

Oxford College

(Affiliated to Tribhuvan University)

Sukkhanagar, Butwal, Rupandehi

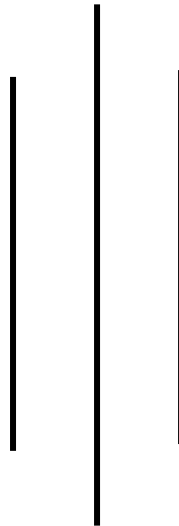


LAB REPORT

Course Code: IT 246

IT Ethics and CyberSecurity

Year: 2081



Submitted By:

Bishal Somare

Submitted To:

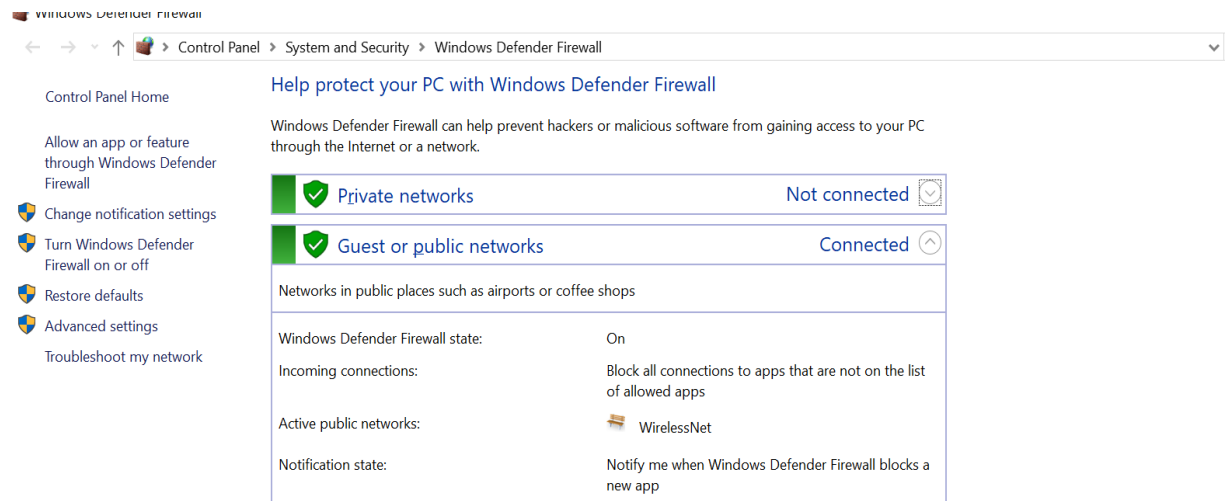
Rahul Shakya

Lab 1: Close TCP Ports in Windows Firewall

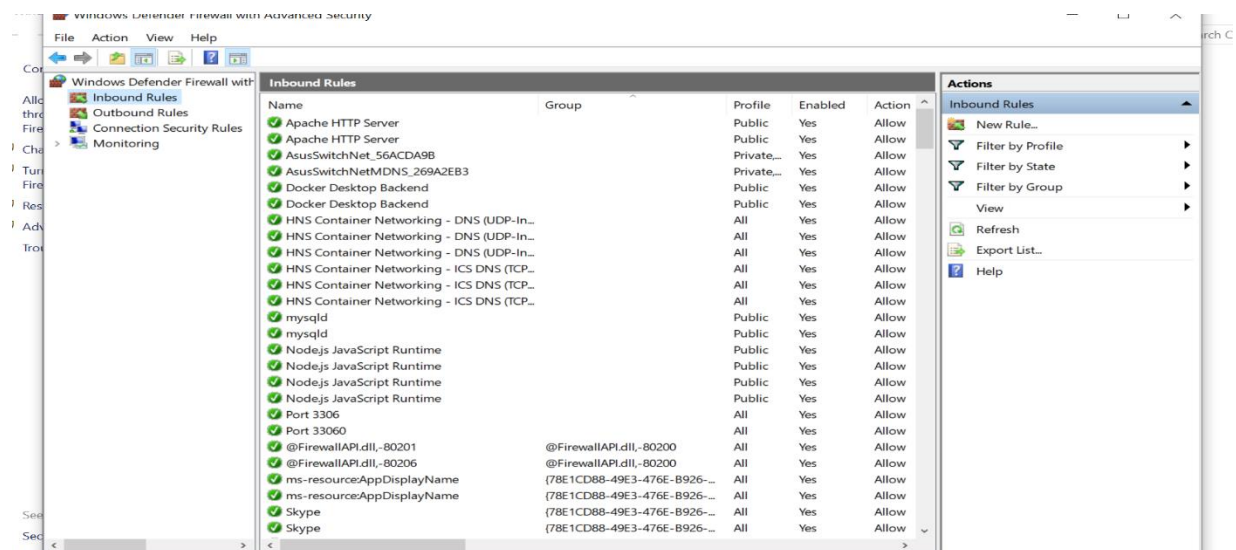
A firewall is a vital component for securing your network, and Windows Firewall offers robust features to manage incoming and outgoing traffic.

Here's how we can close TCP ports using Windows Firewall:

When in the **'Advanced Settings'** of Windows 10 firewall, click the **Advanced settings** link in the left-hand pane of the main firewall dialog. This will bring up the Windows Firewall with Advanced Security window.

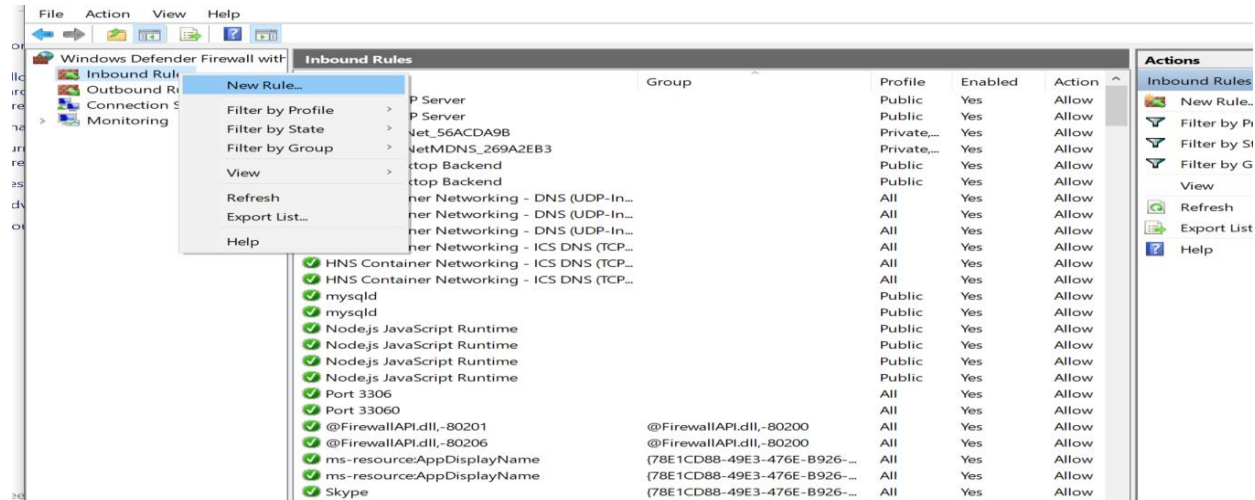


Now, if we can see the firewall window shows a list of rules on the left side. From the list, select Inbound Rules to display the inbound rules section.

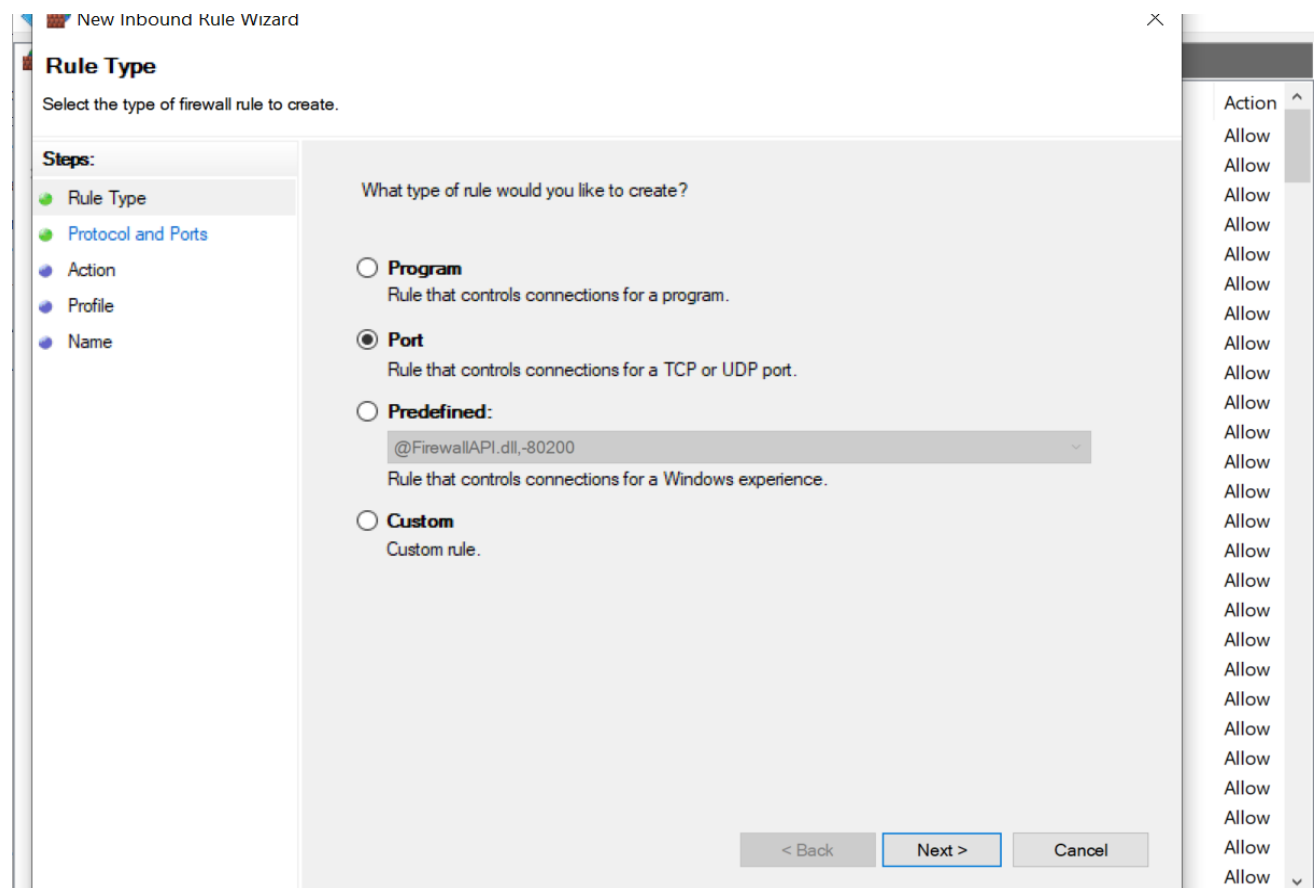


Inbound Rule:

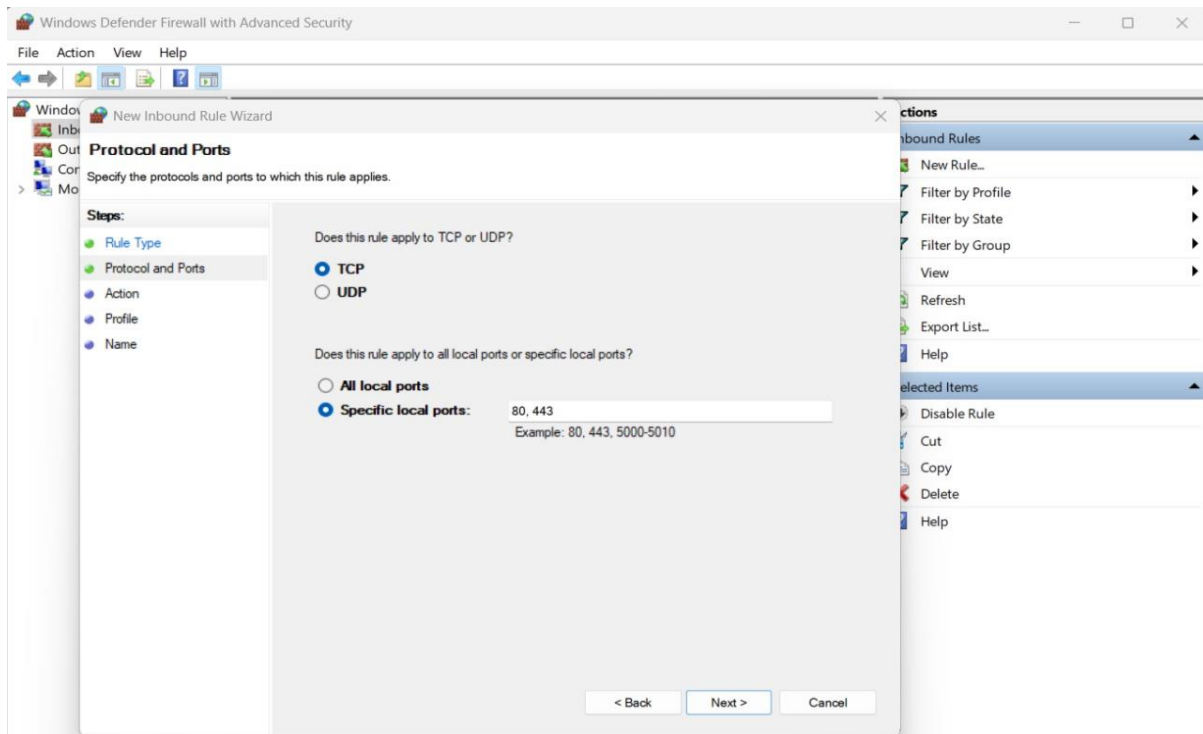
1. Right-click on "Inbound Rules" in the left pane and select "New Rule."



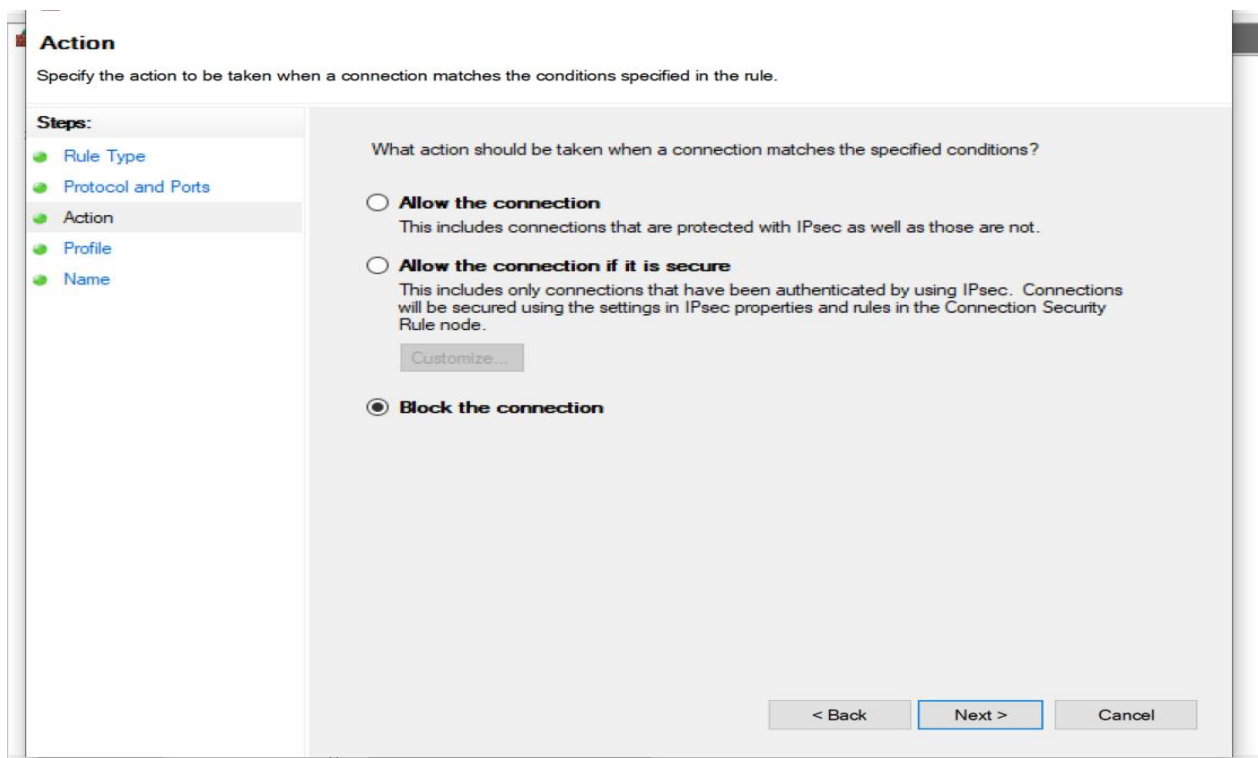
2. Choose "Port" as the rule type and click Next.



3. Select TCP, enter the port number (e.g., 80, 443), and click Next.



4. Choose "Block the connection" and click Next.



5. Check all profiles (Domain, Private, Public) and click Next.

New Incoming 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

6. Provide a name for the rule and click Finish.

New Incoming Rule Wizard

Name

Specify the name and description of this rule.

Steps:

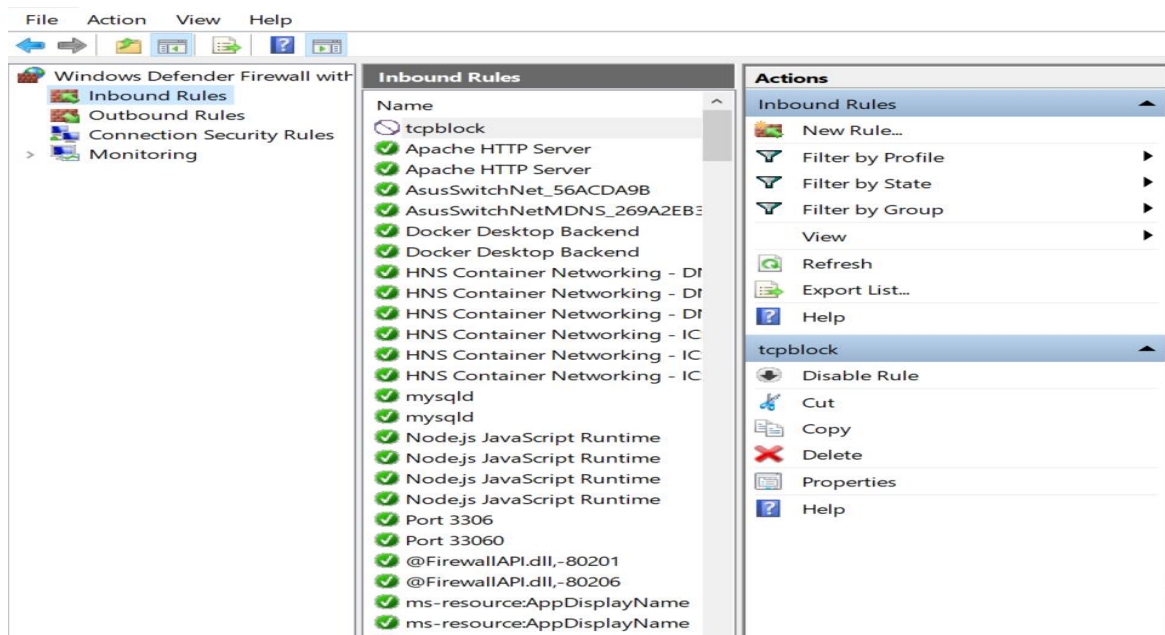
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:
tcpblock

Description (optional):
Block TCP port 80

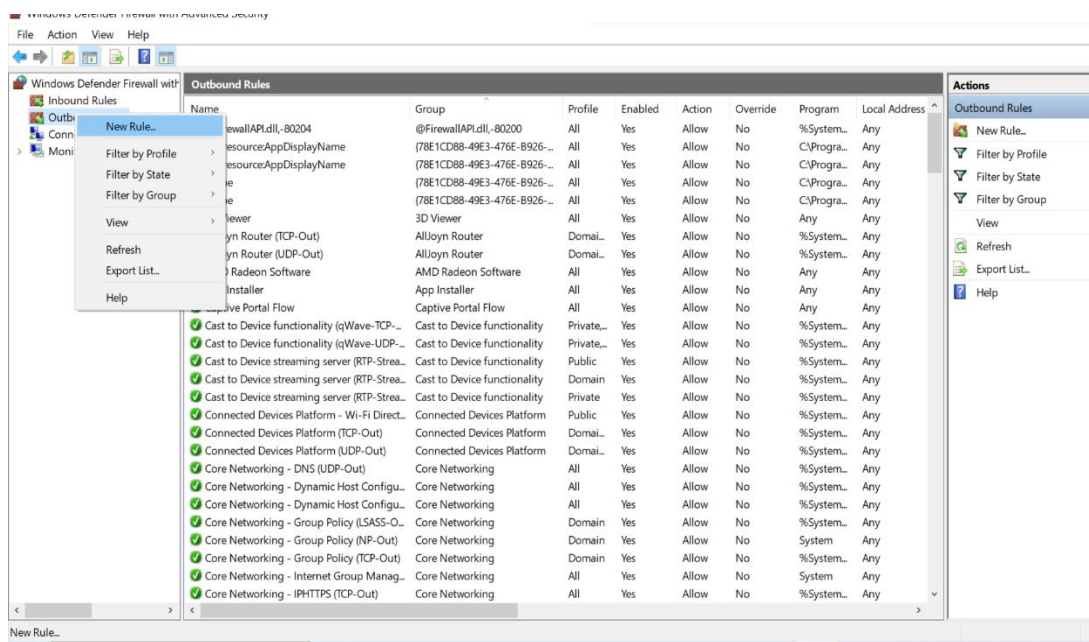
< Back **Finish** Cancel

Now we can see the “tcpblock” on the **Inbound Rules** displaying list.



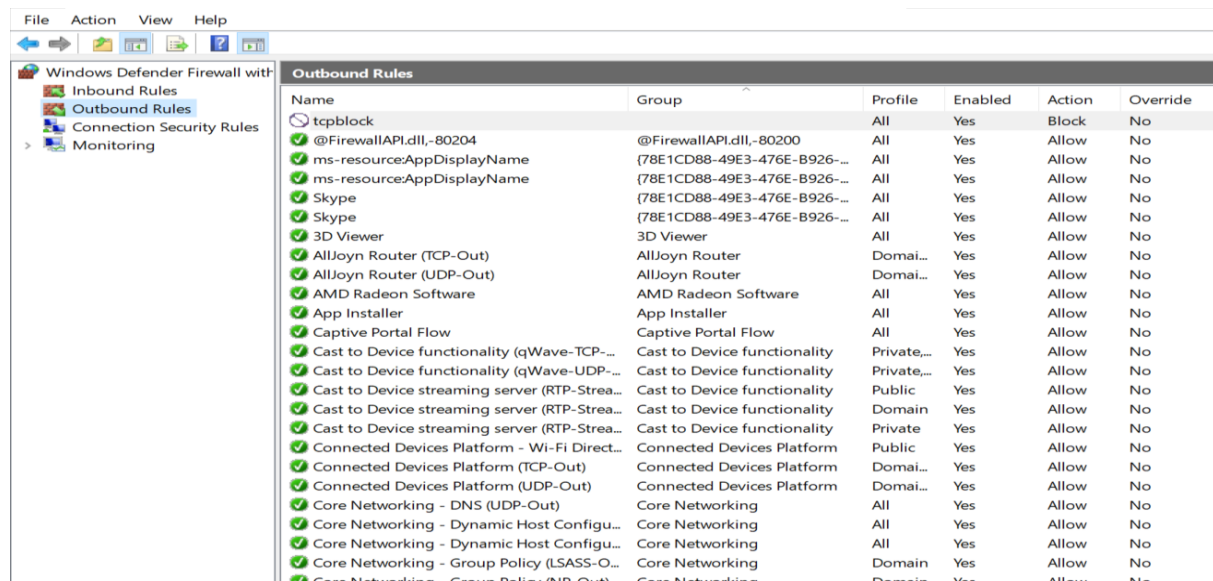
Outbound Rule:

1. Right-click on "Outbound Rules" in the left pane and select "New Rule."



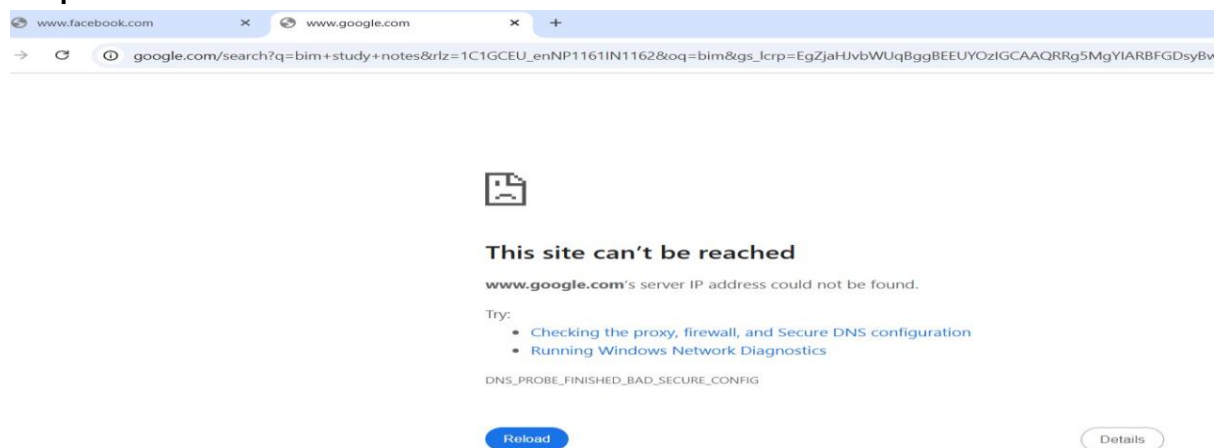
2. Follow steps 3 to 6 from the Inbound Rule section, specifying TCP ports to block outgoing connections.

Now we can see the “tcpblock” on the **Inbound Rules** displaying list.



Outbound Rules						
Name	Group	Profile	Enabled	Action	Override	
tcpblock		All	Yes	Block	No	
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes	Allow	No	
ms-resource:AppDisplayName	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	
ms-resource:AppDisplayName	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	
Skype	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	
Skype	{78E1CD88-49E3-476E-B926-...}	All	Yes	Allow	No	
3D Viewer	3D Viewer	All	Yes	Allow	No	
AllJoyn Router (TCP-Out)	AllJoyn Router	Domain...	Yes	Allow	No	
AllJoyn Router (UDP-Out)	AllJoyn Router	Domain...	Yes	Allow	No	
AMD Radeon Software	AMD Radeon Software	All	Yes	Allow	No	
App Installer	App Installer	All	Yes	Allow	No	
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private...	Yes	Allow	No	
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private...	Yes	Allow	No	
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domain...	Yes	Allow	No	
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domain...	Yes	Allow	No	
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	
Core Networking - Group Policy (LSASS-O...	Core Networking	Domain	Yes	Allow	No	
Core Networking - Group Policy (NB-Out)	Core Networking	Domain	Yes	Allow	No	

Output:



After blocking outbound traffic on **port 80 (HTTP)** and **port 443 (HTTPS)** using Windows Firewall, an attempt to access websites such as **bimstudynotes.com, facebook.com** using **Google Chrome** results in a failed connection.

Since both HTTP and HTTPS ports are blocked:

- The browser cannot establish a TCP connection to the server.
- The request does not reach the website.
- Therefore, the website fails to load.

Lab 2: Securely Sharing Files and Folders in a Windows Network

In a networked environment, sharing files and folders requires careful consideration of permissions to ensure security.

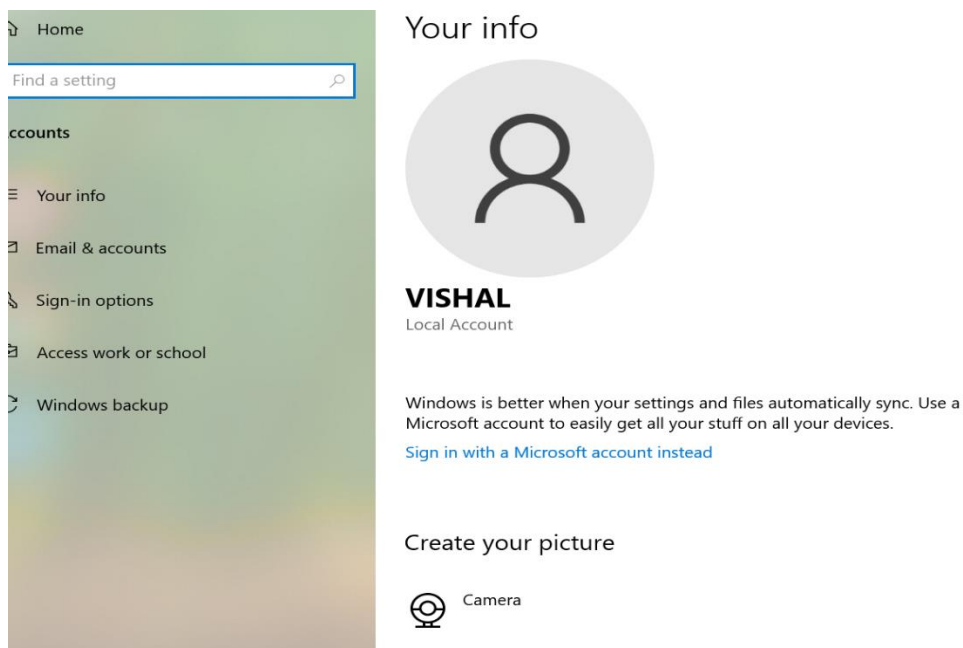
We have to follow these steps to securely share files and folders with others on our network:

Step 1: Create User Accounts

To enhance security, it's advisable not to use administrative accounts for everyday tasks like file sharing. Administrative accounts have elevated privileges, and using them unnecessarily increases the risk of unintentional system changes or malicious activity. Instead, create standard user accounts for everyday use.

- Create a new user (e.g., username: "vishal").

Creating non-administrative user accounts helps maintain the security and integrity of the system by limiting access to sensitive system resources and reducing the likelihood of unauthorized changes.

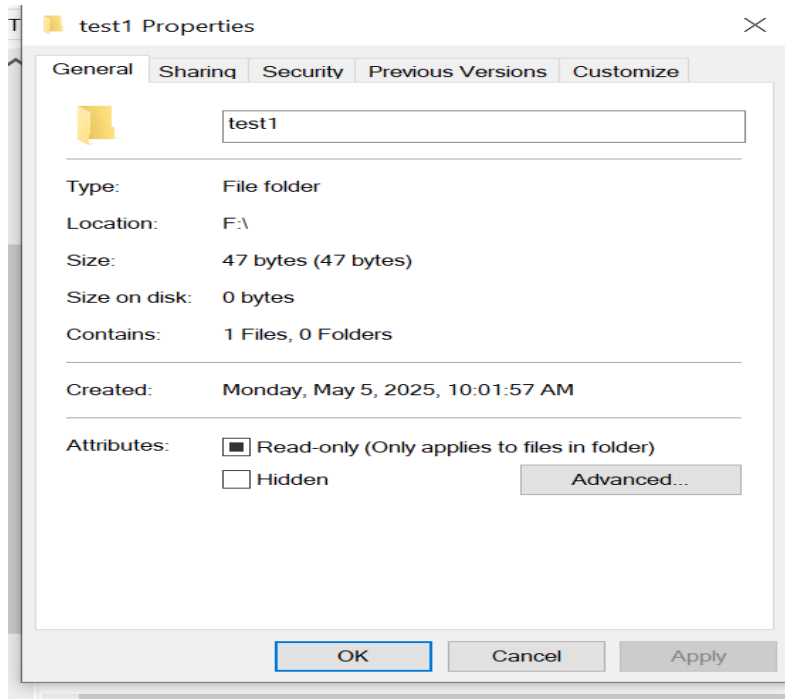


After Creating the New Account, Log in to that Account and Proceed to Step 2.

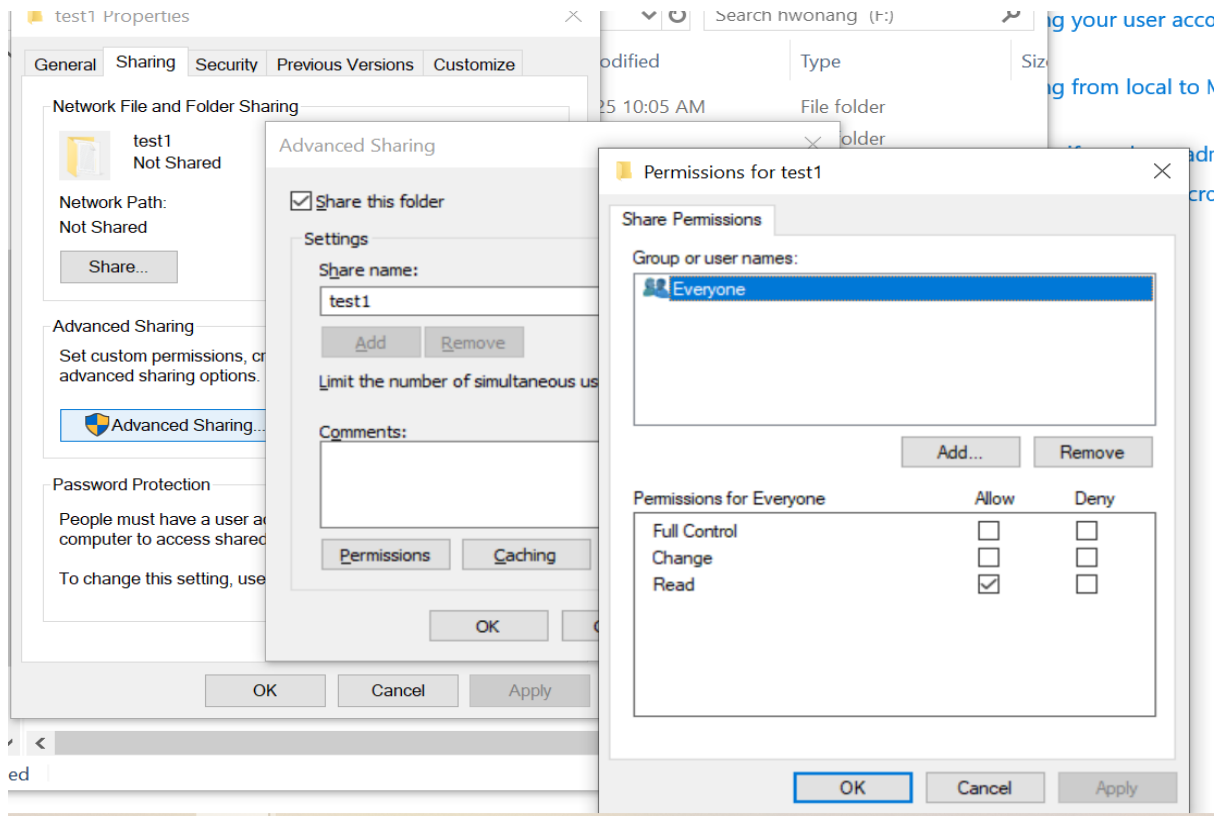
Step 2: Create a Shared Folder

1. Log in to the newly created user account (e.g., "vishal").

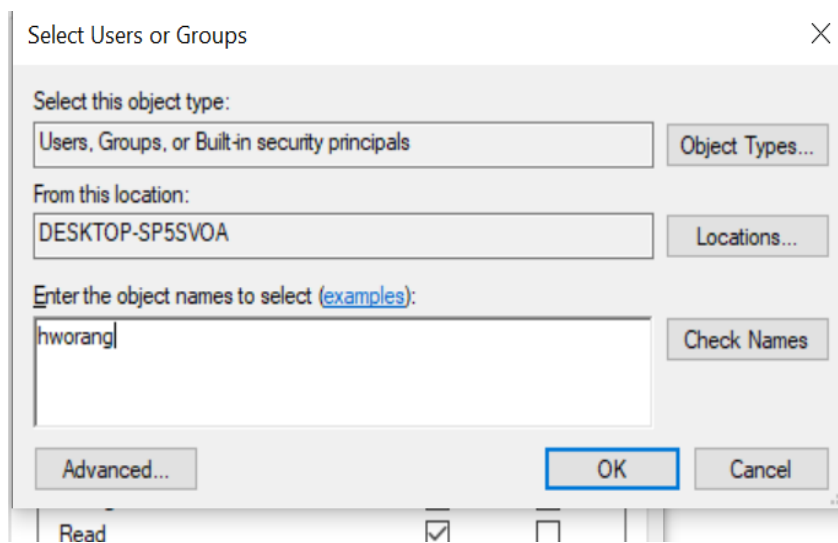
2. Navigate to the drive where you want to create the shared folder (e.g., F drive).
3. Right-click inside the drive and select “New” > “Folder”.
4. Name the new folder (e.g., “test1”) and press “Enter”.
5. Create files within the folder that needed to share on network.
6. Right-click on the folder, select “Properties”, and navigate to the “Sharing” tab.



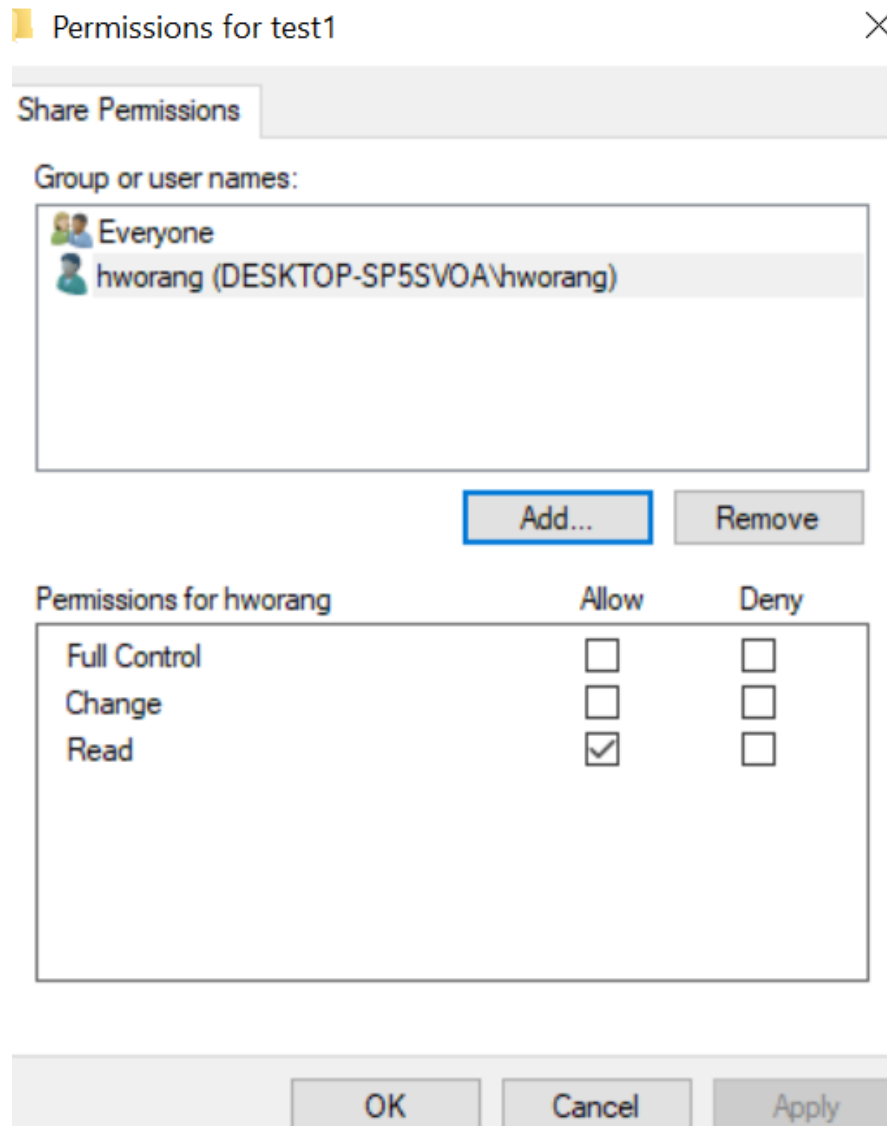
5. Click “Advanced Sharing” and then “Permissions”.



6. Click “Add” to add the previously created users, click “Check Names”, and then “OK”.

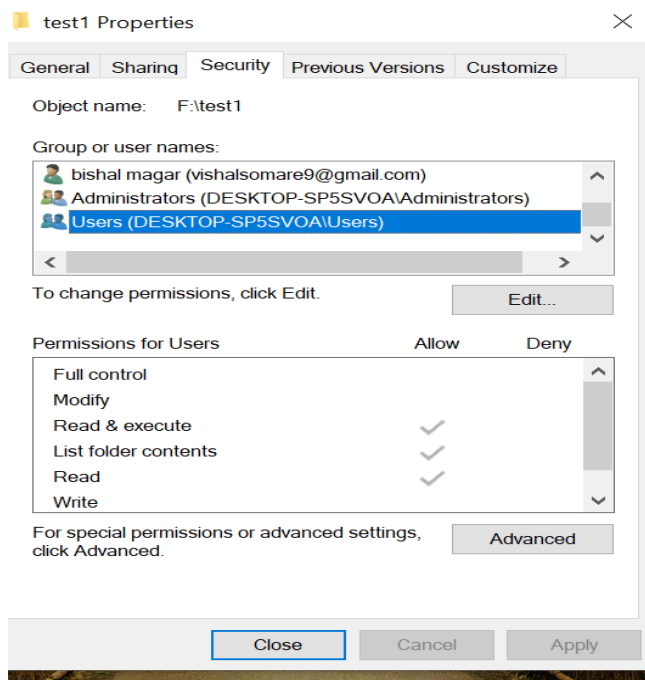


7. Click “Apply”.

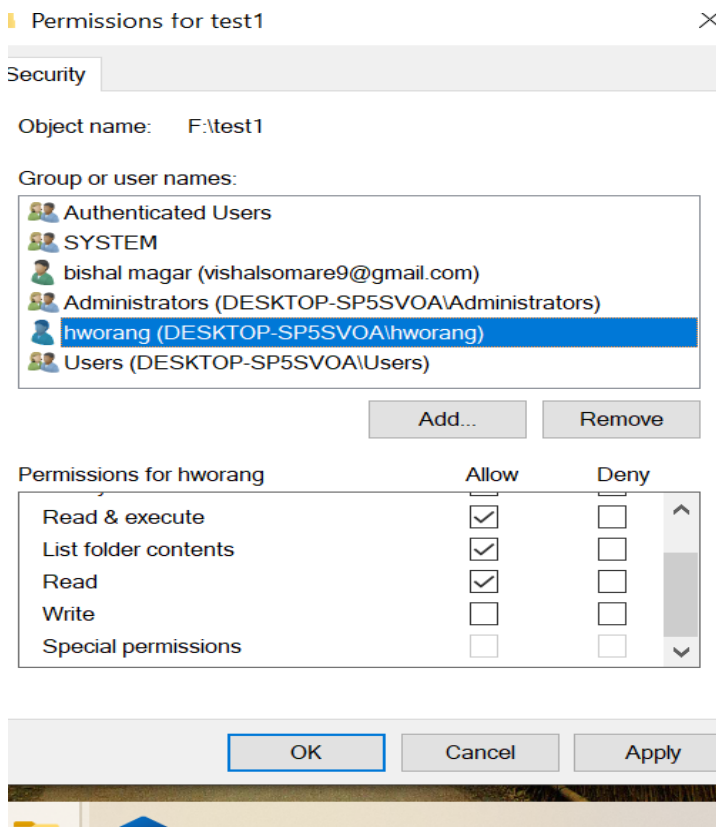


Step 3: Set Security Permissions

1. In the folder properties window, navigate to the "Security" tab.
2. Select the user whose sharing permissions you want to modify and choose "Edit".



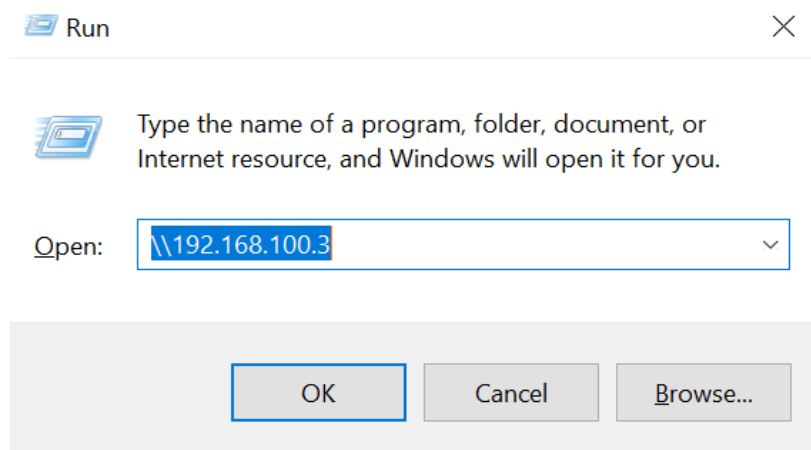
3. Add the previously created users.



4. Click "OK" twice to exit.

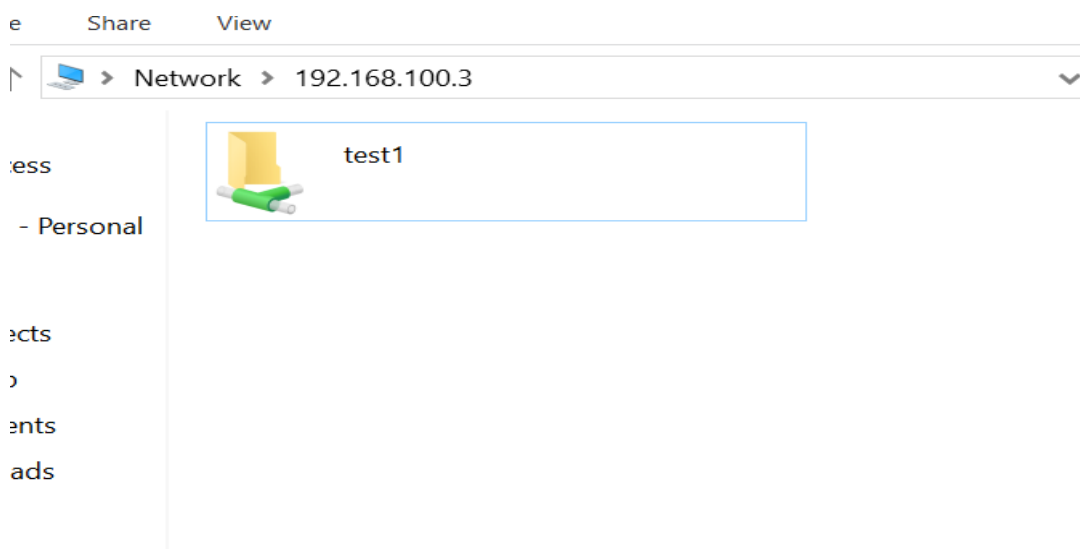
Accessing Shared Files:

1. Enter the IP address of the device containing the shared folder in.



2. Enter the username and password of the device.

3. After authentication, the shared folders will be displayed.



4. Click on the desired folder to access the shared files.

5. Access the shared text files and other content as needed.

By following these steps, you can securely share files and folders within your Windows 10 network, ensuring that only authorized users have access to your shared resources.