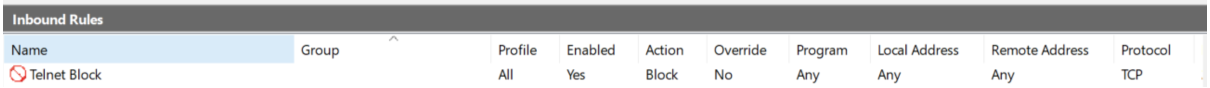
***Step 1** : Enable Telnet services*

***Step 2** : Create a Inbound Rule for blocking tenet services in port 23*

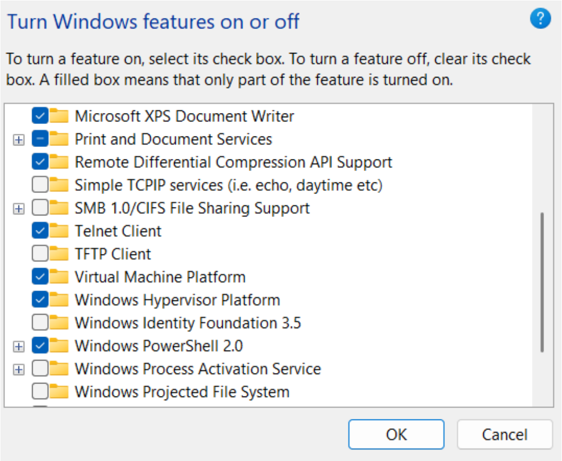
***Step 3**: test the Firewall rule*

***Step 4** : Revert back to normal Rules after testing*



Inbound Rules

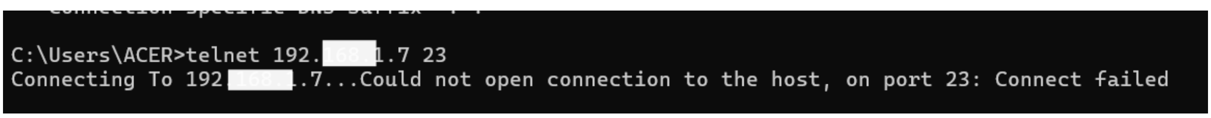
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
🚫 Telnet Block		All	Yes	Block	No	Any	Any	Any	TCP



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Microsoft XPS Document Writer
- ⊞ ■ Print and Document Services
- ☑ Remote Differential Compression API Support
- □ Simple TCPIP services (i.e. echo, daytime etc)
- ⊞ □ SMB 1.0/CIFS File Sharing Support
- ☑ Telnet Client
- □ TFTP Client
- ☑ Virtual Machine Platform
- ☑ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5
- ⊞ ☑ Windows PowerShell 2.0
- ⊞ □ Windows Process Activation Service
- □ Windows Projected File System



```
   Connection-specific DNS Suffix  . :

C:\Users\ACER>telnet 192.[redacted]1.7 23
Connecting To 192[redacted].7...Could not open connection to the host, on port 23: Connect failed
```

Why block port 23 (Telnet)?

- *Telnet is outdated and transmits data (including passwords) in plaintext.*
- *It is vulnerable to sniffing and Man-in-the-Middle (MitM) attacks.*
- *SSH (port 22) is a secure alternative, so port 23 is typically blocked to prevent exploitation.*