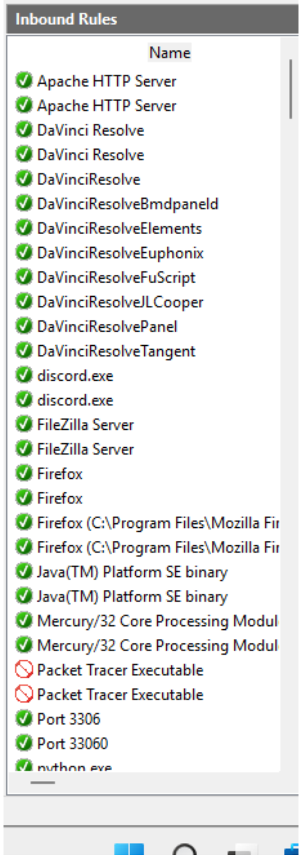
Objective:
To configure Windows Firewall to block inbound traffic on Port 23 (Telnet) and allow inbound traffic on Port 22 (SSH), and verify the configuration through testing.

---

1. Initial Firewall Status

- Opened *Windows Defender Firewall with Advanced Security* to review existing inbound and outbound rules.



Inbound Rules

Name

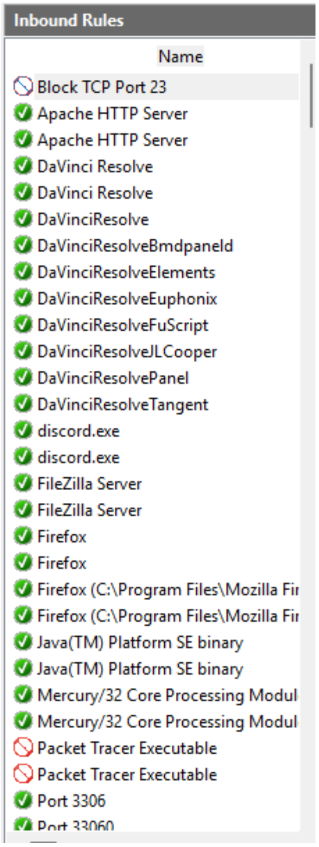
✓ Apache HTTP Server
✓ Apache HTTP Server
✓ DaVinci Resolve
✓ DaVinci Resolve
✓ DaVinciResolve
✓ DaVinciResolveBmdpaneld
✓ DaVinciResolveElements
✓ DaVinciResolveEuphonix
✓ DaVinciResolveFuScript
✓ DaVinciResolveJLCooper
✓ DaVinciResolvePanel
✓ DaVinciResolveTangent
✓ discord.exe
✓ discord.exe
✓ FileZilla Server
✓ FileZilla Server
✓ Firefox
✓ Firefox
✓ Firefox (C:\Program Files\Mozilla Fir
✓ Firefox (C:\Program Files\Mozilla Fir
✓ Java(TM) Platform SE binary
✓ Java(TM) Platform SE binary
✓ Mercury/32 Core Processing Modul
✓ Mercury/32 Core Processing Modul
🚫 Packet Tracer Executable
🚫 Packet Tracer Executable
✓ Port 3306
✓ Port 33060
✓ python.exe

:

---

2. Block Inbound Traffic on Port 23 (Telnet)

Steps performed:

1. Opened *Windows Defender Firewall with Advanced Security*.
2. Selected **Inbound Rules** → **New Rule**.
3. Chose **Port** → **TCP** → **Specific Local Port: 23**.
4. Selected **Block the connection**.
5. Applied to all profiles (Domain, Private, Public).
6. Named the rule `Block TCP Port 23`.
7. 

Inbound Rules

Name

⊘ Block TCP Port 23
✓ Apache HTTP Server
✓ Apache HTTP Server
✓ DaVinci Resolve
✓ DaVinci Resolve
✓ DaVinciResolve
✓ DaVinciResolveBmdpaneld
✓ DaVinciResolveElements
✓ DaVinciResolveEuphonix
✓ DaVinciResolveFuScript
✓ DaVinciResolveJLCooper
✓ DaVinciResolvePanel
✓ DaVinciResolveTangent
✓ discord.exe
✓ discord.exe
✓ FileZilla Server
✓ FileZilla Server
✓ Firefox
✓ Firefox
✓ Firefox (C:\Program Files\Mozilla Fir
✓ Firefox (C:\Program Files\Mozilla Fir
✓ Java(TM) Platform SE binary
✓ Java(TM) Platform SE binary
✓ Mercury/32 Core Processing Modul
✓ Mercury/32 Core Processing Modul
⊘ Packet Tracer Executable
⊘ Packet Tracer Executable
✓ Port 3306
✓ Port 33060

---

3. Test – Verify Port 23 Block

- Method: Ran Nmap and/or Telnet test to check Port 23.

Command used (PowerShell or CMD):

Copy code

```
Test-NetConnection -ComputerName 127.0.0.1 -Port 23
```

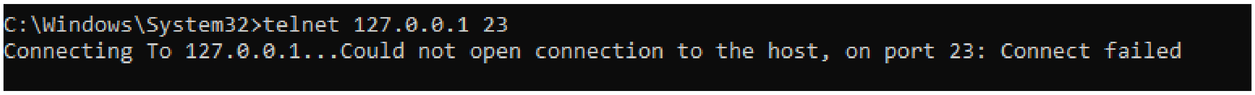
or

nginx

Copy code

```
nmap -p 23 127.0.0.1
```

-
- **Expected result:** Port 23 connection fails / state is “filtered”.



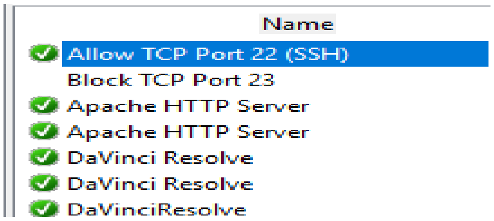
```
C:\Windows\System32>telnet 127.0.0.1 23
Connecting To 127.0.0.1...Could not open connection to the host, on port 23: Connect failed
```

---

4. Allow Inbound Traffic on Port 22 (SSH)

Steps performed:

1. Opened *Windows Defender Firewall with Advanced Security*.
2. Selected **Inbound Rules** → **New Rule**.
3. Chose **Port** → **TCP** → **Specific Local Port: 22**.
4. Selected **Allow the connection**.
5. Applied to all profiles.
6. Named the rule `Allow TCP Port 22 (SSH)`.



Name
✓ Allow TCP Port 22 (SSH)
Block TCP Port 23
✓ Apache HTTP Server
✓ Apache HTTP Server
✓ DaVinci Resolve
✓ DaVinci Resolve
✓ DaVinciResolve

5. Test – Verify Port 22 Allow Rule

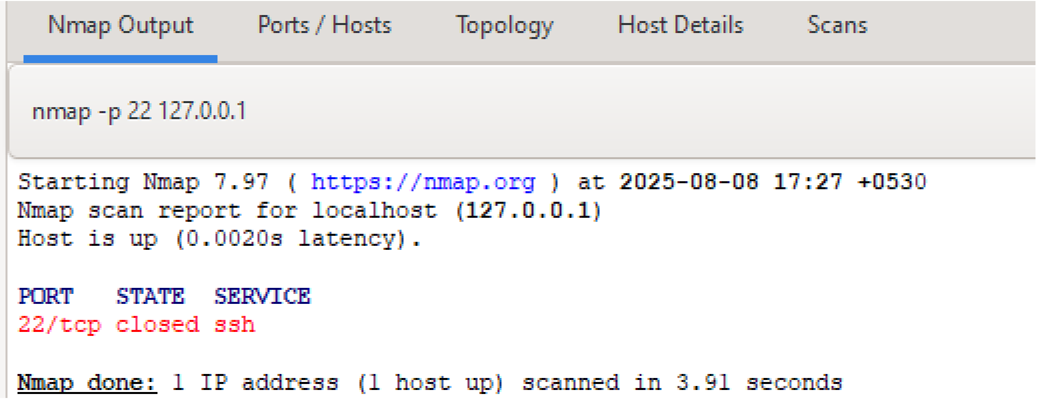
- Without SSH server: Nmap shows **closed** (no service listening) but not **filtered**, meaning firewall is allowing traffic.

- With SSH server installed (OpenSSH Server on Windows): Nmap shows **open**.

Command used:

nginx
Copy code

```
nmap -p 22 127.0.0.1
```



```
nmap -p 22 127.0.0.1
```

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-08 17:27 +0530
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0020s latency).

PORT   STATE  SERVICE
22/tcp closed ssh

Nmap done: 1 IP address (1 host up) scanned in 3.91 seconds
```

6. Conclusion

The firewall was successfully configured to:

- Block inbound traffic on Port 23 (Telnet).

- Allow inbound traffic on Port 22 (SSH).
  Testing confirmed that the firewall rules were applied correctly.
  This demonstrates the ability to configure network filtering rules and verify them using command-line tools.

7. References

- Microsoft Documentation: *Configure Windows Defender Firewall Rules*

- Nmap.org: *Port Scanning Basics*