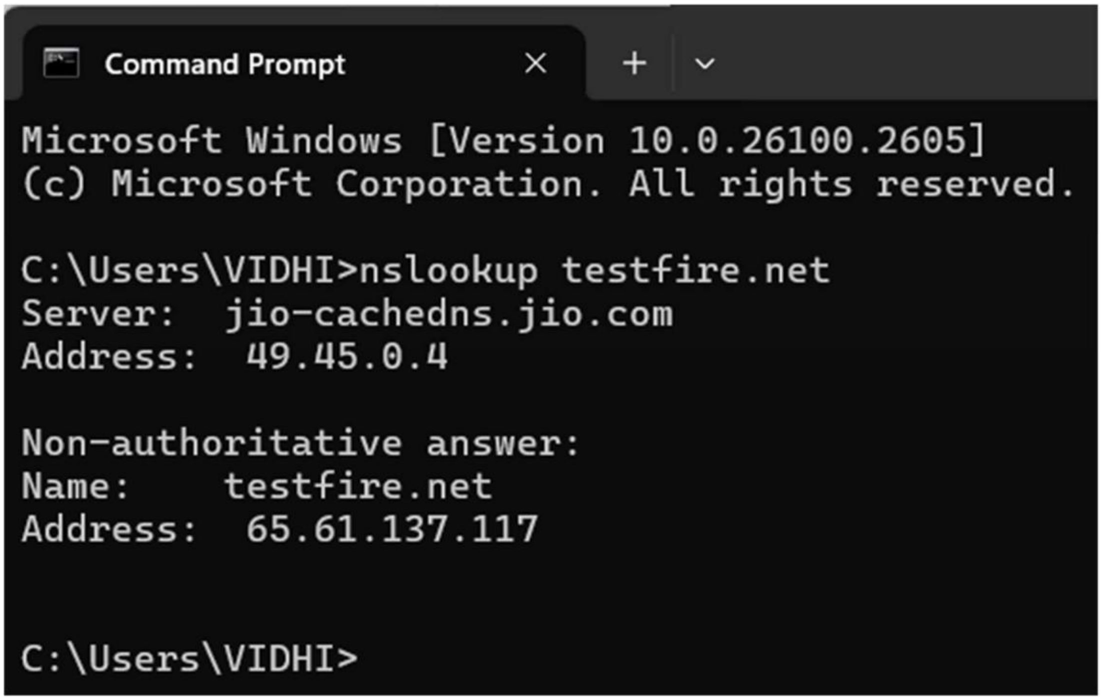
Local port: All Ports
Example: 80, 443, 5000-5010

Remote port: All Ports
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

< Back Next > Cancel

- For **Scope**: Select **Local** or **Remote**, then specify the IP address(es).

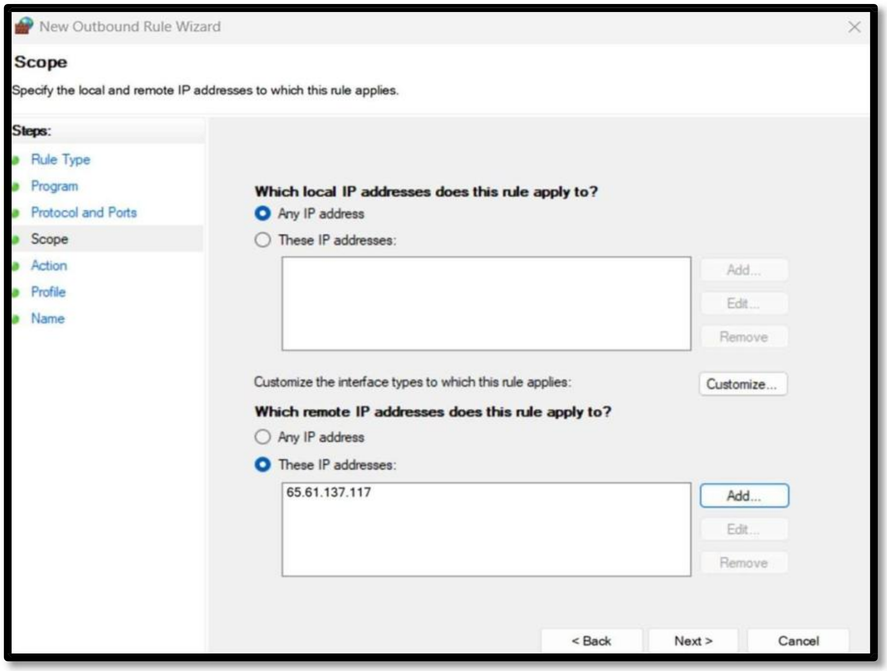


```
Microsoft Windows [Version 10.0.26100.2605]
(c) Microsoft Corporation. All rights reserved.

C:\Users\VIDHI>nslookup testfire.net
Server:  jio-cachedns.jio.com
Address:  49.45.0.4

Non-authoritative answer:
Name:    testfire.net
Address:  65.61.137.117


C:\Users\VIDHI>
```



New Outbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

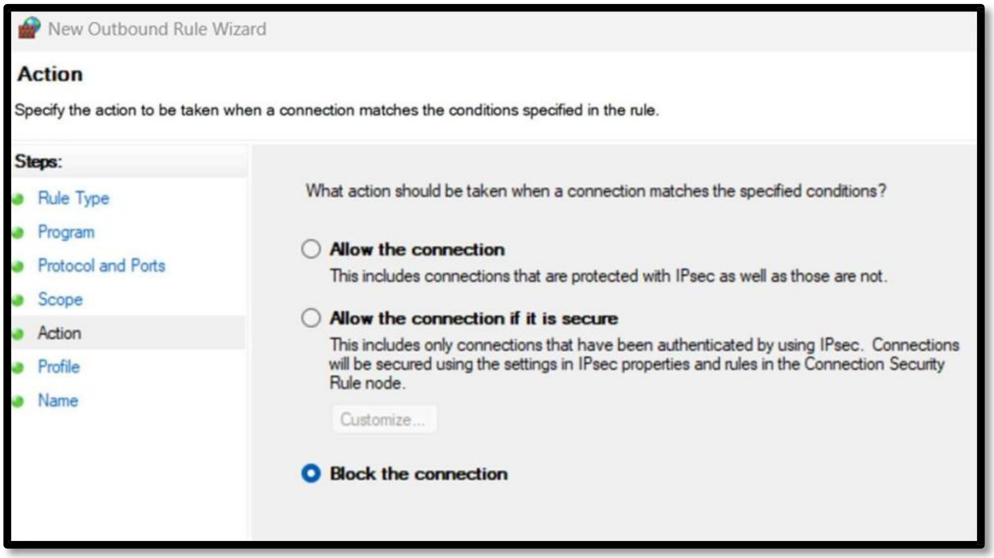
○ Any IP address

● These IP addresses:

65.61.137.117

7. **Set Action**:
    - Choose the action for this rule:
        - **Allow the connection**: Permit the connection.

- **Allow the connection if it is secure**: Allow only secure connections.
- **Block the connection**: Deny the connection.



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

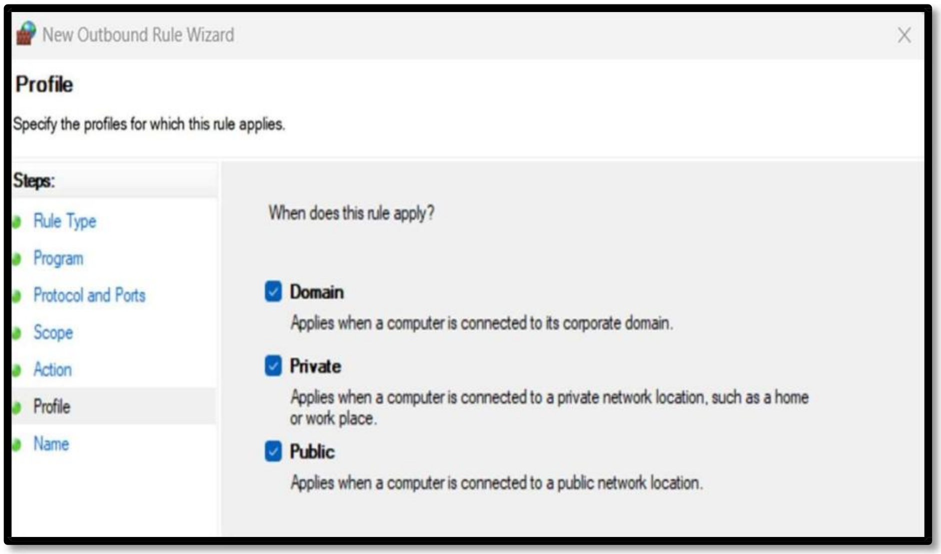
○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

- Click **Next**.

8. **Apply the Rule to Profiles**:
   - Choose the profile(s) where the rule will apply:
     - **Domain**: For domain-connected networks.
     - **Private**: For private networks like home or work.
     - **Public**: For public networks like cafes or airports.



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

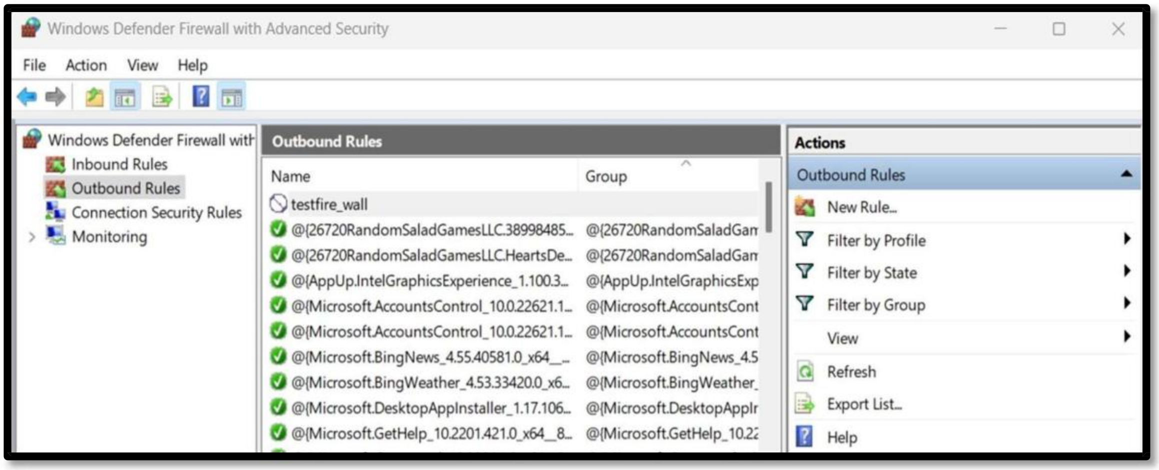
☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

- Click **Next**.

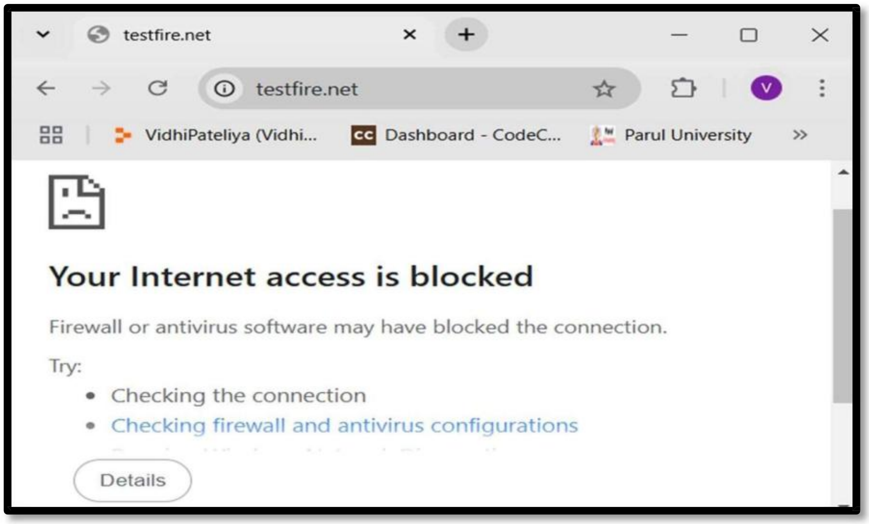
9. **Name and Describe the Rule**:
    - Provide a meaningful name (e.g., "testfire_wall").
    - Optionally, add a description for reference.
    - Click **Finish**.

10. **Verify the Rule**:
    - Go back to the **Inbound Rules** or **Outbound Rules** list.
    - Locate your new rule by name and ensure it is enabled.



Name	Group
testfire_wall	
✓ @{26720RandomSaladGamesLLC.38998485...	@{26720RandomSaladGan
✓ @{26720RandomSaladGamesLLC.HeartsDe...	@{26720RandomSaladGan
✓ @{AppUp.IntelGraphicsExperience_1.100.3...	@{AppUp.IntelGraphicsExp
✓ @{Microsoft.AccountsControl_10.0.22621.1...	@{Microsoft.AccountsCont
✓ @{Microsoft.AccountsControl_10.0.22621.1...	@{Microsoft.AccountsCont
✓ @{Microsoft.BingNews_4.55.40581.0_x64__...	@{Microsoft.BingNews_4.5
✓ @{Microsoft.BingWeather_4.53.33420.0_x6...	@{Microsoft.BingWeather_
✓ @{Microsoft.DesktopAppInstaller_1.17.106...	@{Microsoft.DesktopAppIr
✓ @{Microsoft.GetHelp_10.2201.421.0_x64__8...	@{Microsoft.GetHelp_10.22

11. **Test the Configuration**:
    - Attempt to use the program or port affected by the rule to confirm its behaviour.



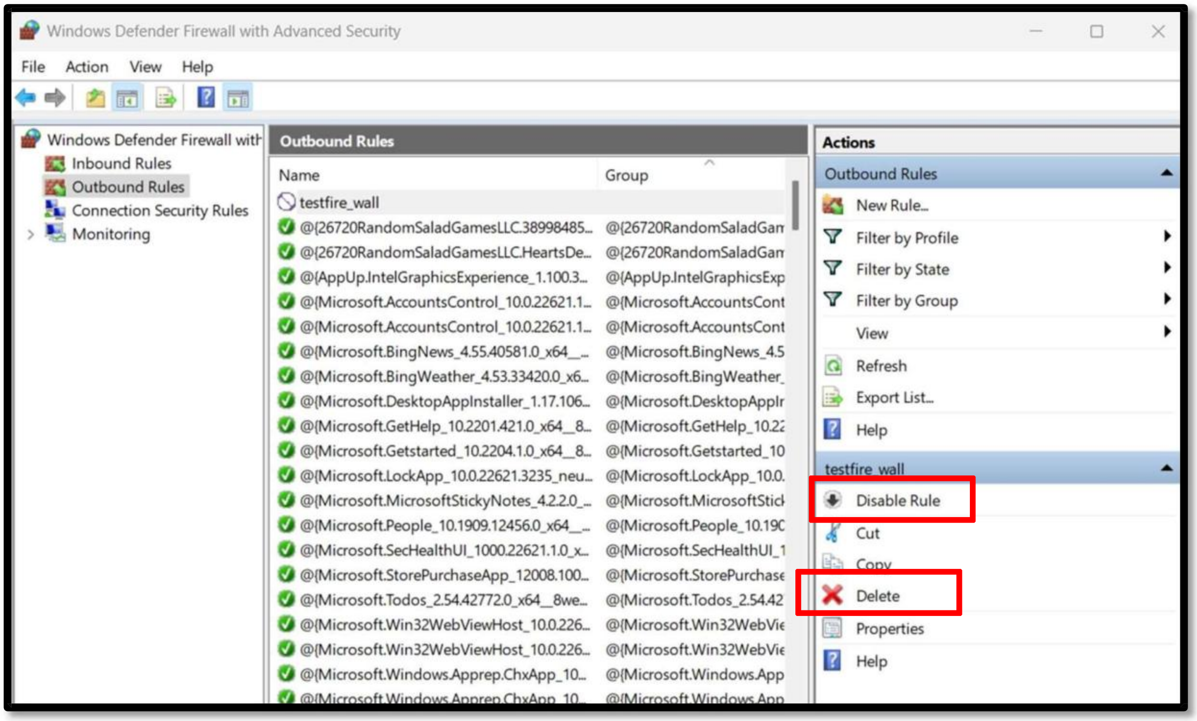
Your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

Try:

- Checking the connection
- Checking firewall and antivirus configurations

12. **Edit or Delete Rules** (if necessary):
    - Right-click the rule and choose **Properties** to modify settings.
    - Select **Disable Rule** or **Delete** to deactivate or remove it.



Name	Group
testfire_wall	
@{26720RandomSaladGamesLLC.38998485...	@{26720RandomSaladGam
@{26720RandomSaladGamesLLC.HeartsDe...	@{26720RandomSaladGam
@{AppUp.IntelGraphicsExperience_1.100.3...	@{AppUp.IntelGraphicsExp
@{Microsoft.AccountsControl_10.0.22621.1...	@{Microsoft.AccountsCont
@{Microsoft.AccountsControl_10.0.22621.1...	@{Microsoft.AccountsCont
@{Microsoft.BingNews_4.55.40581.0_x64__...	@{Microsoft.BingNews_4.5
@{Microsoft.BingWeather_4.53.33420.0_x6...	@{Microsoft.BingWeather_
@{Microsoft.DesktopAppInstaller_1.17.106...	@{Microsoft.DesktopAppIr
@{Microsoft.GetHelp_10.2201.421.0_x64__8...	@{Microsoft.GetHelp_10.22
@{Microsoft.Getstarted_10.2204.1.0_x64__8...	@{Microsoft.Getstarted_10
@{Microsoft.LockApp_10.0.22621.3235_neu...	@{Microsoft.LockApp_10.0.
@{Microsoft.MicrosoftStickyNotes_4.2.2.0_...	@{Microsoft.MicrosoftStick
@{Microsoft.People_10.1909.12456.0_x64__...	@{Microsoft.People_10.190
@{Microsoft.SecHealthUI_1000.22621.1.0_x...	@{Microsoft.SecHealthUI_1
@{Microsoft.StorePurchaseApp_12008.100...	@{Microsoft.StorePurchase
@{Microsoft.Todos_2.54.42772.0_x64__8we...	@{Microsoft.Todos_2.54.42
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebVie
@{Microsoft.Win32WebViewHost_10.0.226...	@{Microsoft.Win32WebVie
@{Microsoft.Windows.Apprep.ChxApp_10...	@{Microsoft.Windows.App
@{Microsoft.Windows.Apprep.ChxApp_10...	@{Microsoft.Windows.App