

Practical No. 8

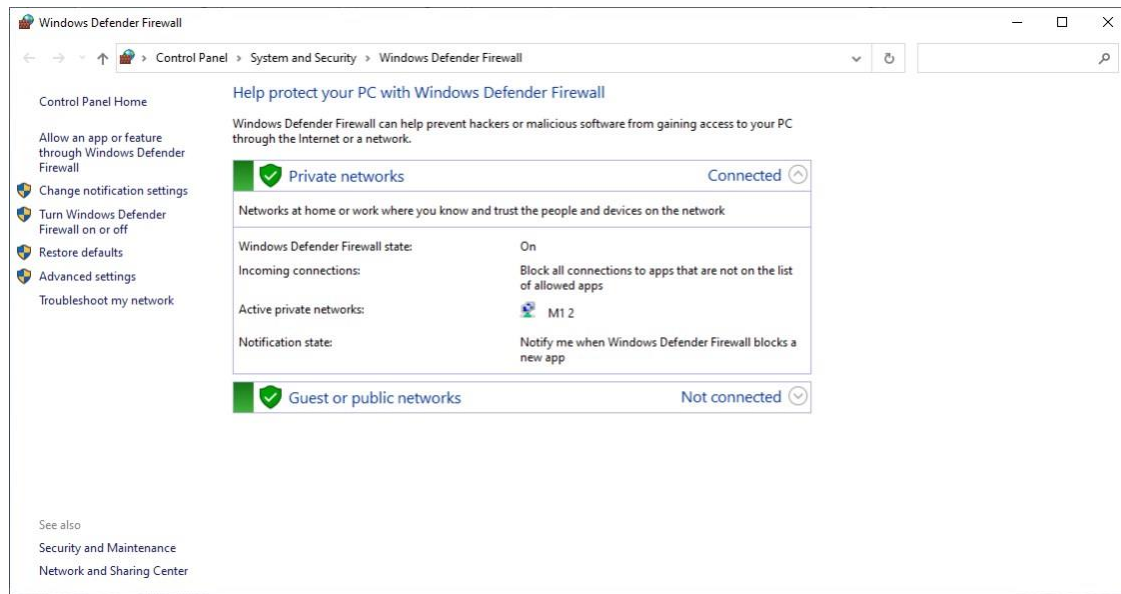
Aim: To configure and test firewall rules to control network traffic, filter packets based on specified criteria, and protect network resources from unauthorized access.

We would use firewall to block

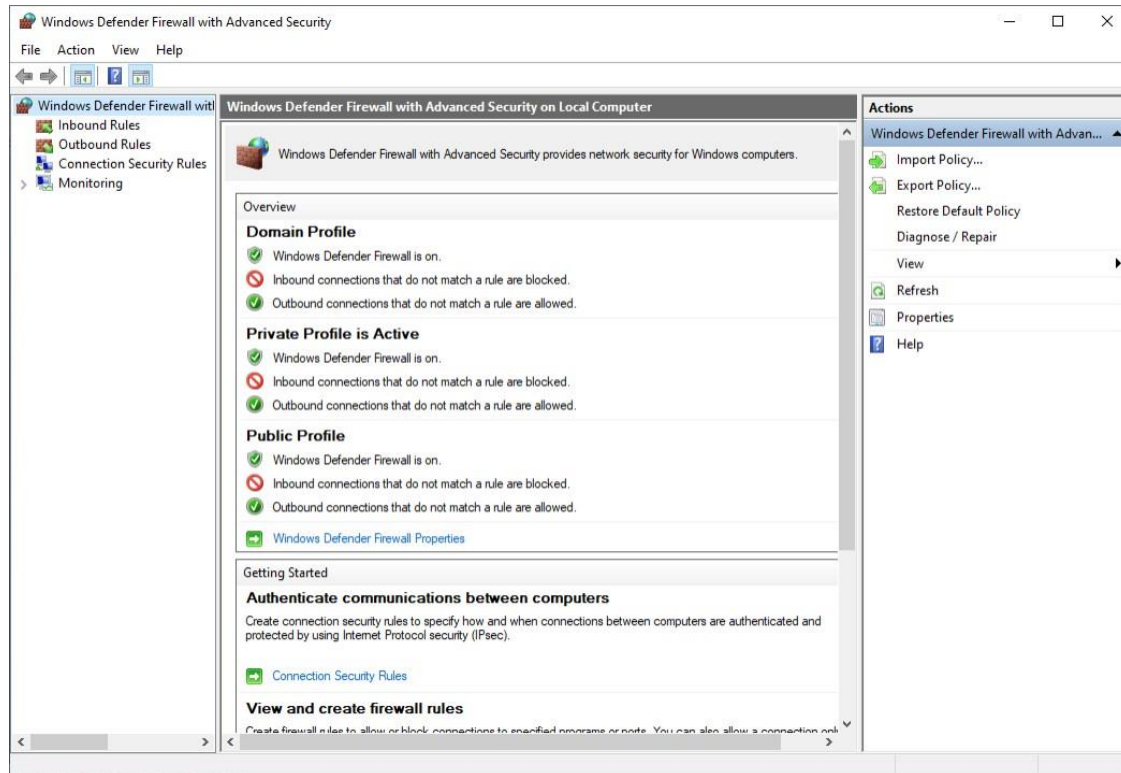
- 1) A Port
- 2) A Website

Part 1: Blocking the HTTP and HTTPS (Port 80 and Port 443) using the Firewall

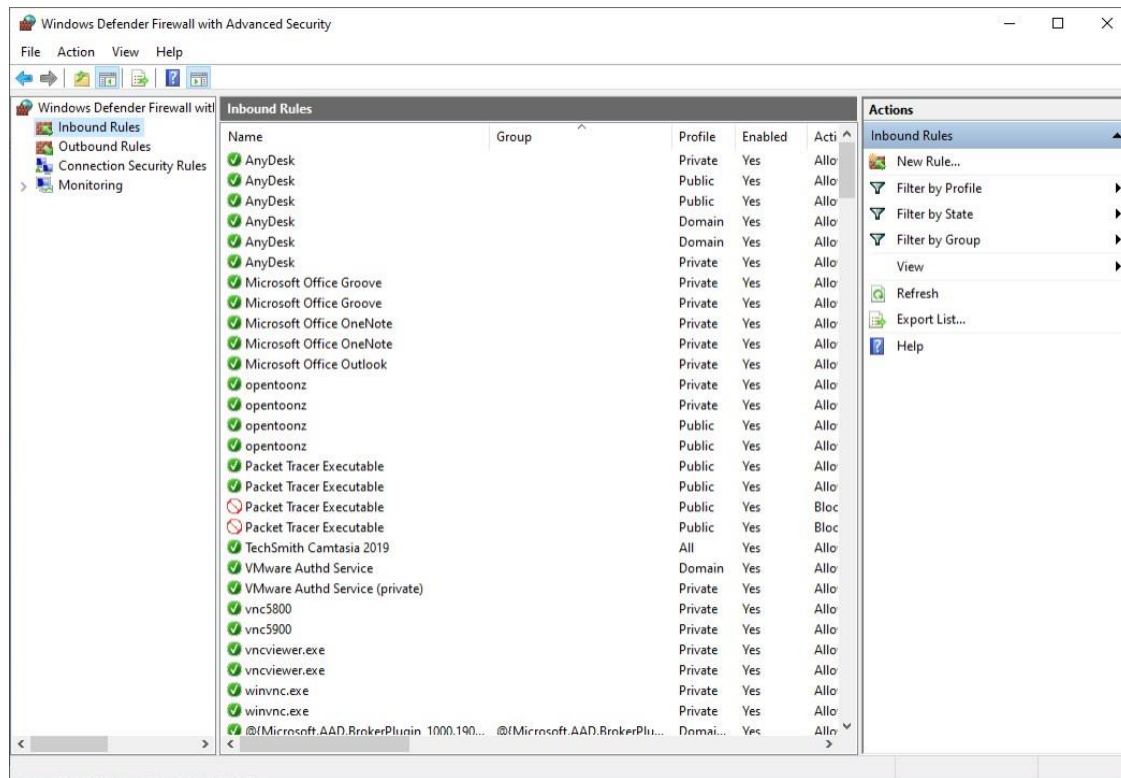
Step 2: We open 'Windows Defender Firewall'



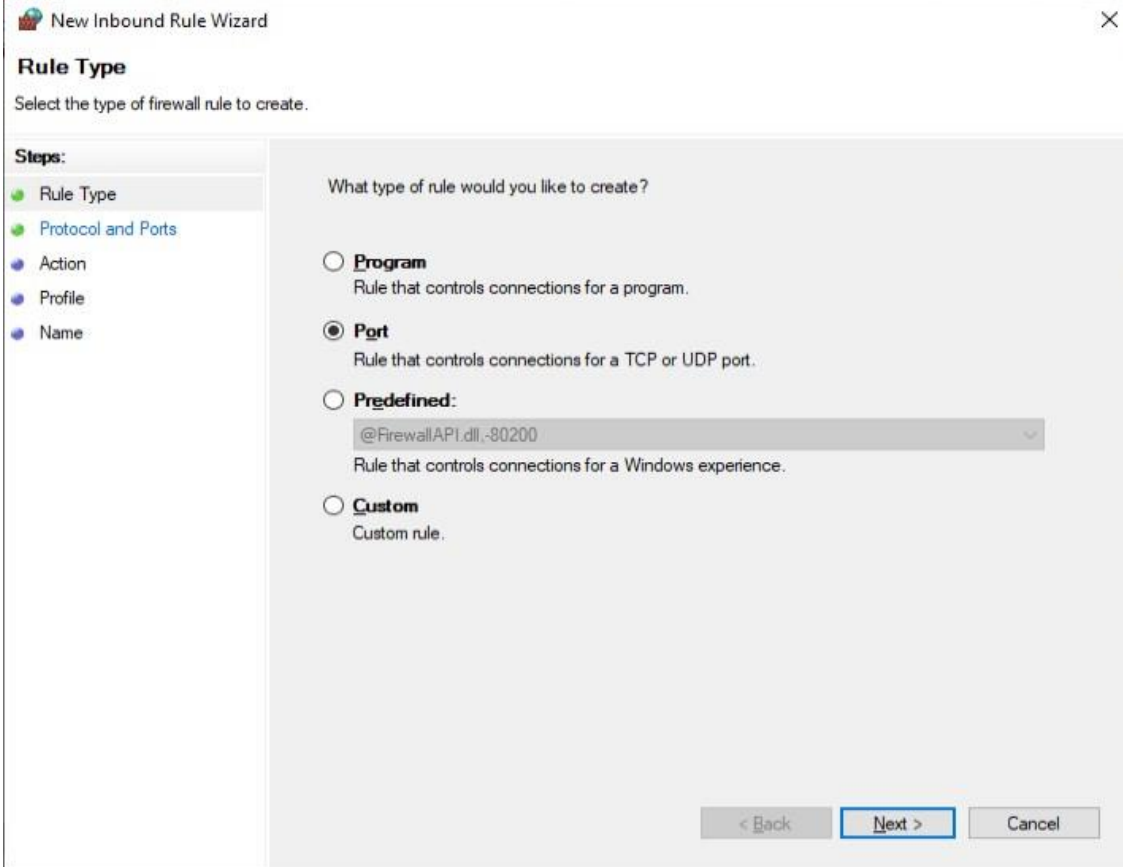
Next we click on 'Advanced settings'



Next we click on 'Inbound Rules'



Then click on 'New Rule'



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Rule Type' step. The left sidebar lists the steps: Rule Type (selected), Protocol and Ports, Action, Profile, and Name. The main area asks 'What type of rule would you like to create?' and offers four options: Program, Port (selected), Predefined (with a dropdown menu showing '@FirewallAPI.dll,-80200'), and Custom. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

New Inbound 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.

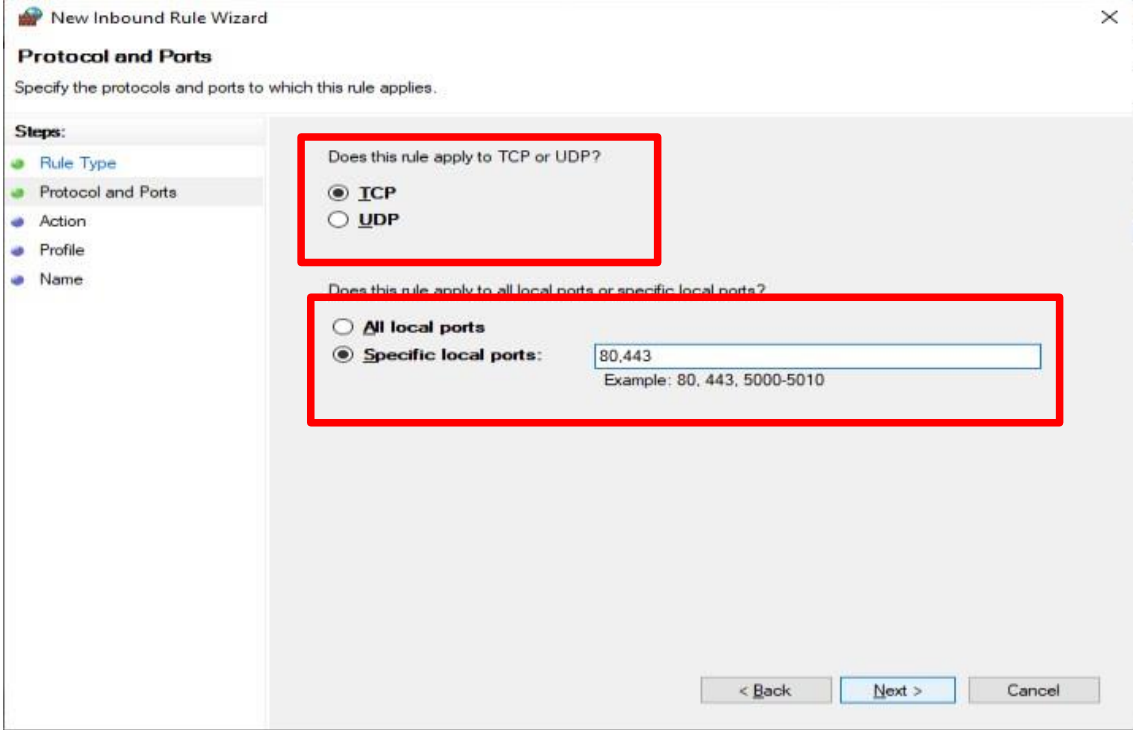
☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

Select the radio button 'Port' and click 'Next' and enter the following



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area asks 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP. Below that, it asks 'Does this rule apply to all local ports or specific local ports?' with radio buttons for All local ports and Specific local ports (selected). A text box next to 'Specific local ports' contains '80,443' and an example '80, 443, 5000-5010'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

New Inbound 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**

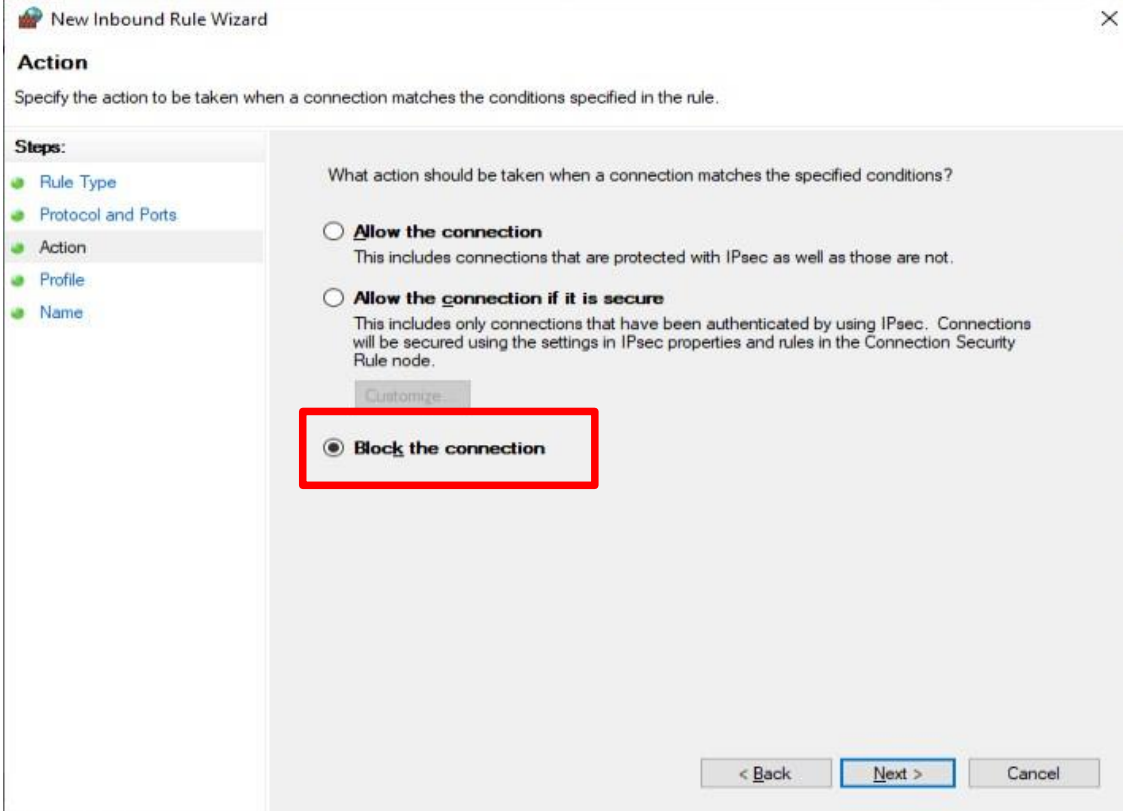
Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

☒ **Specific local ports:** 80,443
Example: 80, 443, 5000-5010

< Back Next > Cancel

After next, we need to finalise the rule



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Block the connection' option is highlighted with a red rectangle. Below the options is a 'Customize...' button. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound Rule Wizard

Action

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

Steps:

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

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

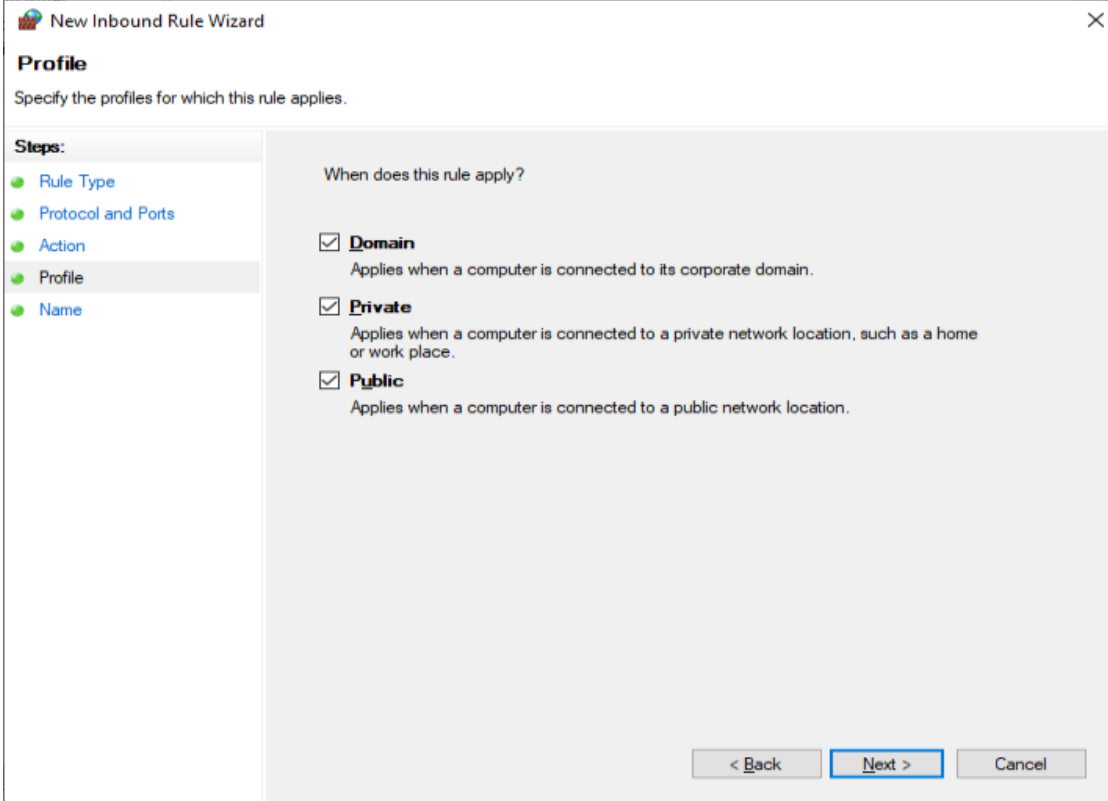
☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **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**

< Back Next > Cancel

Click 'Next' and we get the following



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'When does this rule apply?'. There are three checked checkboxes: 'Domain', 'Private', and 'Public'. Each checkbox has a description of when the rule applies. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound 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?

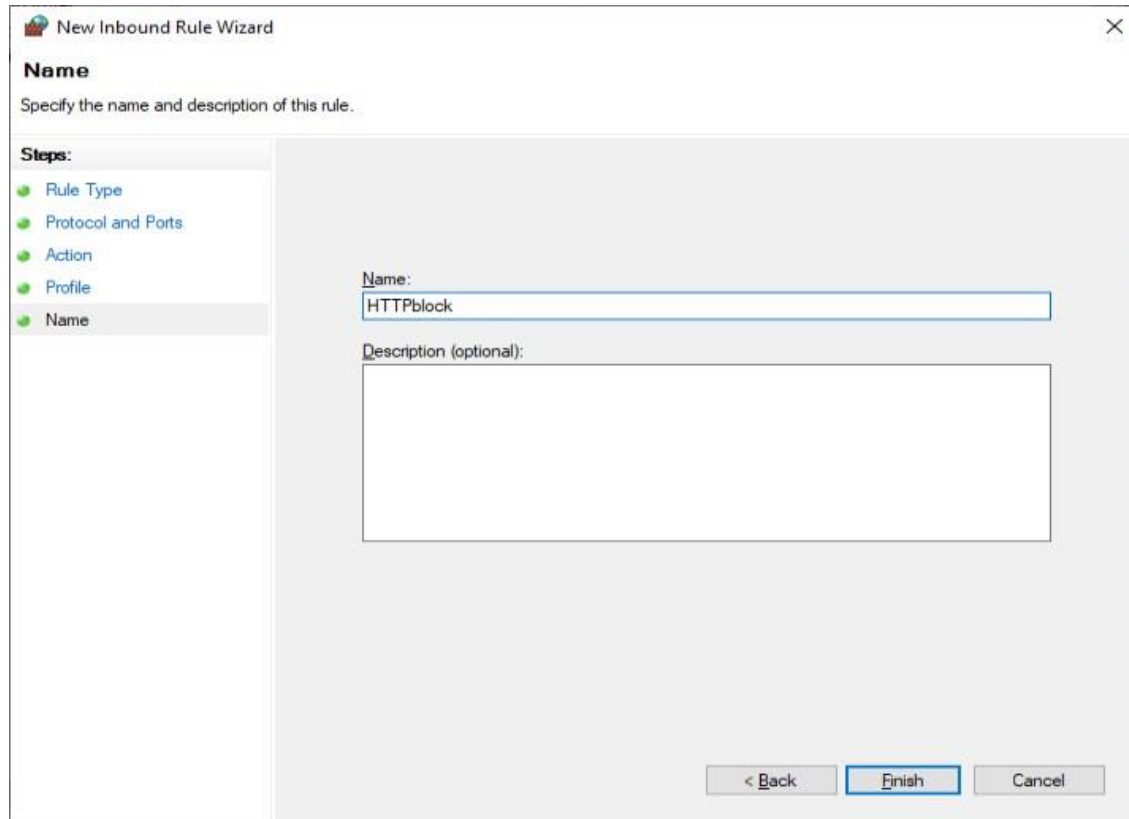
☒ **Domain**
Applies when a computer is connected to its corporate domain.

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

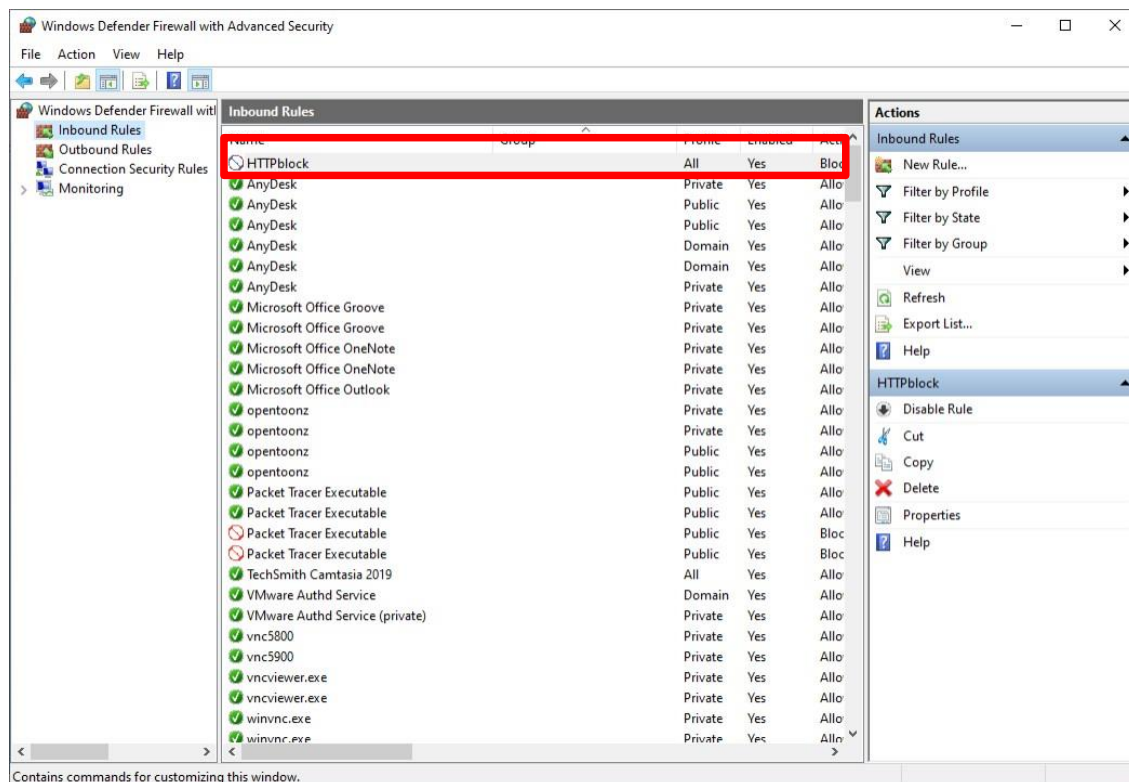
☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

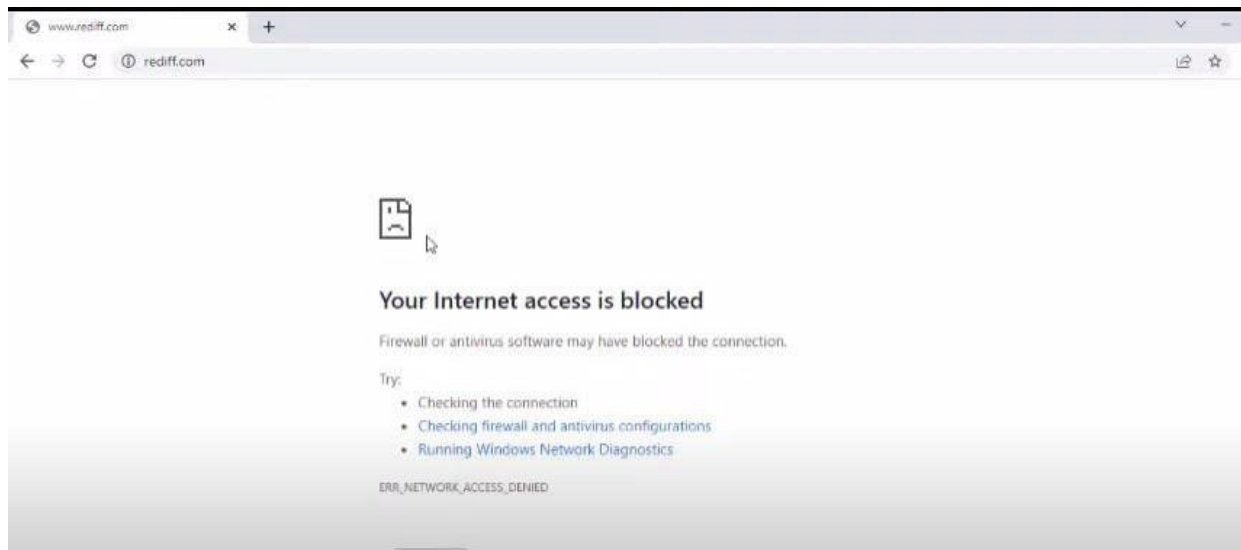
After clicking the 'Next' button we need to name the rule and click finish



The Inbound rule is added

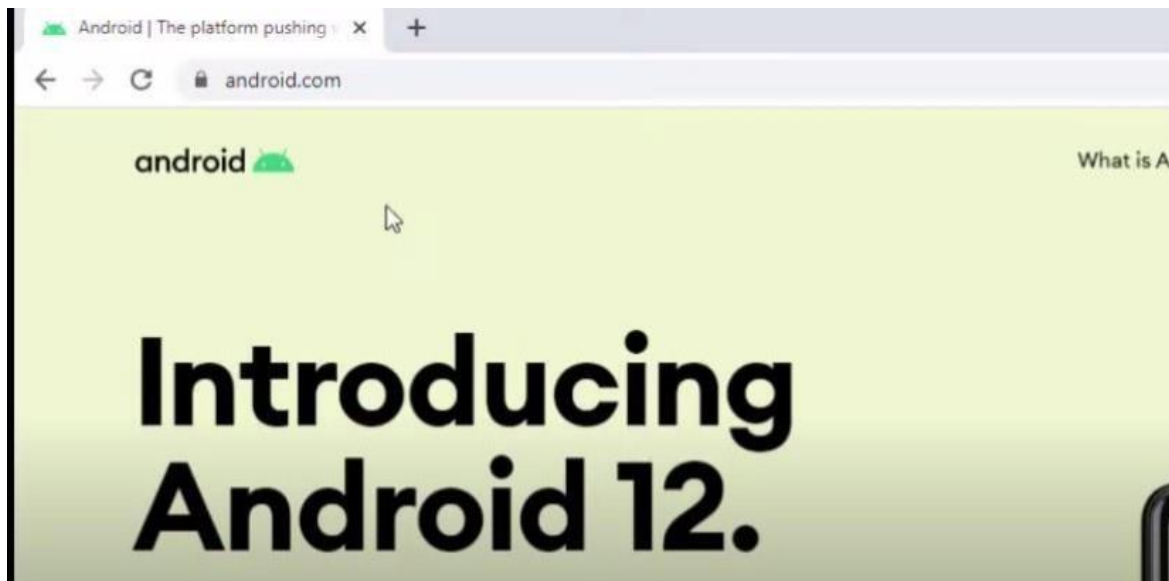


We repeat all the above steps for creating 'Outbound Rules', and then try to access the internet.
We see that the accessed is blocked



Part 2: Blocking the website www.android.com

We open the browser and access the website, which is now accessible



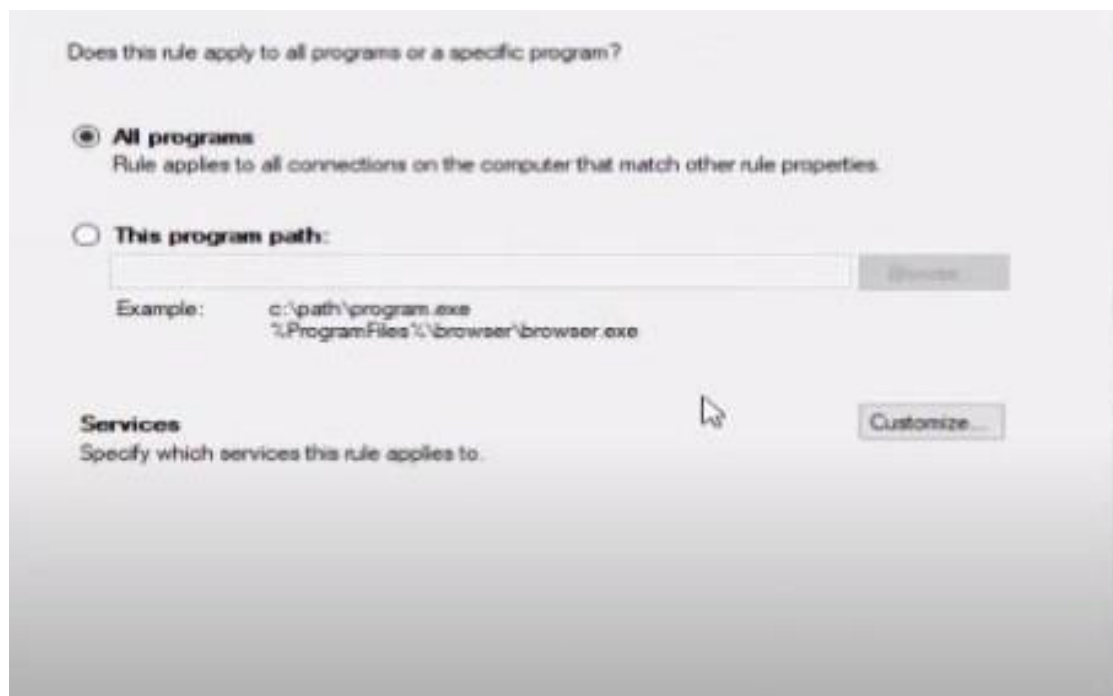
We find the IP addresses of the website using the following command:

nslookup android.com

We save the IP addresses

IPv4	216.58.196.68
IPv6	2404:6800:4009:809::2004

We open the windows Firewall settings and apply the Inbound Rule
Select custom



Select scope

New Inbound 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:

Add...
Edit...
Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

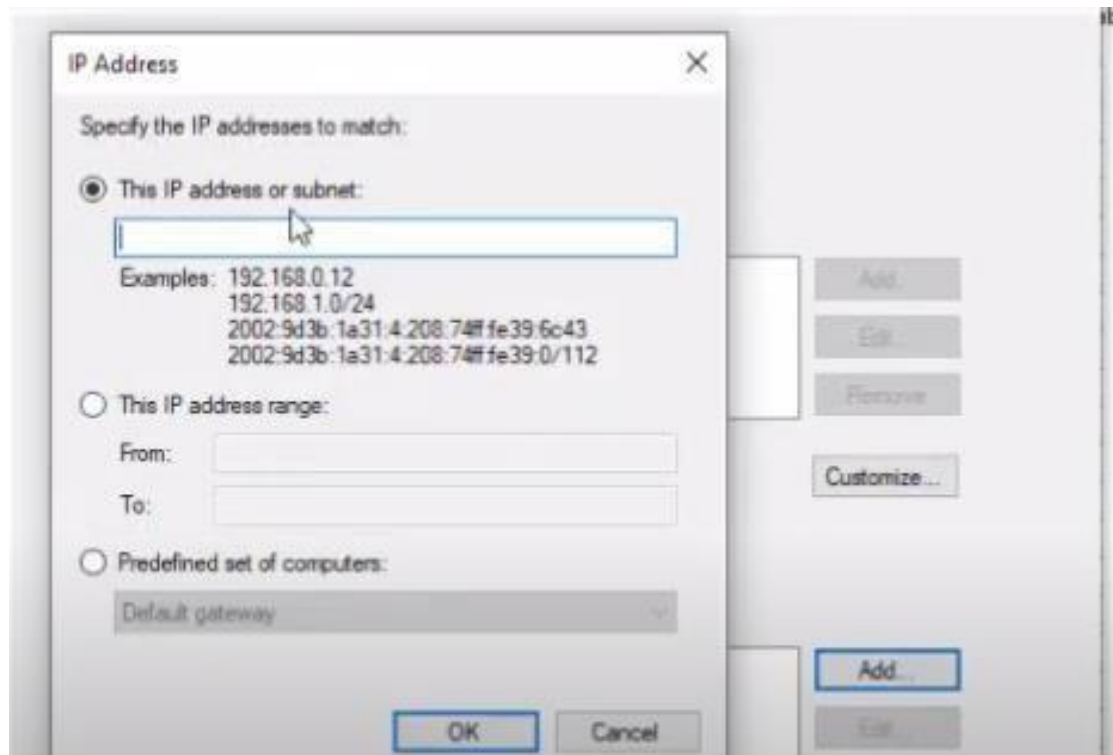
☒ Any IP address

☐ These IP addresses:

Add...
Edit...
Remove

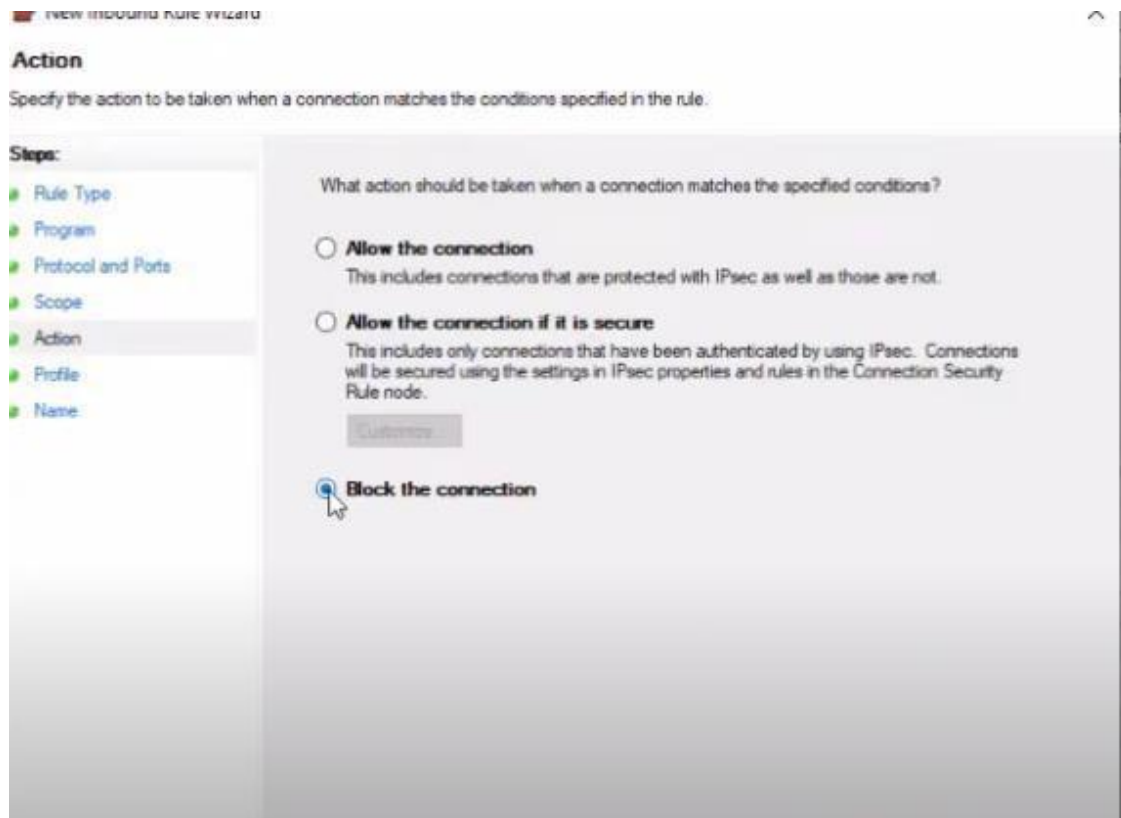
< Back **Next >** Cancel

Select These IP addresses and



Insert the IP addresses both IPv4 and IPv6

Select Block connection



Provide a suitable name and finish



Repeat the above for Outbound Rules

Now if we try to access the website www.android.com , it would be blocked

