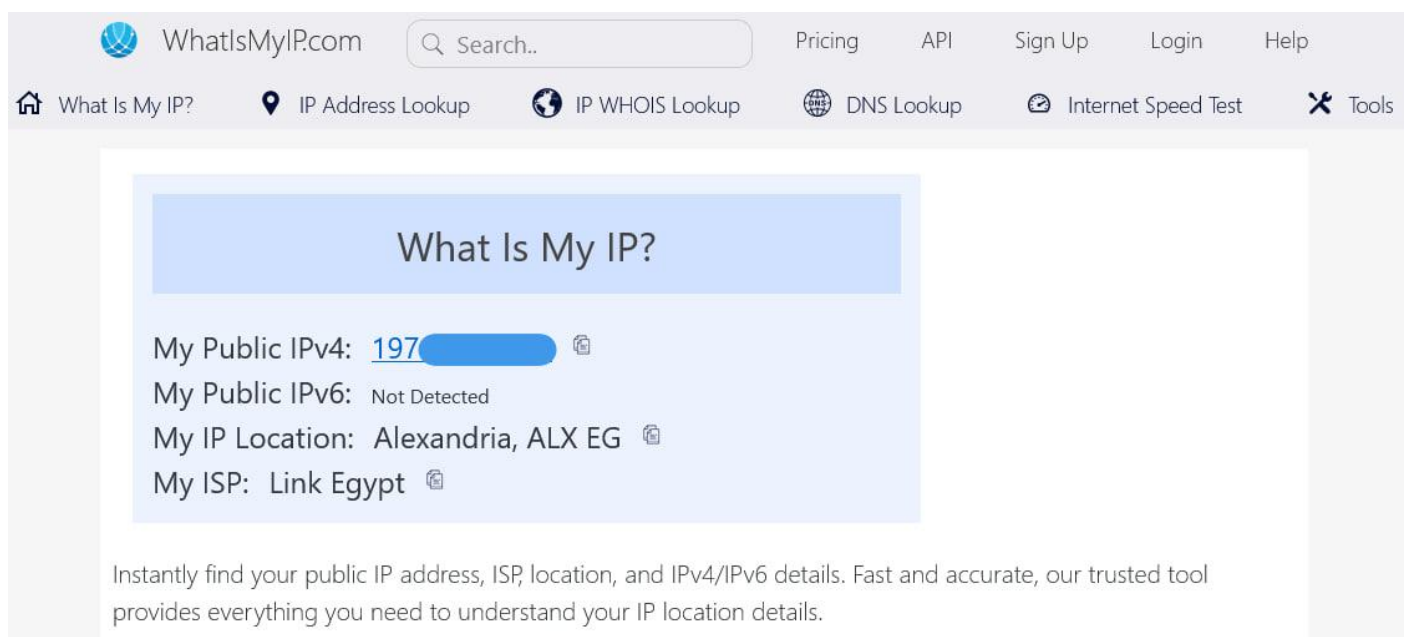


1: Find your mac address → Physical Address → 18-C0-4D-9A-3E-56

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Description . . . . . : Realtek Gaming 2.5GbE Family Controller
Physical Address. . . . . : 18-C0-4D-9A-3E-56
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e29f:66d4:61da:62f9%19(Preferred)
IPv4 Address. . . . . : 192.168.1.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, December 20, 2024 9:51:35 AM
Lease Expires . . . . . : Monday, January 26, 2161 4:25:21 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 102285389
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-65-A4-77-18-C0-4D-9A-3E-56
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled
```

2: Find your real IP addresses



The screenshot shows the homepage of WhatIsMyIP.com. The navigation bar includes links for Pricing, API, Sign Up, Login, and Help. Below the navigation bar, there are icons and labels for various services: What Is My IP?, IP Address Lookup, IP WHOIS Lookup, DNS Lookup, Internet Speed Test, and Tools. The main content area features a large blue box with the title "What Is My IP?". Below the title, the following information is displayed: My Public IPv4: 197 (with a location pin icon), My Public IPv6: Not Detected, My IP Location: Alexandria, ALX EG (with a location pin icon), and My ISP: Link Egypt (with a location pin icon). At the bottom of the main content area, a paragraph states: "Instantly find your public IP address, ISP, location, and IPv4/IPv6 details. Fast and accurate, our trusted tool provides everything you need to understand your IP location details."

3: Find your private IP addresses → IPv4 Address → 192.168.1.100

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::e29f:66d4:61da:62f9%19
IPv4 Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Ipconfig /release → will release the IP and Ipconfig /renew → will renew the IP

4: Find current session and ports on your device

```
PS C:\Users\NourElDin> Netstat -n

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    127.0.0.1:20000         127.0.0.1:49713        ESTABLISHED
    TCP    127.0.0.1:49679       127.0.0.1:49680        ESTABLISHED
    TCP    127.0.0.1:49680       127.0.0.1:49679        ESTABLISHED
    TCP    127.0.0.1:49687       127.0.0.1:49688        ESTABLISHED
    TCP    127.0.0.1:49688       127.0.0.1:49687        ESTABLISHED
    TCP    127.0.0.1:49689       127.0.0.1:49690        ESTABLISHED
    TCP    127.0.0.1:49690       127.0.0.1:49689        ESTABLISHED
    TCP    127.0.0.1:49711       127.0.0.1:49712        ESTABLISHED
    TCP    127.0.0.1:49712       127.0.0.1:49711        ESTABLISHED
    TCP    127.0.0.1:49713       127.0.0.1:20000        ESTABLISHED
    TCP    127.0.0.1:49944       127.0.0.1:49945        ESTABLISHED
    TCP    127.0.0.1:49945       127.0.0.1:49944        ESTABLISHED
    TCP    127.0.0.1:49946       127.0.0.1:49947        ESTABLISHED
    TCP    127.0.0.1:49947       127.0.0.1:49946        ESTABLISHED
    TCP    192.168.1.100:50366   34.107.221.82:80       TIME_WAIT
    TCP    192.168.1.100:50367   34.107.221.82:80       TIME_WAIT
    TCP    192.168.1.100:50368   20.54.37.64:443        ESTABLISHED
    TCP    192.168.1.100:50369   149.154.167.92:443     ESTABLISHED
    TCP    192.168.1.100:50370   149.154.167.92:443     ESTABLISHED
    TCP    192.168.1.100:50375   34.107.243.93:443      TIME_WAIT
    TCP    192.168.1.100:50376   34.107.243.93:443      ESTABLISHED
    TCP    192.168.1.100:50377   52.111.231.21:443      ESTABLISHED
    TCP    192.168.1.100:50378   52.111.236.33:443      ESTABLISHED
    TCP    192.168.1.100:50380   52.113.194.132:443     TIME_WAIT
    TCP    192.168.1.100:50392   20.3.187.198:443       TIME_WAIT
    TCP    192.168.1.100:50398   52.111.236.33:443      ESTABLISHED
    TCP    192.168.1.100:50399   52.111.236.33:443      ESTABLISHED
    TCP    192.168.1.100:50401   52.98.200.194:443      ESTABLISHED
    TCP    192.168.1.100:50403   92.123.48.219:443      ESTABLISHED
    TCP    192.168.1.100:50406   52.109.68.129:443      TIME_WAIT
    TCP    192.168.1.100:50407   13.69.239.73:443       ESTABLISHED

PS C:\Users\NourElDin> Netstat -a

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    0.0.0.0:135           NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:445           NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:5040          NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:5357          NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:49664         NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:49665         NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:49666         NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:49667         NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:49668         NourElDin-PC:0         LISTENING
    TCP    0.0.0.0:49681         NourElDin-PC:0         LISTENING
```

5: Find The IP of the domain Yahoo.com

```
PS C:\Users\NourElDin> Nslookup Yahoo.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     Yahoo.com
Addresses: 2001:4998:24:120d::1:0
           2001:4998:44:3507::8000
           2001:4998:124:1507::f001
           2001:4998:24:120d::1:1
           2001:4998:44:3507::8001
           2001:4998:124:1507::f000
           74.6.143.25
           74.6.231.21
           74.6.231.20
           74.6.143.26
           98.137.11.163
           98.137.11.164
```

6: How to use your local firewall to block a port and stop DOS attack from a zombie device

Open Resource Monitor: Look for the ports that are experiencing high traffic, which could indicate a DOS attack.

Open Windows Defender Firewall with Advanced Security: Control Panel >> System and Security >> Windows Defender Firewall >> advanced settings.

Create an Outbound Rule to Block the Port:

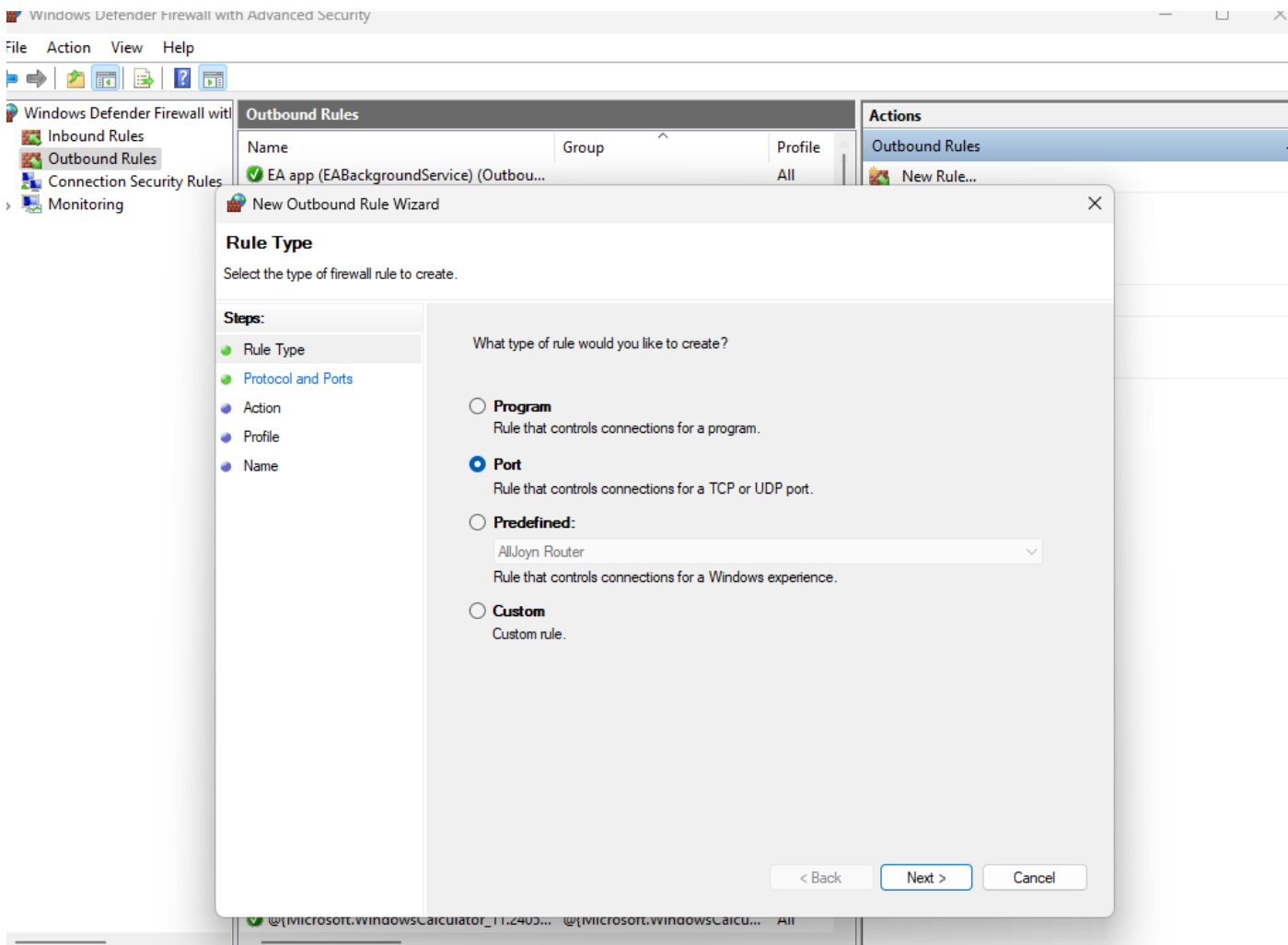
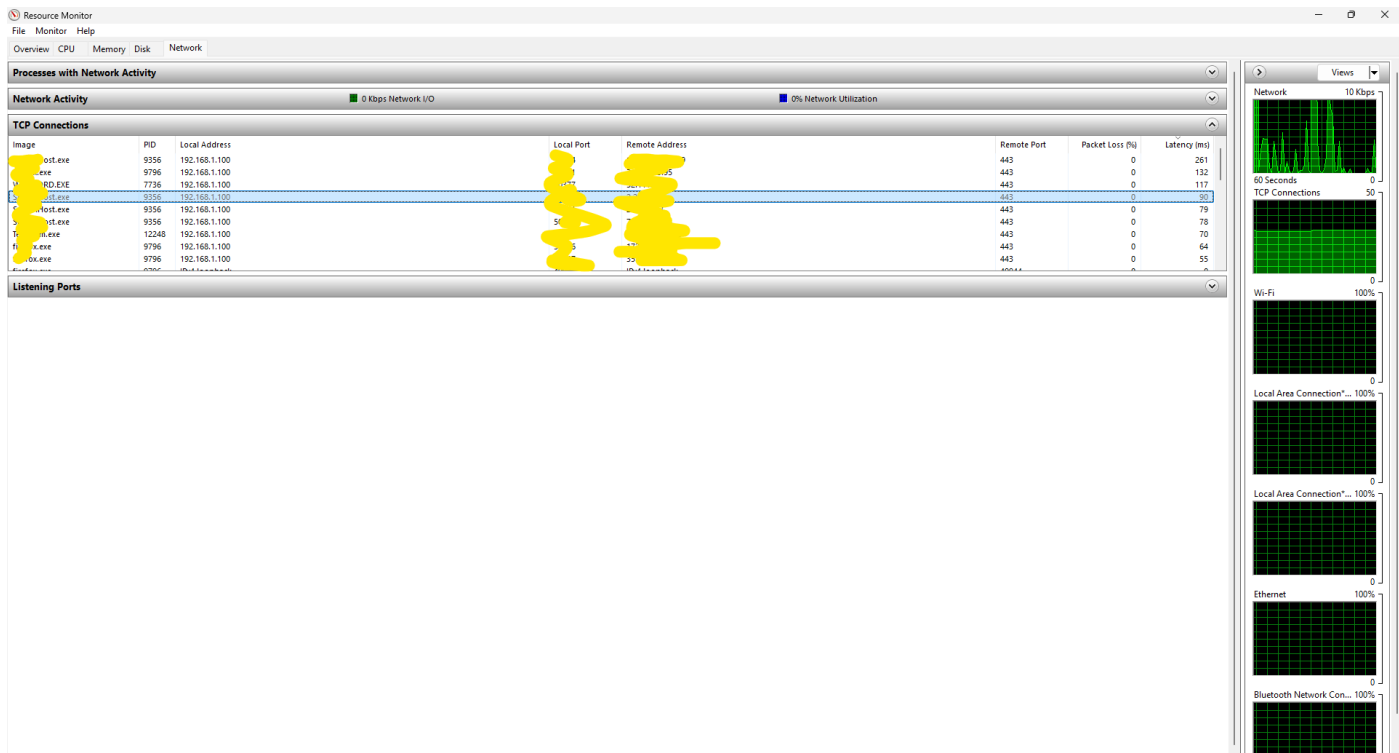
- Click **Outbound Rules** on the left panel.
 - Select **New Rule** on the right-hand side.
 - Choose **Port** and click **Next**.
 - Select **TCP** or **UDP** depending on the protocol of the port being attacked.
 - Enter the specific port number to block and click **Next**.
 - Select **Block the connection** and click **Next**.
 - Choose when the rule applies (Domain, Private, Public) and click **Next**.
 - Name the rule and click **Finish**.
-

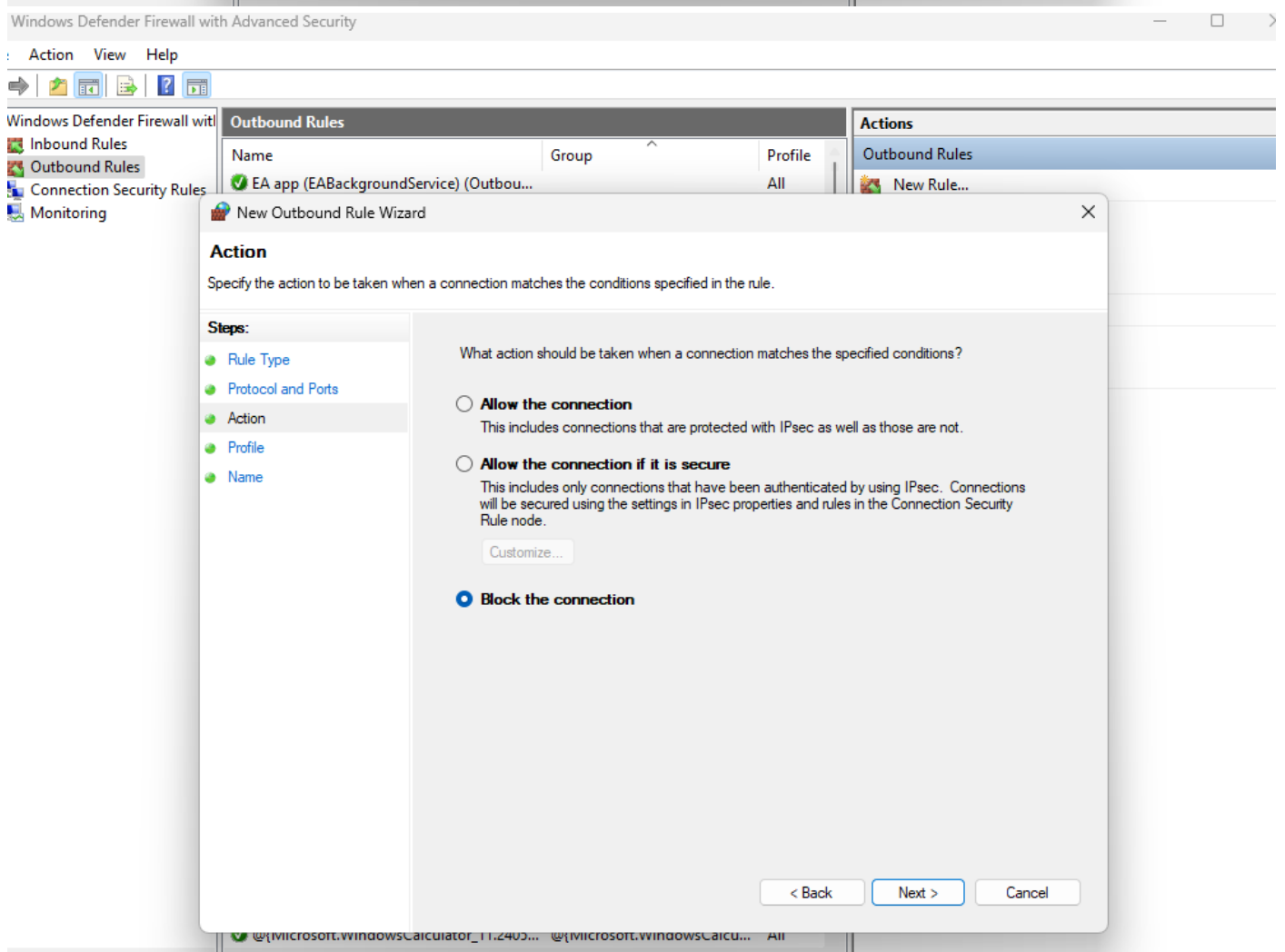
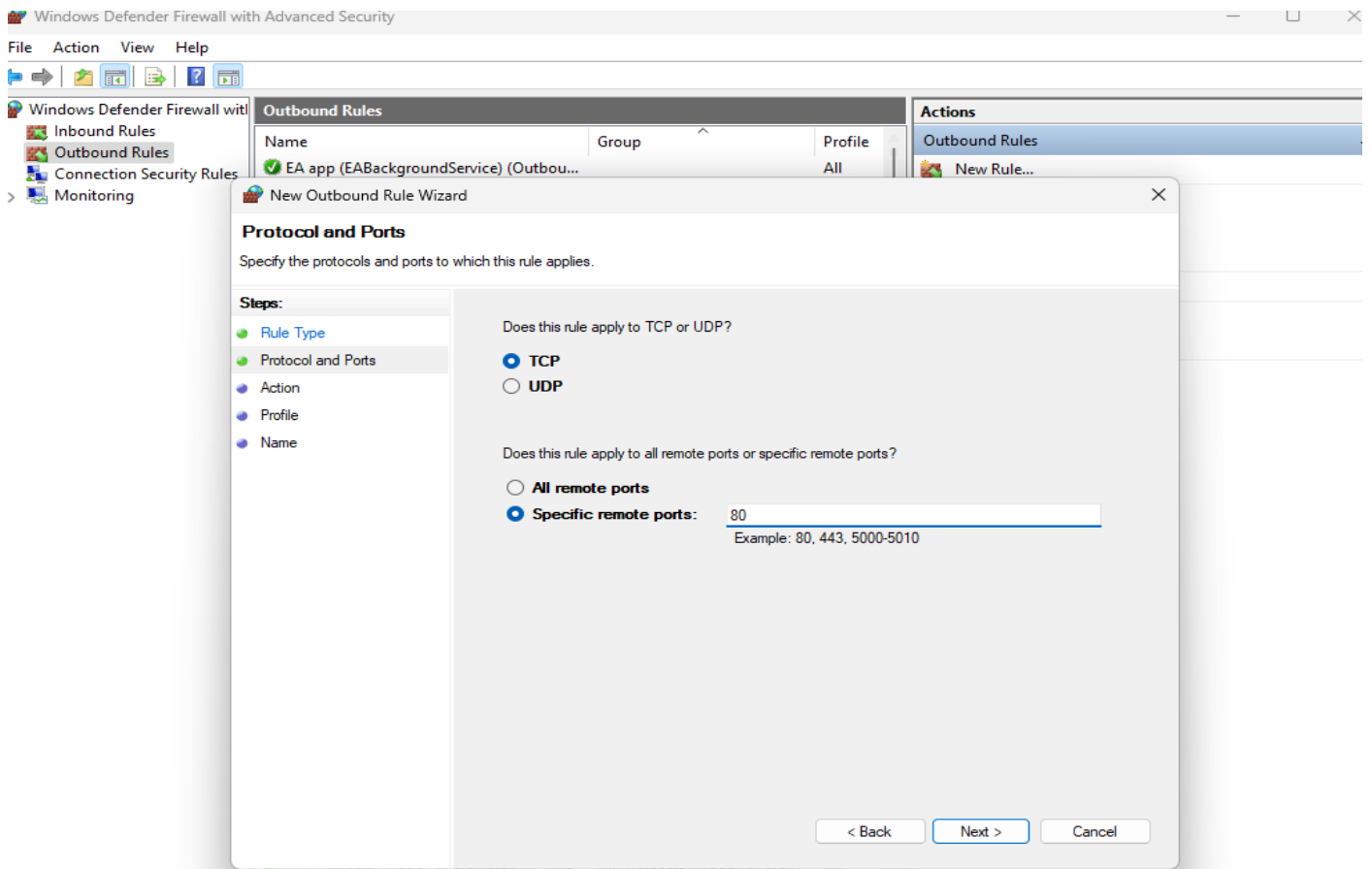
Use IP Blocking to Isolate Zombie Device:

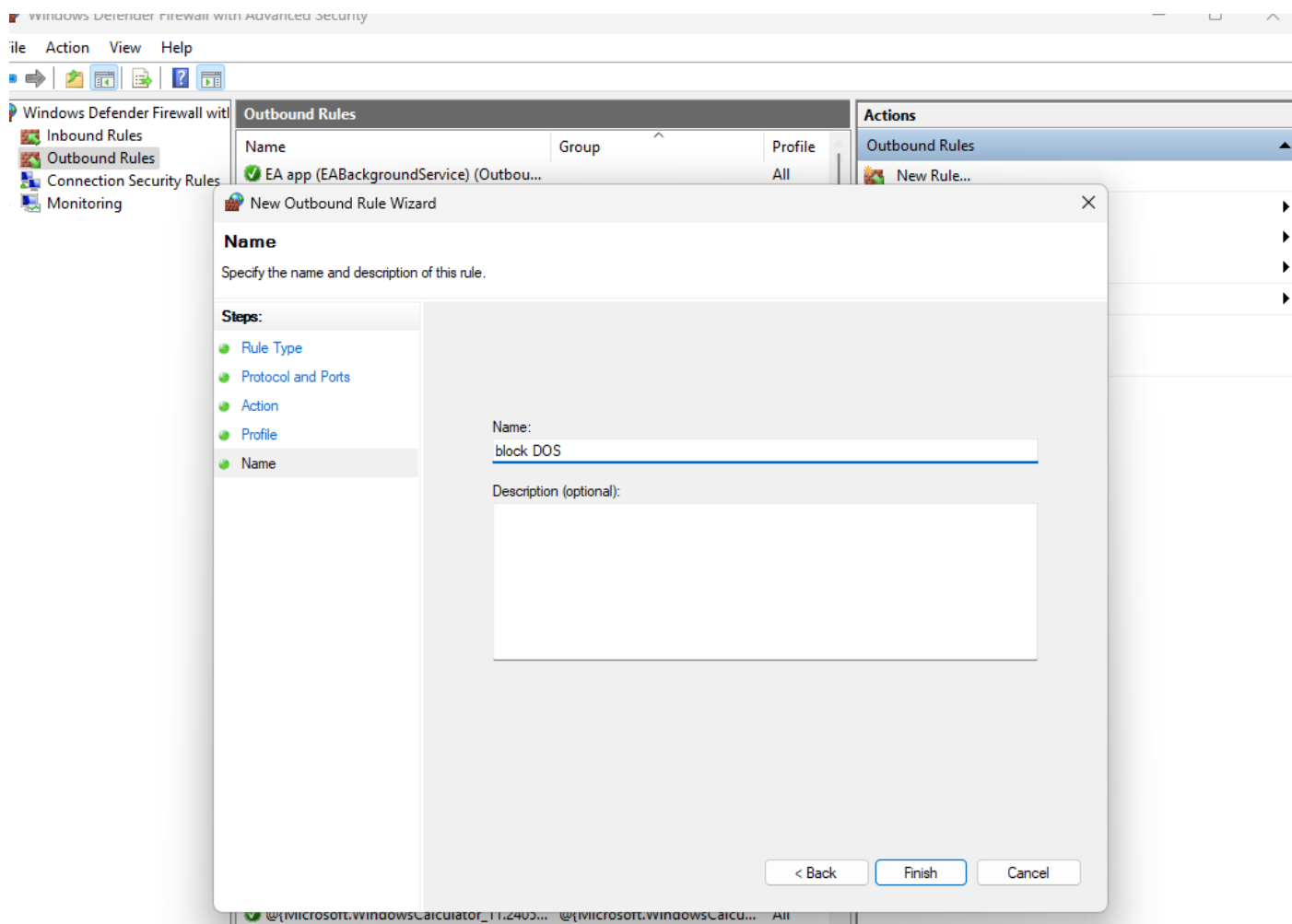
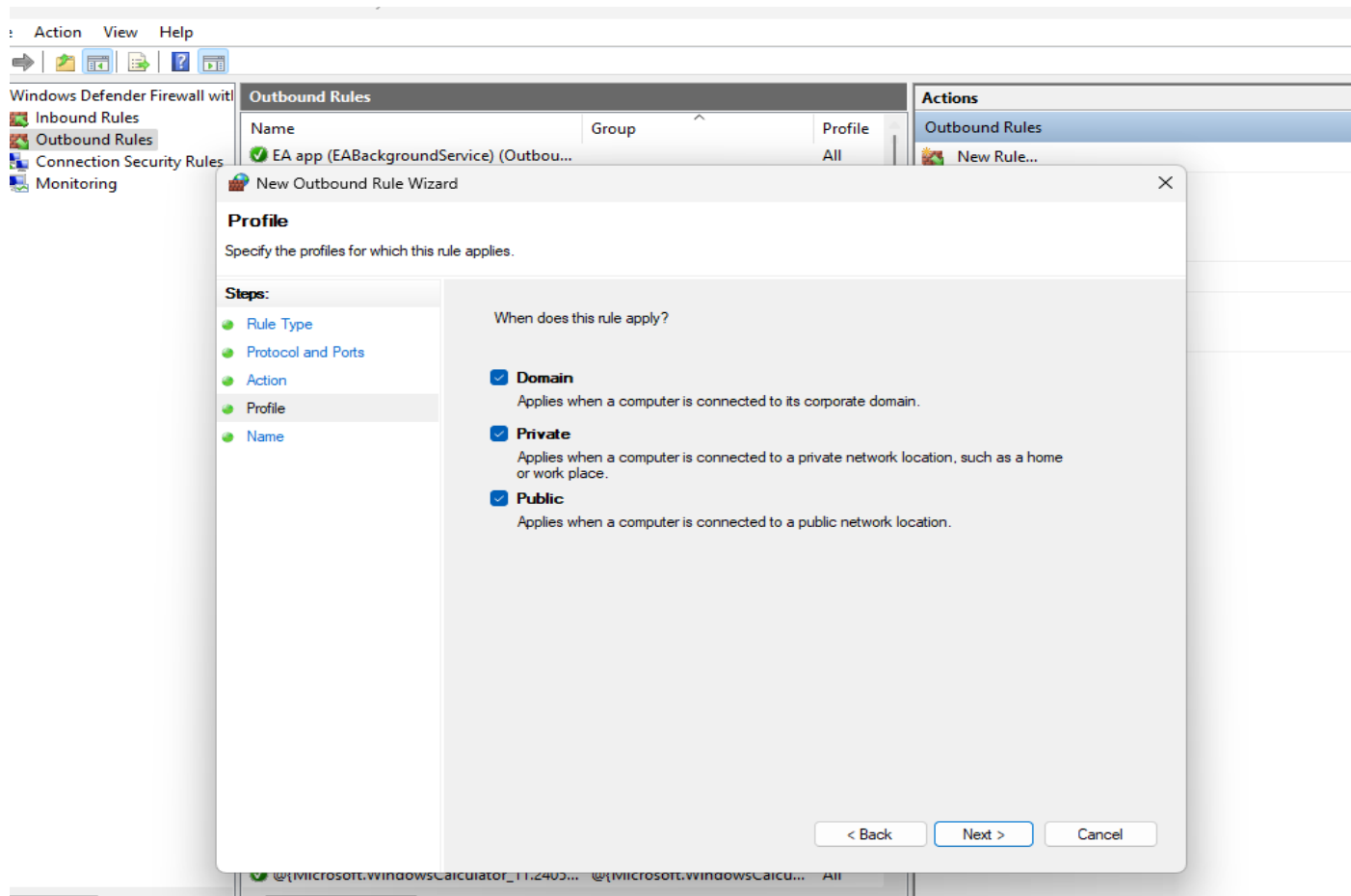
Identify the IP of the zombie device: open **CMD** and type **netstat -n**, Look for repeated suspicious connections from the same IP.

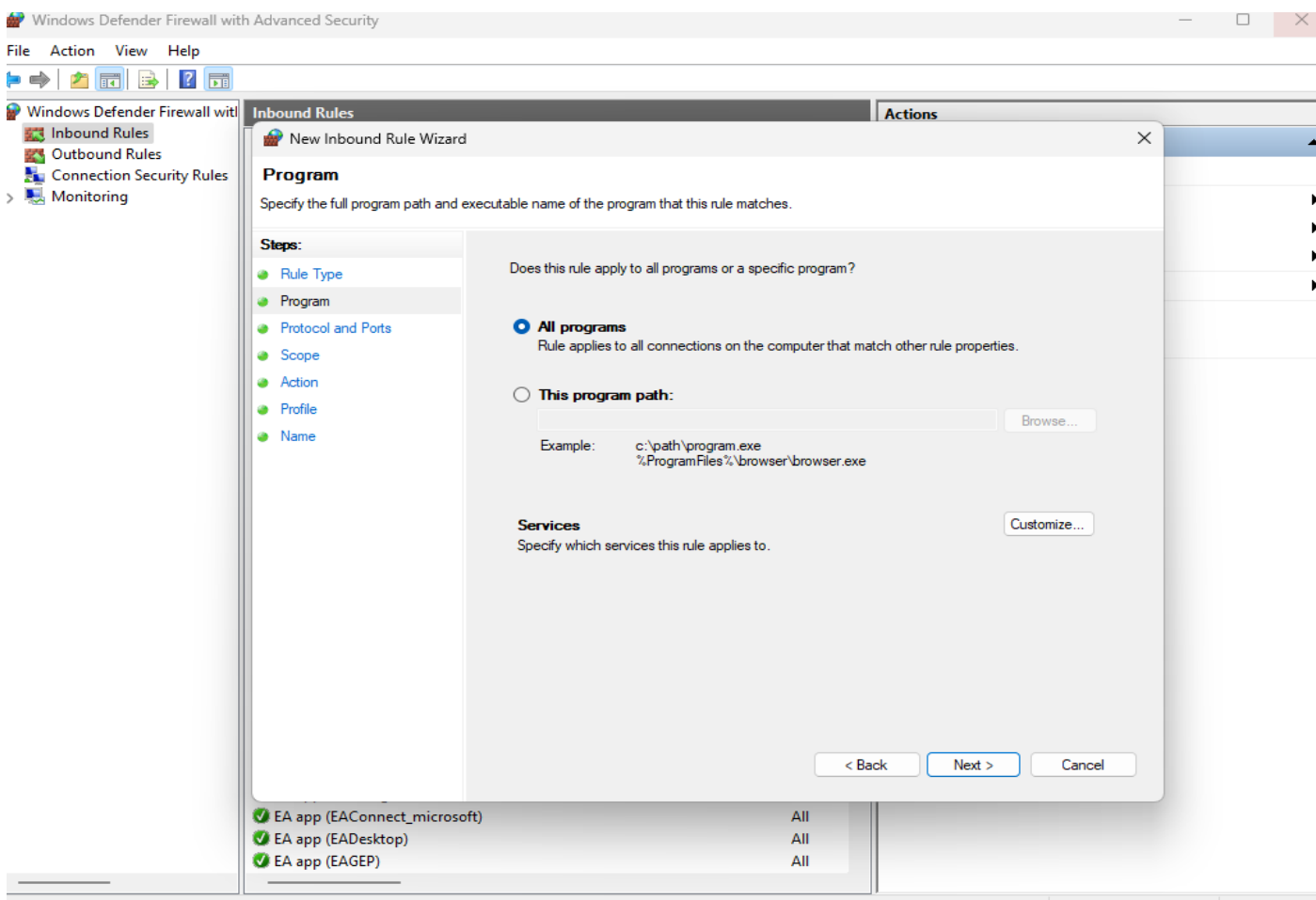
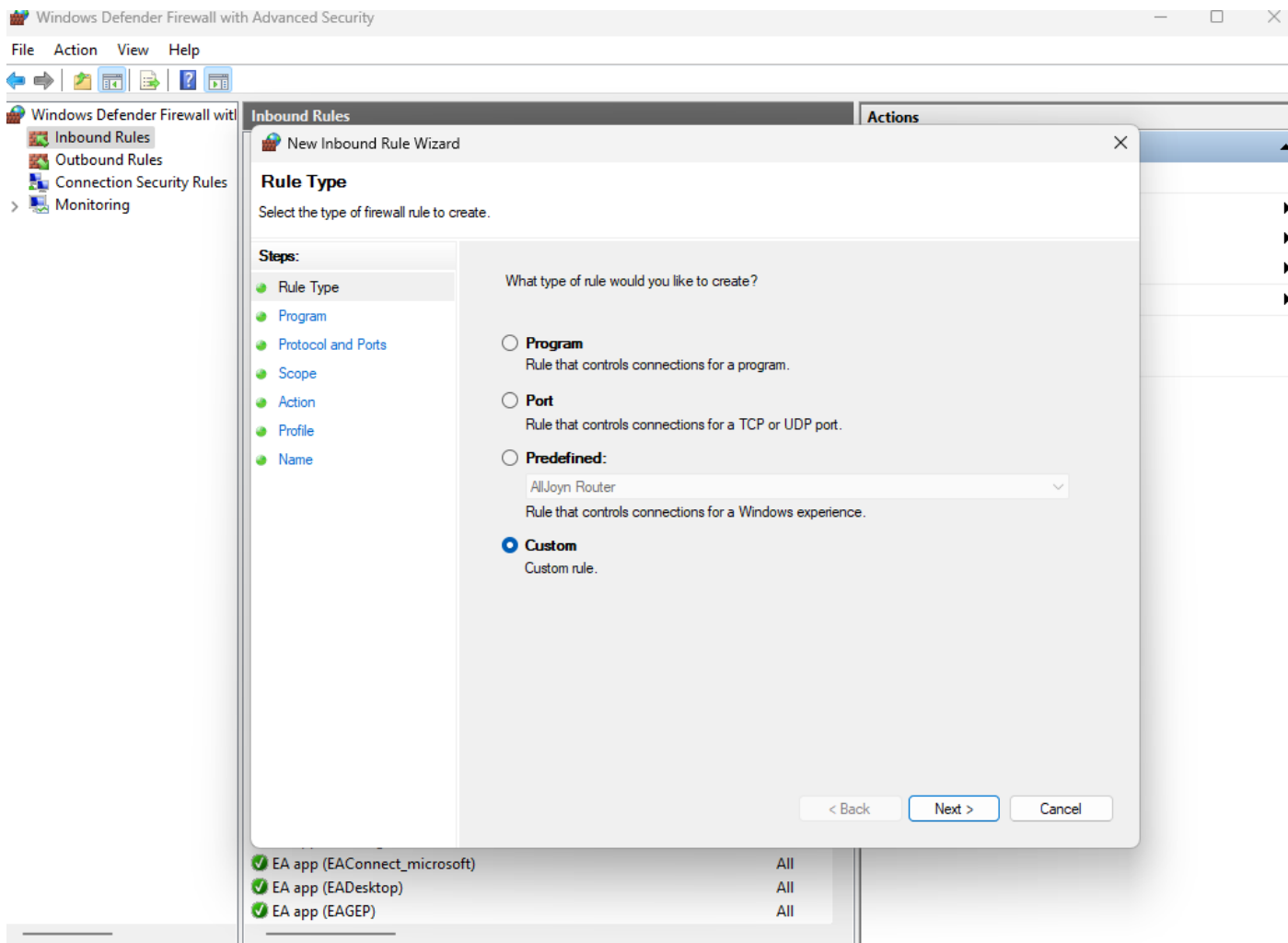
Block the IP Address:

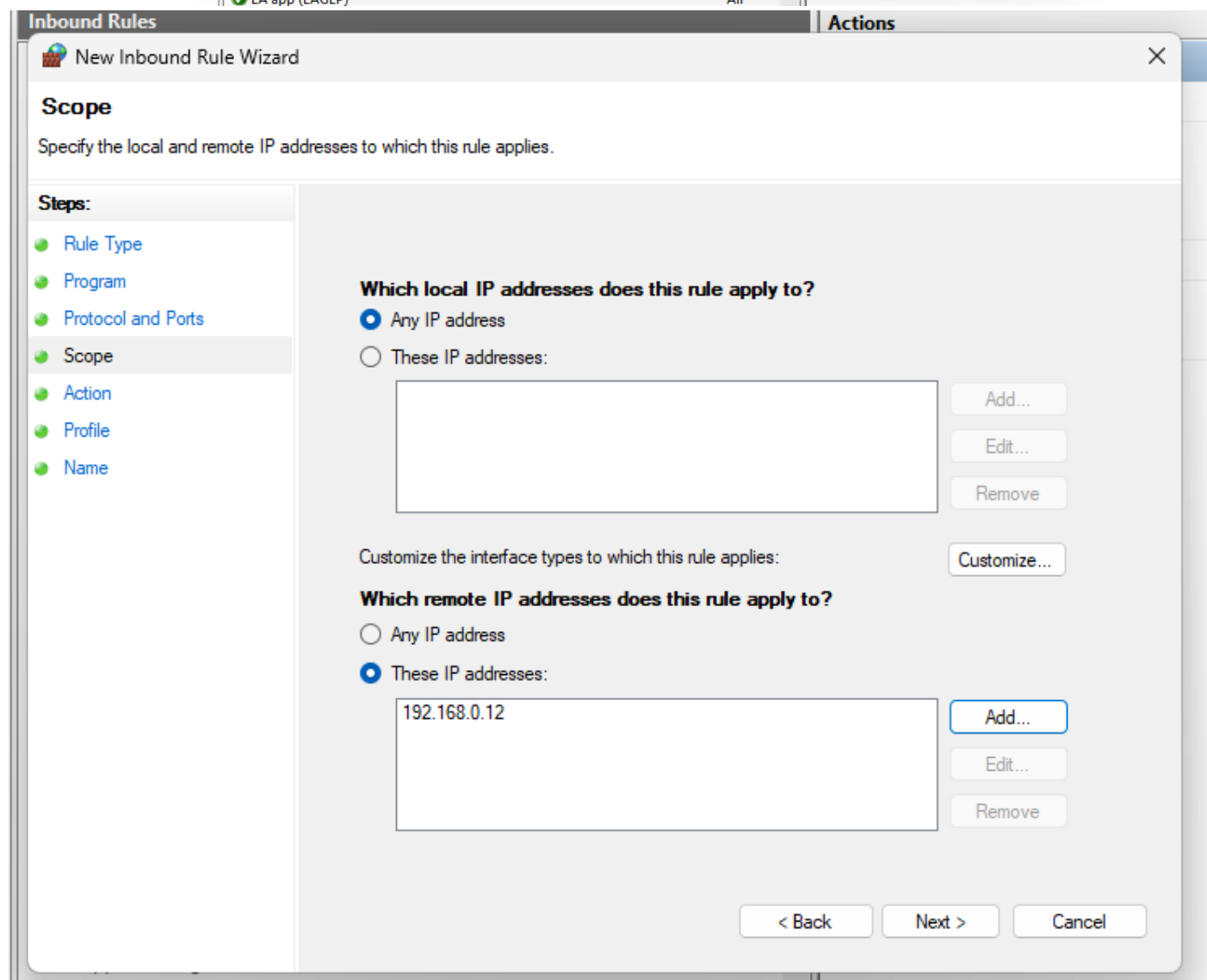
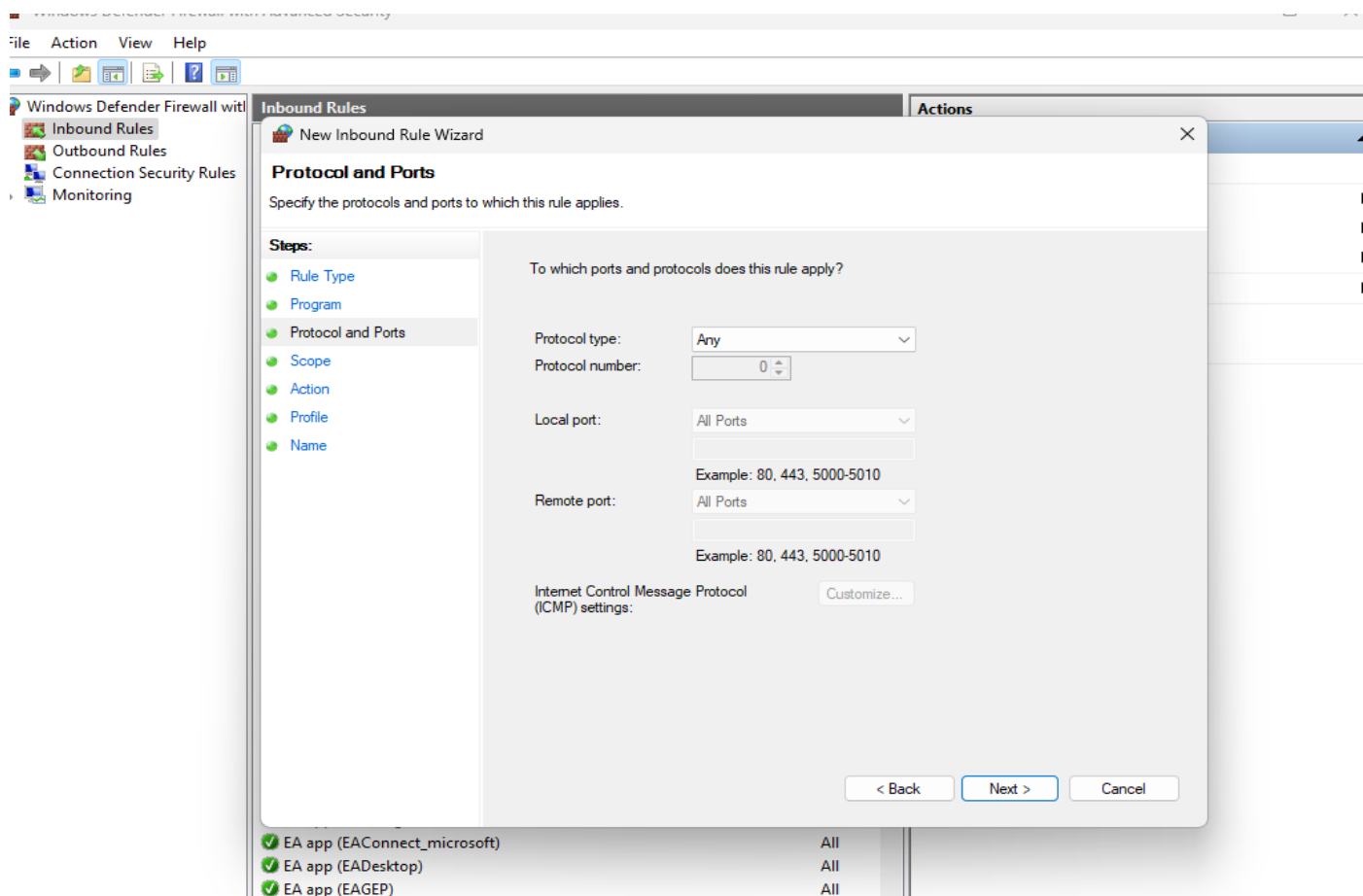
- In the **Windows Defender Firewall with Advanced Security**, create a **New Rule**.
- Select **Custom** and click **Next**.
- Select **All Programs** to apply to all programs.
- Under **Protocol and Ports**, leave it as-is and click **Next**.
- Under **Scope**, enter the zombie device's IP in the **Which remote IP addresses this applies to** section.
- Select **Block the connection** and click **Next**.
- Choose when the rule applies (Domain, Private, Public) and click **Next**.
- Name the rule and click **Finish**.

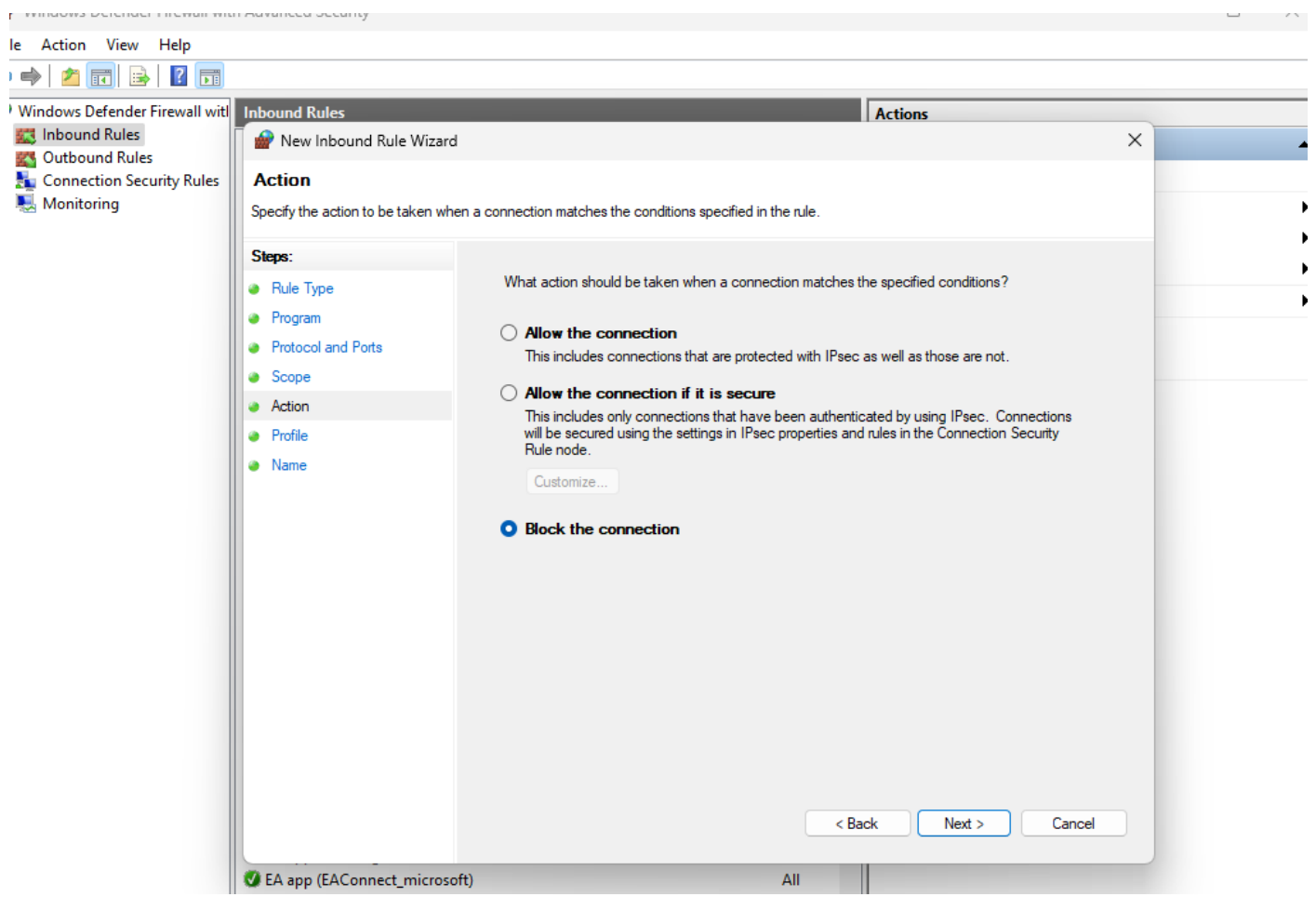












7: Use the VirtualBox tool to host the two different OS on your machine

1. **Open VirtualBox** and click New.
2. **Name Your VM**
3. **Select the ISO File**
4. **Allocate Resources and click finish**
5. **Start the VM**

