Task 4 (Elevate Labs)

Date:26-09-2025

Task 4: Setup and Use a Firewall on Windows/Linux

Objective of the task: Configuring and testing basic firewall rules to allow or block traffic.

Tools Used: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

Windows Firewall:

> Windows Firewall (now called Windows Defender Firewall) is Microsoft's built-in firewall that helps protect Windows PCs from unauthorized access and harmful network traffic.

Features of Windows Firewall:

- Pre-installed & Free – Comes with every Windows OS, no need for extra software.
- Inbound & Outbound Filtering – Can control both incoming and outgoing traffic.
- Profiles – Has different rules for:
- Domain Network (workplace network)
- Private Network (home/trusted network)
- Public Network (cafes, airports, etc.)
- Application Control – Prompts you to allow or block applications (like when you install a game or program that needs internet access).
- Custom Rules – Lets you create rules to block/allow traffic by port, protocol, or IP address.

How to check whether Firewall is turned on/off:

Navigate to Windows Security from start menu then click on Firewall and network protection

We can set firewall rules to specific application, service, or a program

Using Port Number→ Block or allow the traffic

Using Custom rule

How to create a custom rule in windows firewall: -

Steps to Create a Custom Rule:

Step1: Open Windows Firewall

- Press Win + R → type wf.msc → press Enter.
- (This opens Windows Defender Firewall with Advanced Security.)

Step2: Choose Rule Type

- In the left panel, click Inbound Rules (for traffic coming into your PC) or Outbound Rules (for traffic leaving your PC).
- On the right side, click New Rule…

Step3: Select Rule Type

Options will appear:

- Program → Block or allow a specific app.
- Port → Block or allow traffic on a specific port (e.g., 80 for HTTP).
- Predefined → Choose from Windows services.
- Custom → Advanced control (specific IPs, protocols, etc.).
- Select one (e.g., Port) → click Next.

Step4: Define Rule Details

- Example (Port):
- Choose TCP or UDP.
- Enter port number(s) (e.g., 80).
- Click Next.

Step5: Action

Choose what to do with the connection:

- Allow the connection
- Allow if secure
- Block the connection
- Pick one → click Next.

Step6: Profile

Select when the rule applies:

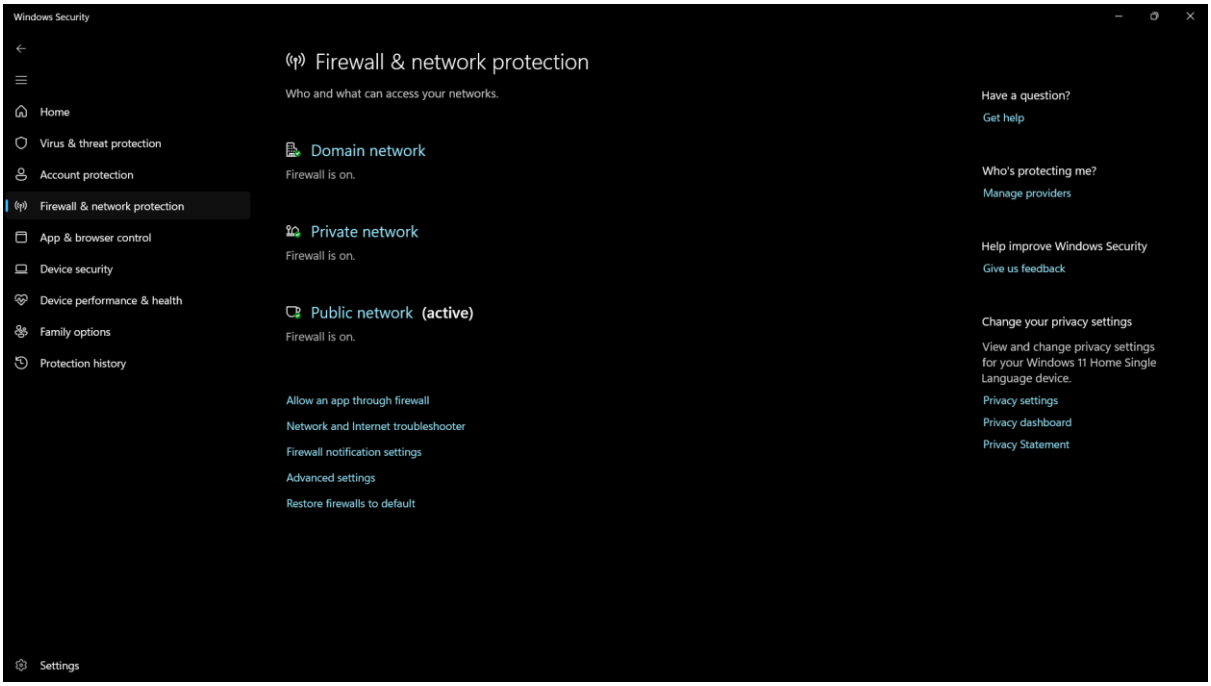
- Domain
- Private
- Public

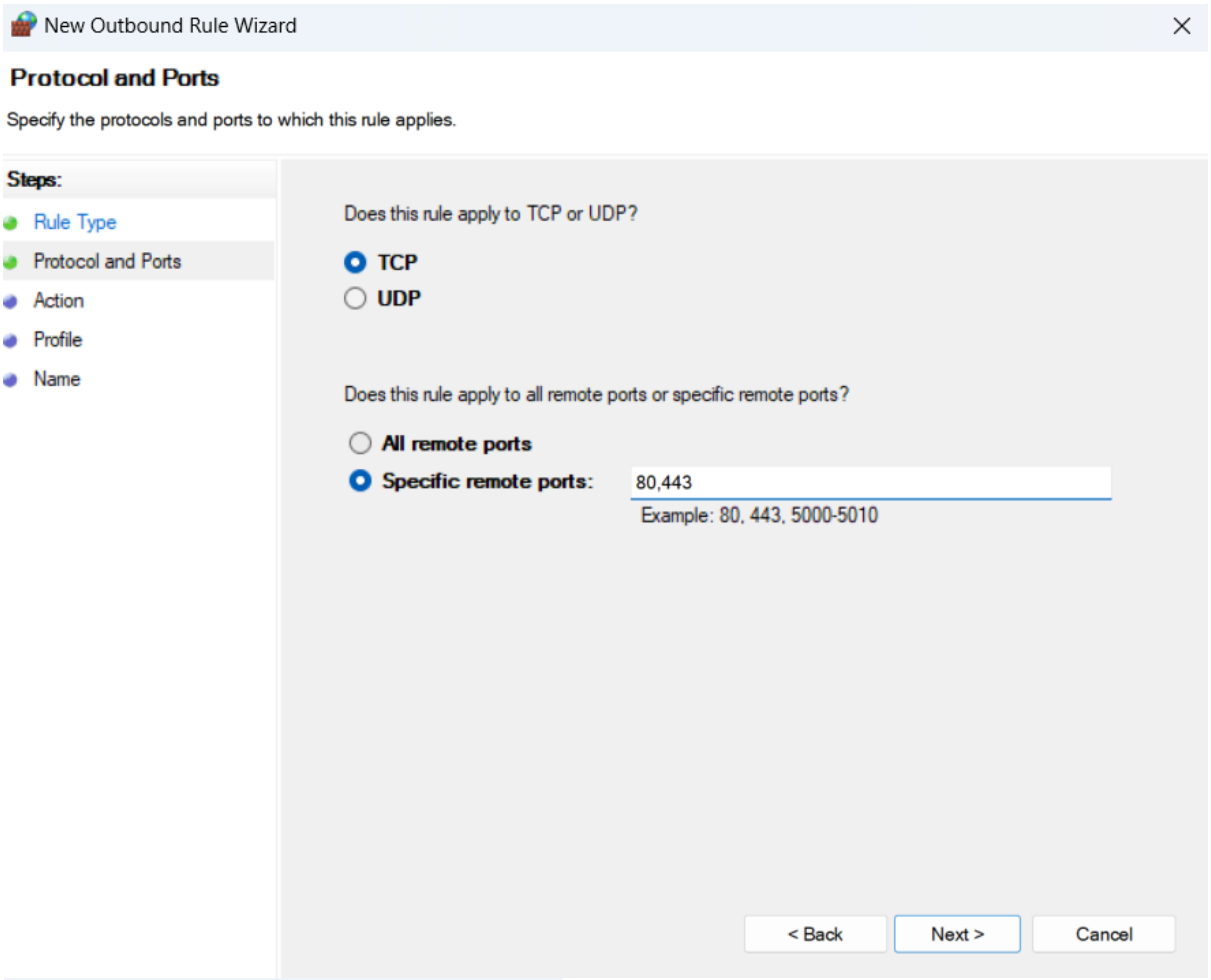
(You can select all three if unsure.)

Step7: Name the Rule

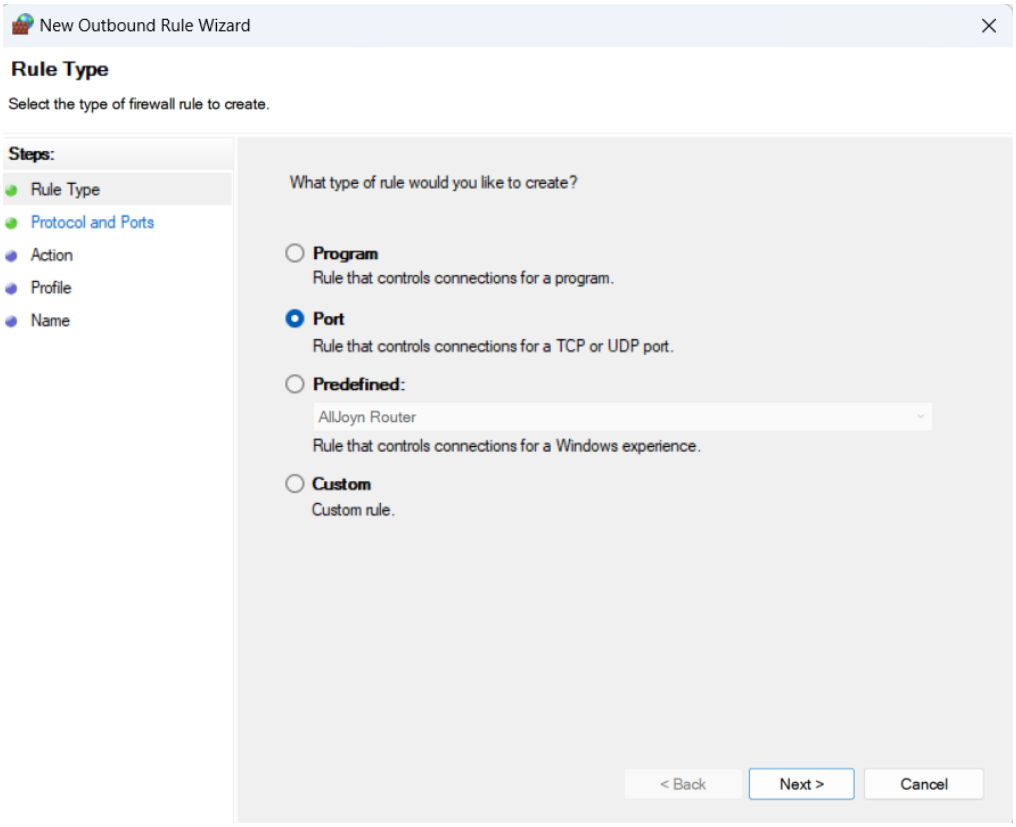
- Give it a meaningful name (e.g., Block Port 80).
- Click Finish.

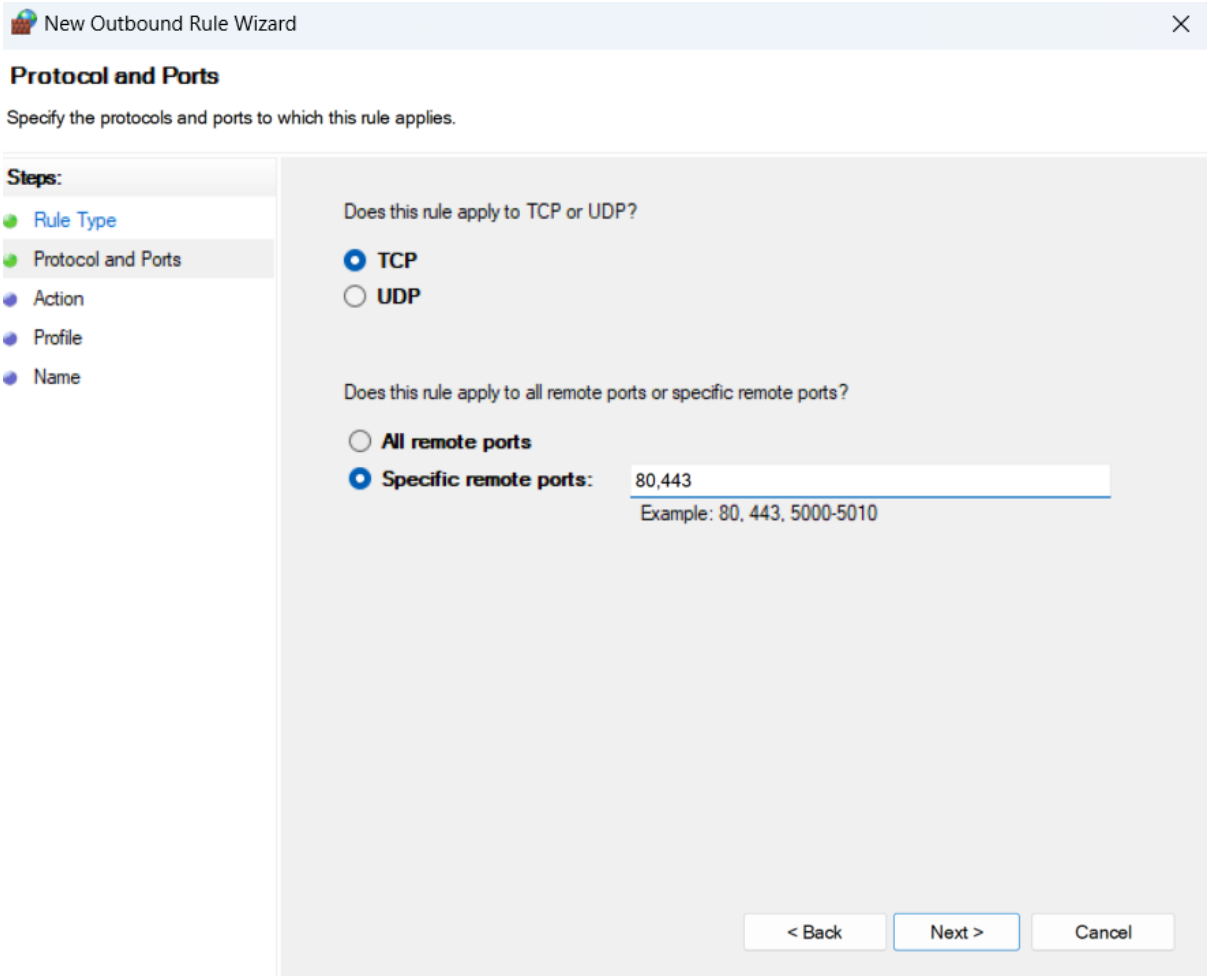
Screenshots:

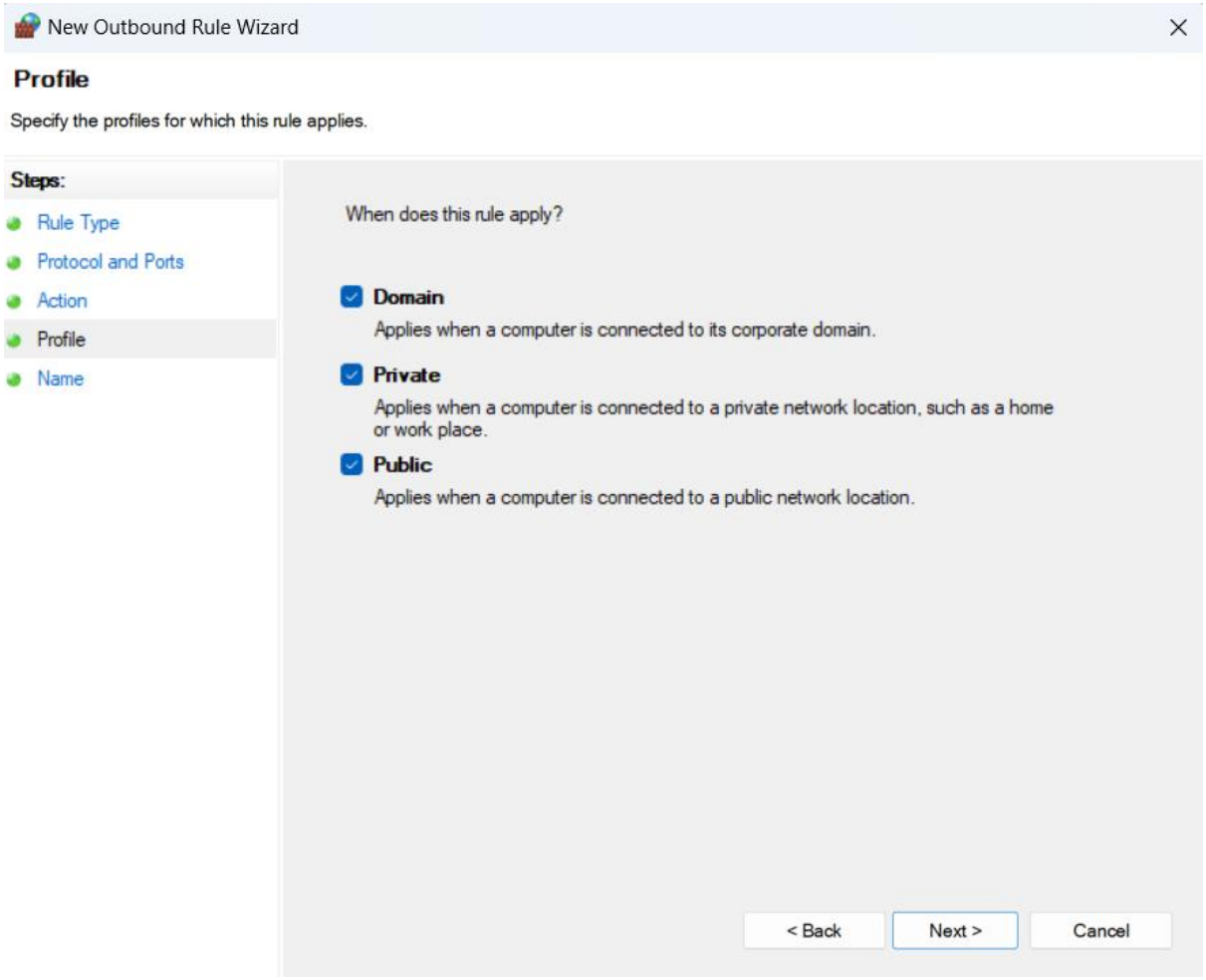


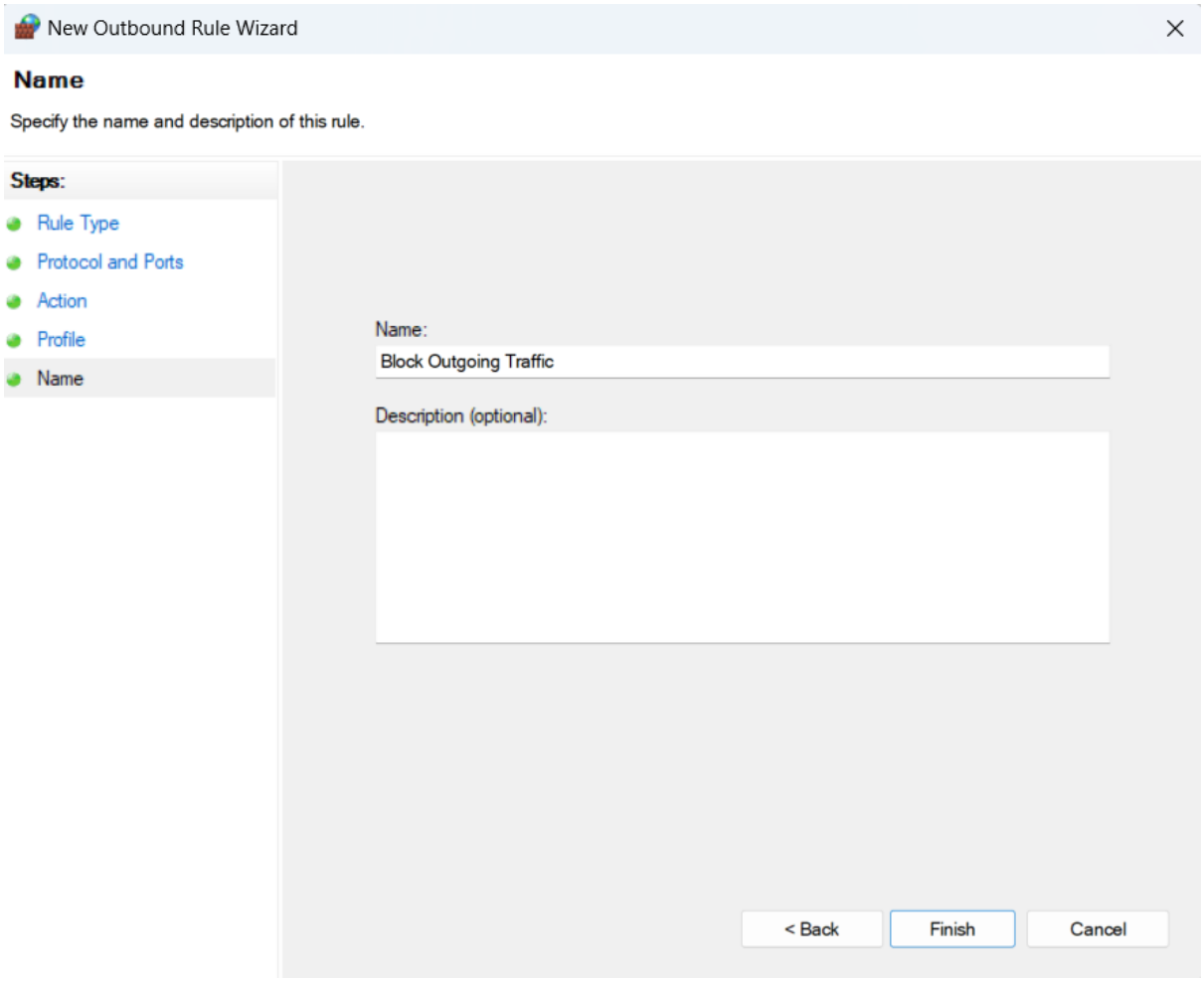

New Outbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all remote ports or specific remote ports?
All remote ports
Specific remote ports:
80,443
Example: 80, 443, 5000-5010
< Back
Next >
Cancel

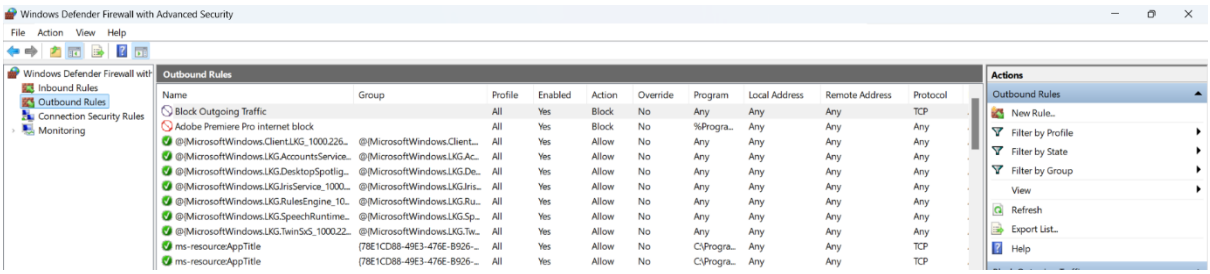

Windows Defender Firewall with
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

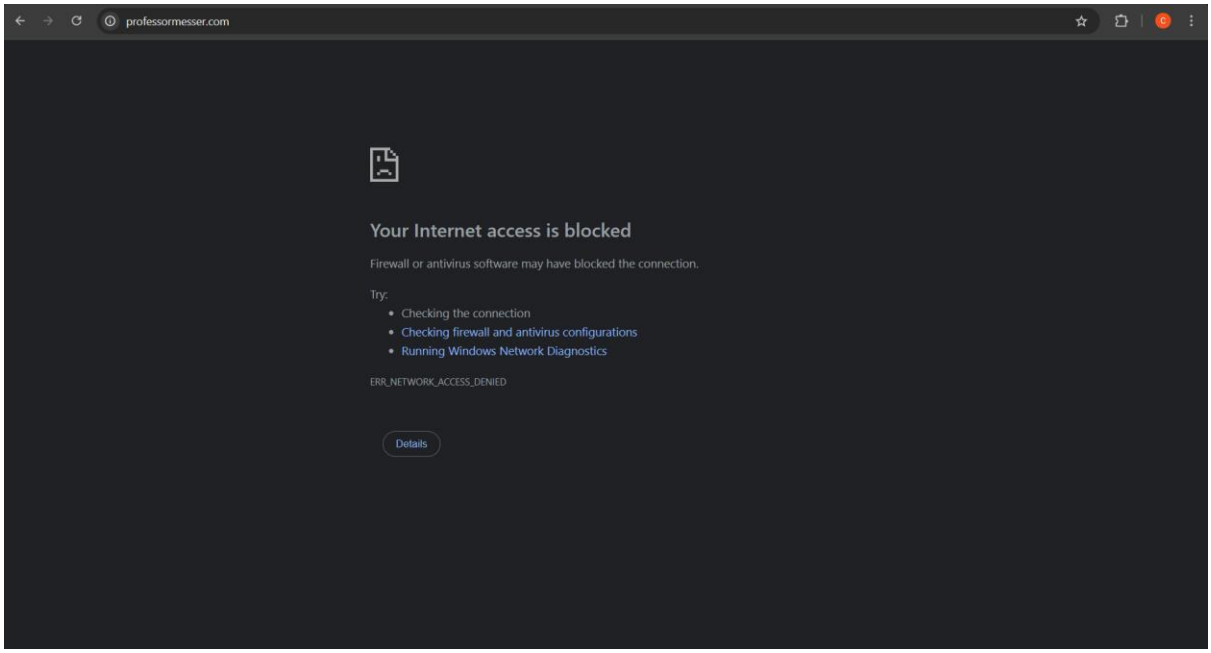

New Outbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


New Outbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all remote ports or specific remote ports?
All remote ports
Specific remote ports:
80,443
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Outbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
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.
< Back
Next >
Cancel


New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Block Outgoing Traffic
Description (optional):
< Back
Finish
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
Block Outgoing Traffic All Yes Block No Any Any Any TCP
Adobe Premiere Pro internet block All Yes Block No %Progra.. Any Any Any
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help



Summary how firewall filters work: -

A firewall filters traffic by examining network packets and applying rules to decide whether to allow, block, or restrict them.

How it works: -

1.Checks source & destination → IP addresses, domain names.

2.Inspects ports & protocols → e.g., port 80 (HTTP), port 443 (HTTPS).

3.Examines application traffic → which program is sending/receiving data.

4.Applies security rules → based on user-defined or default policies.

5.Takes action → allows safe traffic, blocks suspicious or unauthorized traffic.