TASK 4: SETUP AND USE A FIREWALL ON WINDOWS/LINUX

Objective:

To configure and manage a firewall on both Windows and Linux systems in order to control network traffic, enhance system security, and prevent unauthorized access by creating and testing specific inbound and outbound traffic rules.

Tools Used:

- OS: Windows and Linux.

Procedure:

Windows Firewall Configuration:

Step 1: Open Firewall Configuration Tool

- Press Win + R, type control firewall.cpl, and press Enter.
- Click **"Advanced Settings"** to access **Windows Defender Firewall with Advanced Security**.

Step 2: List Current Firewall Rules

- Click on **Inbound Rules** and **Outbound Rules** to view all active and inactive rules.

Step 3: Block Inbound Traffic on Port 23 (Telnet)

- Go to **Inbound Rules** → Click **New Rule**.
- Select **Port**, click **Next**.
- Choose **TCP** → Enter **23** as the port number → Click **Next**.
- Select **Block the connection** → Click **Next**.
- Apply rule to all profiles → Name the rule "Block Telnet" → Click **Finish**.

Step 4: Test the Rule

- Open Command Prompt and run:

```
telnet localhost 23
```

- The connection should fail, indicating the rule works.

Step 5: (SSH Step Not Required on Windows)

Step 6: Remove the Test Rule

- Go to **Inbound Rules** → Locate "Block Telnet" → Right-click → **Delete**.

Linux Firewall Configuration:

Step 1: Check if UFW is Installed

```
sudo ufw status
```

- If not installed, install it:

```
sudo apt update
sudo apt install ufw
```

Step 2: Enable UFW

```
sudo ufw enable
```

- This activates the firewall with default rules (deny all incoming, allow outgoing).

Step 3: Check Firewall Status

```
sudo ufw status numbered
```

- Displays current rules and their status.

Step 4: Allow Essential Services (e.g., SSH)

```
sudo ufw allow 22
```

- Allows SSH access (important for remote connections).

Step 5: Deny Specific Port (e.g., Telnet on Port 23)

```
sudo ufw deny 23
```

- Blocks any inbound traffic on Telnet port (common vulnerability).

Step 6: Test the Rule

```
telnet localhost 23
```

- Should return "connection refused" or "failed," confirming the block is working.

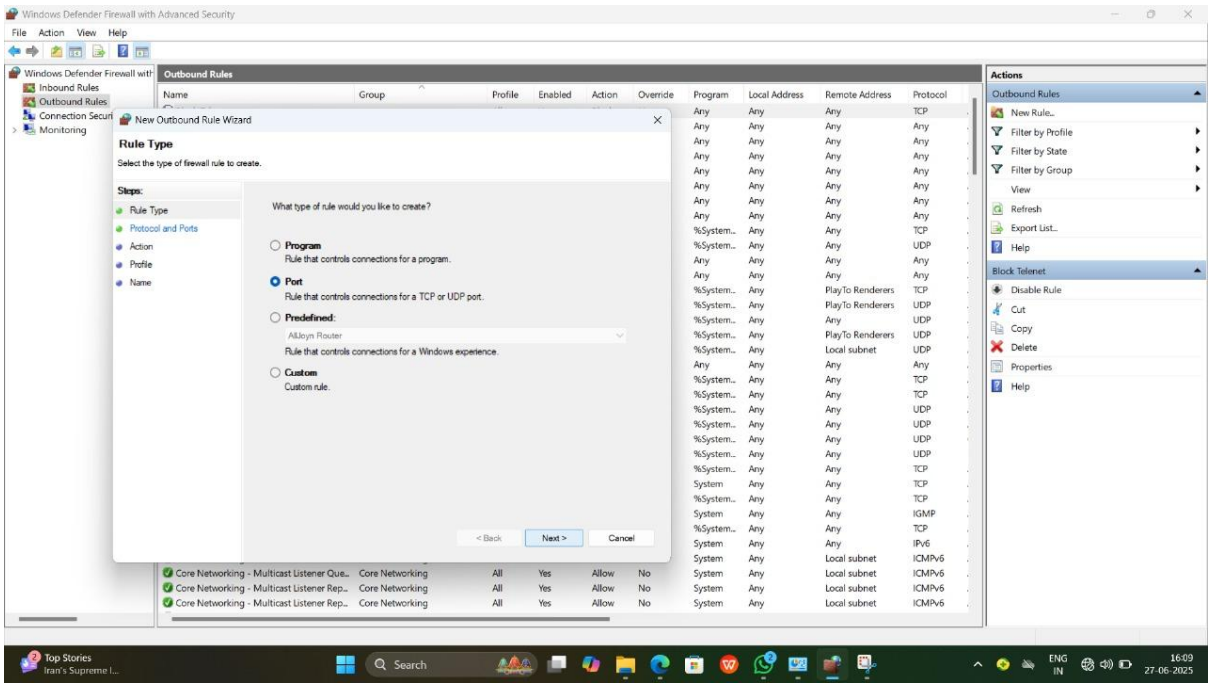
Step 7: Delete/Remove a Rule

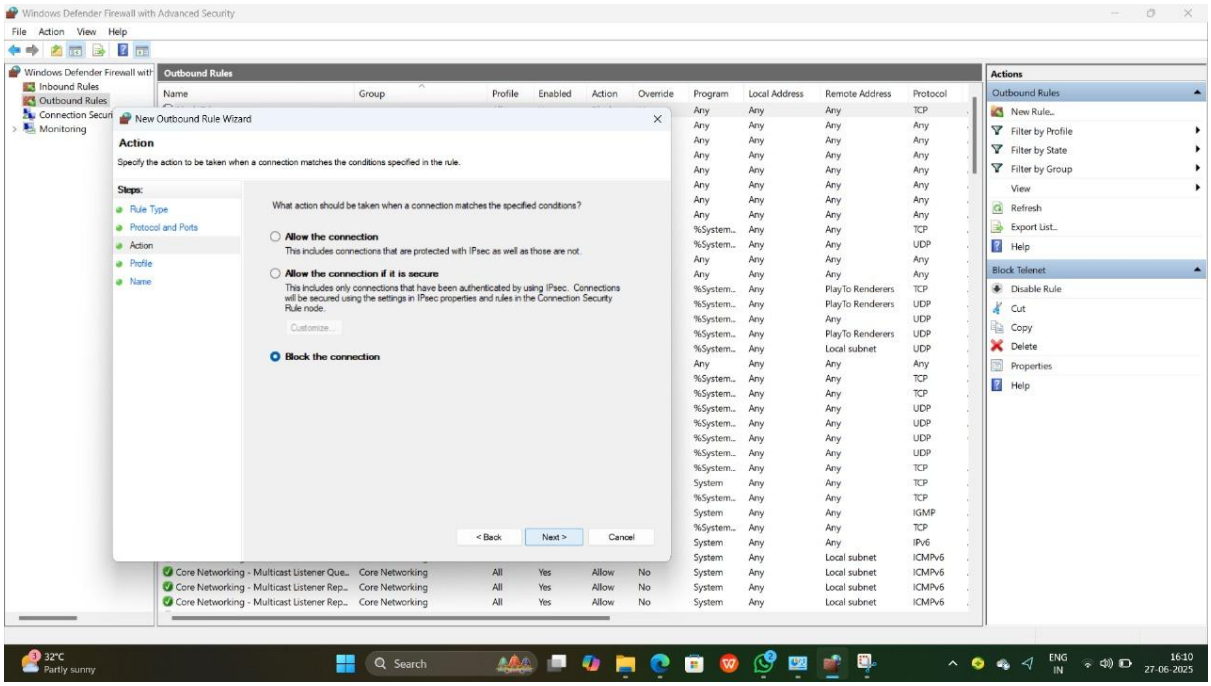
```
sudo ufw delete deny 23
```

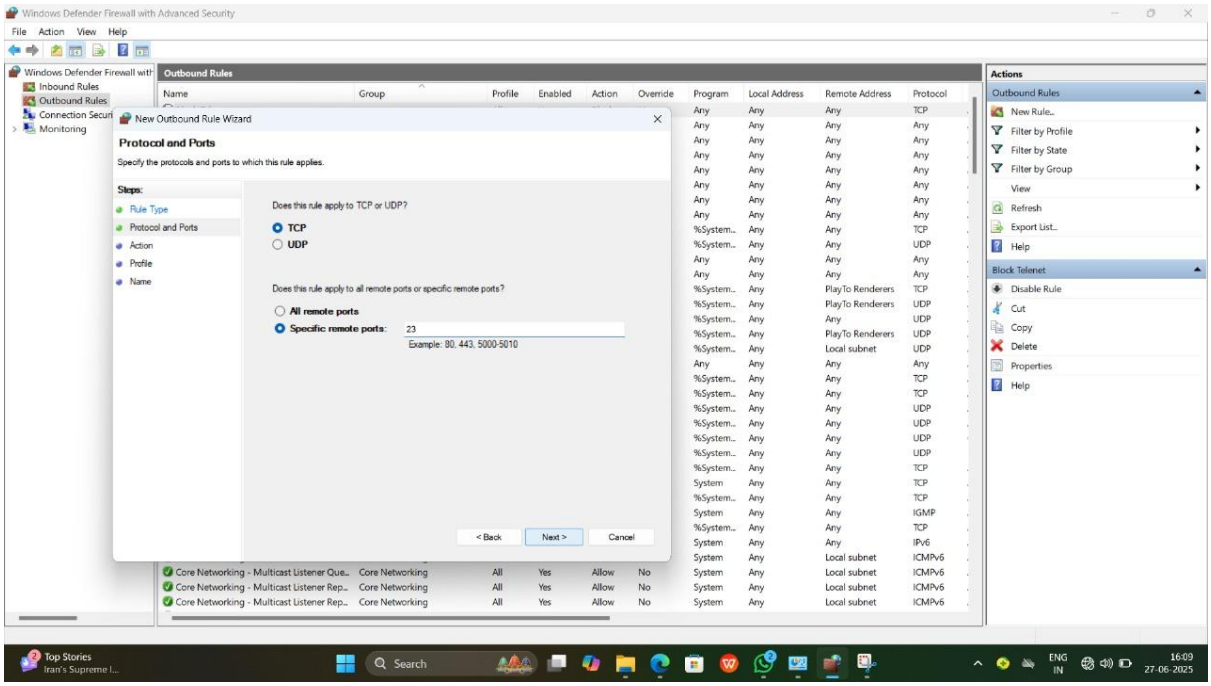
- Removes the block on port 23.

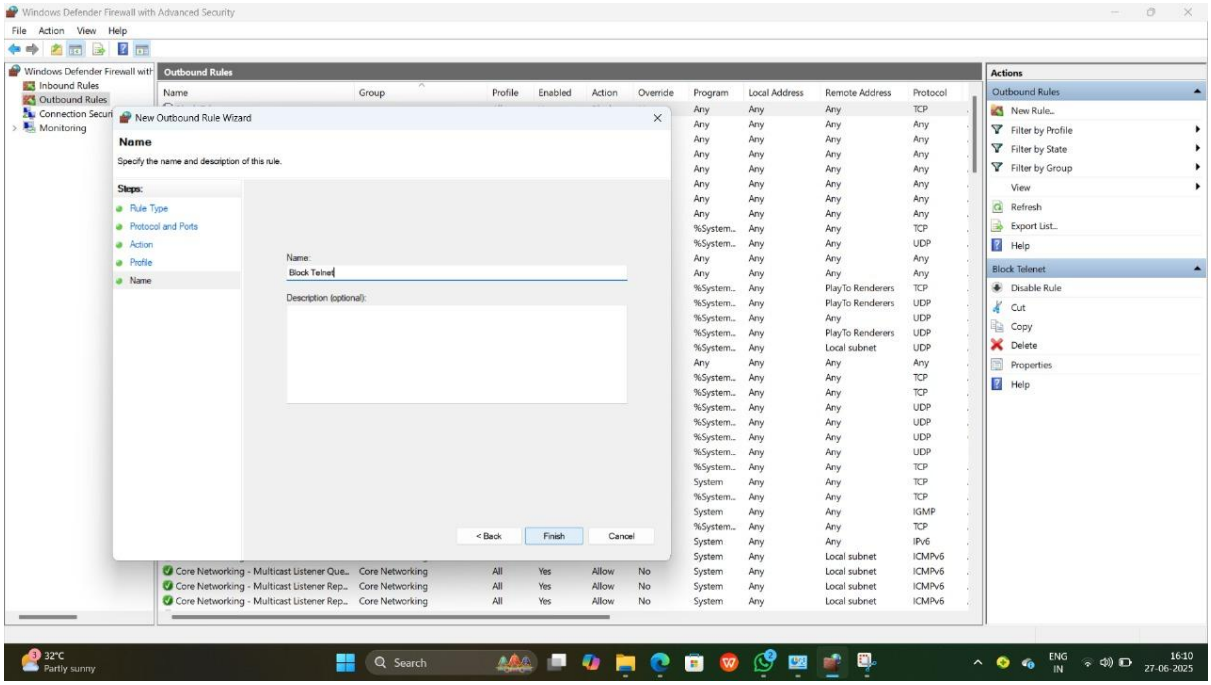
Screenshots:

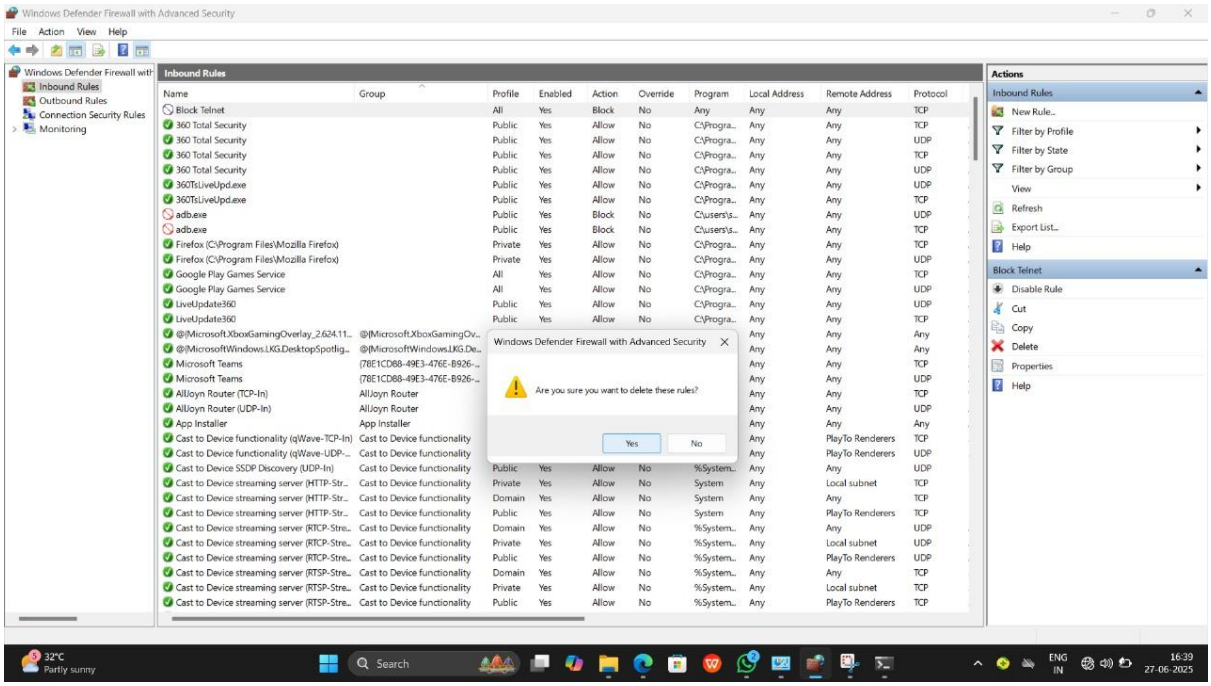
Windows:






Windows Defender Firewall with Advanced Security
File Action View Help
Outbound Rules
New Outbound 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 remote ports or specific remote ports?
All remote ports
Specific remote ports: 23
Example: 80, 443, 5000-5010
< Back
Next >
Cancel
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Block Telnet
Disable Rule
Cut
Copy
Delete
Properties
Help


Windows Defender Firewall with Advanced Security
File Action View Help
Outbound Rules
New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Block Telnet
Description (optional):
< Back
Finish
Cancel
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Block Telnet
Disable Rule
Cut
Copy
Delete
Properties
Help


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 Profile Enabled Action Override Program Local Address Remote Address Protocol
Block Telnet All Yes Block No Any Any Any TCP
360 Total Security Public Yes Allow No C:\Progra... Any Any TCP
360 Total Security Public Yes Allow No C:\Progra... Any Any UDP
360 Total Security Public Yes Allow No C:\Progra... Any Any TCP
360 Total Security Public Yes Allow No C:\Progra... Any Any UDP
360TsLiveUpd.exe Public Yes Allow No C:\Progra... Any Any UDP
360TsLiveUpd.exe Public Yes Allow No C:\Progra... Any Any TCP
adb.exe Public Yes Block No C:\users\s... Any Any UDP
adb.exe Public Yes Block No C:\users\s... Any Any TCP
Firefox (C:\Program Files\Mozilla Firefox) Private Yes Allow No C:\Progra... Any Any TCP
Firefox (C:\Program Files\Mozilla Firefox) Private Yes Allow No C:\Progra... Any Any UDP
Google Play Games Service All Yes Allow No C:\Progra... Any Any TCP
Google Play Games Service All Yes Allow No C:\Progra... Any Any UDP
LiveUpdate360 Public Yes Allow No C:\Progra... Any Any UDP
LiveUpdate360 Public Yes Allow No C:\Progra... Any Any TCP
Microsoft Teams {78E1CD88-49E3-476E-B926-... Any Any TCP
Microsoft Teams {78E1CD88-49E3-476E-B926-... Any Any UDP
AllJoyn Router (TCP-In) AllJoyn Router Any Any TCP
AllJoyn Router (UDP-In) AllJoyn Router Any Any UDP
App Installer App Installer Any Any Any
Cast to Device functionality (qWave-TCP-In) Cast to Device functionality Any PlayTo Renderers TCP
Cast to Device functionality (qWave-UDP-... Cast to Device functionality Any PlayTo Renderers UDP
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes Allow No %System... Any Any UDP
Cast to Device streaming server (HTTP-Str... Cast to Device functionality Private Yes Allow No System Any Local subnet TCP
Cast to Device streaming server (HTTP-Str... Cast to Device functionality Domain Yes Allow No System Any Any TCP
Cast to Device streaming server (HTTP-Str... Cast to Device functionality Public Yes Allow No System Any PlayTo Renderers TCP
Cast to Device streaming server (RTCP-Stre... Cast to Device functionality Domain Yes Allow No %System... Any Any UDP
Cast to Device streaming server (RTCP-Stre... Cast to Device functionality Private Yes Allow No %System... Any Local subnet UDP
Cast to Device streaming server (RTCP-Stre... Cast to Device functionality Public Yes Allow No %System... Any PlayTo Renderers UDP
Cast to Device streaming server (RTSP-Stre... Cast to Device functionality Domain Yes Allow No %System... Any Any TCP
Cast to Device streaming server (RTSP-Stre... Cast to Device functionality Private Yes Allow No %System... Any Local subnet TCP
Cast to Device streaming server (RTSP-Stre... Cast to Device functionality Public Yes Allow No %System... Any PlayTo Renderers TCP
Windows Defender Firewall with Advanced Security
Are you sure you want to delete these rules?
Yes
No
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Block Telnet
Disable Rule
Cut
Copy
Delete
Properties
Help
32°C
Partly sunny
Search
ENG
IN
16:39
27-06-2025

Linux:


kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ sudo apt install telnet
Upgrading:
inetutils-telnet
Installing:
telnet
Summary:
Upgrading: 1, Installing: 1, Removing: 0, Not Upgrading: 2196
Download size: 173 kB
Space needed: 73.7 kB / 64.6 GB available
Continue? [Y/n] y
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.6-1
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.6-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.6-1
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.6-1
Get:1 http://kali.download/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.6-1 [130 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.6-1 [43.2 kB]
Fetched 173 kB in 1min 26s (2,009 B/s)
(Reading database ... 391224 files and directories currently installed.)
Preparing to unpack .../inetutils-telnet_2%3a2.6-1_amd64.deb ...
Unpacking inetutils-telnet (2:2.6-1) over (2:2.5-4) ...
Selecting previously unselected package telnet.
Preparing to unpack .../telnet_0.17+2.6-1_all.deb ...
Unpacking telnet (0.17+2.6-1) ...
Setting up inetutils-telnet (2:2.6-1) ...
Setting up telnet (0.17+2.6-1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...
(kali㉿kali)-[~/Desktop]
$ 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)-[~/Desktop]
$ sudo ufw allow 22
Rule added
Rule added (v6)
(kali㉿kali)-[~/Desktop]
$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)
(kali㉿kali)-[~/Desktop]

Conclusion:

In this task, we learned how to set up and use a firewall on both Windows and Linux. We added rules to block unwanted traffic (like Telnet on port 23) and allowed important connections (like SSH on port 22). This helped us understand how firewalls protect our system by controlling which network traffic is allowed or blocked. Firewalls are important for keeping our computers safe from unauthorized access.