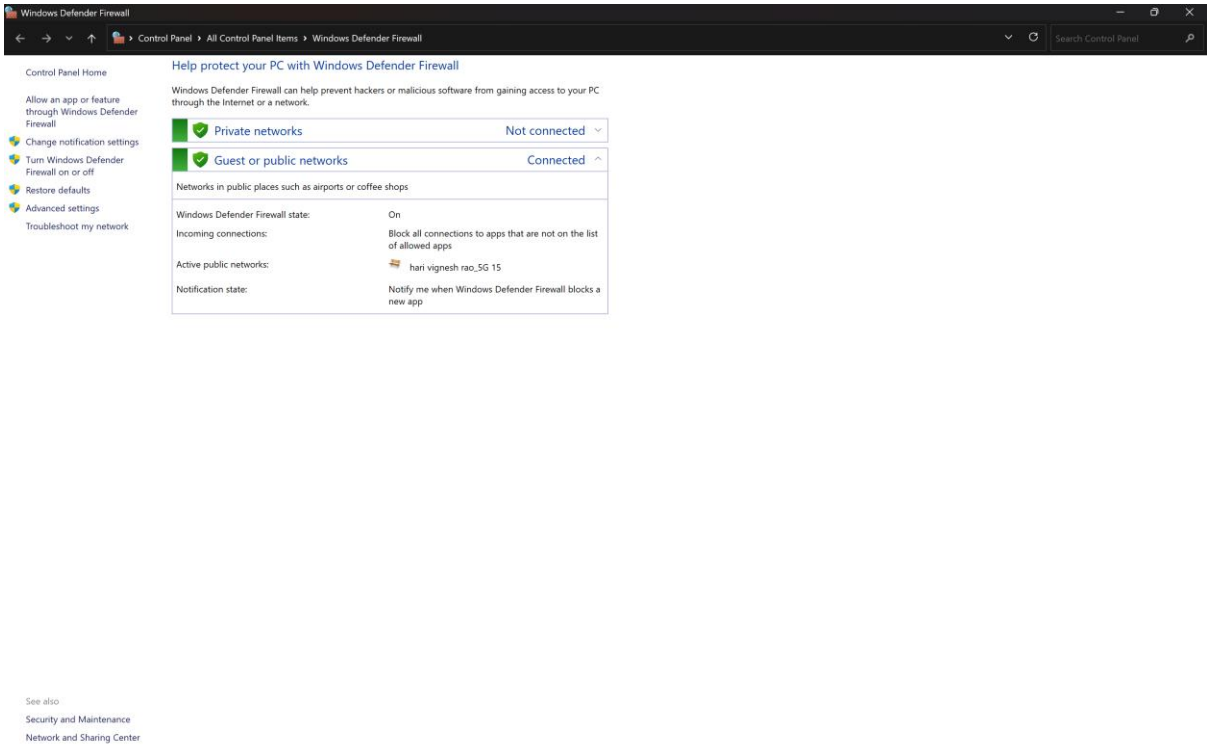


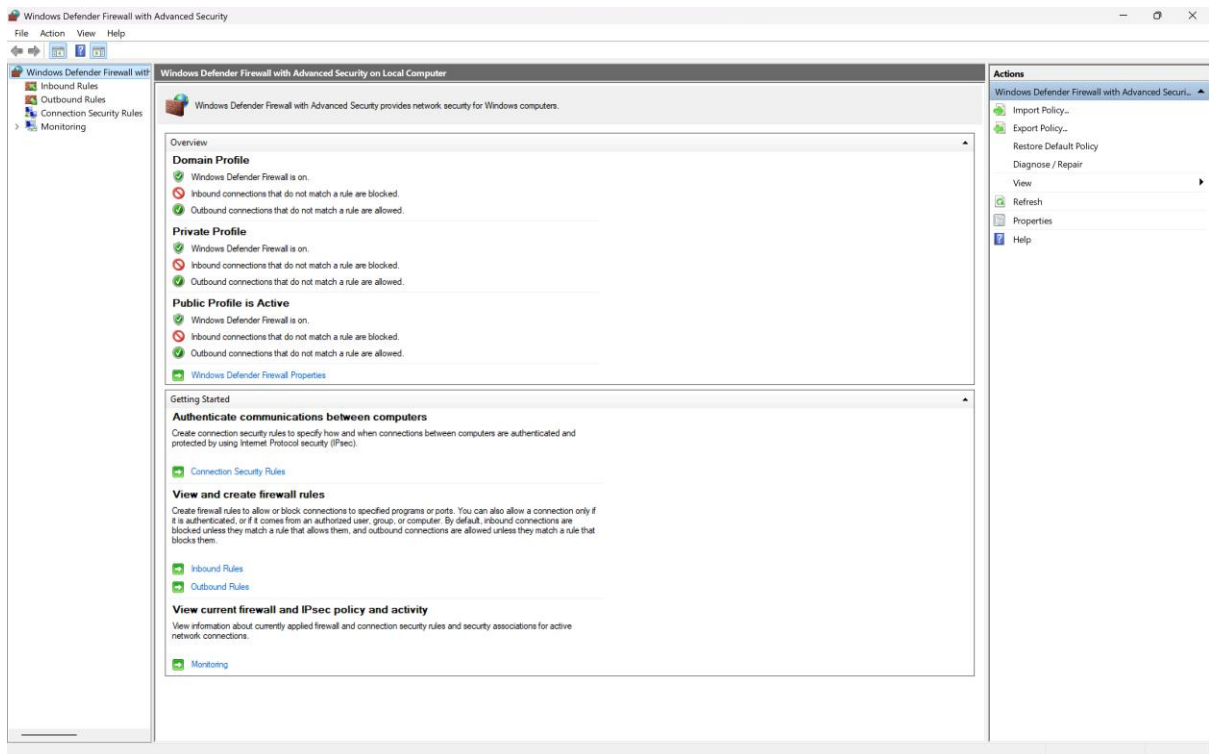
CYBER SECURITY LAB-1 FIREWALL

HARI VIGNESH RAO 23BD1A052Q

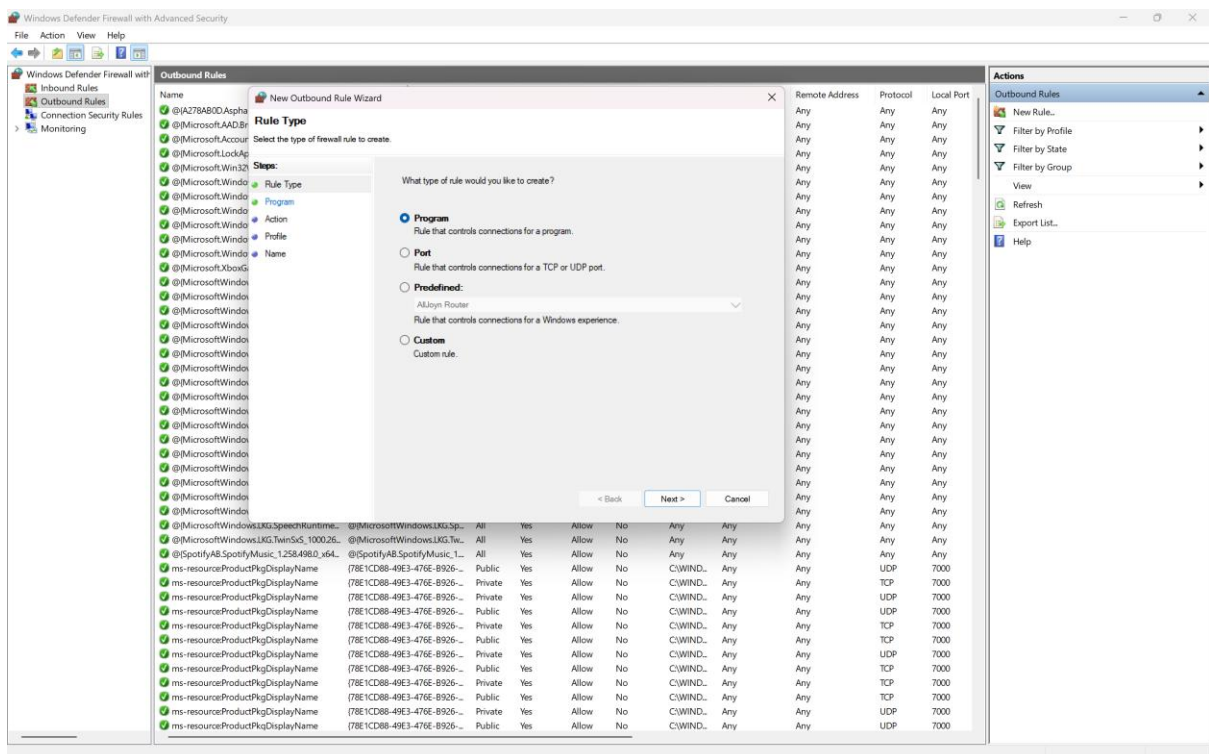
1. Windows Defender Firewall



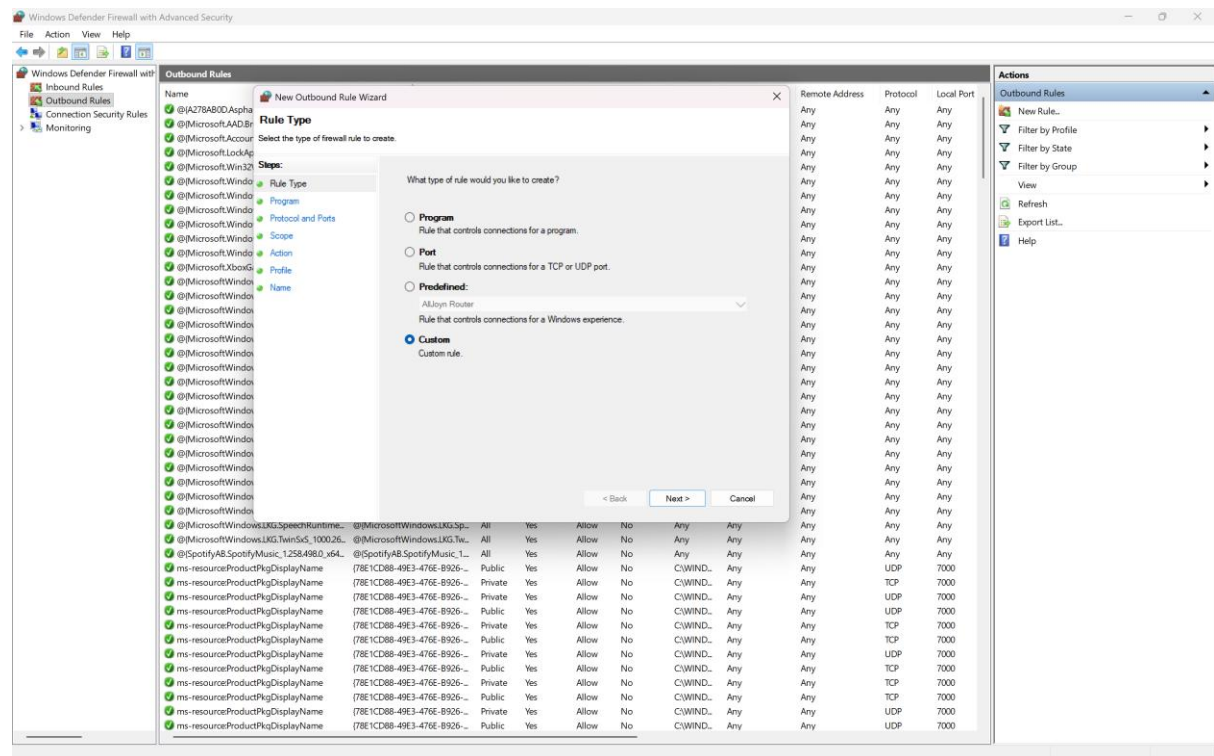
2. Windows Defender Firewall With Advanced Security



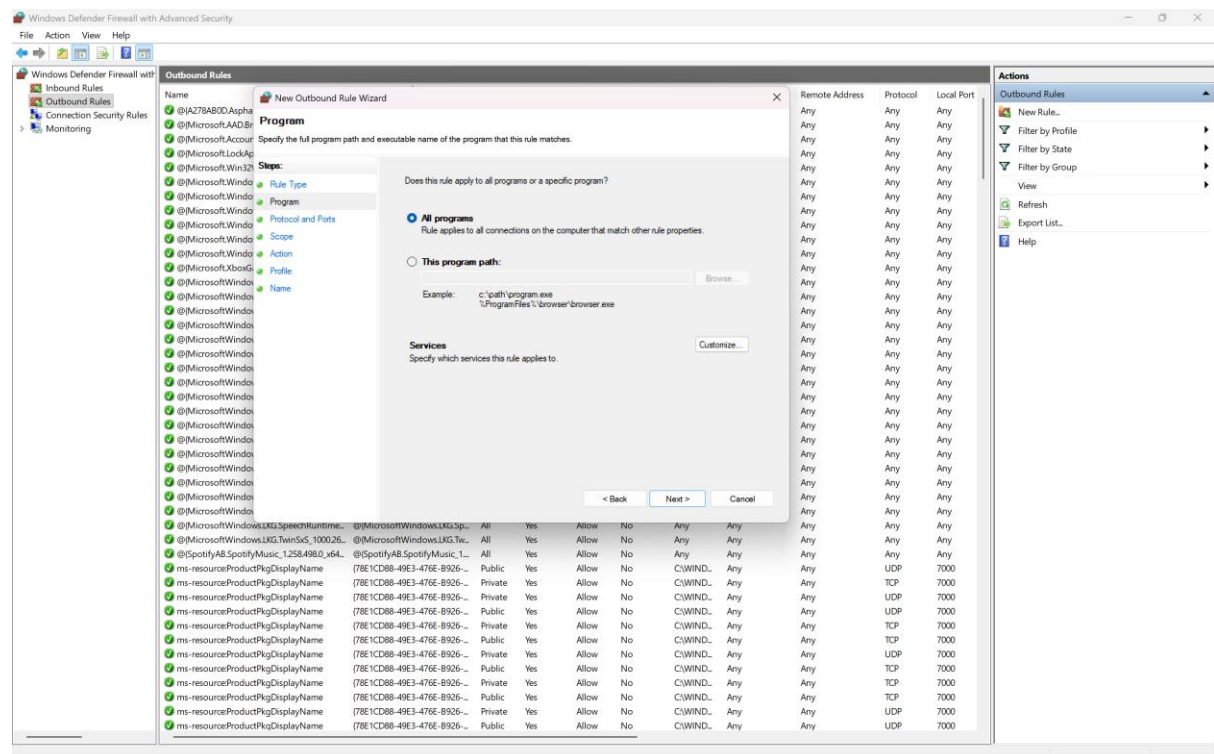
3. New Outbound Rule



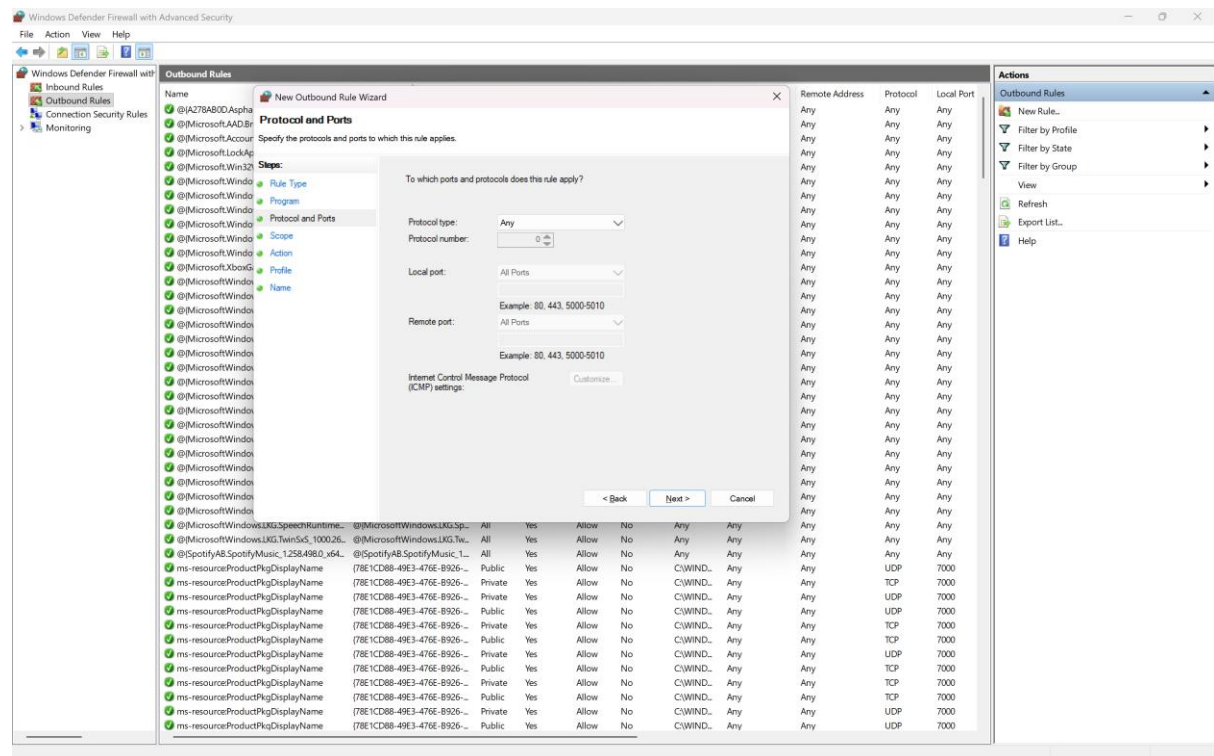
4. Select Custom



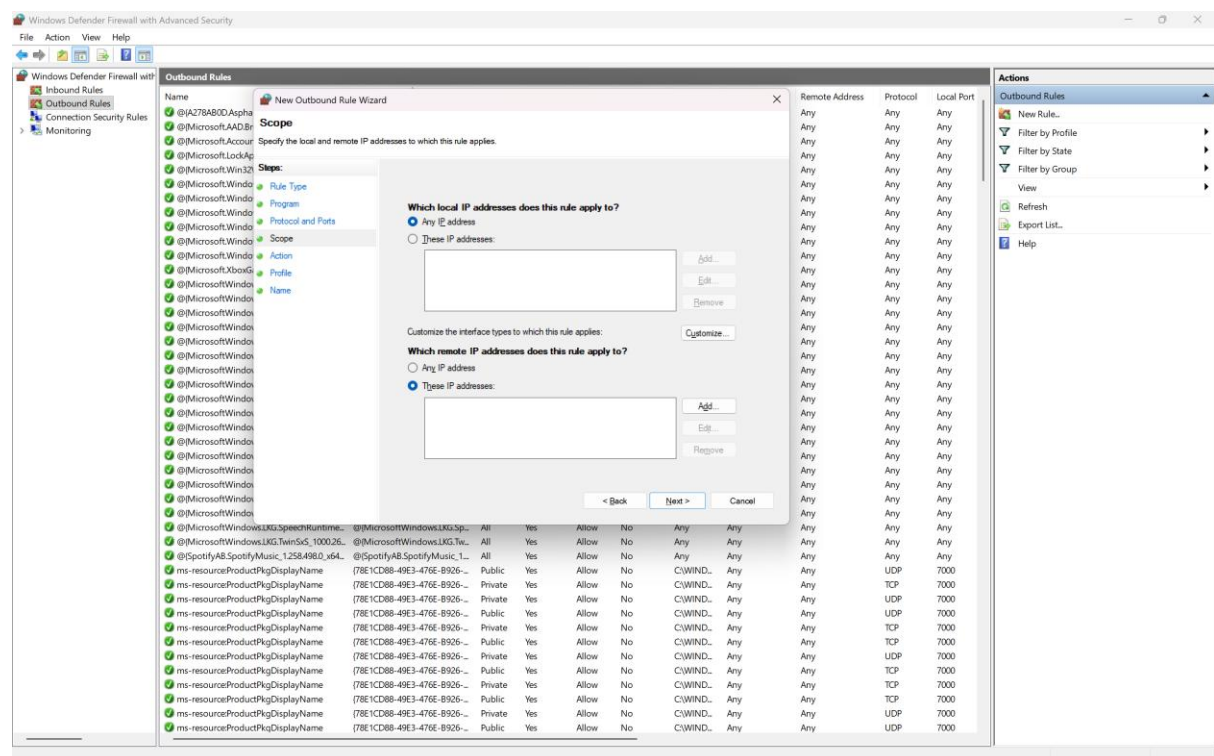
5. All Programs



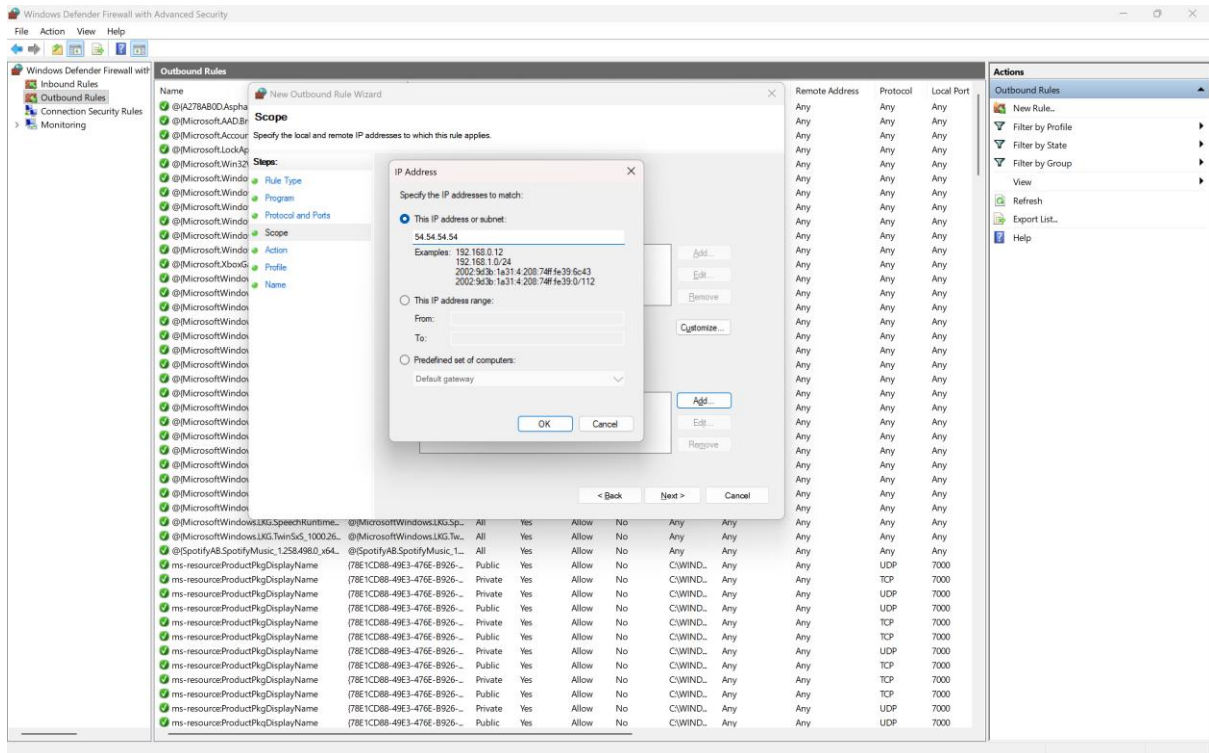
6.Protocol Type Any



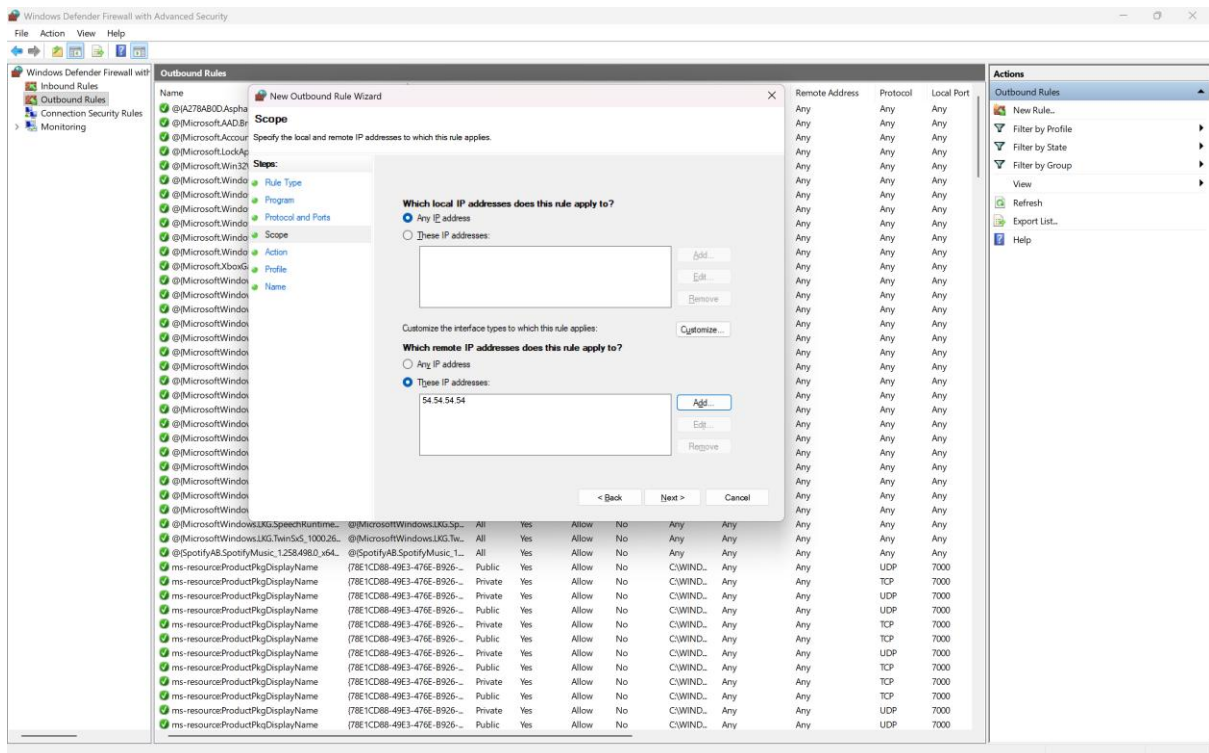
7. These Ip Addresses



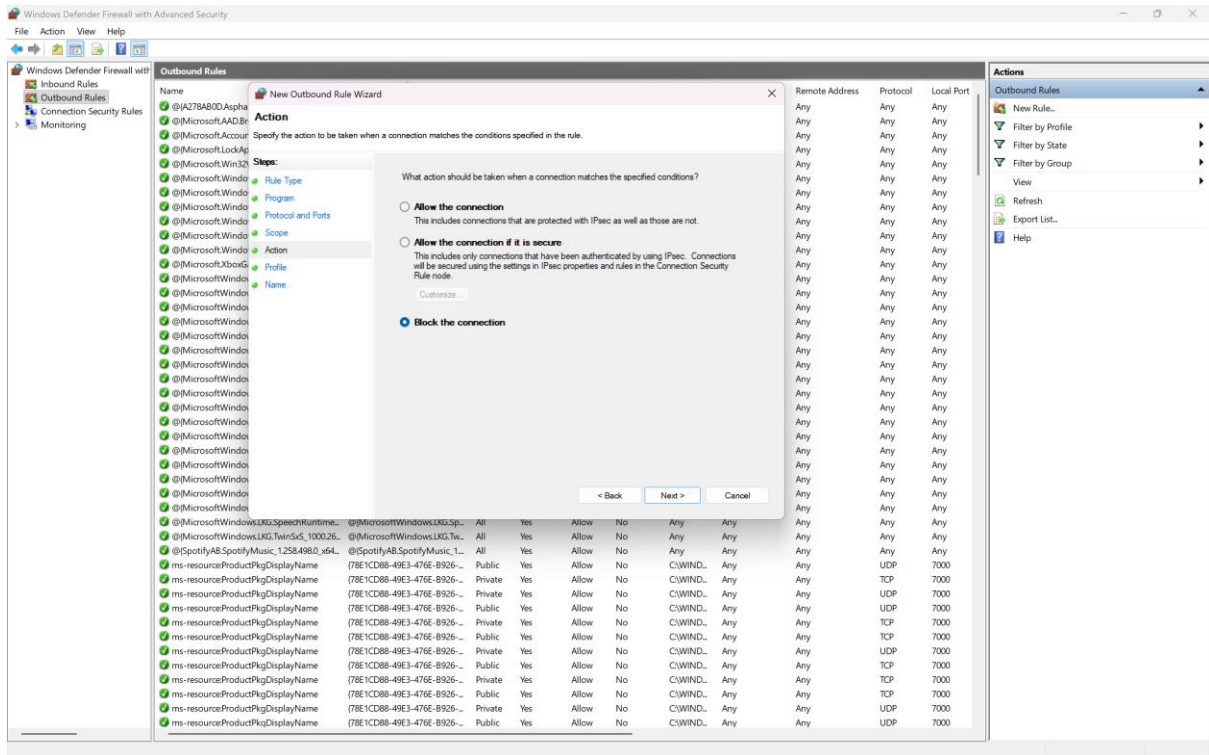
8. Add



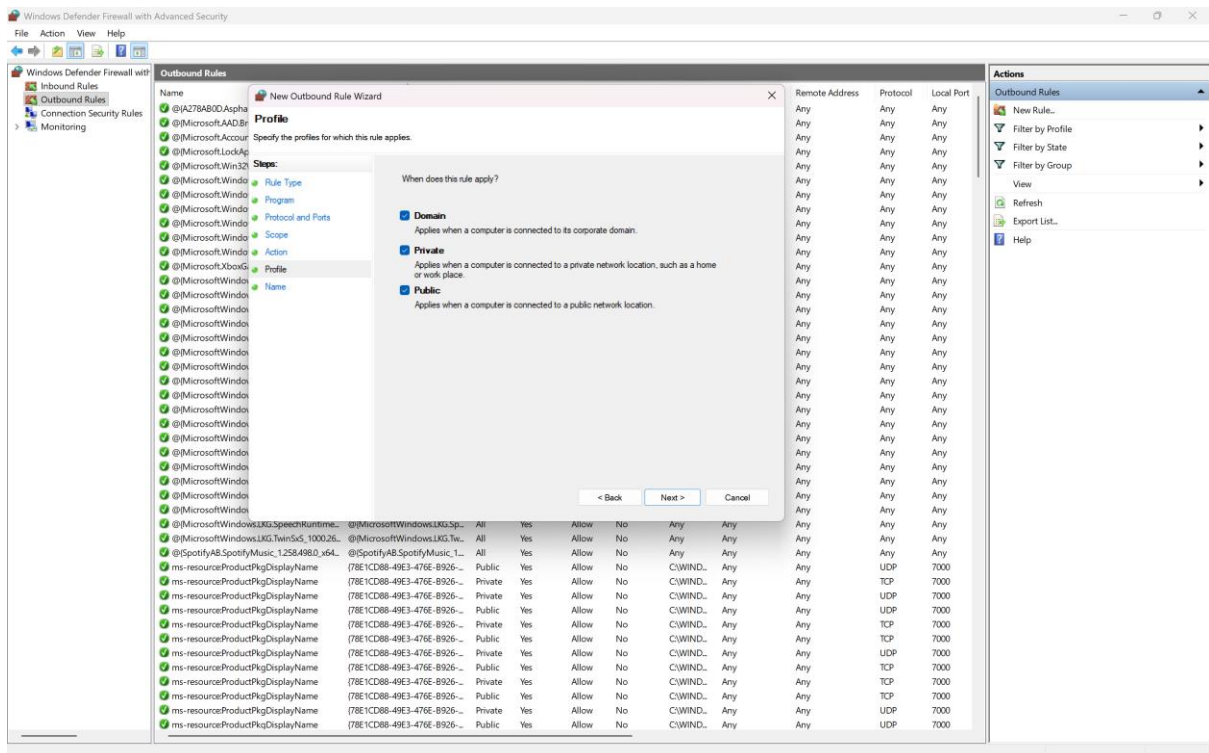
9. ok



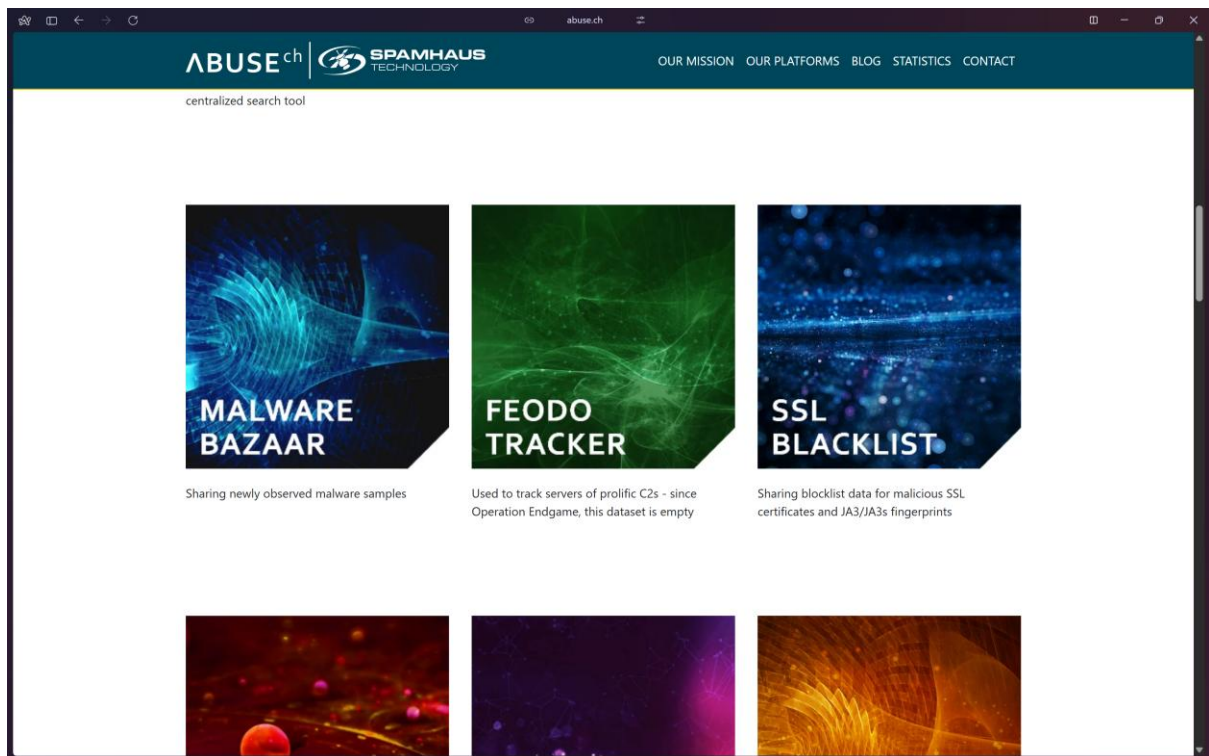
10. Block the connection



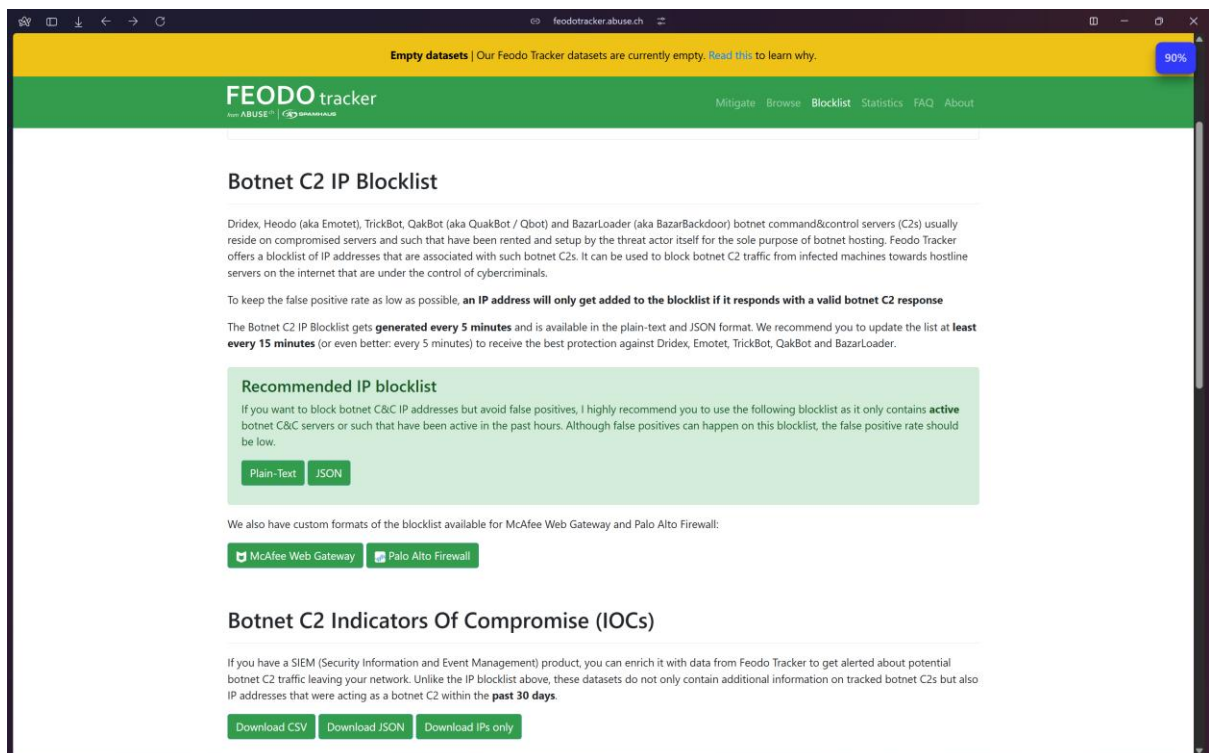
11. Rules to Apply



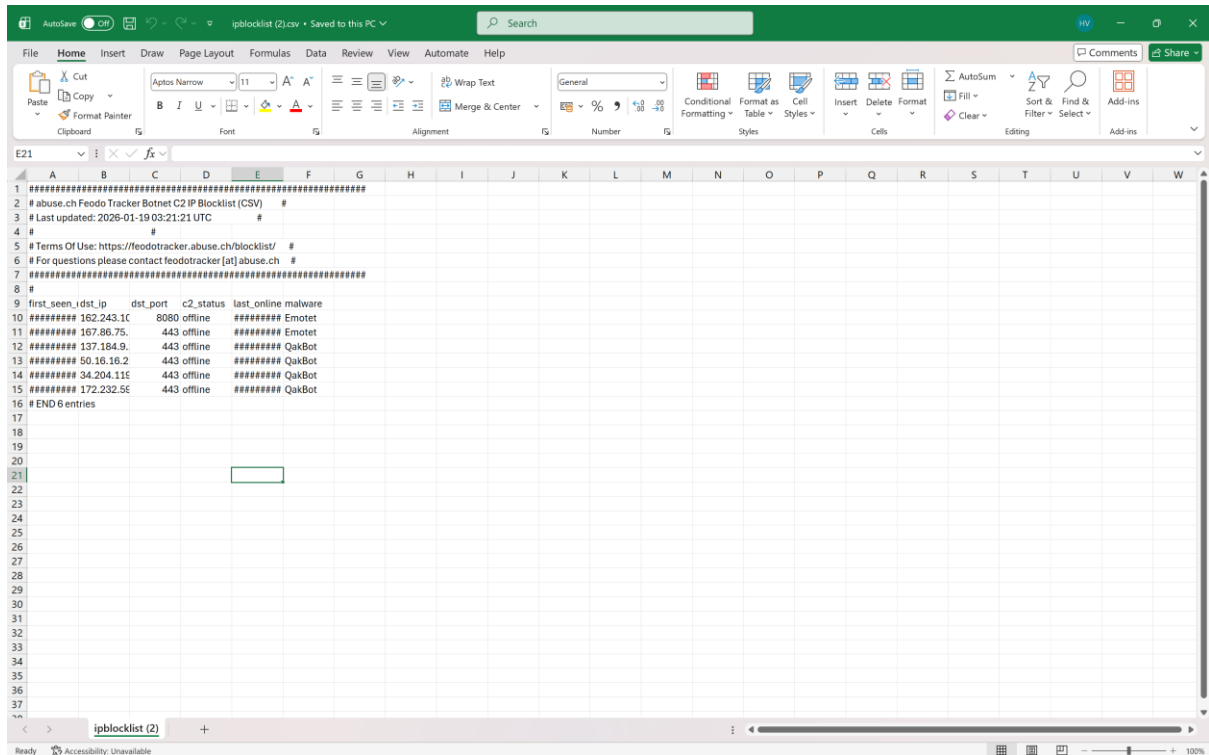
14. Abuse.ch for Blocking list of Ip's



15. Download all the list of blocking ip's

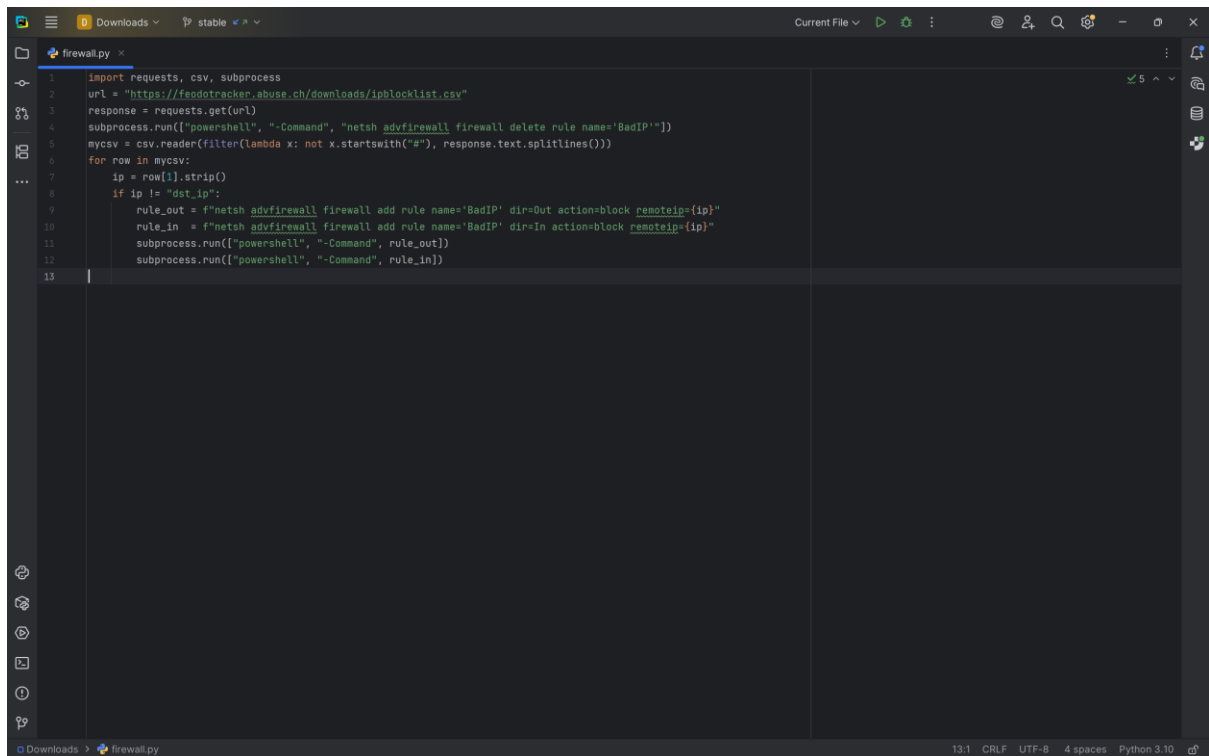


16. List of Block Ip's in .csv



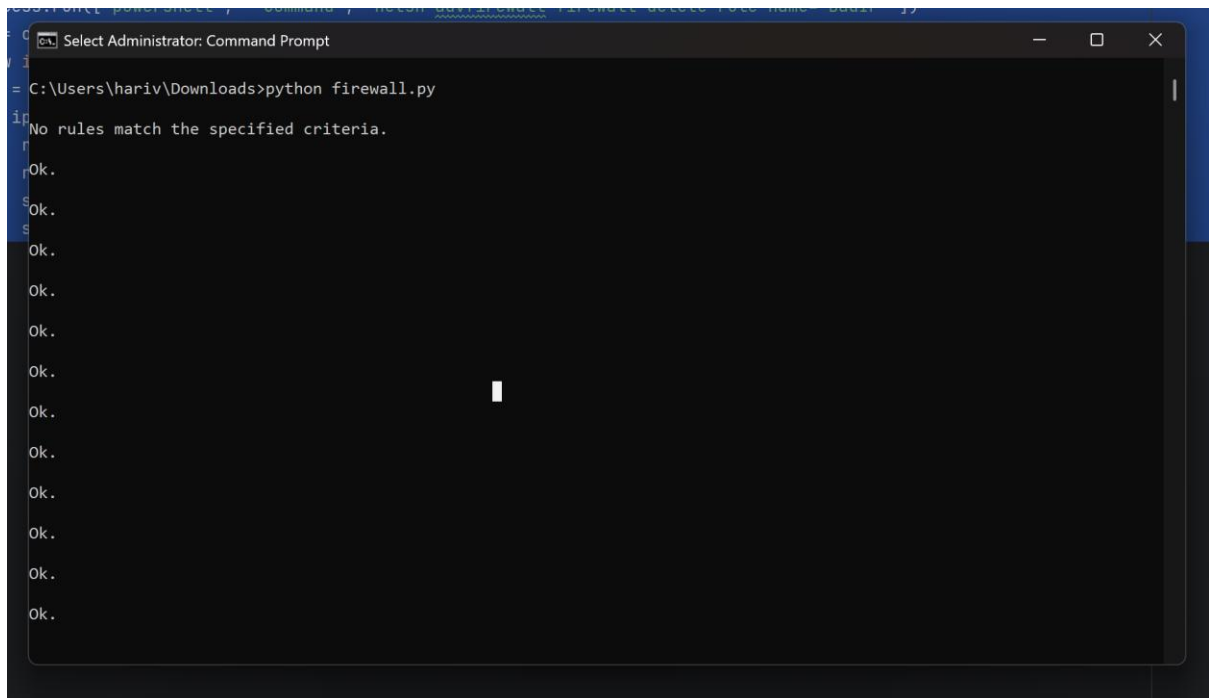
first_seen	dst_ip	dst_port	c2_status	last_online	malware
162.243.16	8080	offline	#####	Emotet	
167.86.75	443	offline	#####	Emotet	
137.184.9	443	offline	#####	QakBot	
50.16.16.2	443	offline	#####	QakBot	
34.204.116	443	offline	#####	QakBot	
172.232.56	443	offline	#####	QakBot	

17. Python firewall.py code to block all the list of Ip's

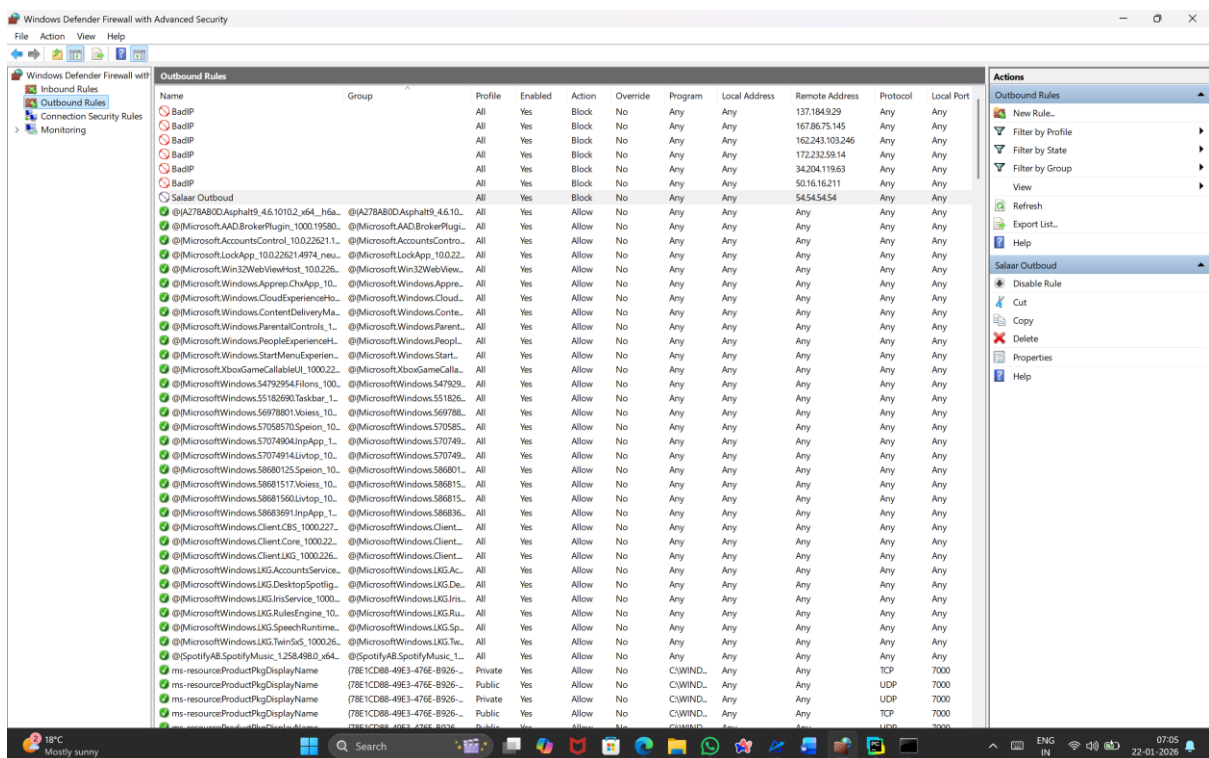


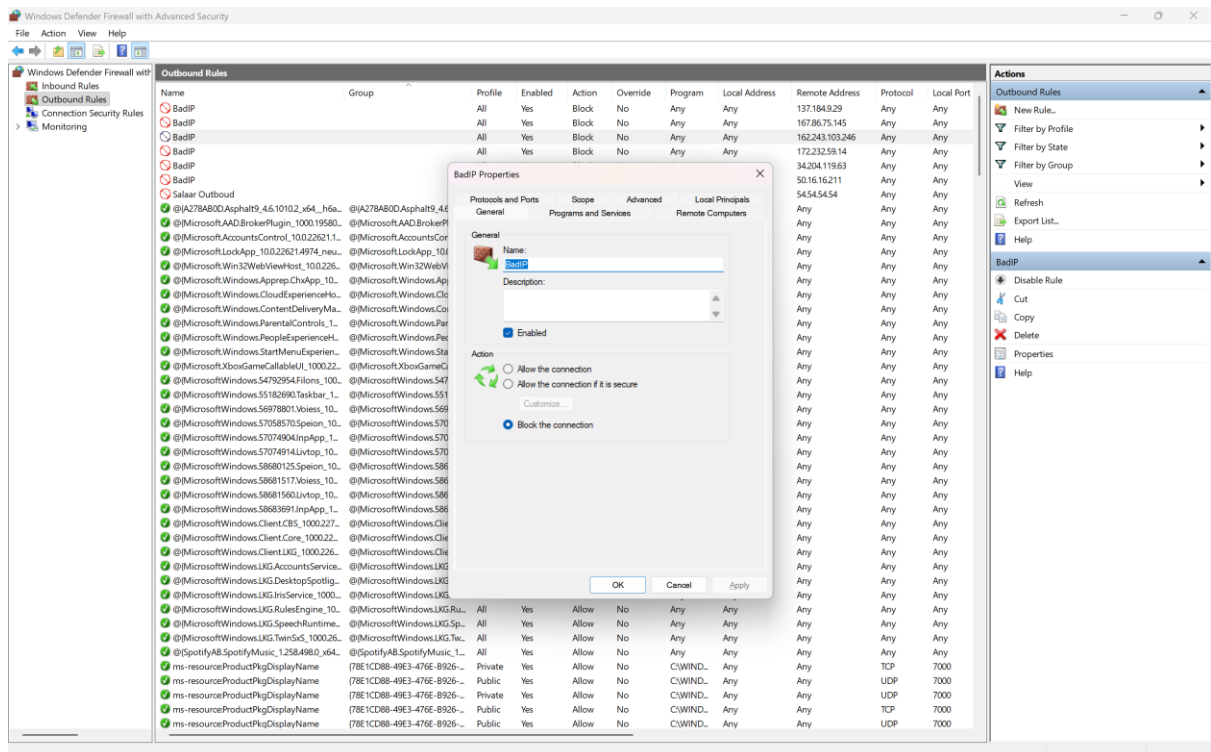
```
1 import requests, csv, subprocess
2 url = "https://feodotracker.abuse.ch/downloads/ipblocklist.csv"
3 response = requests.get(url)
4 subprocess.run(["powershell", "-Command", "netsh advfirewall firewall delete rule name='BadIP'"])
5 mycsv = csv.reader(filter(lambda x: not x.startswith("#"), response.text.splitlines()))
6 for row in mycsv:
7     ip = row[1].strip()
8     if ip != "dst_ip":
9         rule_out = f"netsh advfirewall firewall add rule name='BadIP' dir=Out action=block remoteip={ip}"
10        rule_in = f"netsh advfirewall firewall add rule name='BadIP' dir=In action=block remoteip={ip}"
11        subprocess.run(["powershell", "-Command", rule_out])
12        subprocess.run(["powershell", "-Command", rule_in])
13
```

18. Output



19.Badip in Outbound rules





BadIP Properties

General

Programs and Services

Remote Computers

Protocols and Ports

Scope

Advanced

Local Principals

Local IP address



☒ Any IP address

☐ These IP addresses:

Add...

Edit...

Remove

Remote IP address



☐ Any IP address

☒ These IP addresses:

Add...

Edit...

Remove

OK

Cancel

Apply