Setup and Use a Firewall on Windows/Linux

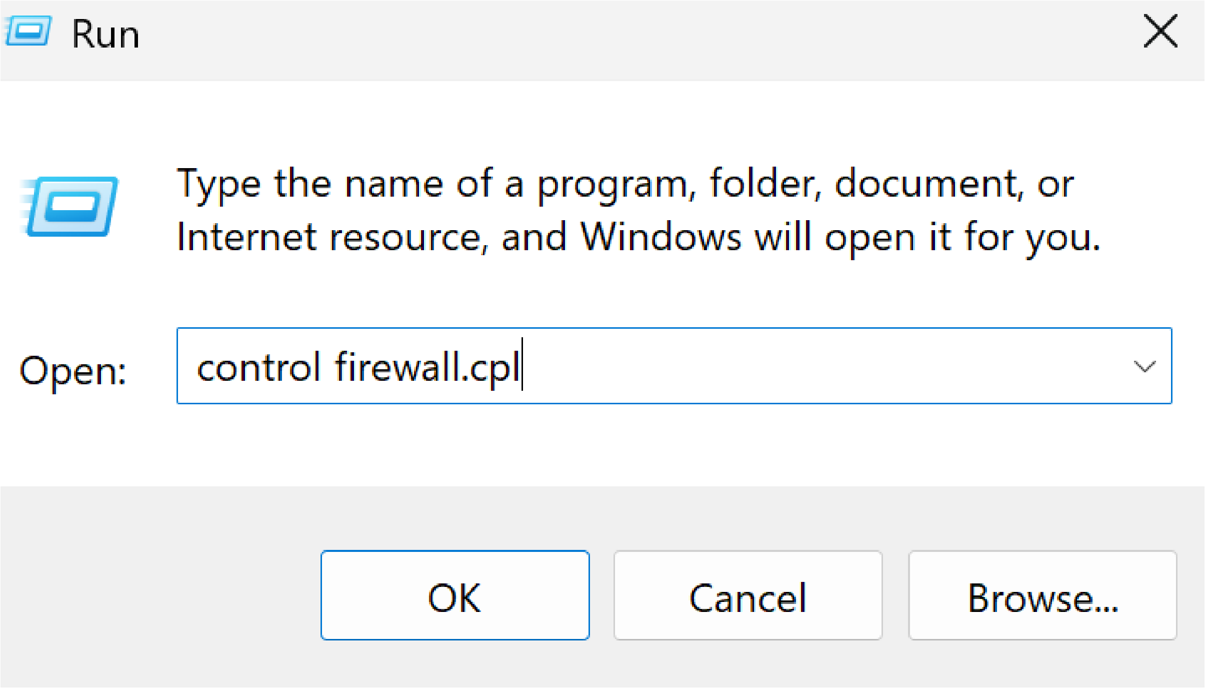
Objective: Configure and test basic firewall rules to allow or block traffic.

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

Deliverables: Screenshot/configuration file showing firewall rules applied.

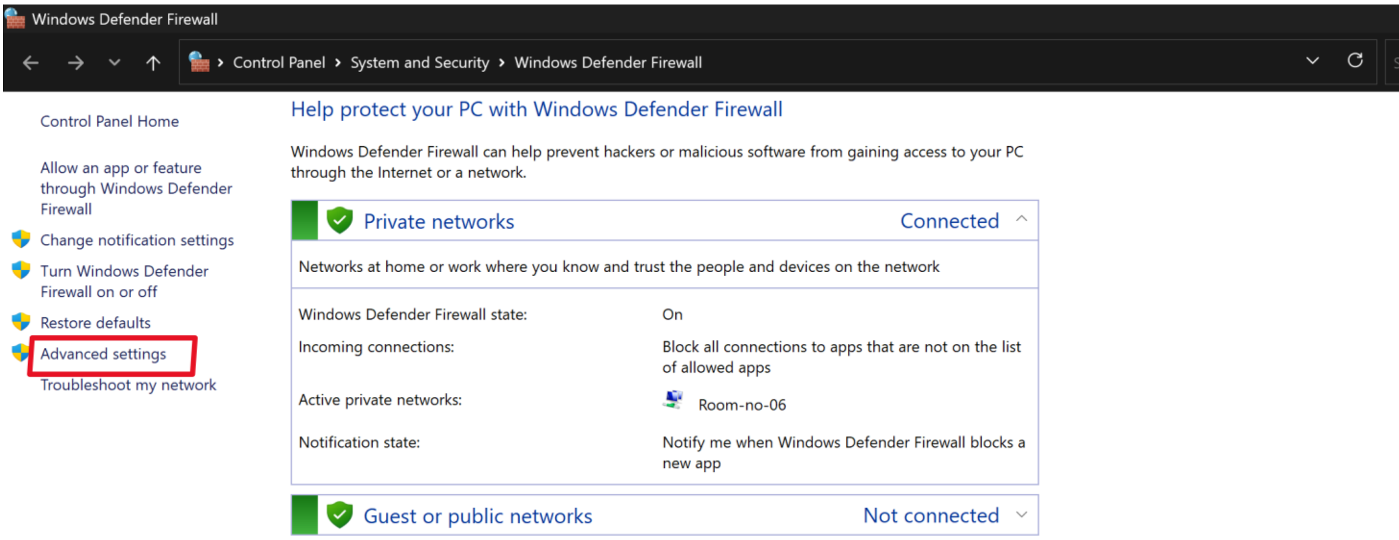
commands or GUI steps used.

We are using here windows defender firewall and configure the rules.


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

Open: control firewall.cpl

After running a command: control firewall.cpl we get this window. now click on advance settings >


Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

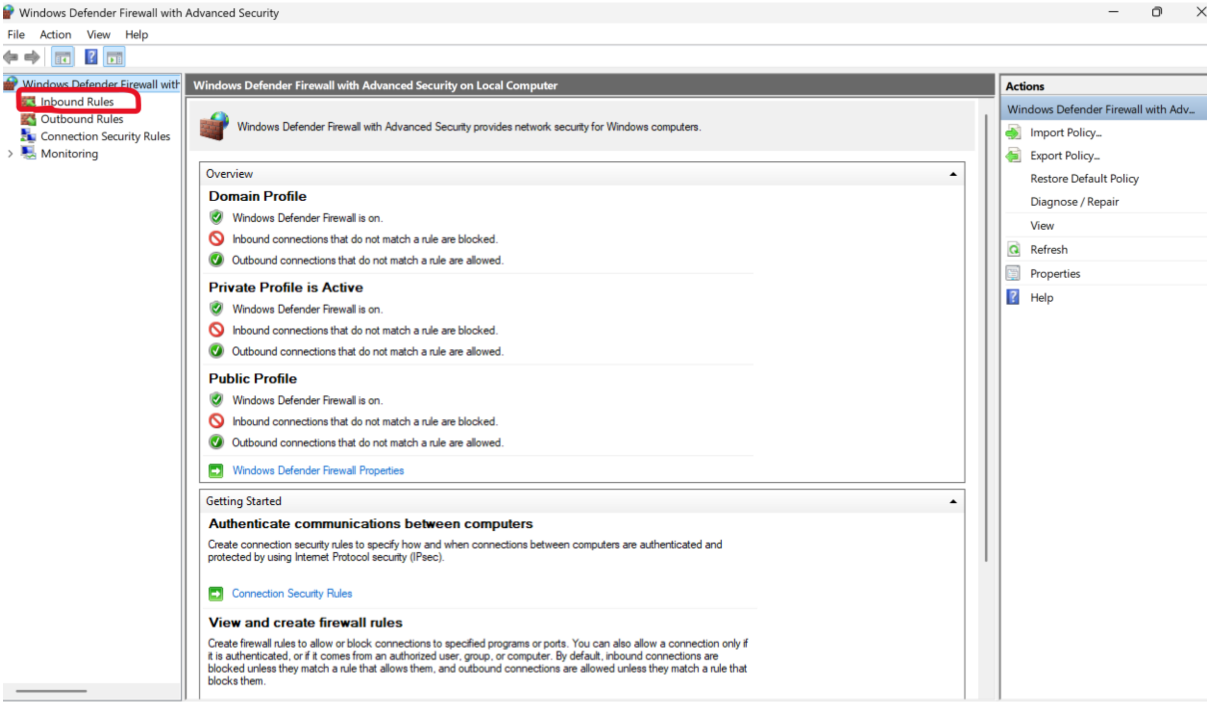
Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Room-no-06
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks Not connected

Then we get the below window that show inbound and outbound firewall rules.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

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 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.

Public 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.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

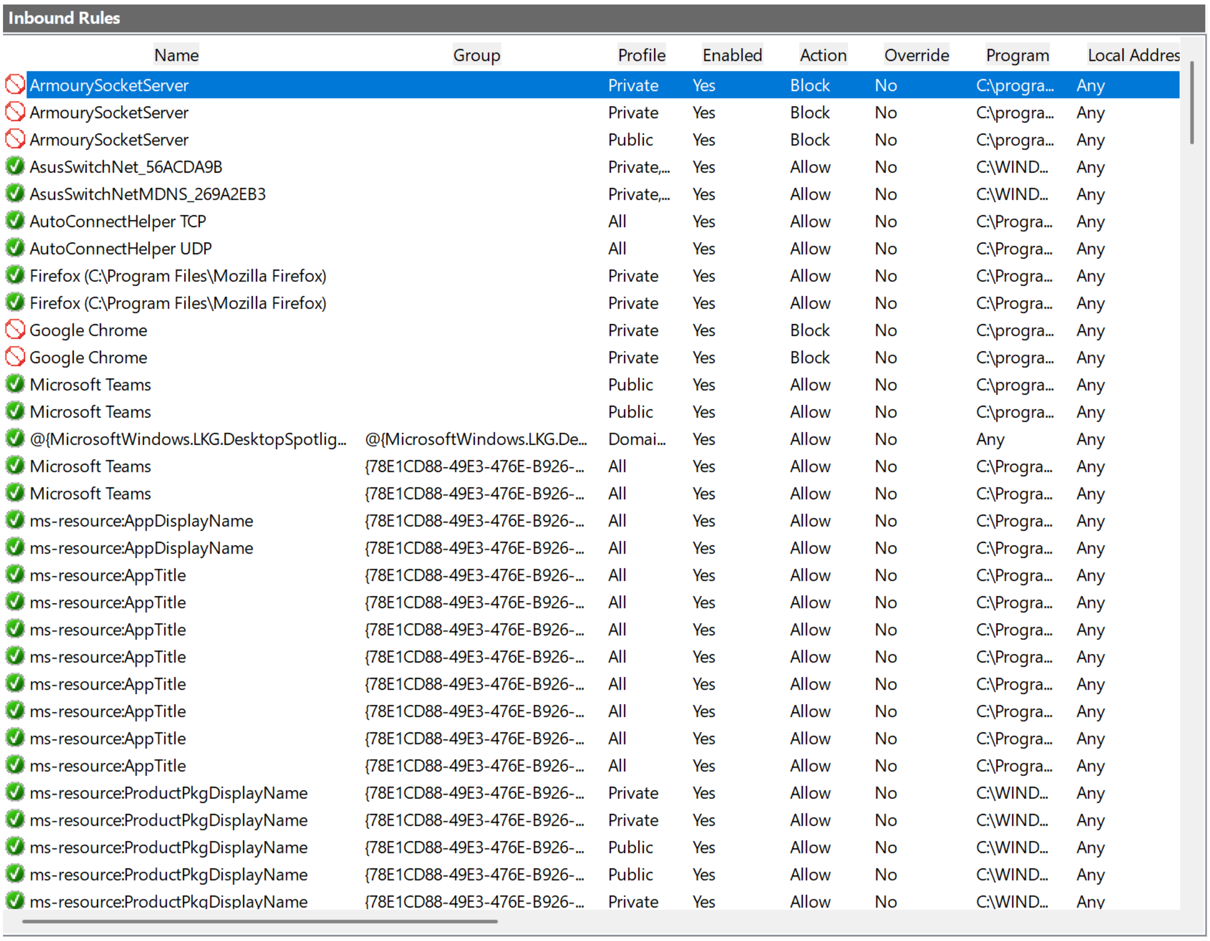
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

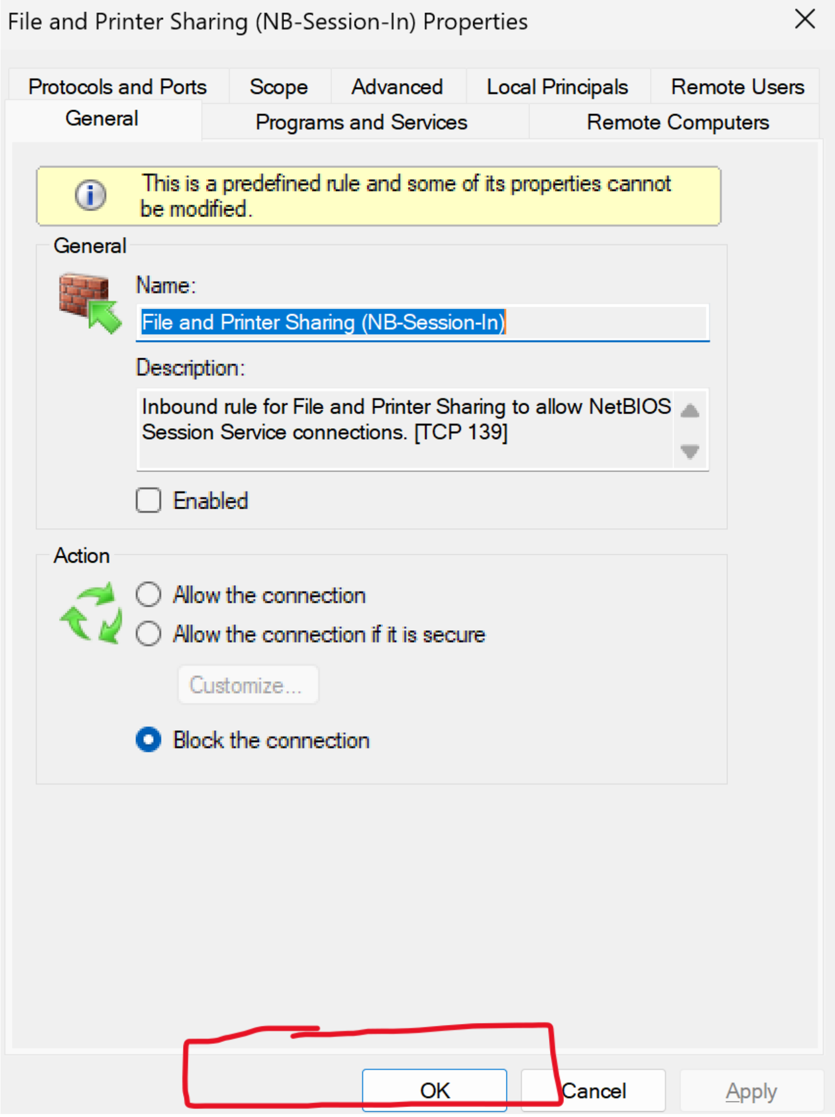
List of inbound current firewall rules.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Addres
⊘ ArmourySocketServer		Private	Yes	Block	No	C:\progra...	Any
⊘ ArmourySocketServer		Private	Yes	Block	No	C:\progra...	Any
⊘ ArmourySocketServer		Public	Yes	Block	No	C:\progra...	Any
✓ AsusSwitchNet_56ACDA9B		Private,...	Yes	Allow	No	C:\WIND...	Any
✓ AsusSwitchNetMDNS_269A2EB3		Private,...	Yes	Allow	No	C:\WIND...	Any
✓ AutoConnectHelper TCP		All	Yes	Allow	No	C:\Progra...	Any
✓ AutoConnectHelper UDP		All	Yes	Allow	No	C:\Progra...	Any
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any
⊘ Google Chrome		Private	Yes	Block	No	C:\progra...	Any
⊘ Google Chrome		Private	Yes	Block	No	C:\progra...	Any
✓ Microsoft Teams		Public	Yes	Allow	No	C:\progra...	Any
✓ Microsoft Teams		Public	Yes	Allow	No	C:\progra...	Any
✓ @{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	Domai...	Yes	Allow	No	Any	Any
✓ Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppDisplayName	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppDisplayName	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
✓ ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any
✓ ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any
✓ ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any
✓ ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any
✓ ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any

Now we set a rule to block a port 139 on firewall for inbound traffic. click ok to apply changes.



File and Printer Sharing (NB-Session-In) Properties

This is a predefined rule and some of its properties cannot be modified.

General

Name: File and Printer Sharing (NB-Session-In)

Description: Inbound rule for File and Printer Sharing to allow NetBIOS Session Service connections. [TCP 139]

□ Enabled

Action

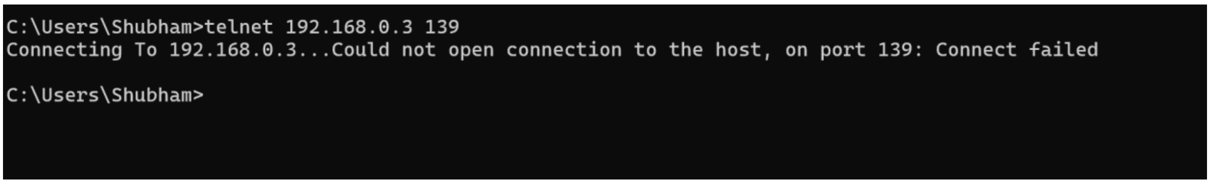
○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

Then we check for the open port using command line, weather the rule is applied or not.

If the port is open then we get a blank screen with cursor, if it is closed we get a “connection failed” message.



```
C:\Users\Shubham>telnet 192.168.0.3 139
Connecting To 192.168.0.3...Could not open connection to the host, on port 139: Connect failed

C:\Users\Shubham>
```

Hence the inbound rule is applied for the port 139 to block it.

Summary how firewall filters traffic

A firewall filters network traffic by examining data packets and comparing them to predefined security rules. These rules determine whether to allow or block the traffic based on criteria like source and destination IP addresses, port numbers, and protocols. Essentially, the firewall acts as a gatekeeper, controlling which data can enter and leave a network based on these rules, ensuring only safe and legitimate traffic is permitted.