

Practical No - 08

Firewall Configuration and Rule-based Filtering

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

Theory:

Firewalls are network security devices or software applications designed to monitor, filter, and control incoming and outgoing network traffic based on a set of predetermined security rules. The primary purpose of a firewall is to act as a barrier between a trusted internal network (such as a company's internal network) and untrusted external networks (like the internet), in order to prevent unauthorized access, data breaches, and other potential cyber threats.

Firewalls operate by inspecting network packets (small units of data) as they pass through the firewall and making decisions about whether to allow or block the traffic based on a set of predefined rules. These rules can be configured to specify which types of traffic are permitted and which are denied. Firewalls can be implemented in various locations within a network, including at the network perimeter, on individual devices, or even within cloud environments.

There are several types of firewalls, including:

1. **Packet Filtering Firewalls:** These examine network packets and decide whether to allow or block them based on criteria like source and destination IP addresses, port numbers, and protocols. While they are relatively simple, they lack the ability to inspect the actual content of the data packets.
2. **Stateful Inspection Firewalls:** Also known as dynamic packet filtering firewalls, these maintain a state table to keep track of active connections and only allow incoming traffic that matches an existing, legitimate connection. This approach is more secure than basic packet filtering.
3. **Proxy Firewalls:** Proxy firewalls act as intermediaries between the internal network and the external network. They receive requests from internal users, then initiate and manage connections to external resources on behalf of those users. This can provide an additional layer of security by hiding internal network details.
4. **Application Layer Firewalls:** These operate at the application layer of the OSI model and can understand the context of the traffic, such as the specific application or service being accessed. They are capable of making more fine-grained decisions based on the actual content of the traffic.

5. **Next-Generation Firewalls (NGFW):** NGFWs combine traditional firewall functionality with advanced features such as intrusion prevention, deep packet inspection, and application-aware filtering. They are designed to provide more comprehensive protection against modern threats.

Firewalls play a crucial role in network security by helping organizations establish a strong defence against unauthorized access, malware, and various cyber attacks. However, it's important to note that while firewalls are an essential component of a comprehensive cyber- security strategy, they are not a standalone solution. They should be used in conjunction with other security measures such as antivirus software, intrusion detection systems, regular softwareupdates, and user training to ensure a robust defence against evolving threats.

Using a firewall to block unauthorized access is an important aspect of securing your network and systems. Firewalls act as barriers between your network and potential threats from the internet or other external sources. Here's a step-by-step guide on how to use a firewall to block unauthorized access:

1. **Choose the Right Firewall:**

There are hardware firewalls (devices that are placed between your network and the internet) and software firewalls (installed on individual computers or servers). Choose the type that best suits your needs.

2. **Install and Configure the Firewall:**

For software firewalls, install the firewall software on the computers or servers you want to protect. For hardware firewalls, follow the manufacturer's instructions to set it up between your network and the internet.

3. **Define Security Policies:**

Determine which types of traffic are allowed and which are denied. This can involve specifying rules that allow or block traffic based on criteria such as IP addresses, ports, and protocols.

4. **Block Unauthorized Access:**

Create rules to block access from unauthorized IP addresses or ranges. For example, you might block IP addresses known for malicious activities or any IP address that doesn't have a legitimate reason to access your network.

5. **Allow Necessary Traffic:**

Configure rules to allow access to the services and applications that are essential for your business operations. For instance, if you have a web server, you'll need to allow incoming traffic on port 80 or 443.

6. **Regularly Update Rules:**

Keep your firewall rules up to date. New threats can emerge, and you might need to adjust your rules accordingly.

7. Use Application Layer Filtering:

Modern firewalls can inspect traffic at the application layer, allowing you to block specific applications or services. This can help prevent unauthorized access to potentially risky services.

8. Intrusion Detection and Prevention Systems (IDPS):

Consider integrating an IDPS with your firewall. These systems can detect and prevent intrusion attempts by analyzing network traffic and patterns.

9. Logging and Monitoring:

Enable logging on your firewall to keep track of connection attempts and blocked traffic. Regularly review the logs to identify potential security issues.

10. Testing and Adjusting:

Regularly test your firewall's effectiveness by attempting to access your network from different scenarios. This can help you identify any gaps in your security and adjust your rules accordingly.

11. Keep Firewall Software Updated:

If you're using software firewalls, make sure to keep the firewall software up to date with the latest security patches.

12. Educate Users:

Even with a firewall in place, user awareness is essential. Educate your users about safe online practices, such as not clicking on suspicious links or downloading unknown files.

Remember that while firewalls are a valuable part of network security, they are not a complete solution. It's important to adopt a multi-layered security approach that includes regular updates, patches, antivirus software, intrusion detection, and employee training.

We would use firewall to block

- 1) A Port
- 2) A Program
- 3) A Website

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

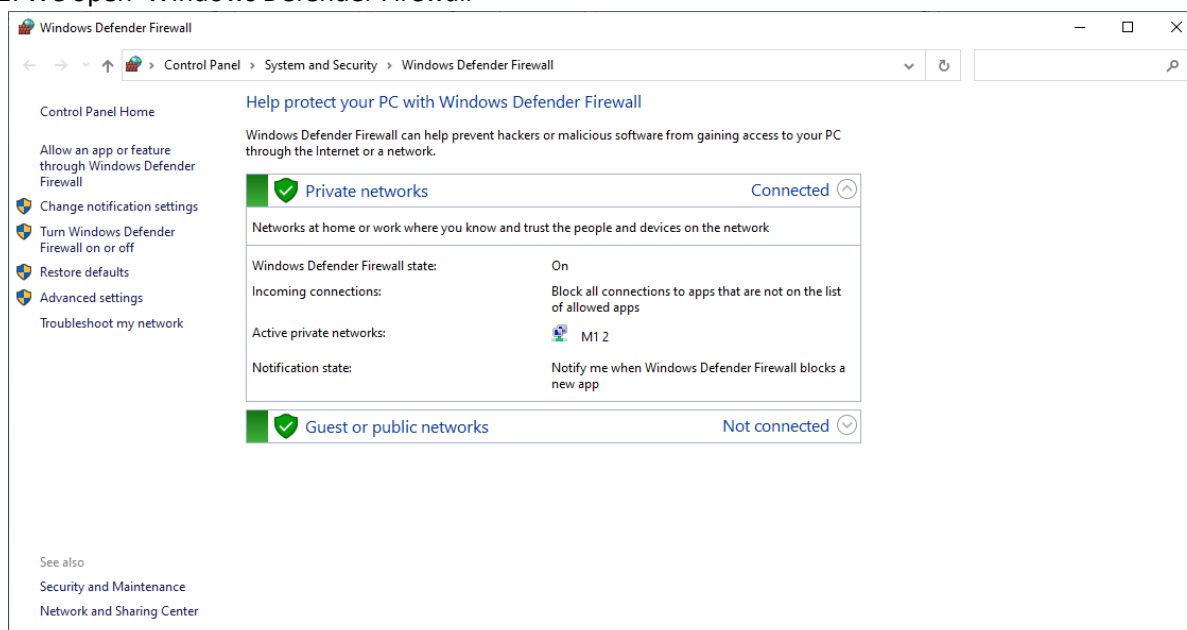
Before starting with the blocking port process, we note that the applications running at the server-end are identified with the well-known Port numbers, some of the commonly used are as follows

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
25	TCP	SMTP
53	UDP, TCP	DNS
80	TCP	HTTP (W/W)
110	TCP	POP3
443	TCP	SSL

We perform the blocking Port operation as follows:

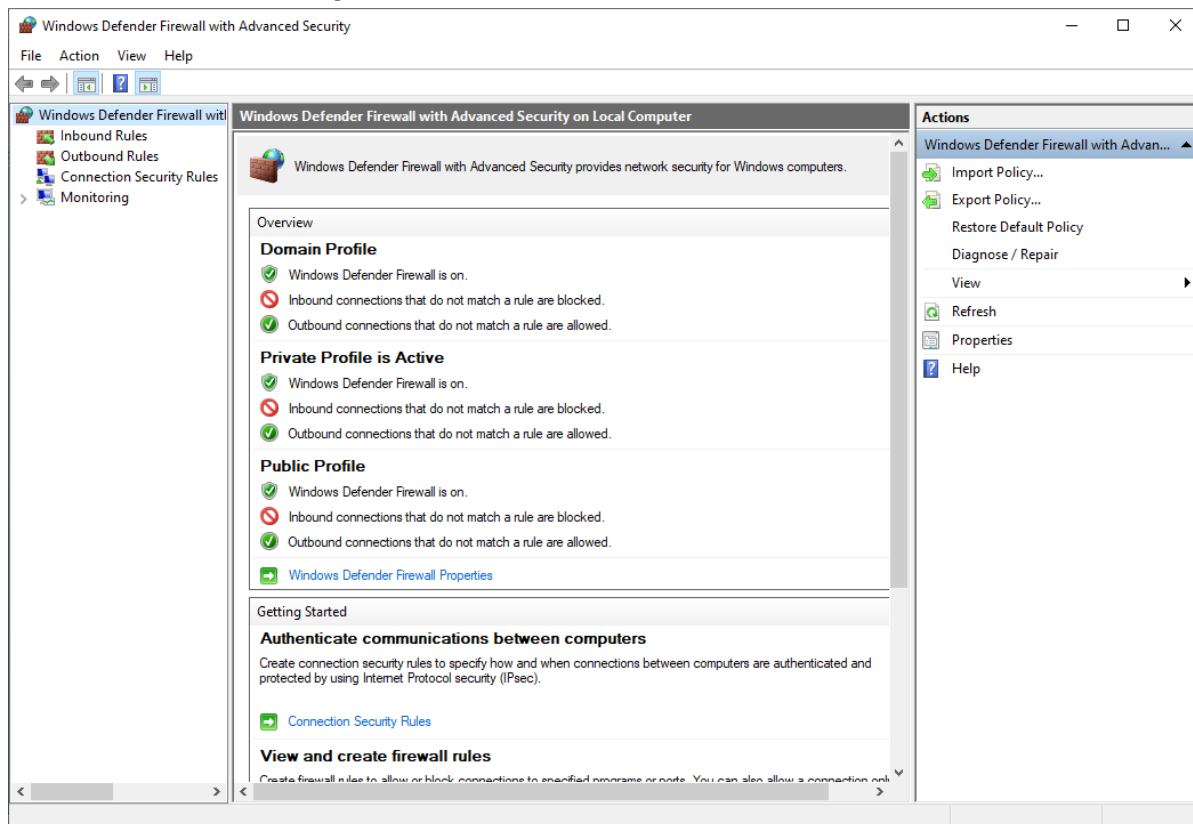
Step 1: We access any website through the browser and confirm that the HTTP/HTTPS protocols are working.

Step 2: We open 'Windows Defender Firewall'

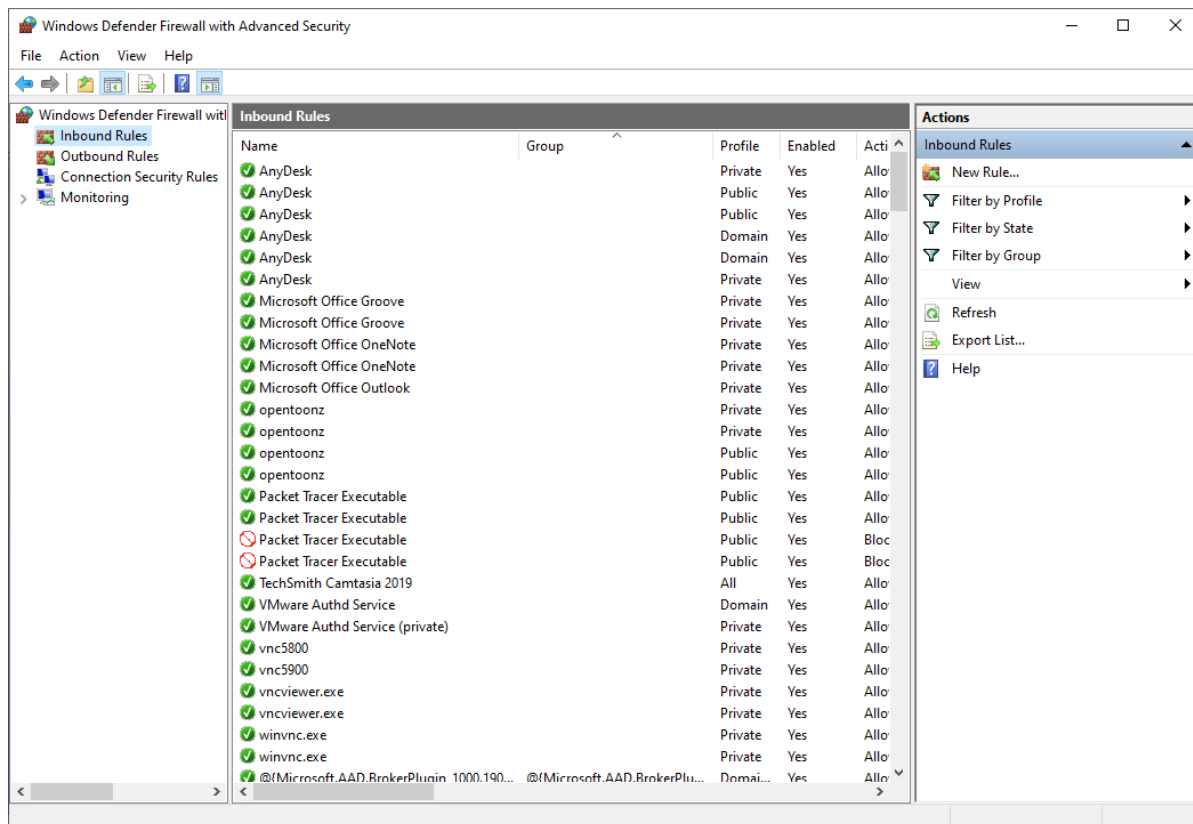


Information and Network Security

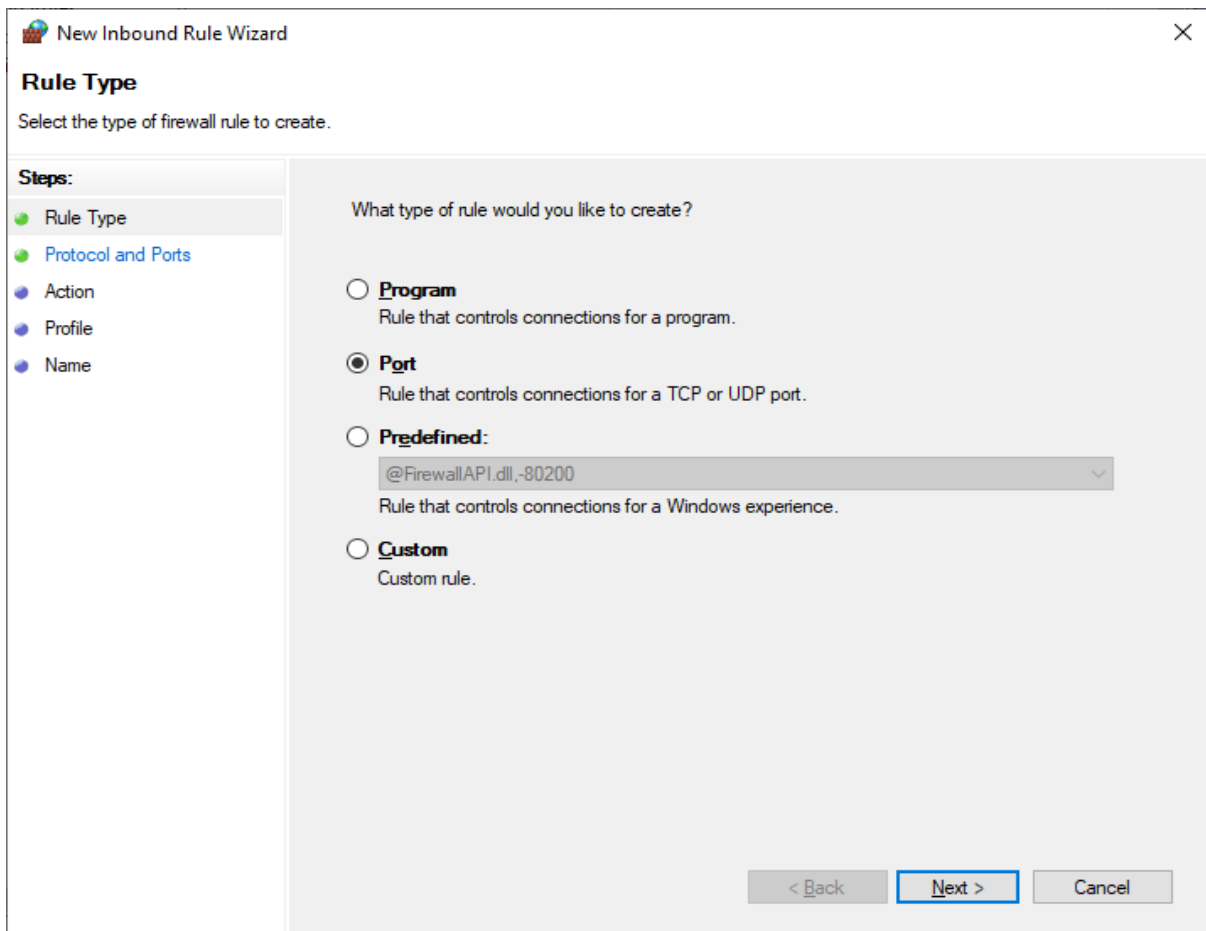
Next we click on 'Advanced settings'



Next we click on 'Inbound Rules'



Then click on 'New Rule'



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.

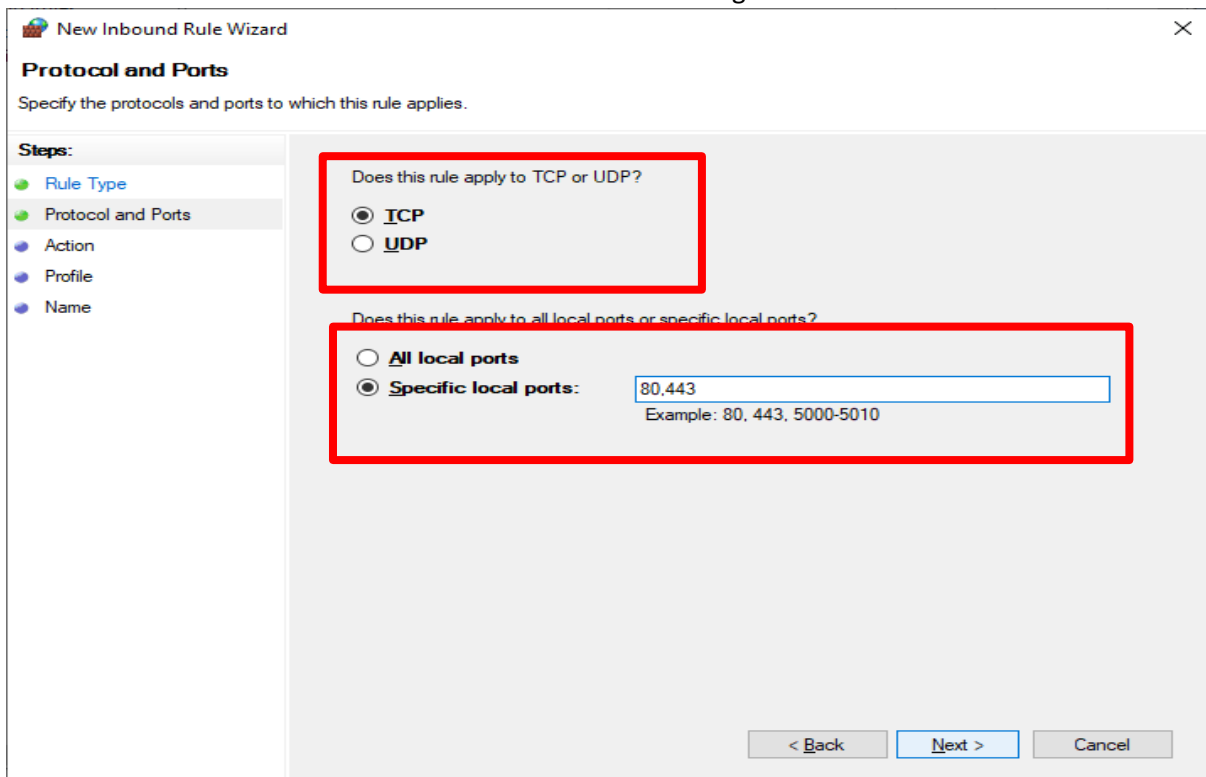
☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **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



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?

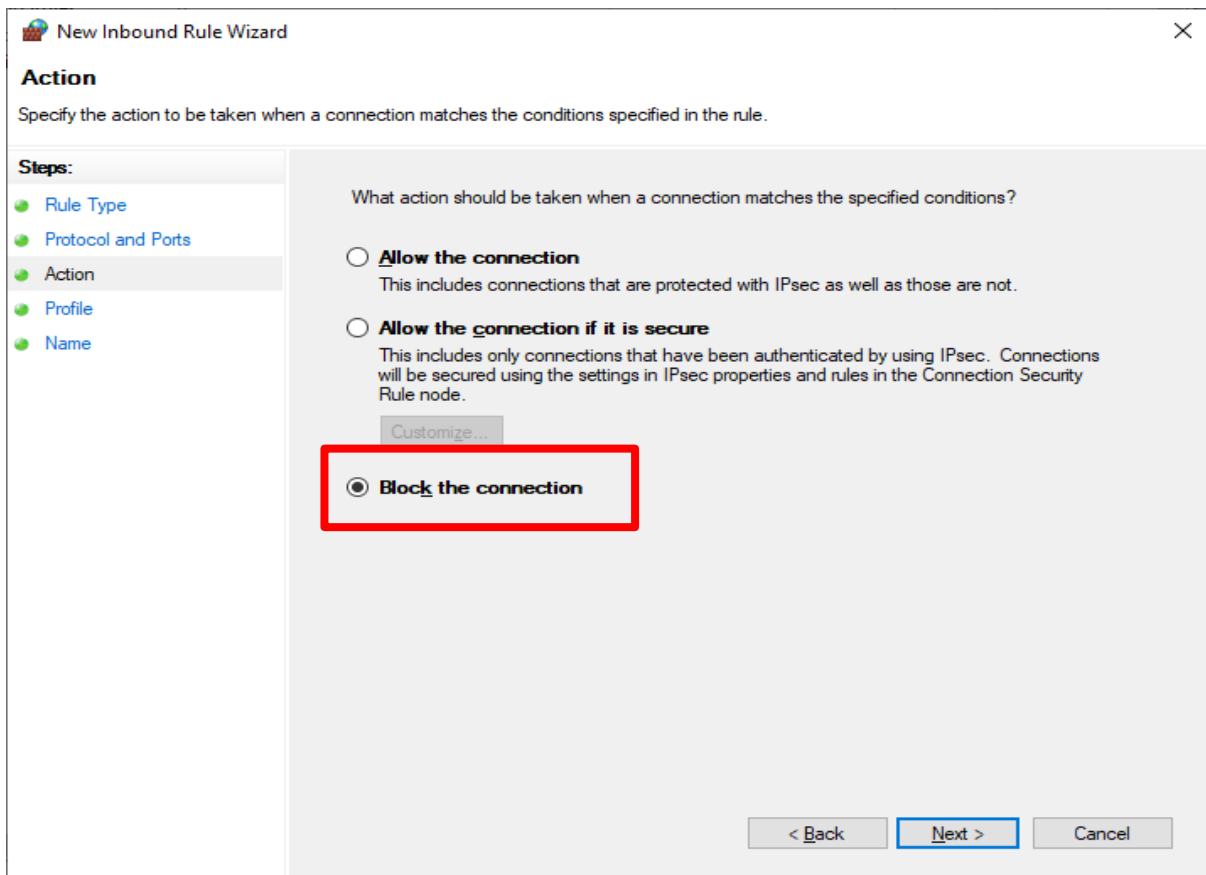
☐ **All local ports**

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

< Back Next > Cancel

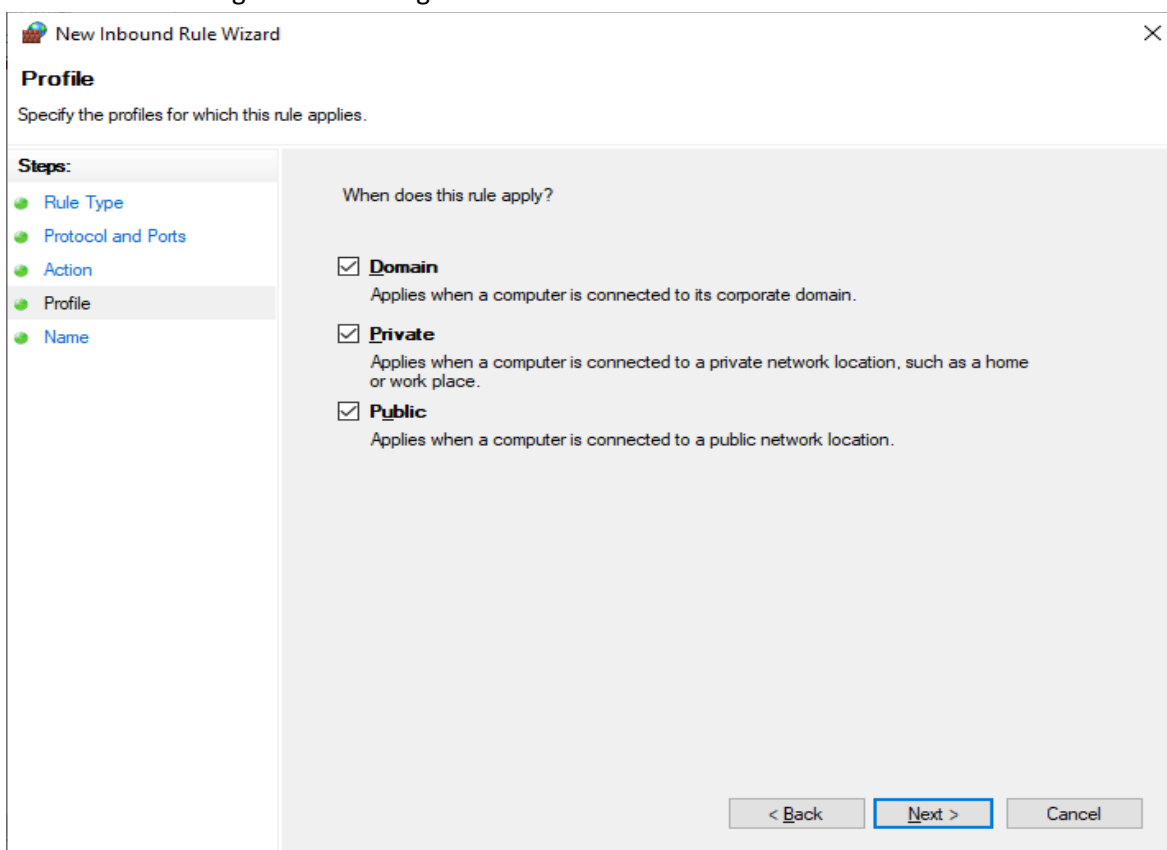
Information and Network Security

After next, we need to finalise the rule



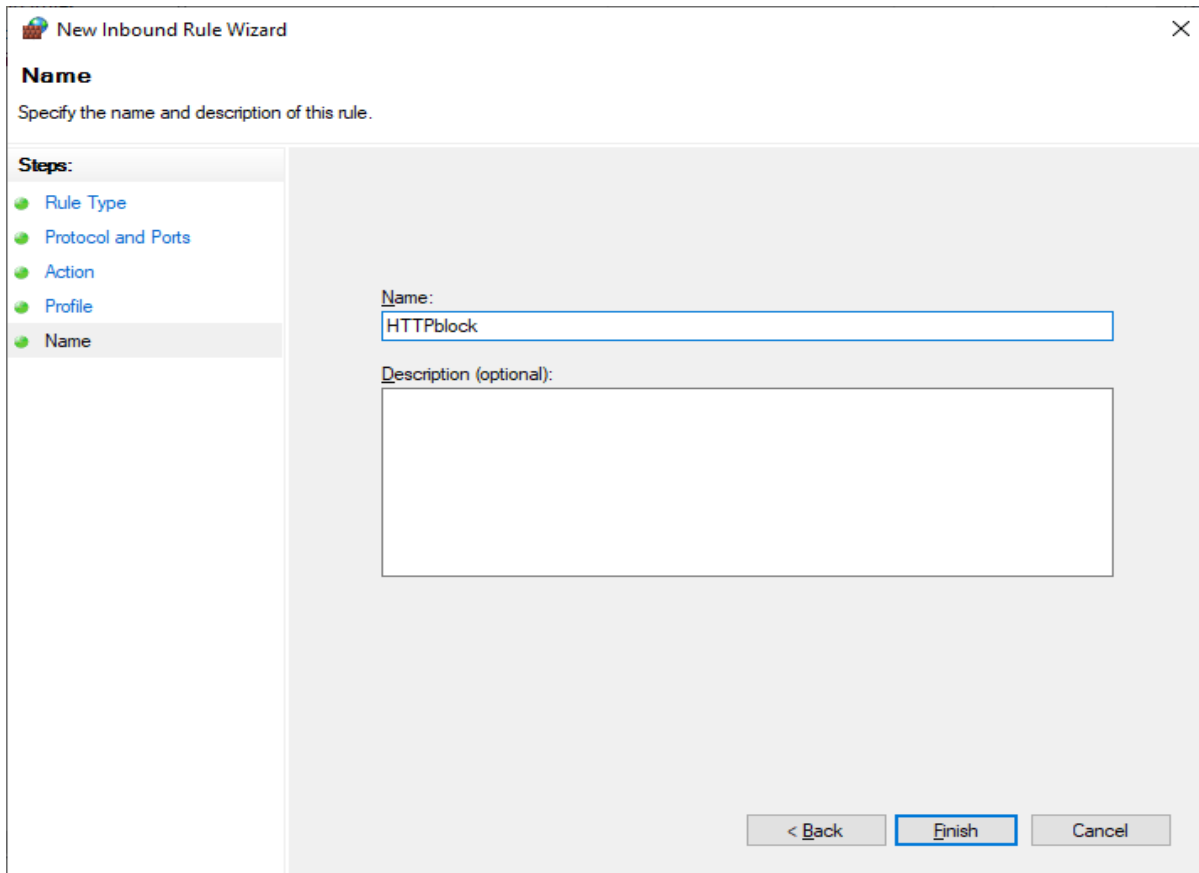
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action' (highlighted), 'Profile', and 'Name'. The main area asks 'What action should be taken when a connection matches the specified conditions?' and offers three options: 'Allow the connection' (radio button), 'Allow the connection if it is secure' (radio button), and 'Block the connection' (radio button, highlighted with a red rectangle). Below the first two options is a 'Customize...' button. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

Click 'Next' and we get the following



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main area asks 'When does this rule apply?' and offers three checked options: '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.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

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



The 'New Inbound Rule Wizard' dialog box is shown. The 'Name' step is selected in the 'Steps' list on the left. The 'Name' field contains 'HTTPblock'. The 'Description (optional)' field is empty. The 'Finish' button is highlighted.

Name
Specify the name and description of this rule.

Steps:

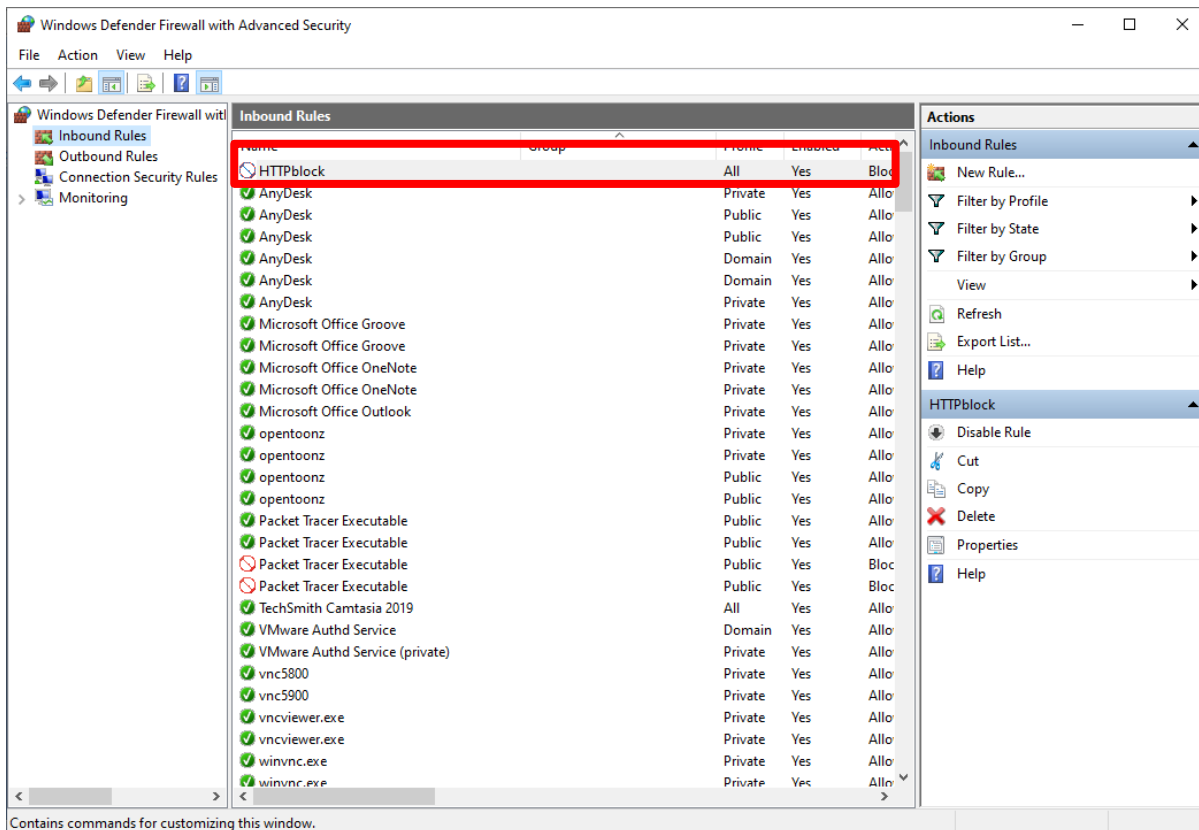
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:
HTTPblock

Description (optional):

< Back Finish Cancel

The Inbound rule is added

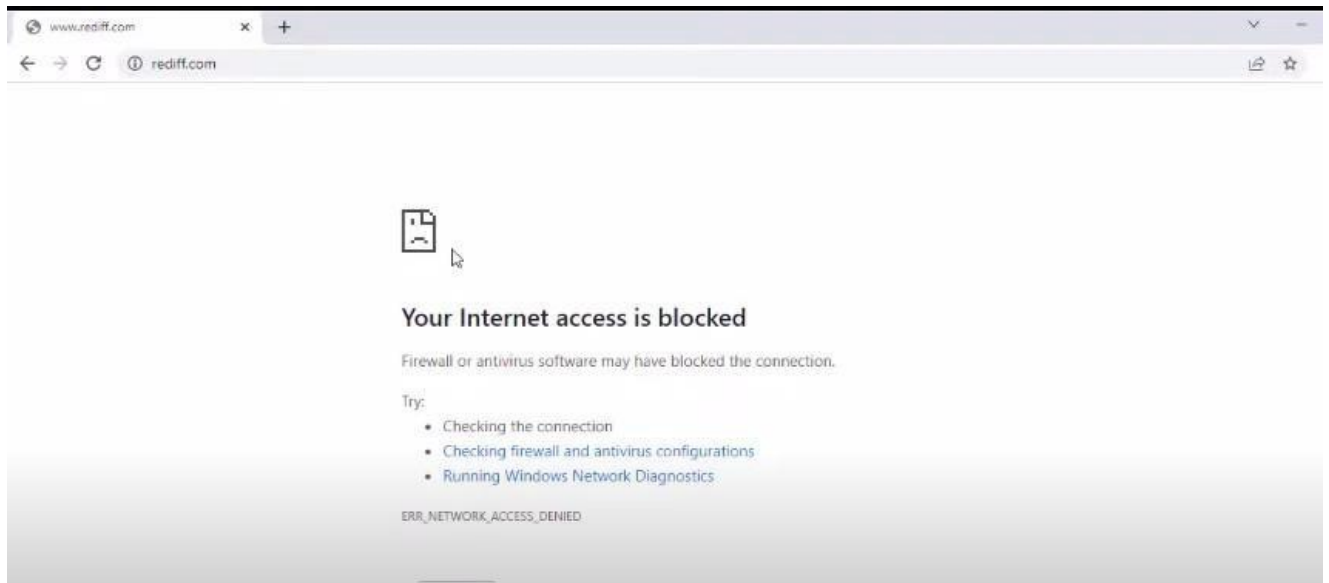


The 'Windows Defender Firewall with Advanced Security' window is shown. The 'Inbound Rules' tab is selected. A red box highlights the 'HTTPblock' rule at the top of the list. The 'Actions' pane on the right shows the 'HTTPblock' rule selected.

Name	Group	Profile	Enabled	Action
HTTPblock		All	Yes	Block
AnyDesk		Private	Yes	Allow
AnyDesk		Public	Yes	Allow
AnyDesk		Public	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Private	Yes	Allow
Microsoft Office Groove		Private	Yes	Allow
Microsoft Office Groove		Private	Yes	Allow
Microsoft Office OneNote		Private	Yes	Allow
Microsoft Office OneNote		Private	Yes	Allow
Microsoft Office Outlook		Private	Yes	Allow
opentoonz		Private	Yes	Allow
opentoonz		Private	Yes	Allow
opentoonz		Public	Yes	Allow
opentoonz		Public	Yes	Allow
Packet Tracer Executable		Public	Yes	Block
Packet Tracer Executable		Public	Yes	Block
Packet Tracer Executable		Public	Yes	Block
TechSmith Camtasia 2019		All	Yes	Allow
VMware Authd Service		Domain	Yes	Allow
VMware Authd Service (private)		Private	Yes	Allow
vnc5800		Private	Yes	Allow
vnc5900		Private	Yes	Allow
vncviewer.exe		Private	Yes	Allow
vncviewer.exe		Private	Yes	Allow
winvnc.exe		Private	Yes	Allow
winvnc.exe		Private	Yes	Allow

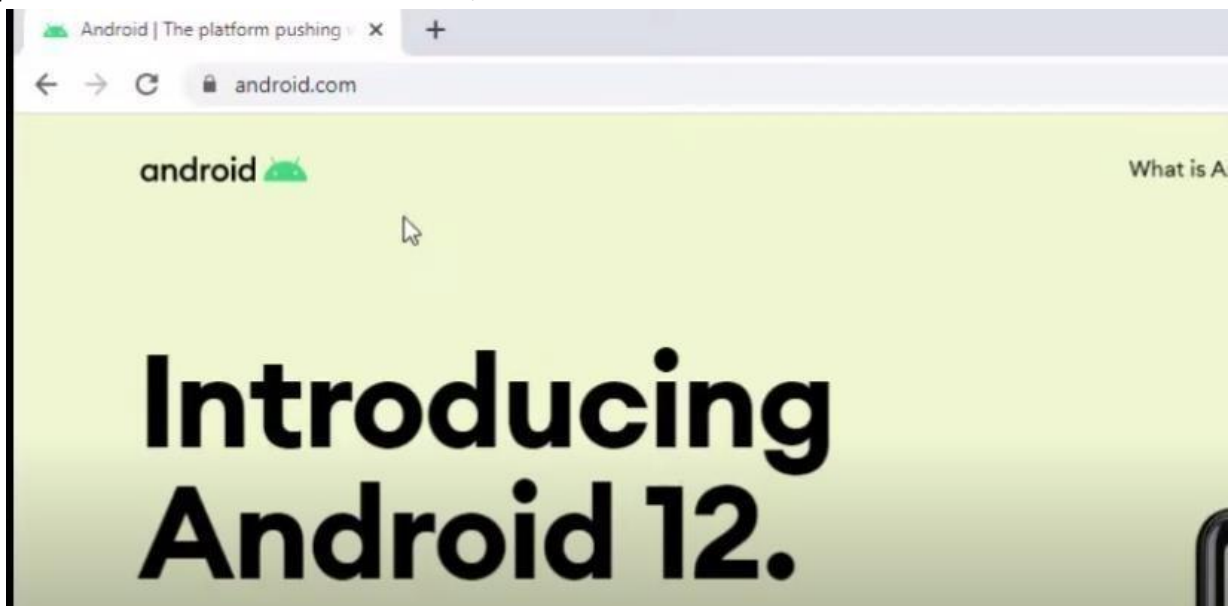
Contains commands for customizing this window.

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

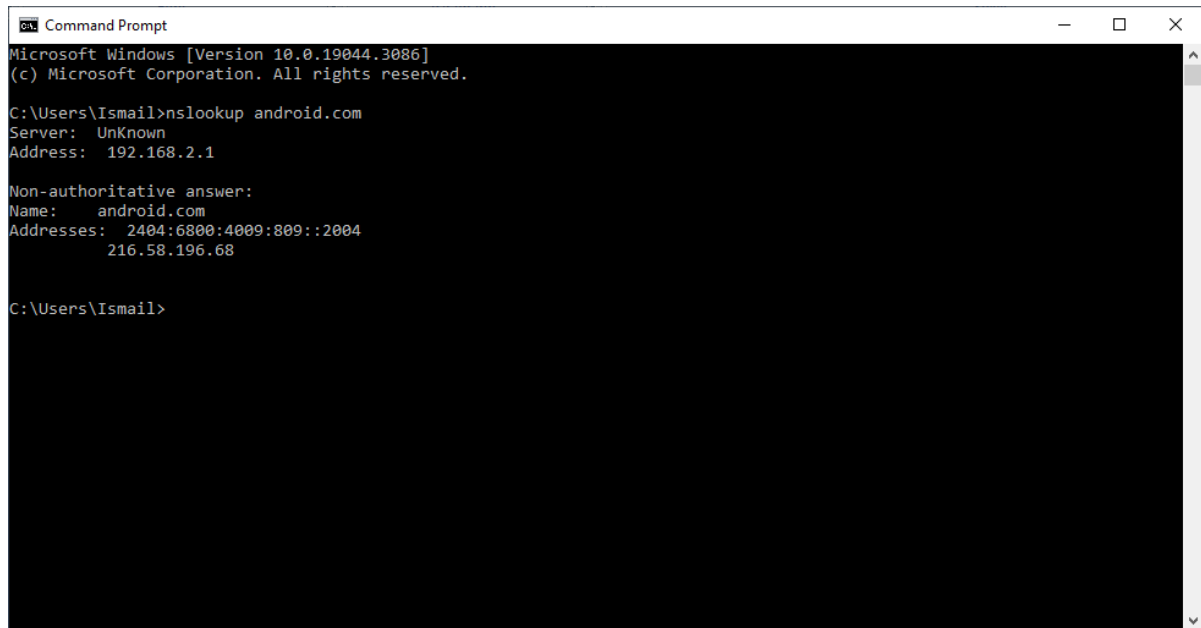


Part 2: Blocking the website www.android.com

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



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



```
Command Prompt
Microsoft Windows [Version 10.0.19044.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ismail>nslookup android.com
Server: UnKnown
Address: 192.168.2.1

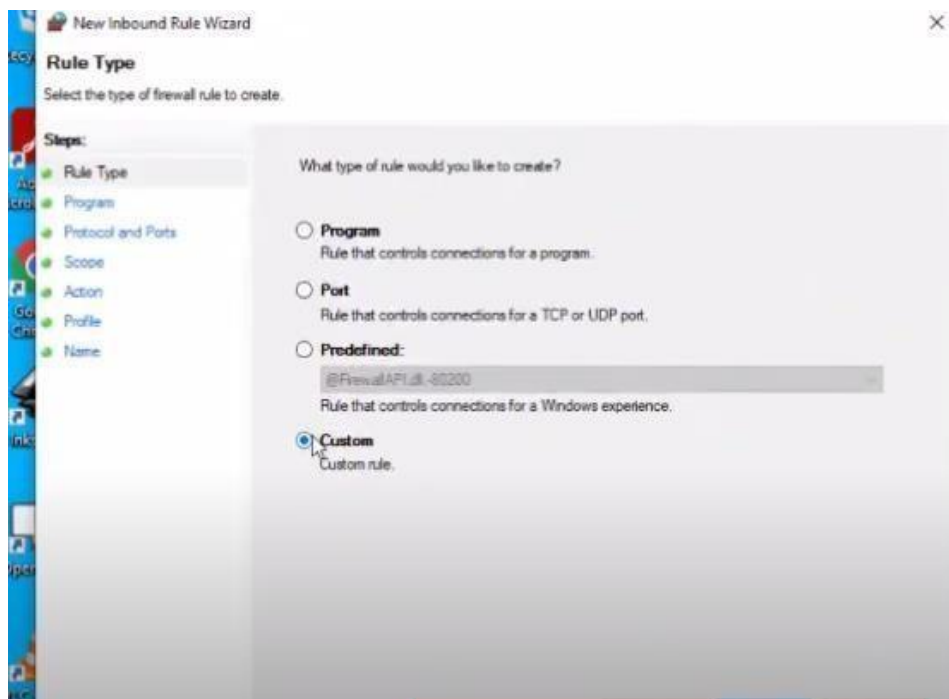
Non-authoritative answer:
Name: android.com
Addresses: 2404:6800:4009:809::2004
          216.58.196.68

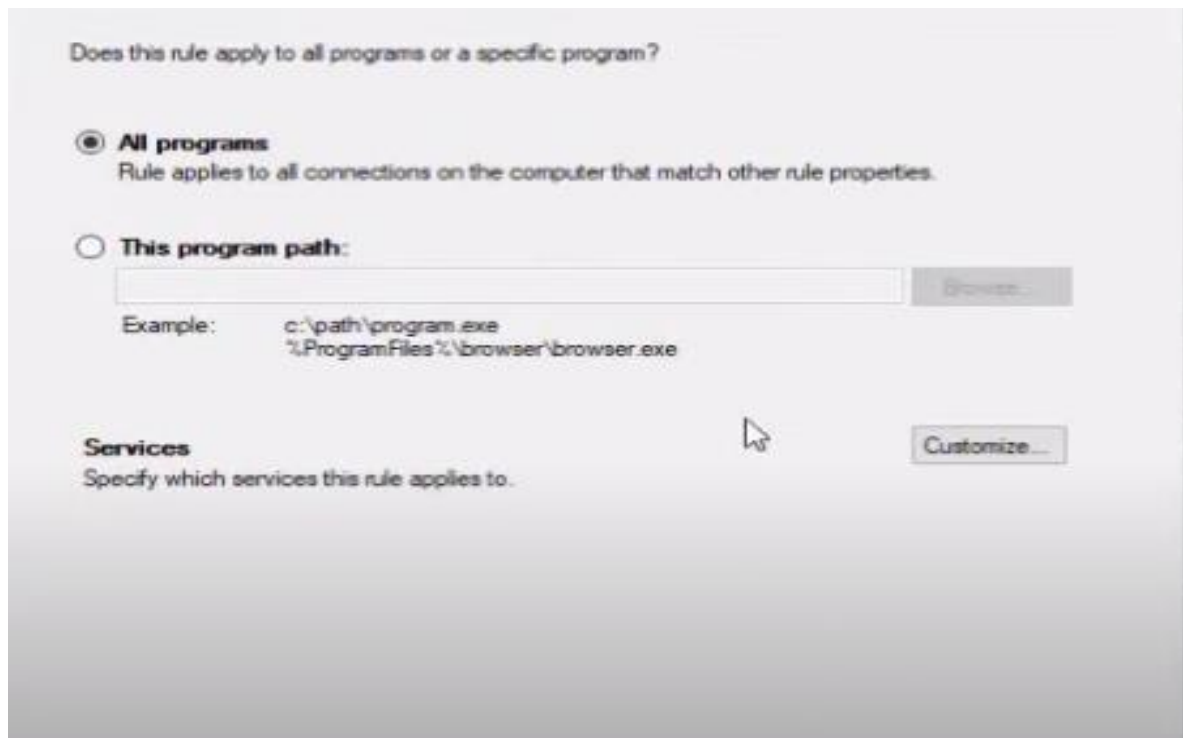
C:\Users\Ismail>
```

We save the IP addresses

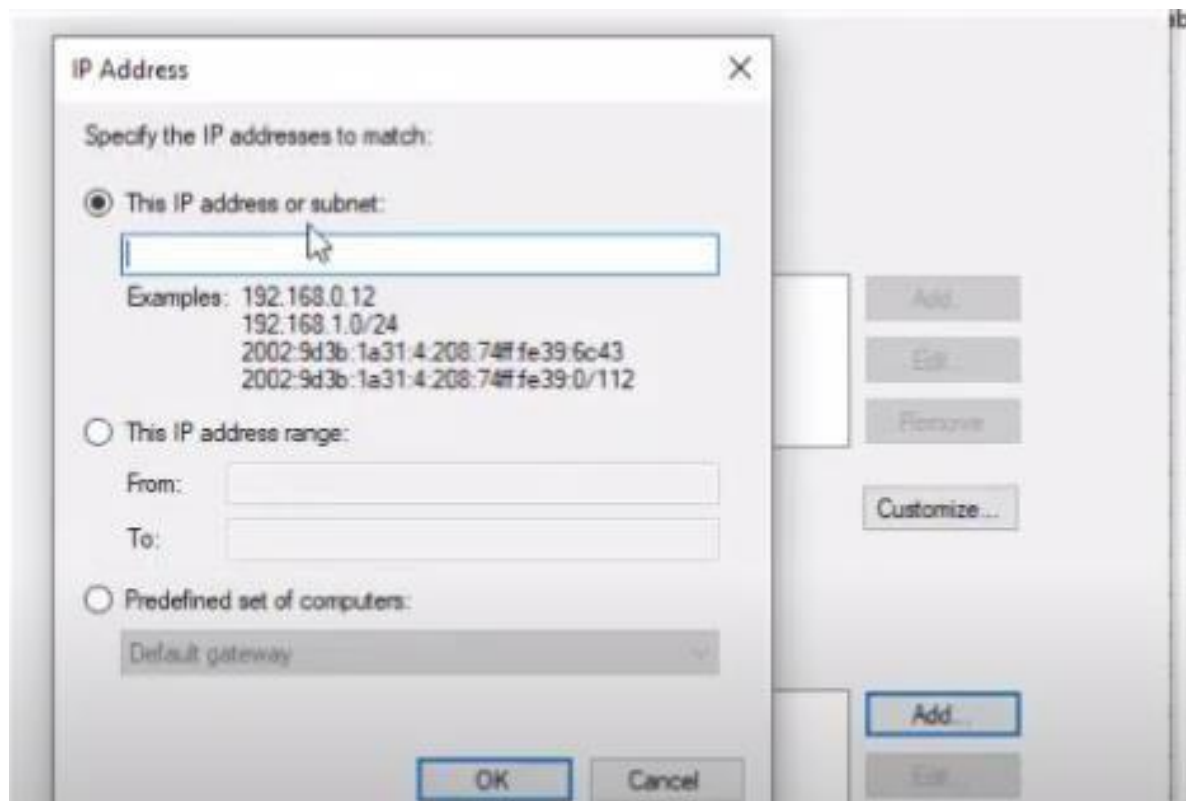
IPv4	216.58.196.68
IPv6	2404:6800:4009:809::2004

We open the windows Firewall settings and apply the Inbound Rule

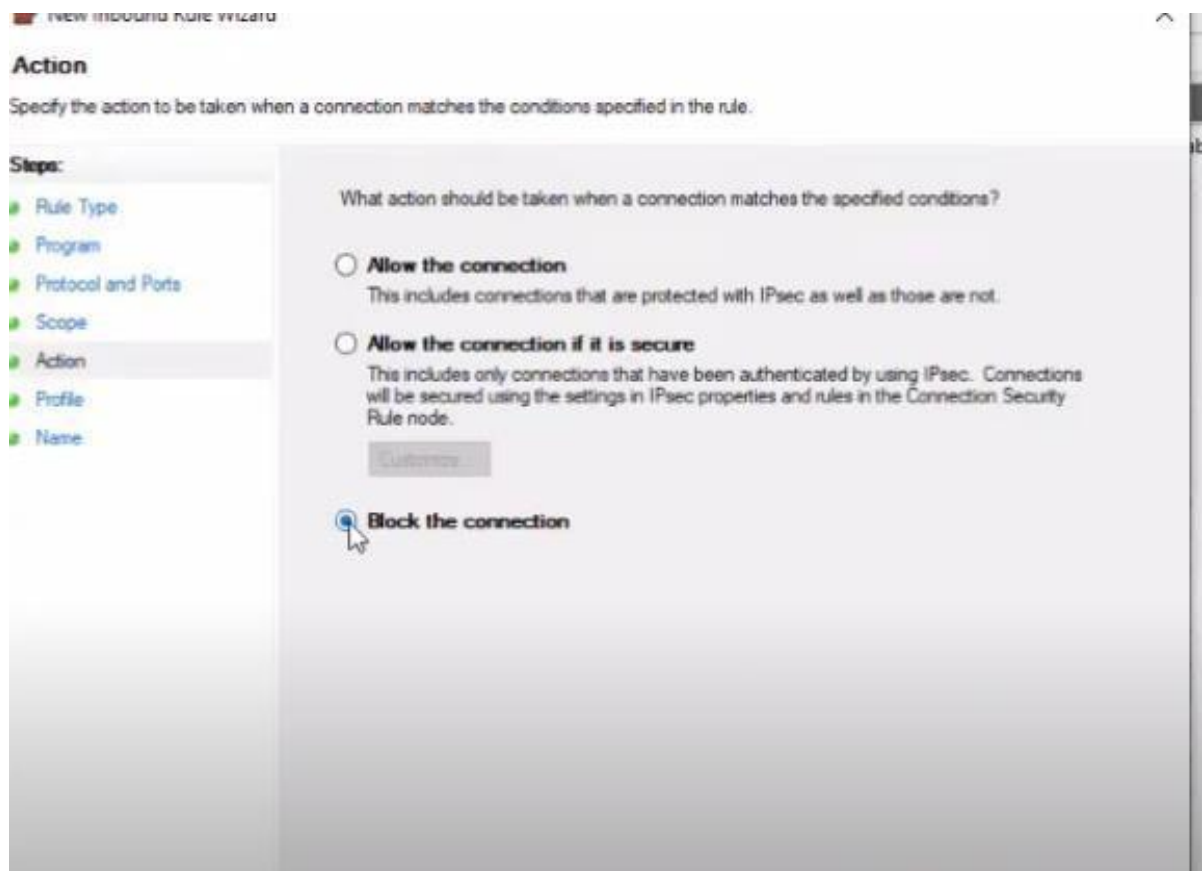




Insert the IP addresses both IPv4 and IPv6



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

