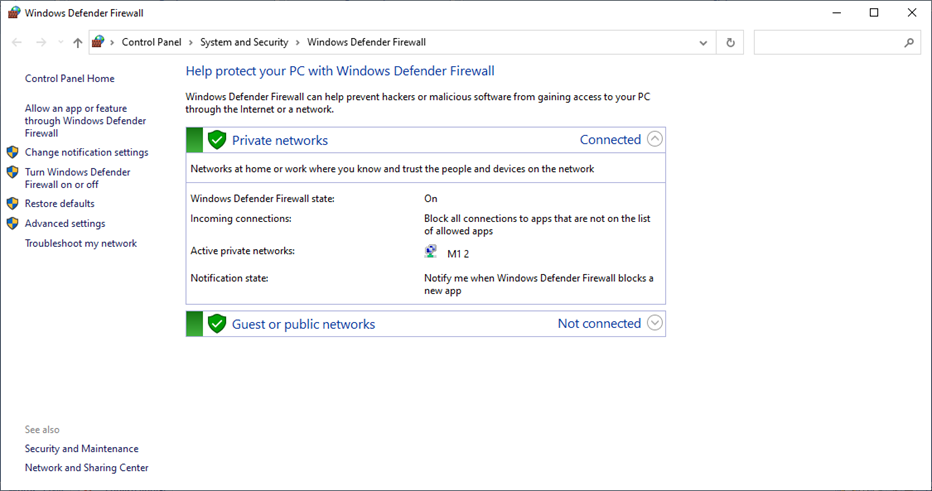
**Practical - 10**

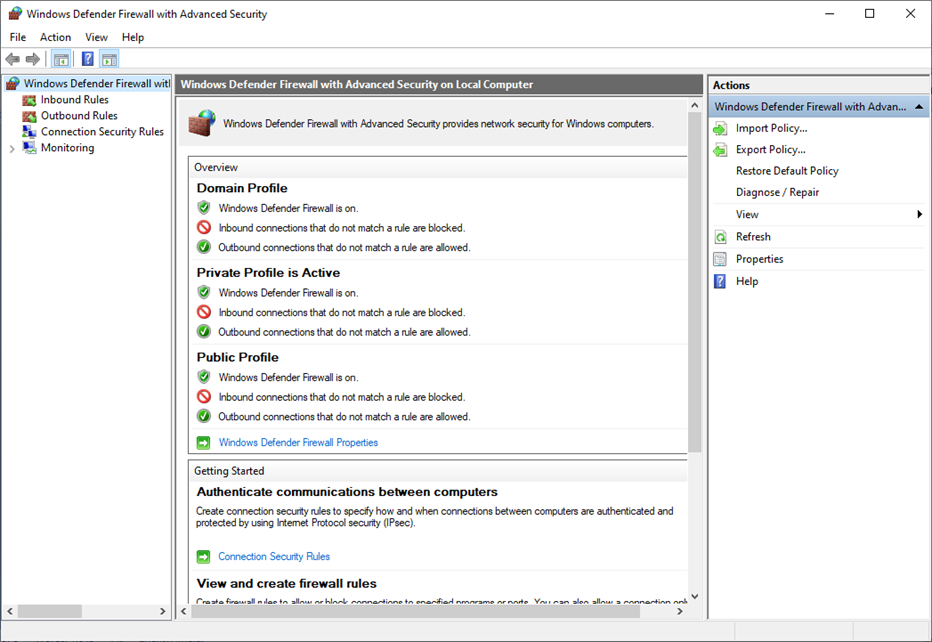
**Aim: Firewall Configuration and Rule- based Filtering**

### Part 1: Blocking the Port

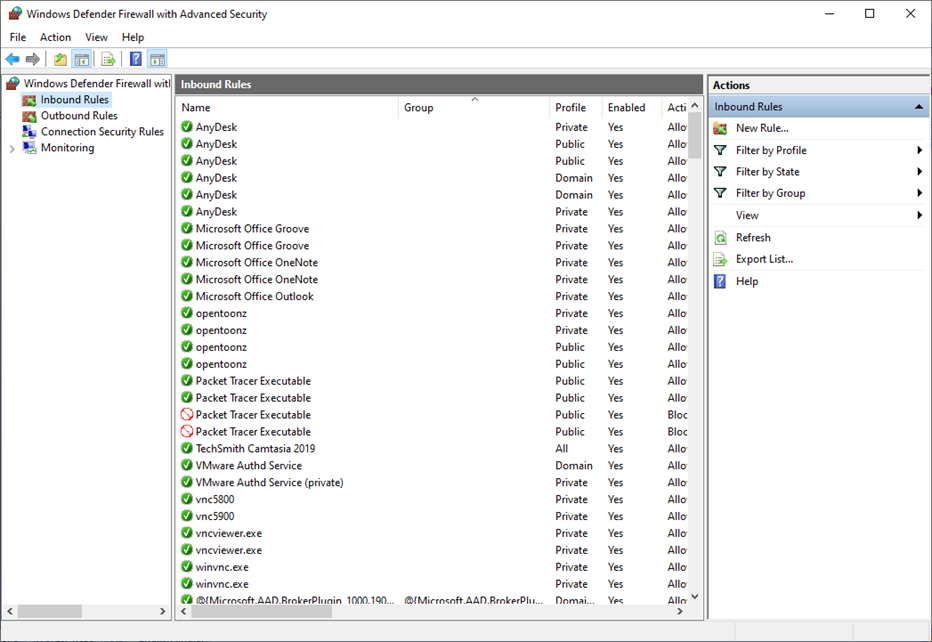
We access any website through the browser and confirm that the HTTP/HTTPS protocols are working.



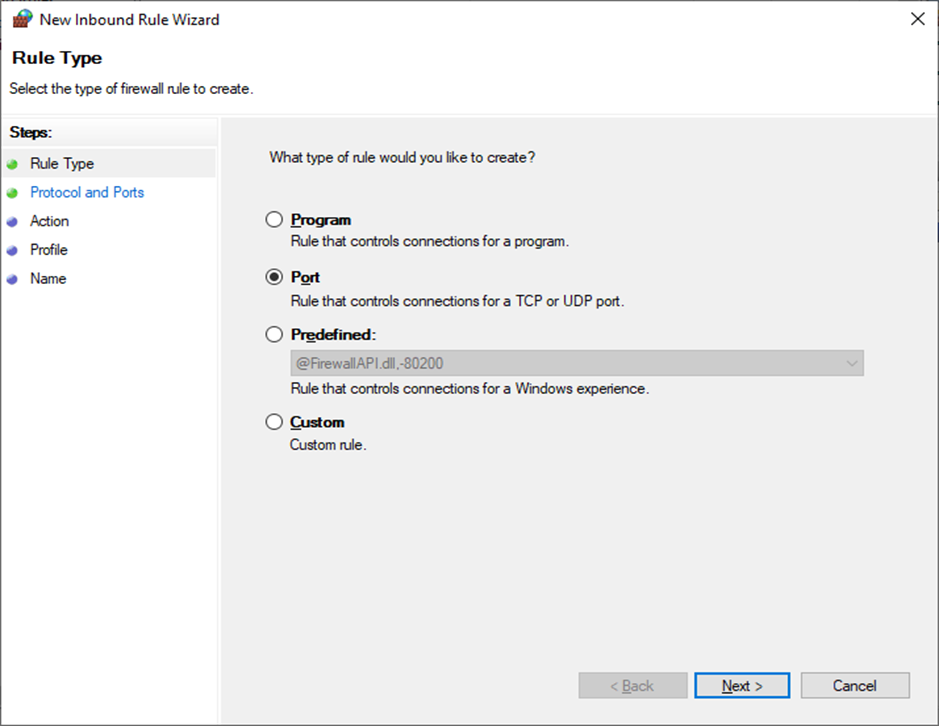
Step 2: We open ‘Windows Defender Firewall’



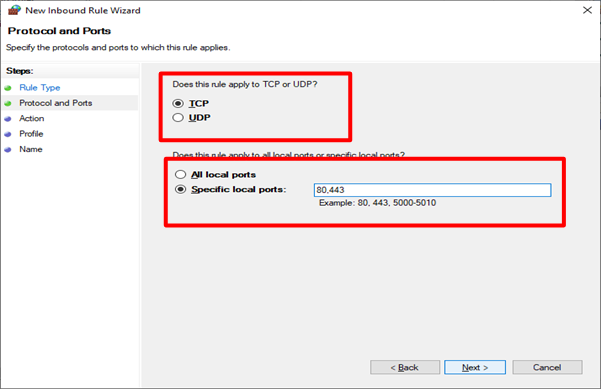
Next we click on ‘Inbound Rules’



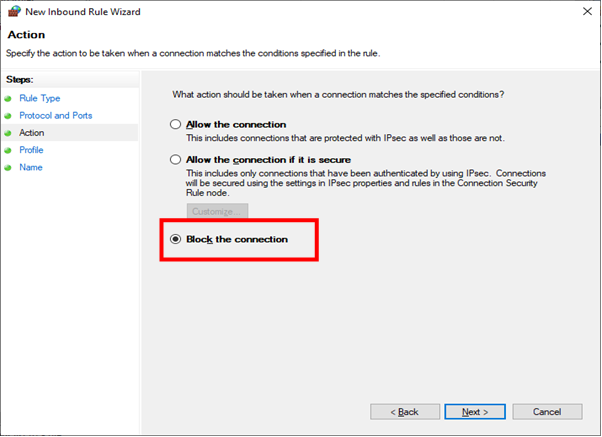
Then click on ‘New Rule’



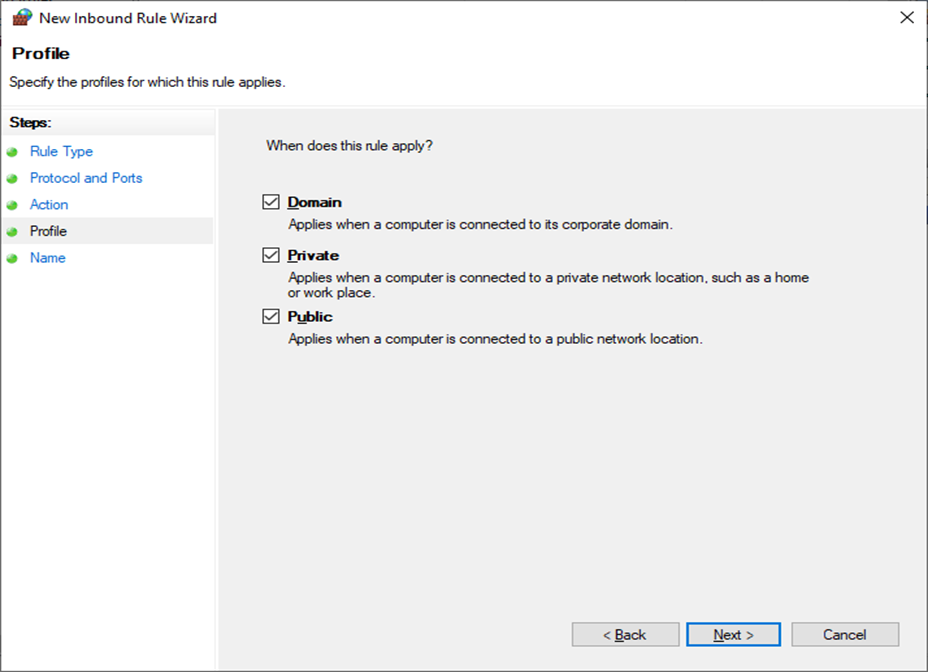
Select the radio button ‘Port’ and click ‘Next’ and enter the following



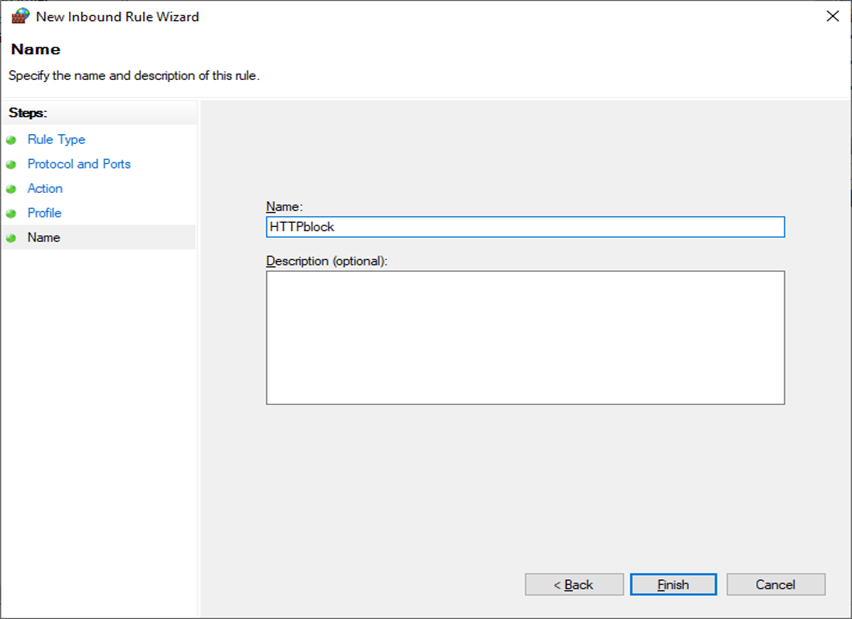
After next, we need to finalise the rule



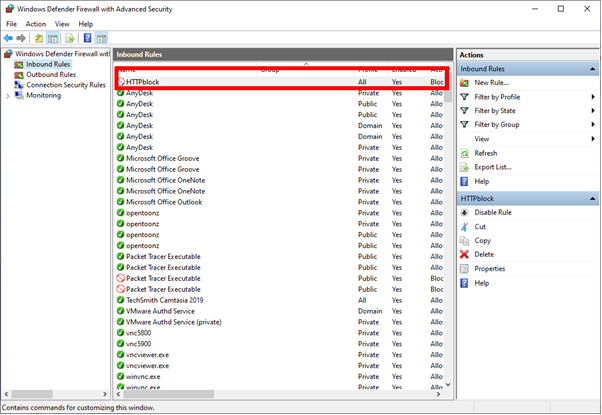
Click ‘Next’ and we get the following



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

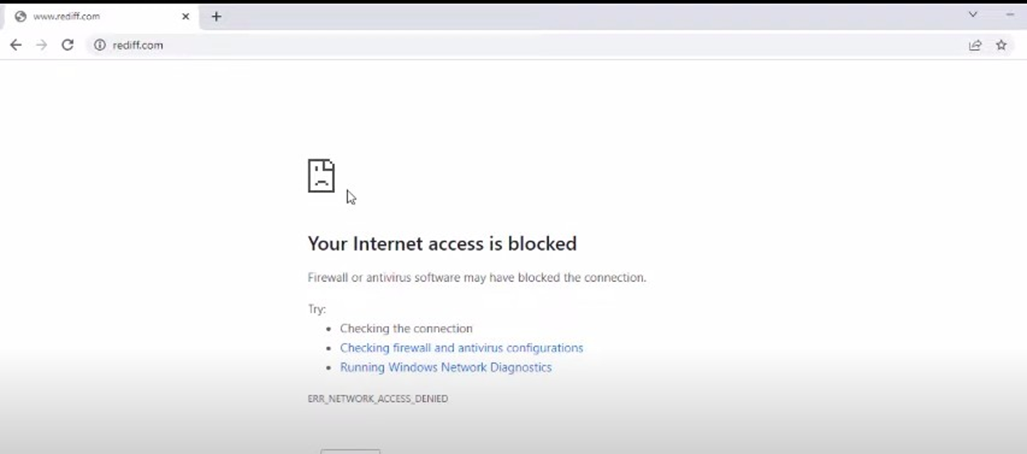


The Inbound rule is added



We repeat all the above steps for creating ‘Outbound Rules’, and then try to access the internet.

We see that the accessed is blocked



### 

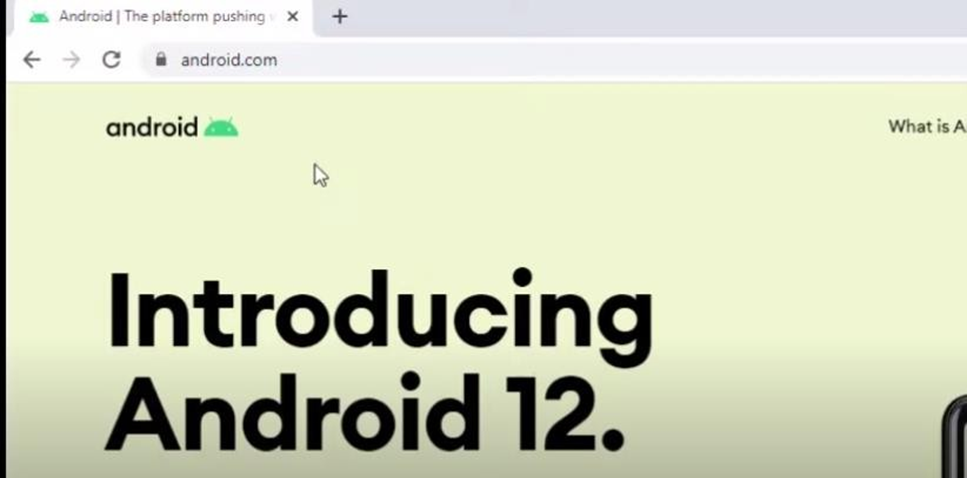
### 

### 

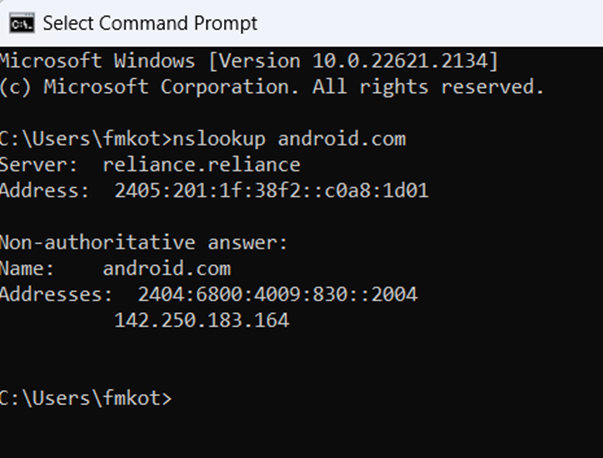
### 

### Part 2: Blocking the website [www.android.com](http://www.android.com/)

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



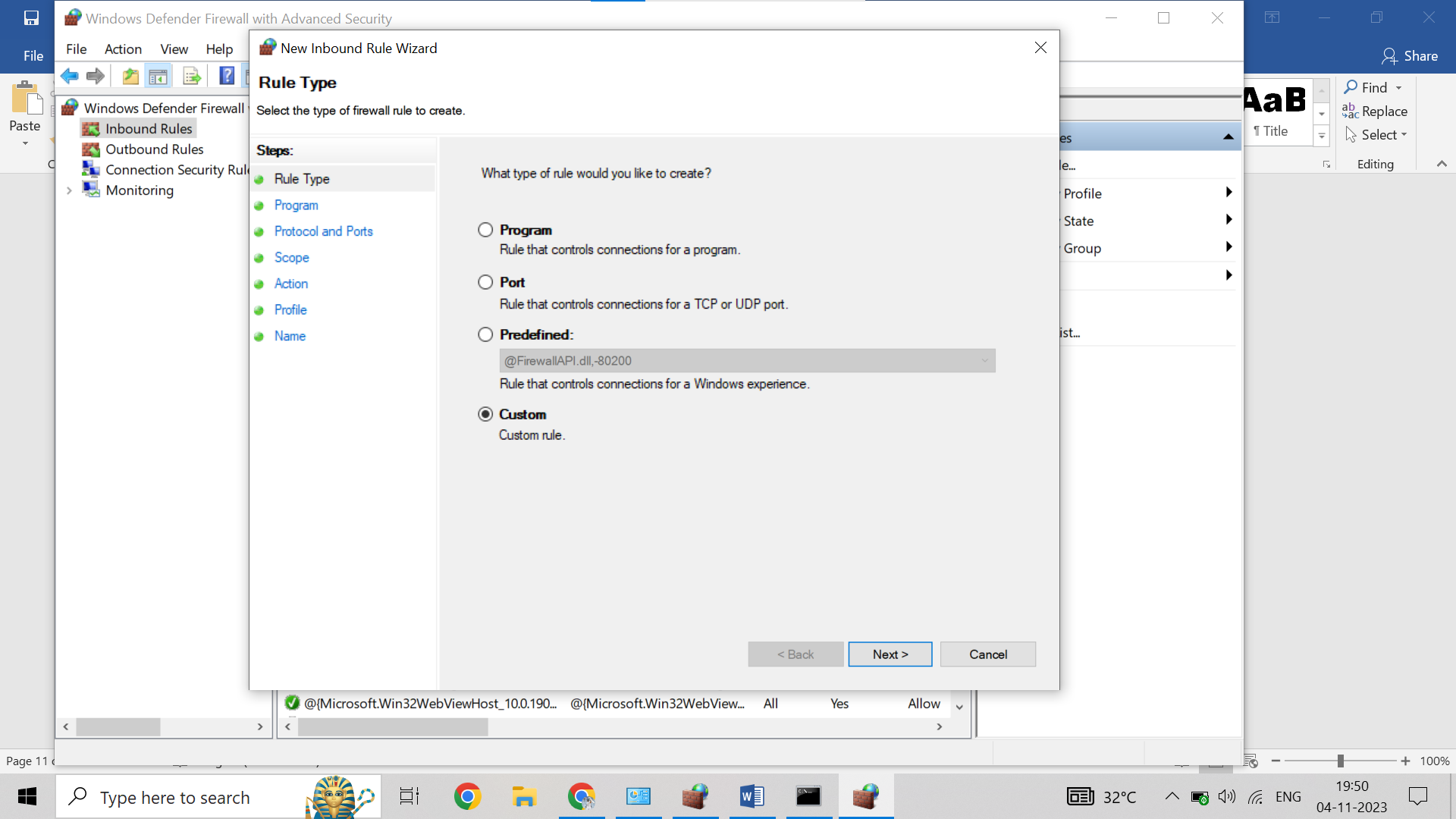
We find the IP addresses of the website using the following command

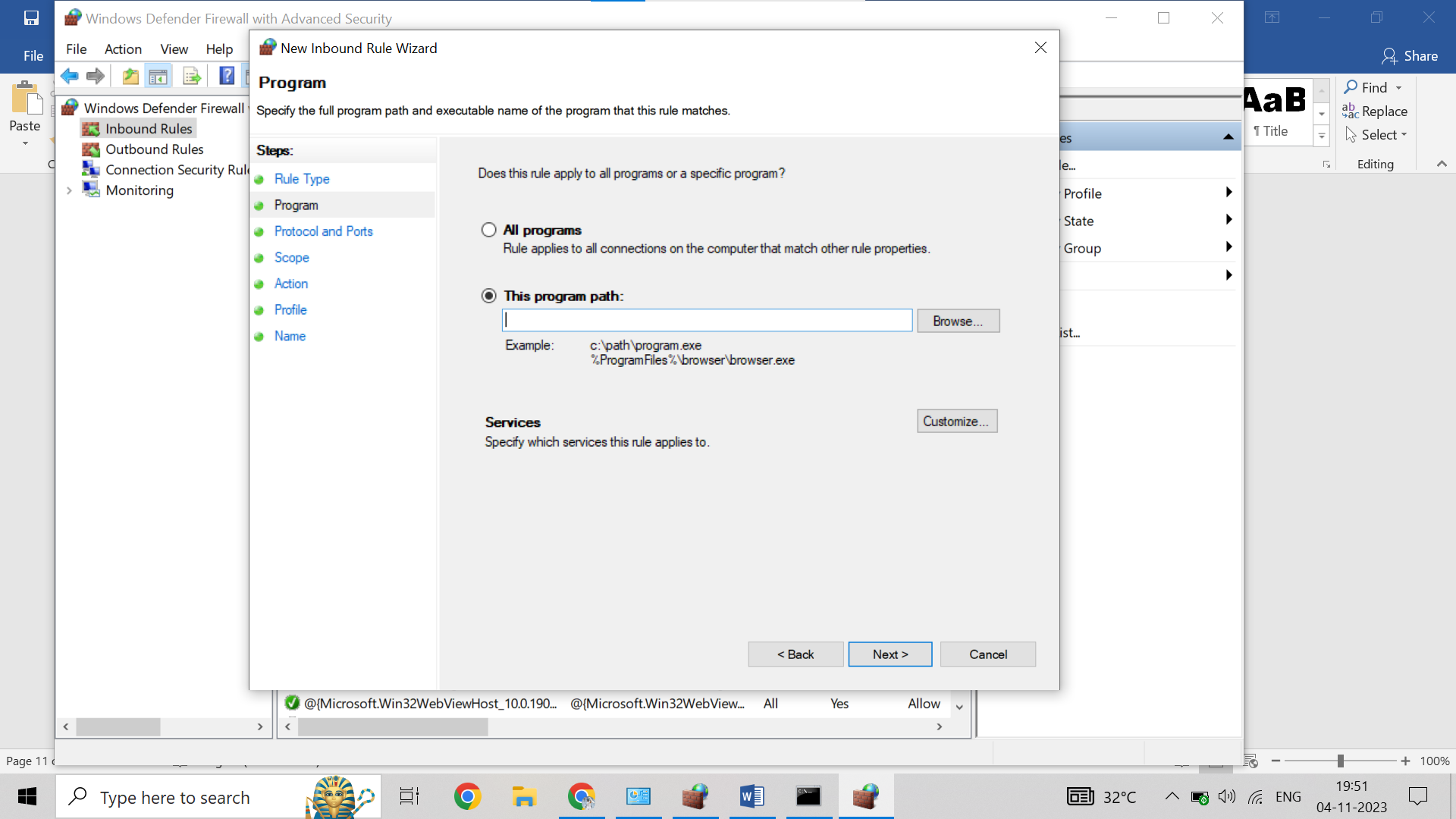


We save the IP addresses

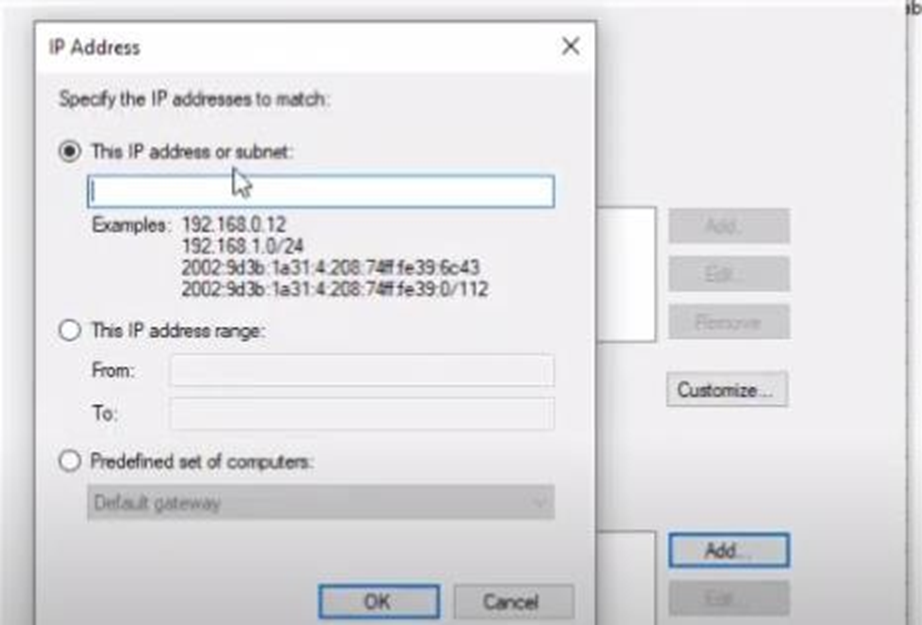
| IPv4 | 216.58.196.68 |
| --- | --- |
| IPv6 | 2404:6800:4009:809::2004 |

We open the windows Firewall settings and apply the Inbound Rule

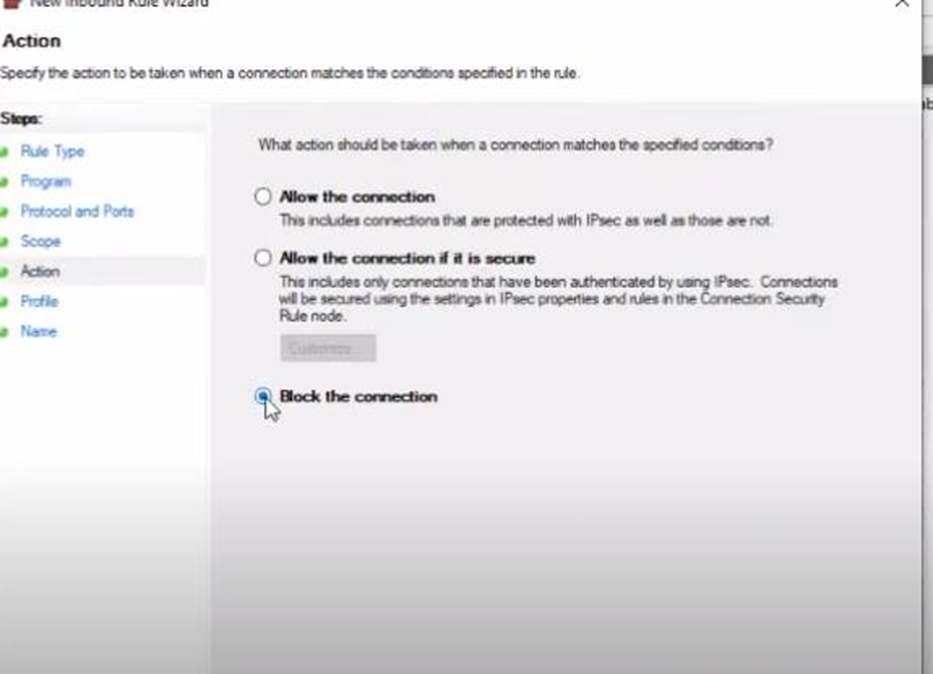




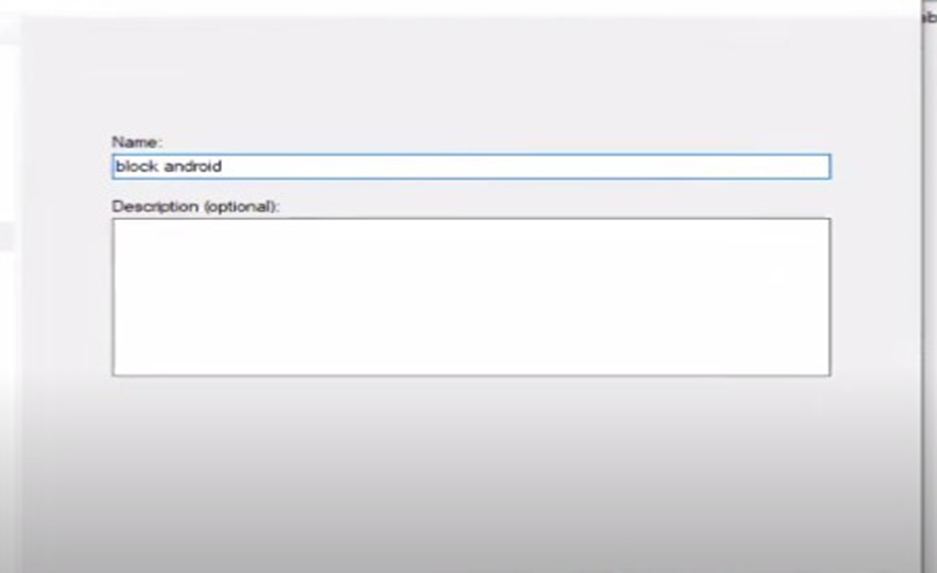
Insert the IP addresses both IPv4 and IPv6



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

