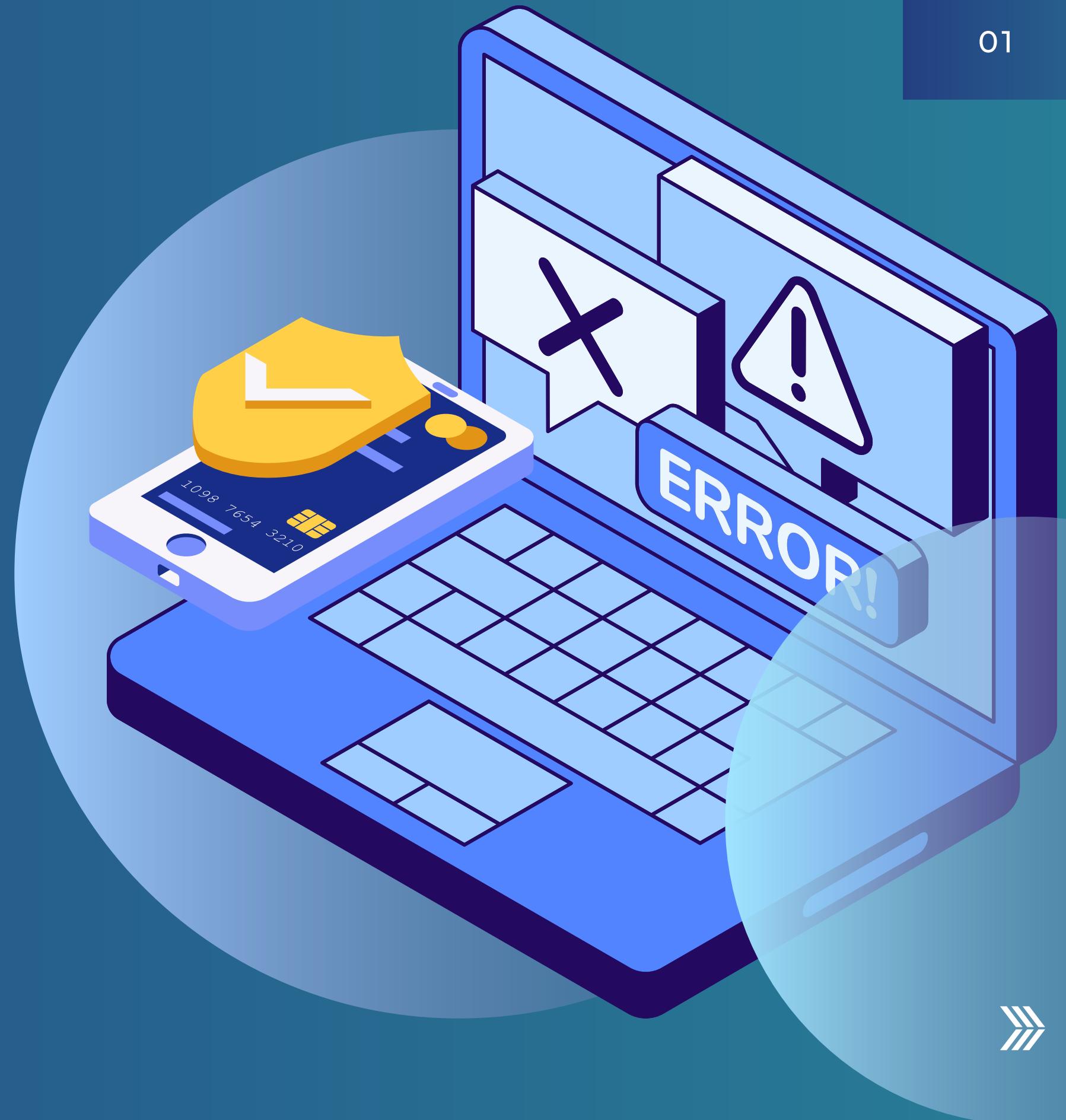




TASK 4 : SETUP AND USE A FIREWALL ON WINDOWS/LINUX

Objective: Configure and test basic firewall rules to allow or block traffic.

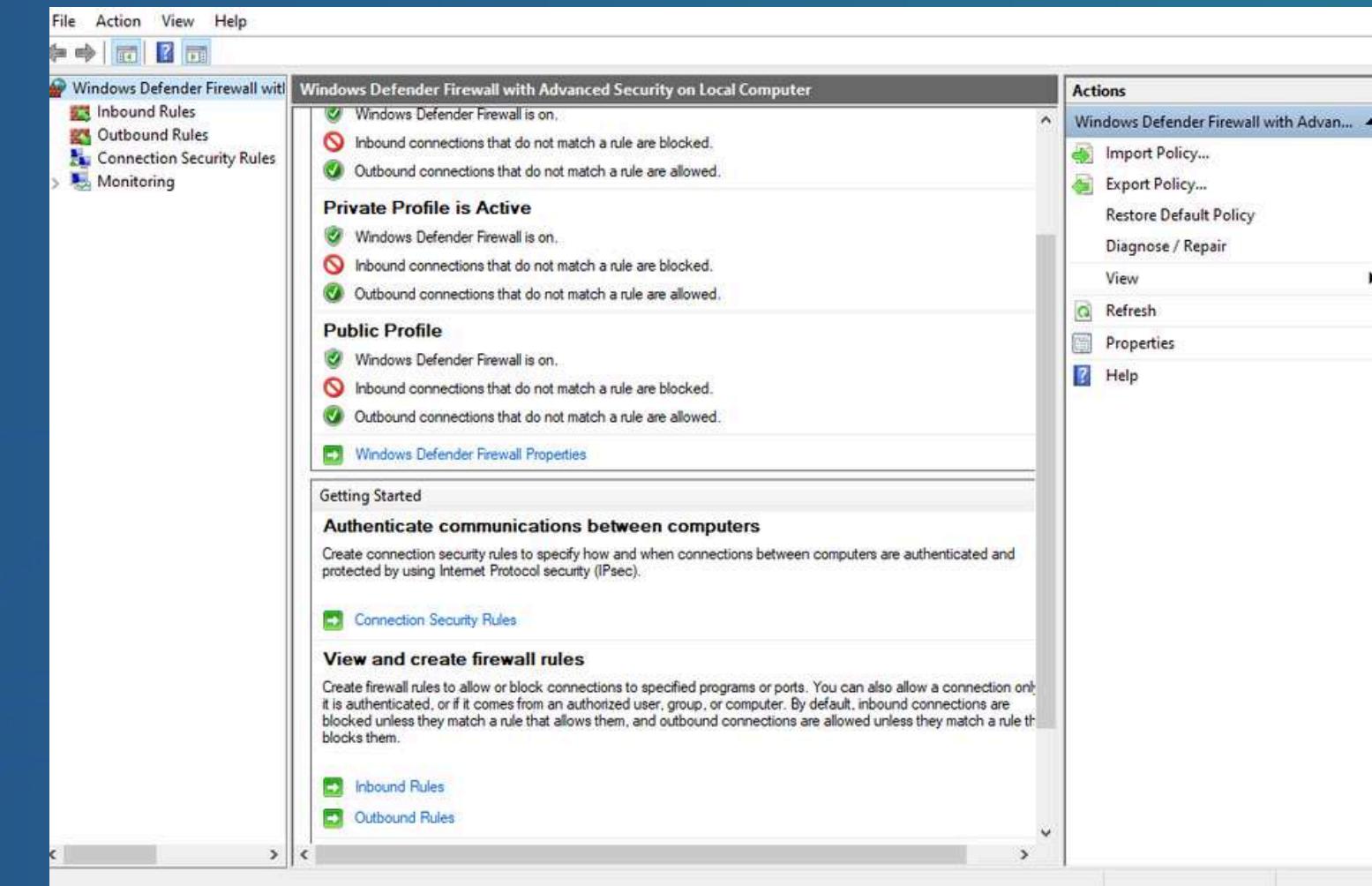
01





1. Open firewall configuration tool (Windows Firewall or terminal for UFW).

I opened Windows Defender Firewall with Advanced Security by searching for “wf.msc” in the Start menu.





2. List current firewall rules.

Inbound

File Action View Help

Inbound Rules

Name	Group	Profile	Enabled	Action
Log Options+ Agent	All	Yes	All	
Logi Plugin Service	All	Yes	All	
Microsoft Lync	Public	Yes	All	
Microsoft Lync	Public	Yes	All	
Microsoft Lync UcMapi	Public	Yes	All	
Microsoft Lync UcMapi	Public	Yes	All	
Microsoft Office Outlook	Public	Yes	All	
@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	All
@FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes	All
Microsoft Teams	(78E1CD88-49E3-476E-B926-...)	All	Yes	All
Microsoft Teams	(78E1CD88-49E3-476E-B926-...)	All	Yes	All
Microsoft Teams	(78E1CD88-49E3-476E-B926-...)	All	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Private	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Private	Yes	All
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes	All
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes	All
App Installer	App Installer	Domain	Yes	All
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	All
BranchCache Hosted Cache Server (HTTP-...	BranchCache - Hosted Cach...	All	No	All
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	All
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	All
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	All
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	All
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	All
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	All
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	All

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Outbound

File Action View Help

Outbound Rules

Name	Group	Profile	Enabled	Action
KMS-R@1n	All	Yes	All	
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes	All
Microsoft Teams	(78E1CD88-49E3-476E-B926-...)	All	Yes	All
Microsoft Teams	(78E1CD88-49E3-476E-B926-...)	All	Yes	All
Microsoft Teams	(78E1CD88-49E3-476E-B926-...)	All	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Private	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Private	Yes	All
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public	Yes	All
3D Viewer	3D Viewer	All	Yes	All
AllJoyn Router (TCP-Out)	AllJoyn Router	Domain	Yes	All
AllJoyn Router (UDP-Out)	AllJoyn Router	Domain	Yes	All
App Installer	App Installer	All	Yes	All
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	All
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All	No	All
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	All
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	All
Captive Portal Flow	Captive Portal Flow	All	Yes	All
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	All
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	All
Cast to Device streaming server (RTP-St...	Cast to Device functionality	Domain	Yes	All
Cast to Device streaming server (RTP-St...	Cast to Device functionality	Private	Yes	All
Cast to Device streaming server (RTP-St...	Cast to Device functionality	Public	Yes	All
Cloud Identity (TCP-Out)	Cloud Identity	All	Yes	All
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	All
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domain	Yes	All
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domain	Yes	All
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	All

Actions

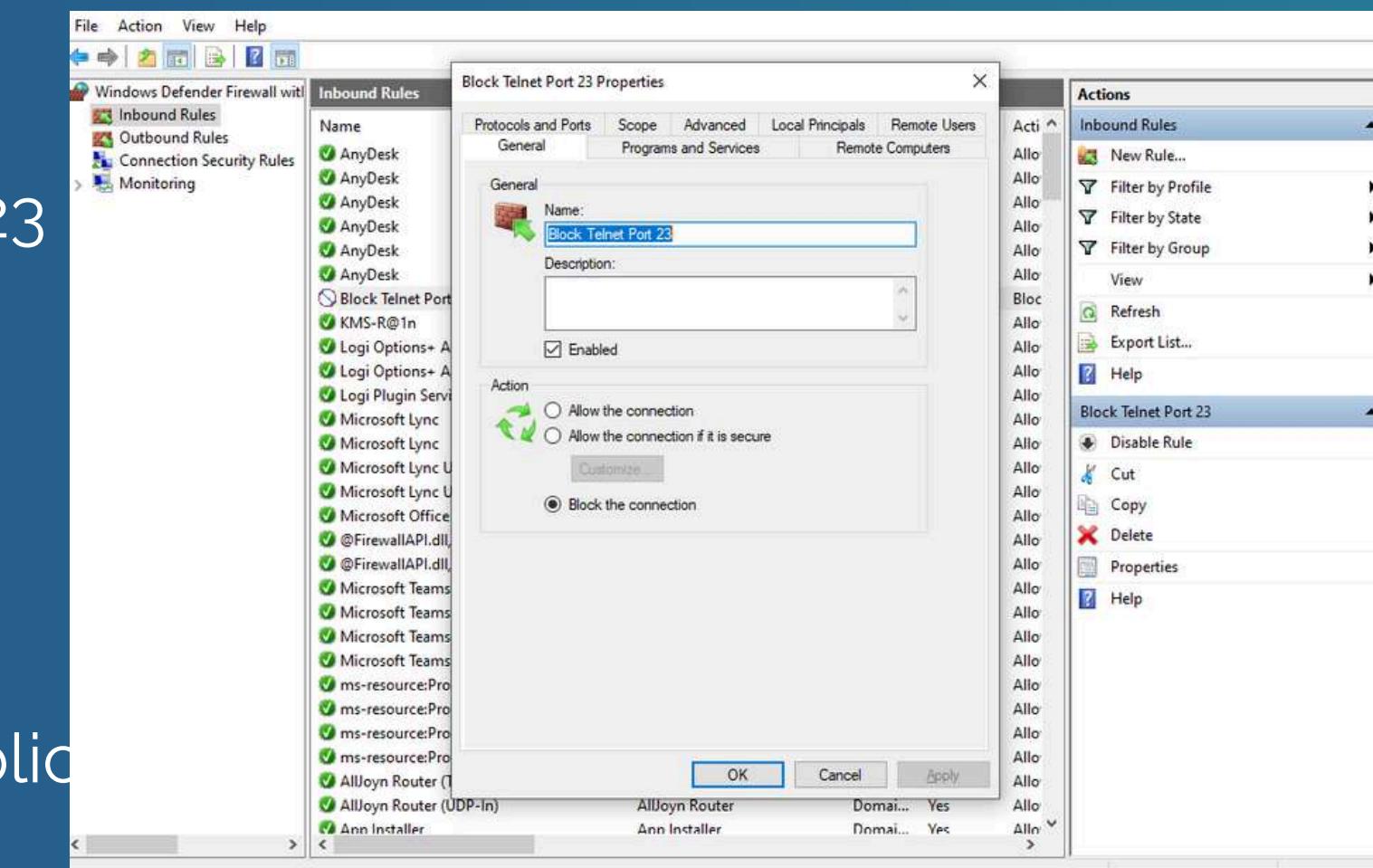
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help



3. Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet)

Created a New Inbound Rule to Block Port 23 (Telnet):

- Went to Inbound Rules → New Rule
- Selected Port
- Chose TCP
- Entered port 23
- Selected Block the connection
- Applied rule to Domain, Private, and Public
- Named it “Block Telnet Port 23”



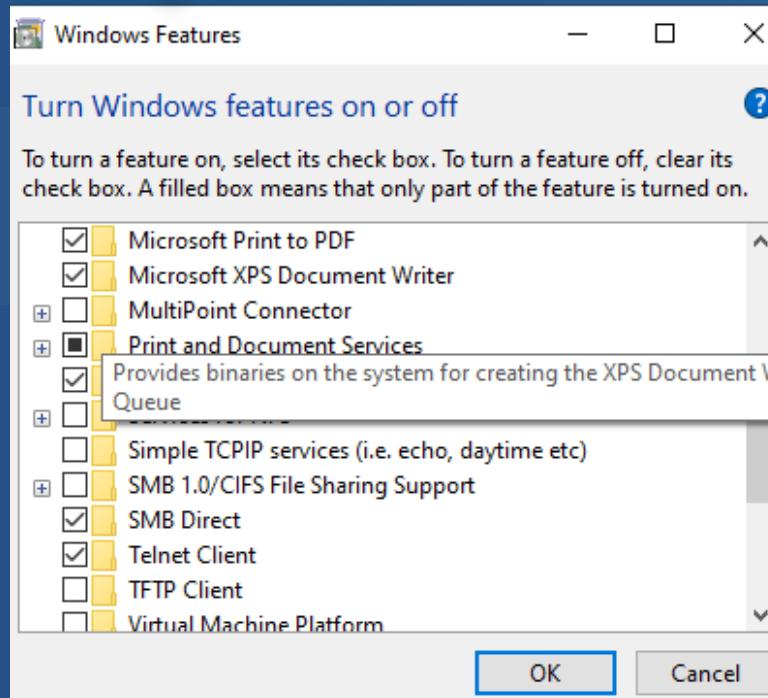


4. Test the rule by attempting to connect to that port locally or remotely.

Enable Telnet on Windows

- Press Windows Key type “Turn Windows features on or off”
- Scroll down
- Tick Telnet Client
- Click OK

Wait for installation to finish



Tested the Rule

- telnet 127.0.0.1 23
- telnet localhost 23

```
C:\Windows\system32>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed

C:\Windows\system32>
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

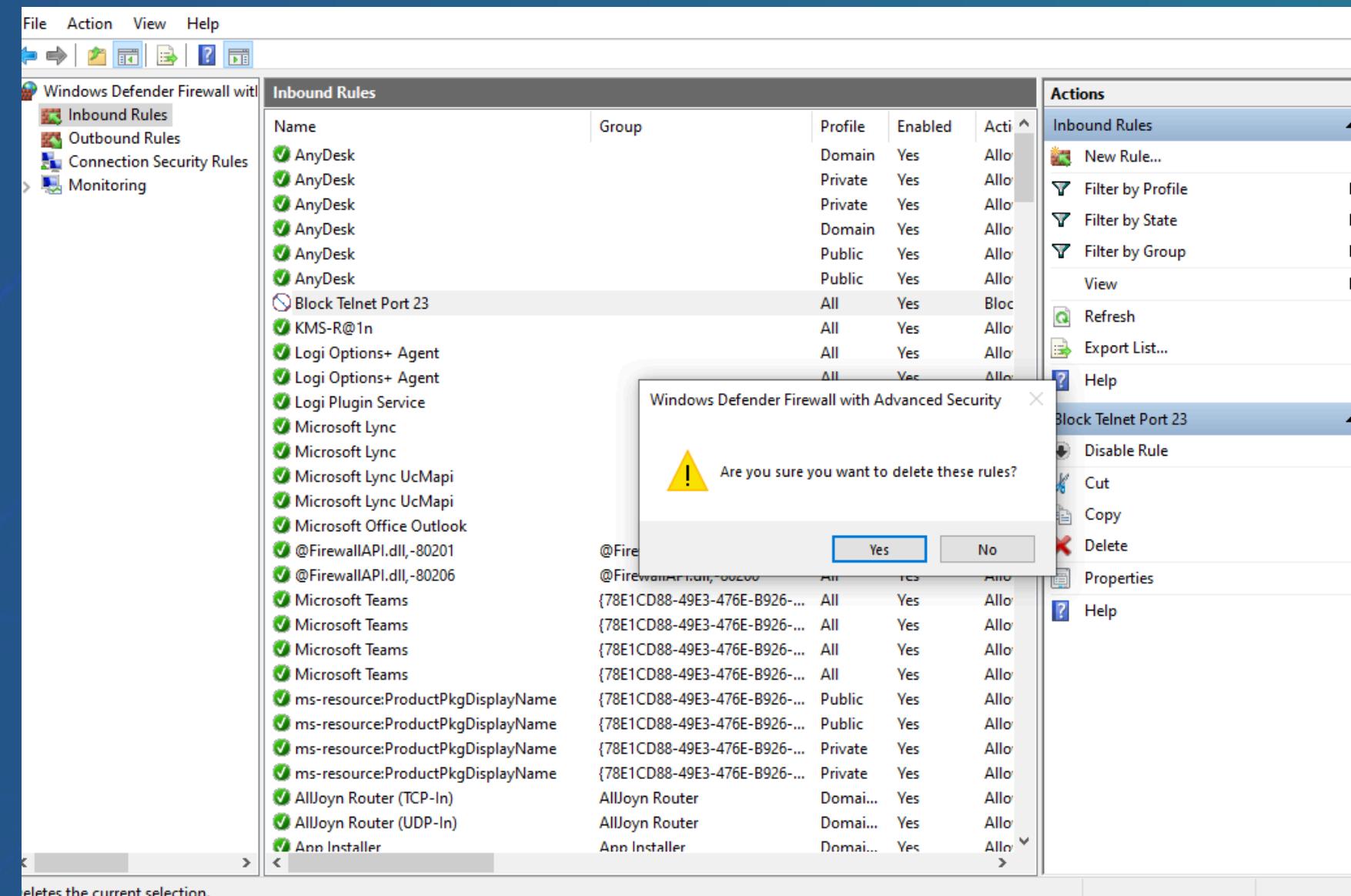
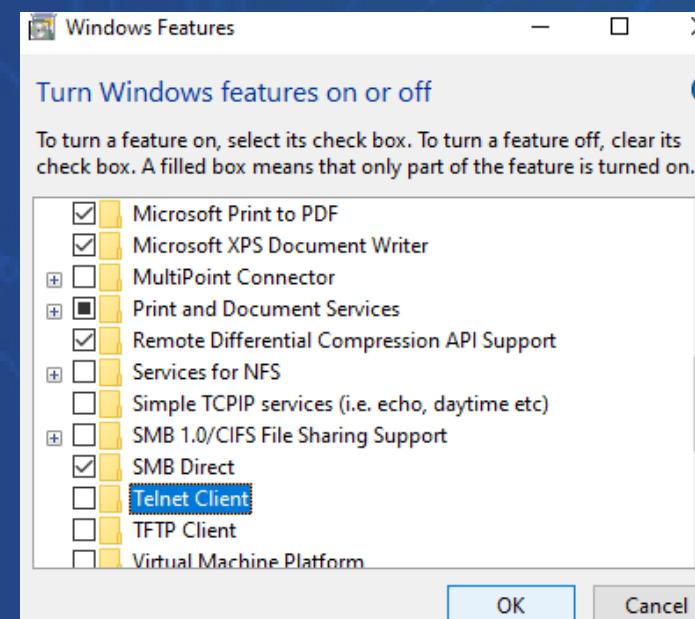
C:\Windows\system32>
C:\Windows\system32>
```





6. Remove the test block rule to restore original state.

After completing the test, I returned to Inbound Rules, selected Block Telnet Port 23, and deleted it to restore the firewall to its original state.





8. Summarize how firewall filters traffic.

- A firewall filters traffic by checking each incoming or outgoing packet against defined rules.
- If a packet matches a rule (allow/block), the firewall applies that action.
- This protects the system by controlling which ports, services, and applications can communicate.





08

THANK YOU!

