Task 4: Set Up and Use a Firewall on Windows/Linux

OBJECTIVE: Configure and test basic Firewall rules to allow or block traffic.

LEARN TO CONFIGURE AND MANAGE FIREWALL RULES TO CONTROL INBOUND/OUTBOUND TRAFFIC AND UNDERSTAND HOW FIREWALLS FILTER NETWORK TRAFFIC.

TOOLS USED:

- **FOR WINDOWS: WINDOWS DEFENDER FIREWALL (WITH ADVANCED SECURITY)**
- **FOR LINUX: UFW (UNCOMPLICATED FIREWALL)**

IN THIS TASK, WE WILL BLOCK THE TELNET PROTOCOL USING WINDOWS DEFENDER FIREWALL FOR WINDOWS & UFW FOR LINUX TO SET UP A FIREWALL.

Port 23 is used by the Telnet protocol, which enables remote connections to a computer. But here's the problem:

- Telnet is unencrypted → anything typed (username, password, commands) is sent in plain text over the network.
- Attackers can sniff this data using tools like Wireshark or tcpdump.
- Hackers target port 23 in port scans looking for open Telnet services, especially on older or misconfigured devices (routers, IoT devices, Linux servers).
- In modern security, Telnet is considered unsafe, and SSH (port 22) is used instead for remote access because it's encrypted.

What Happens After Blocking Inbound Port 23?

Once you apply this rule in Windows Firewall or UFW:

- Any external device trying to connect to your system over port 23 (e.g., using a Telnet client) will be denied.
- If a Telnet server is running on your system, nobody will be able to reach it from outside.
- This does not affect internal applications that don't use that port.
- If someone runs a port scan against your machine, port 23 will appear as closed or filtered, making it invisible or unreachable.

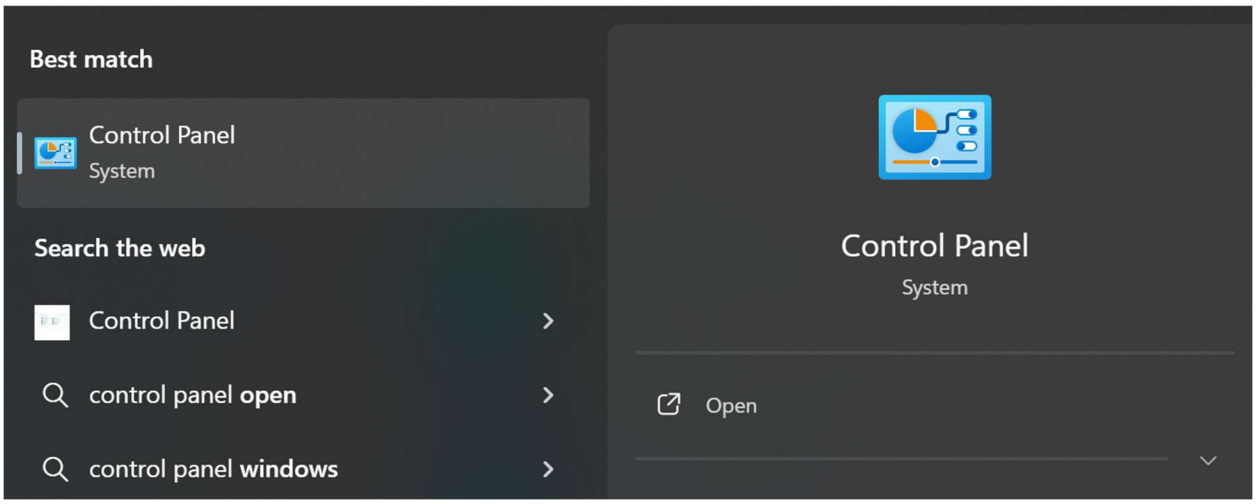
Why It Matters for Cybersecurity:

- Blocking unused and risky ports like 23 (Telnet) reduces your attack surface.
- It's part of a "default-deny" security model, where you only open what is needed.
- Even if Telnet is not running, blocking the port prevents future vulnerabilities if someone accidentally enables it.

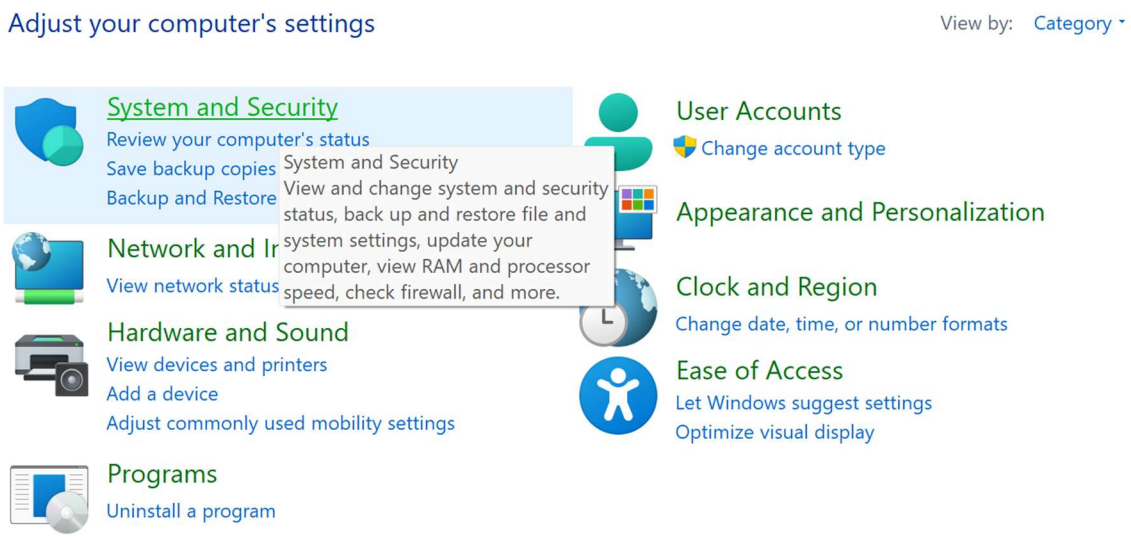
After blocking port 23, you stop any remote Telnet attempts to your machine, securing it from a legacy and insecure protocol. This is a proactive firewall rule used in real-world system hardening.

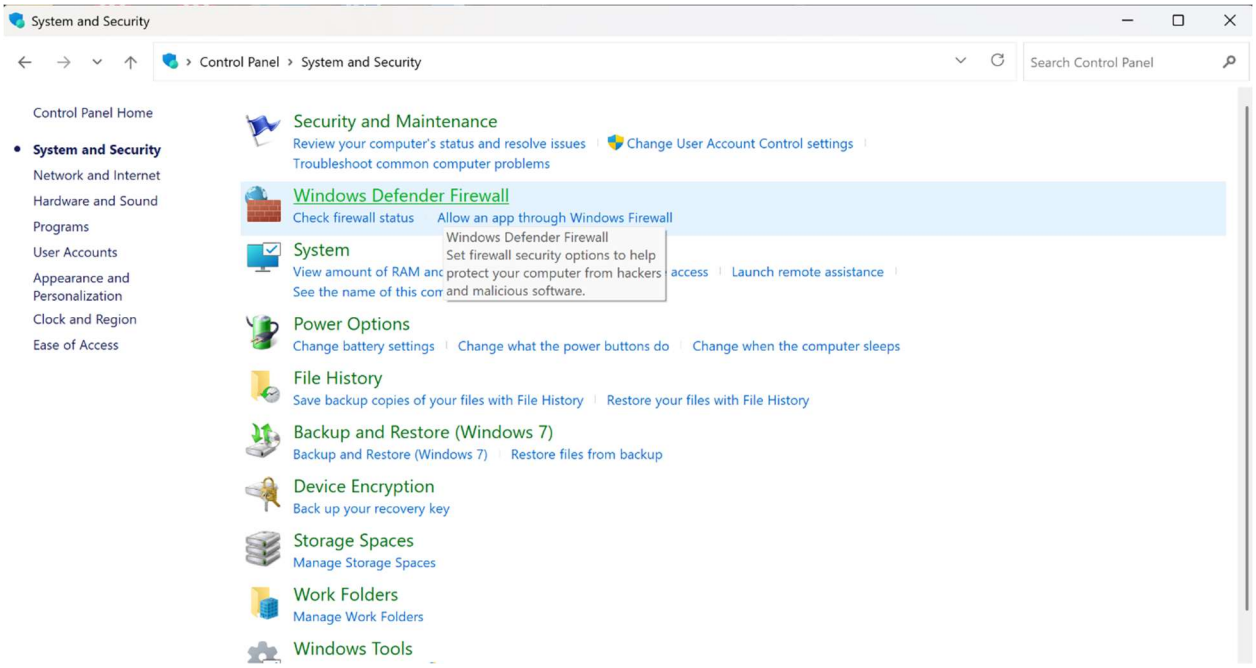
WINDOWS FIREWALL (GUI-BASED)

Go to Control Panel

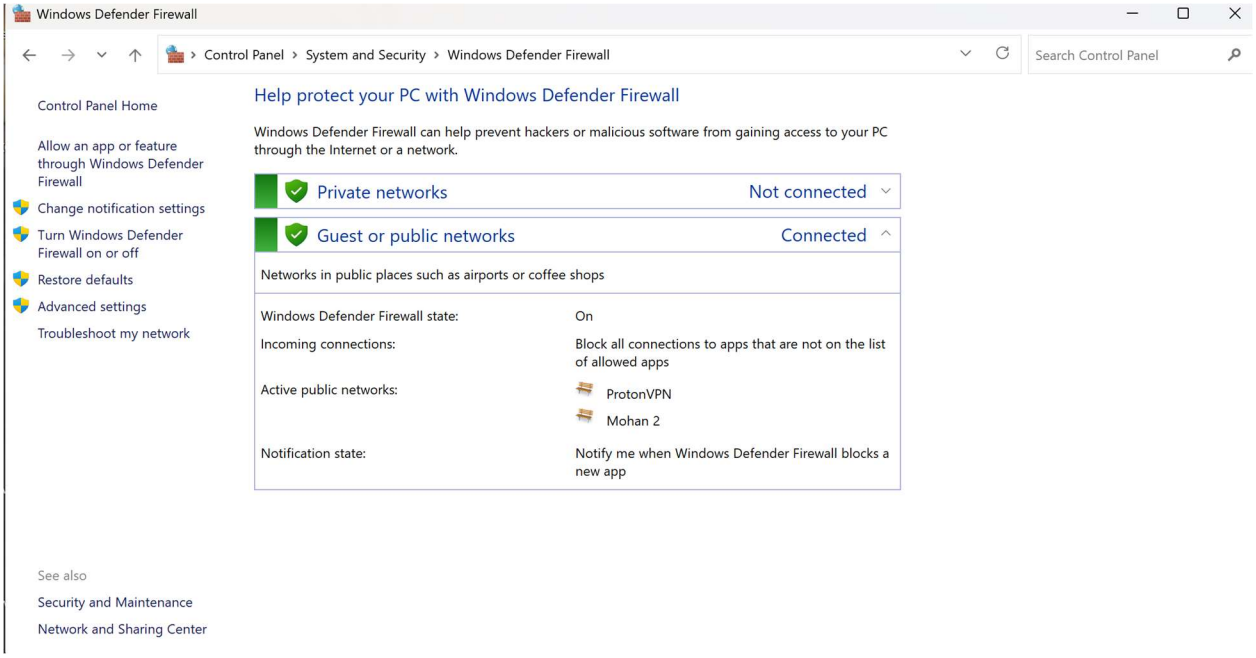


Go to System and Security

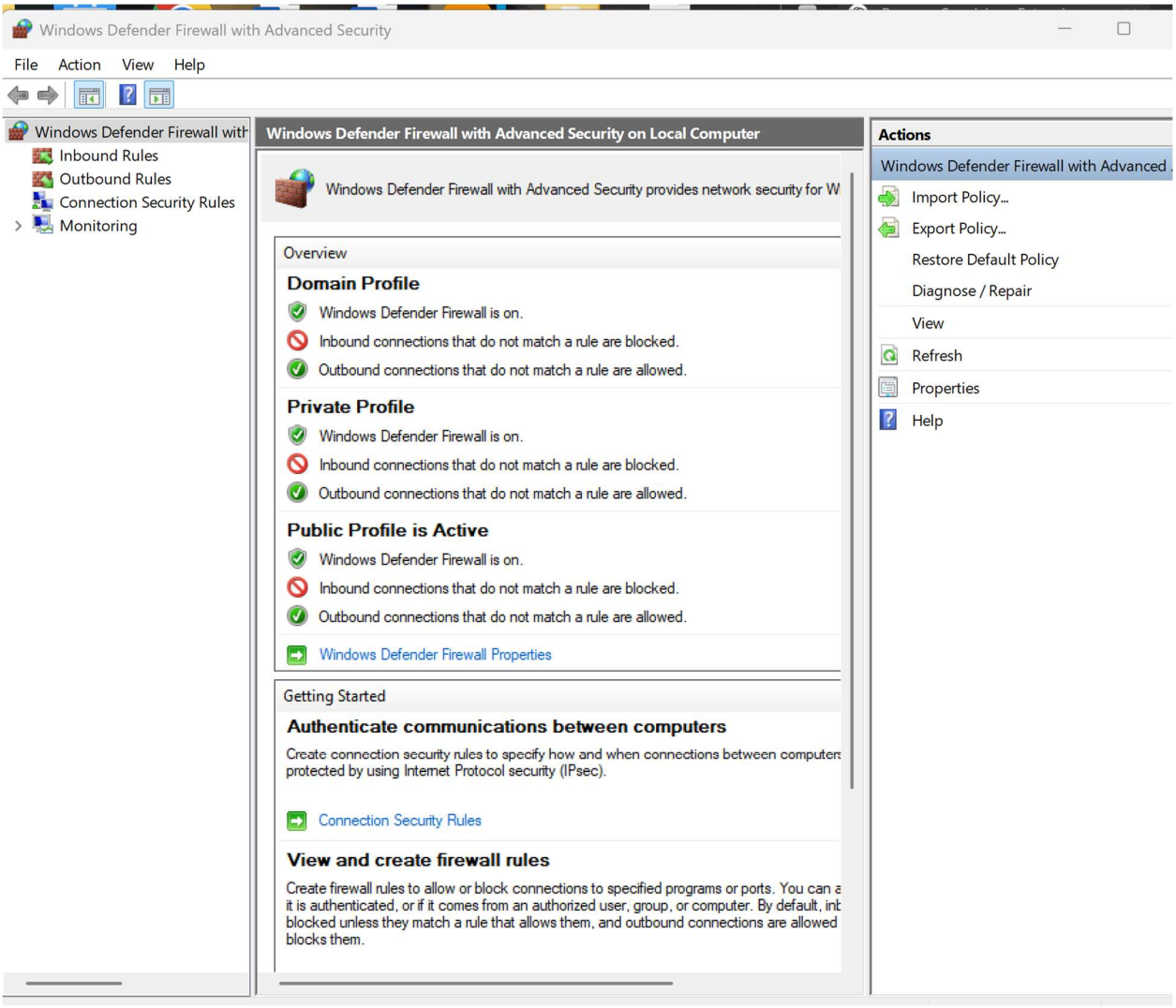




Select Windows Defender Firewall



Click on "Advanced Settings" (left pane) to open Windows Firewall with Advanced Security.

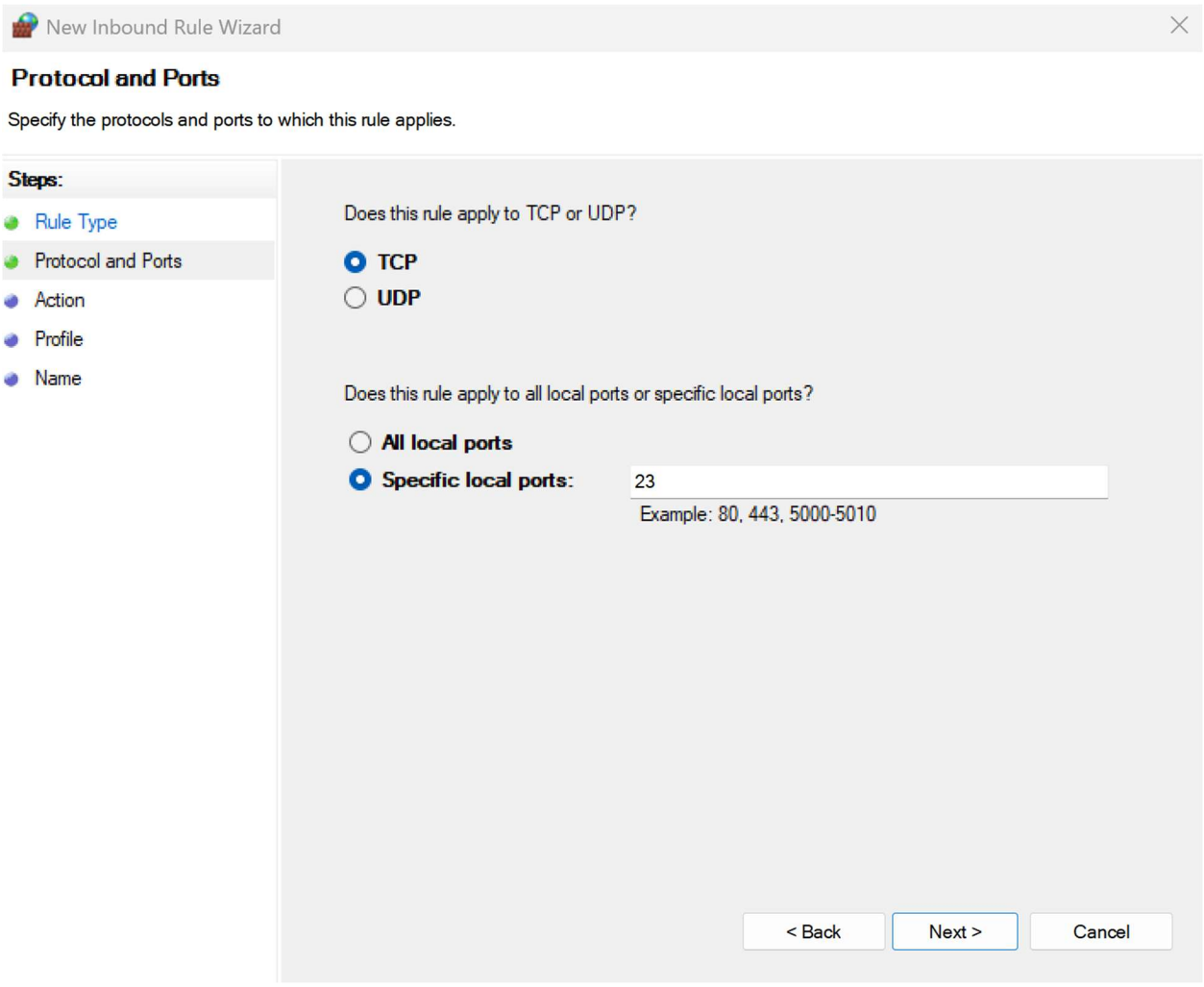


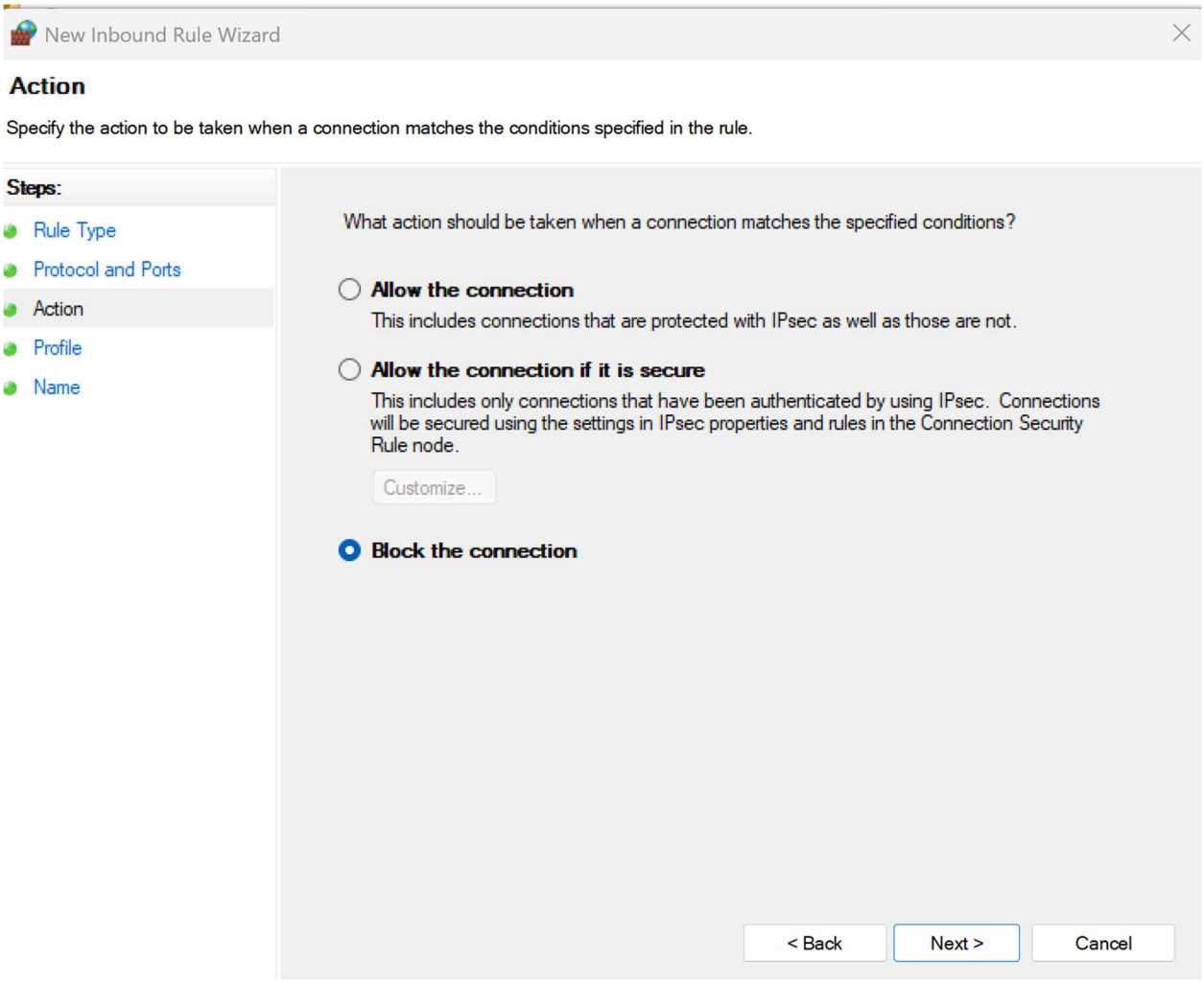
In the left pane, click on Inbound Rules or Outbound Rules

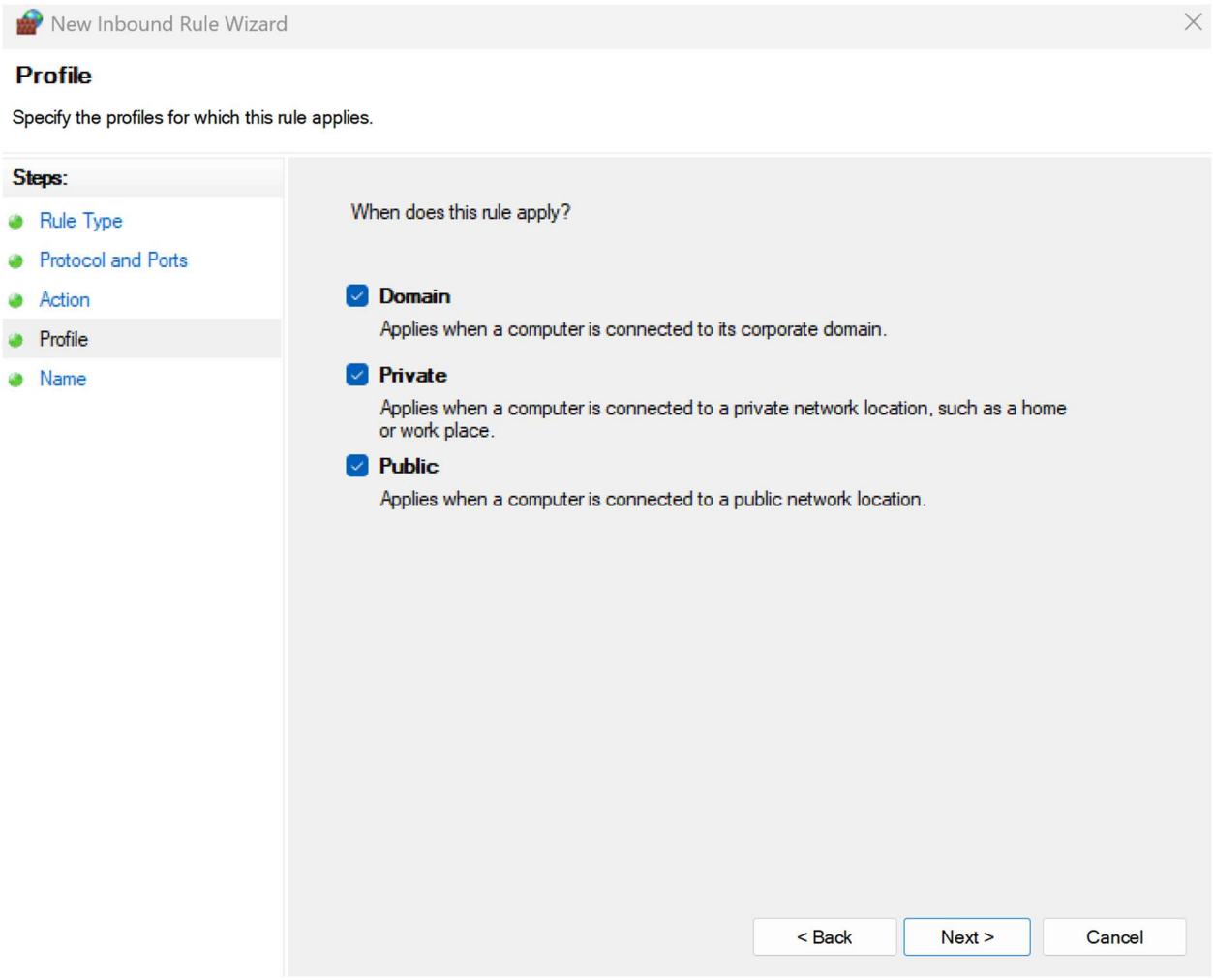
You'll see a list of existing rules

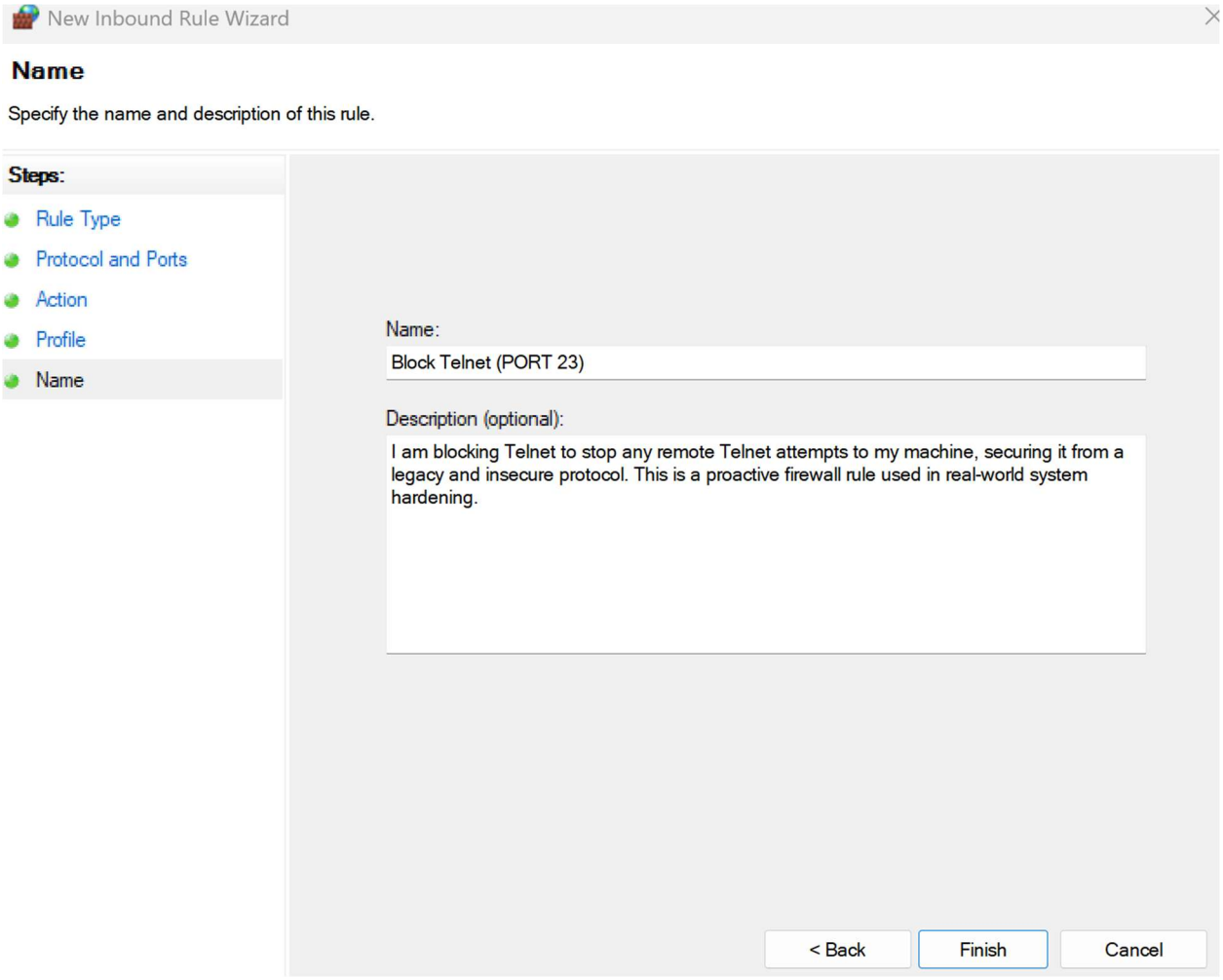
Block Inbound Traffic on Port 23 (Telnet)

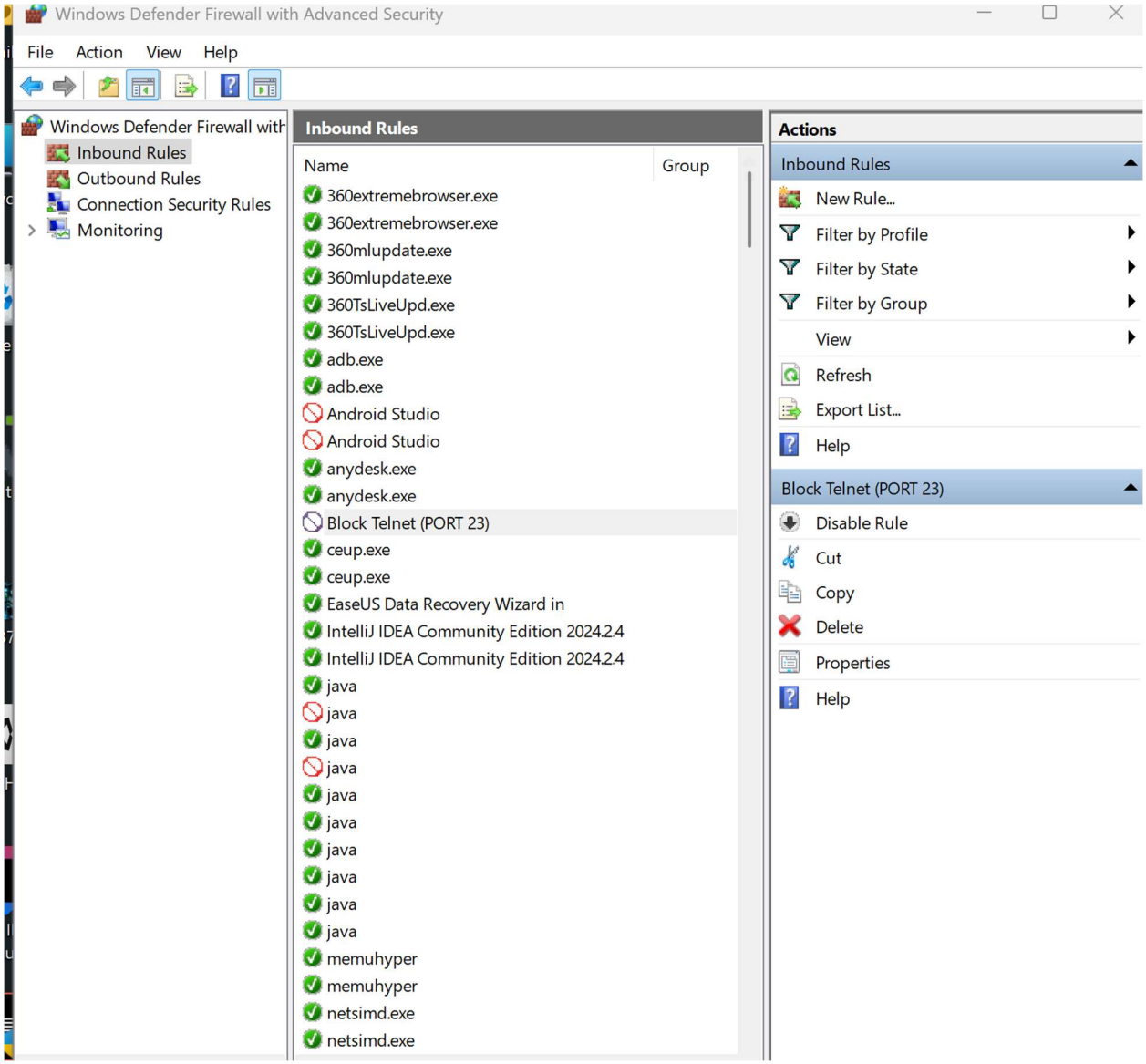
- In the right pane, click New Rule...
- Select Port, click Next
- Choose TCP, enter 23 in the Specific local ports field → Next
- Choose Block the connection → Next
- Apply to Domain, Private, and Public → Next
- Name it something like "Block Telnet (Port 23)", click Finish

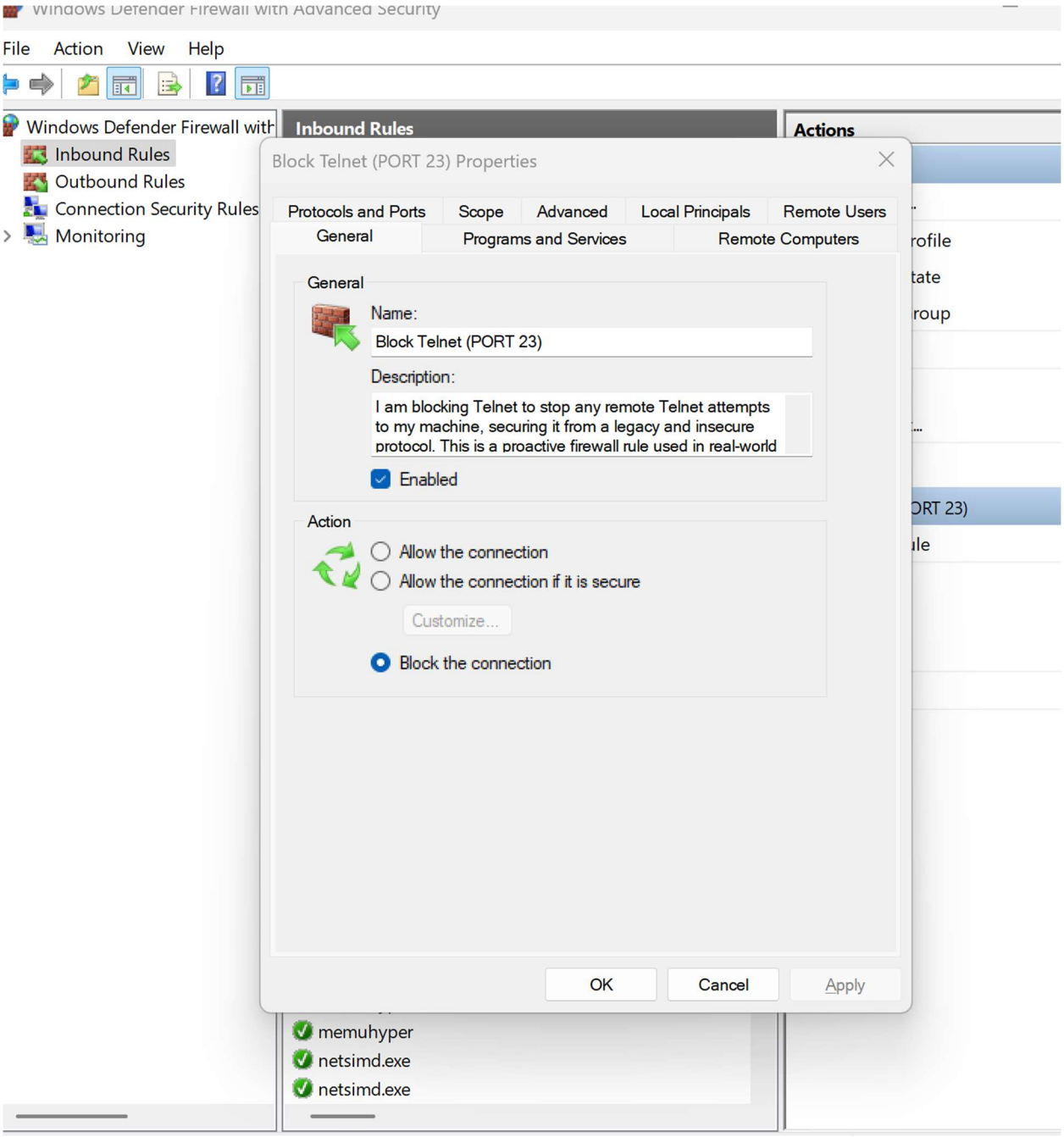

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
23
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


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.
Customize...
Block the connection
< Back
Next >
Cancel


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


New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Block Telnet (PORT 23)
Description (optional):
I am blocking Telnet to stop any remote Telnet attempts to my machine, securing it from a legacy and insecure protocol. This is a proactive firewall rule used in real-world system hardening.
< Back
Finish
Cancel


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
360extremebrowser.exe
360extremebrowser.exe
360mlupdate.exe
360mlupdate.exe
360TsLiveUpd.exe
360TsLiveUpd.exe
adb.exe
adb.exe
Android Studio
Android Studio
anydesk.exe
anydesk.exe
Block Telnet (PORT 23)
ceup.exe
ceup.exe
EaseUS Data Recovery Wizard in
IntelliJ IDEA Community Edition 2024.2.4
IntelliJ IDEA Community Edition 2024.2.4
java
java
java
java
java
java
java
java
java
memuhyper
memuhyper
netsimd.exe
netsimd.exe
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Block Telnet (PORT 23)
Disable Rule
Cut
Copy
Delete
Properties
Help



LINUX FIREWALL USING UFW (COMMAND-LINE)

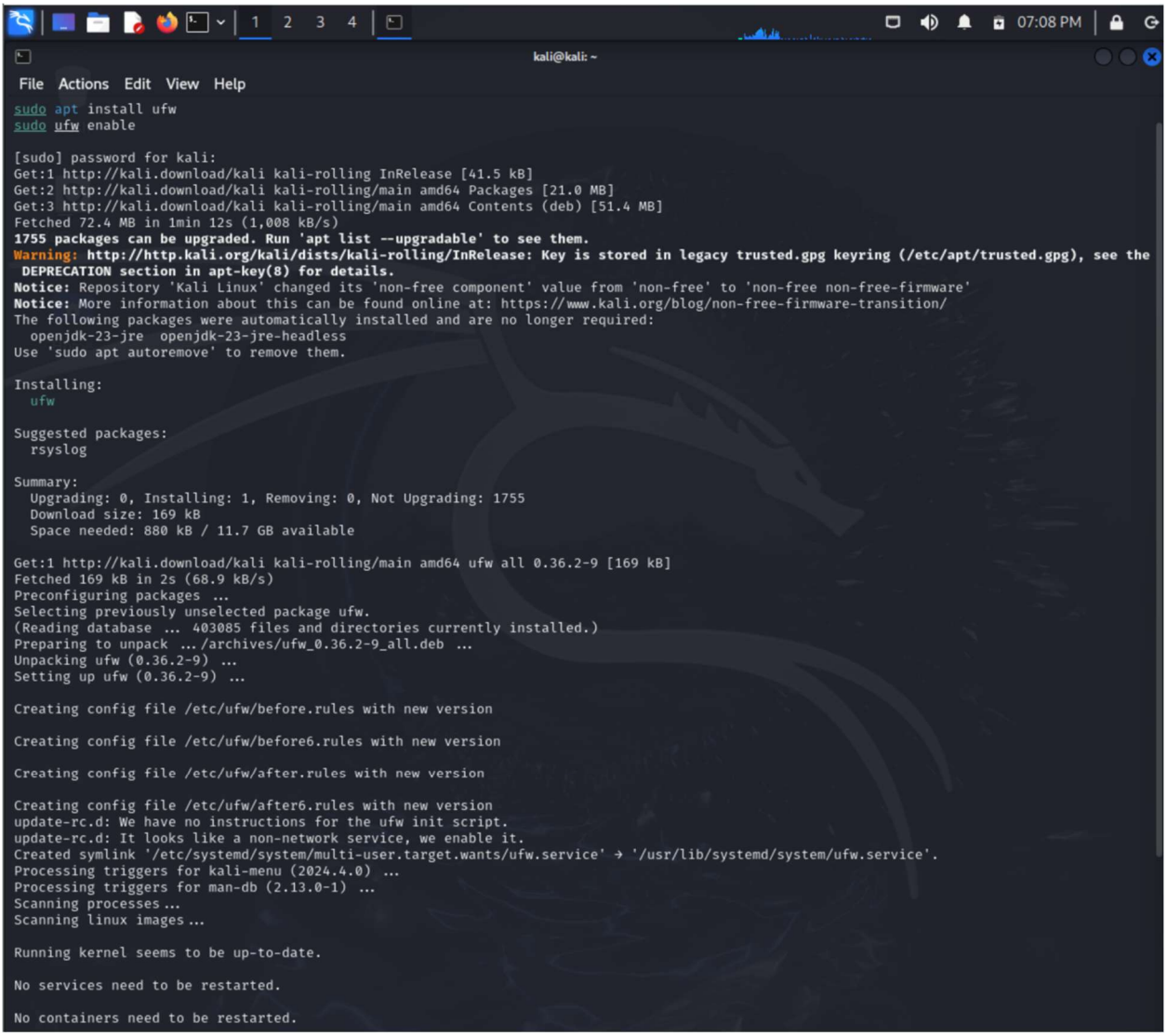
Install and enable UFW (if not already installed)

In the Terminal, write

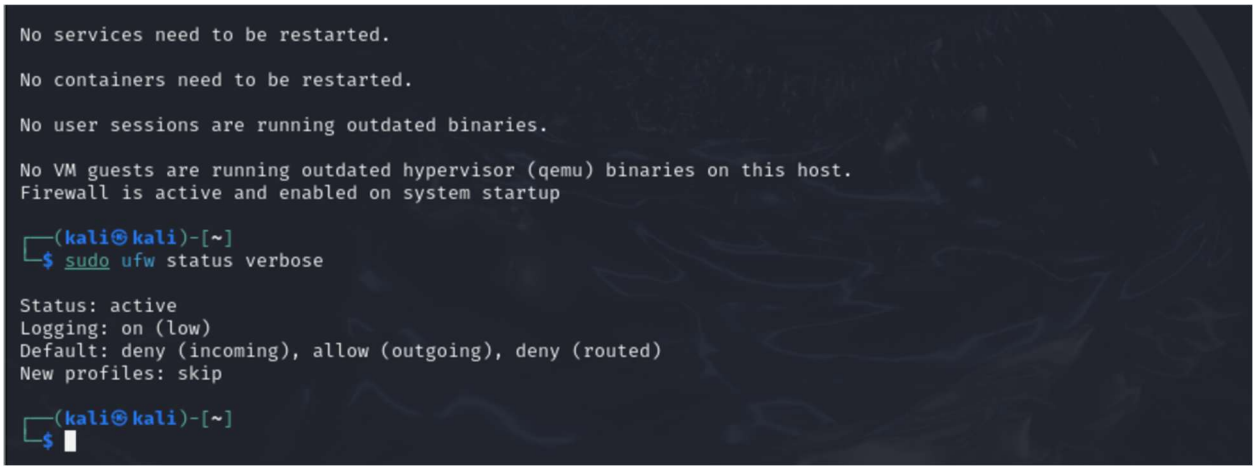
```
sudo apt update
```

sudo apt install ufw

sudo ufw enable



Check Current Firewall Status – sudo ufw status verbose



Block Inbound Traffic on Port 23 (Telnet) and Test

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose

Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ telnet localhost 23

Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22/tcp

Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$
```

Check firewall status - sudo ufw status numbered.

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     DENY IN     Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 23/tcp (v6)                DENY IN     Anywhere (v6)
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)


┌──(kali㉿kali)-[~]
└─$
```