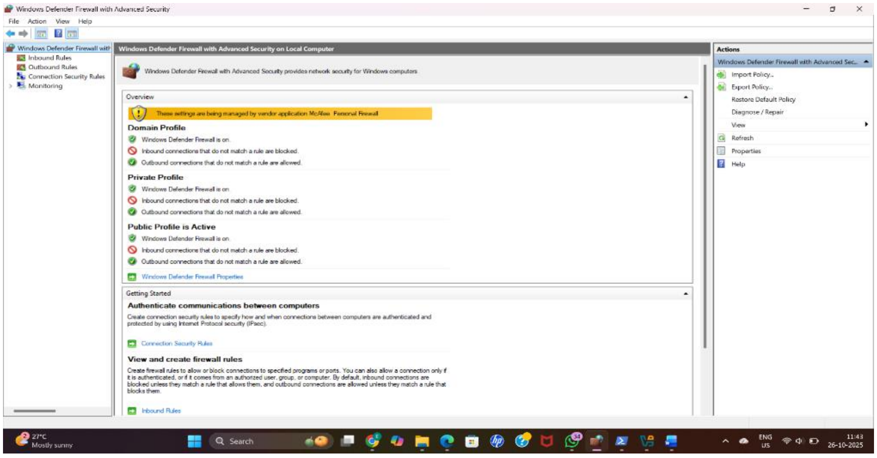
Task 4 : Setup and Use a Firewall on Windows/Linux

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



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers

Overview

These settings are being managed by vendor application McAfee Personal Firewall

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

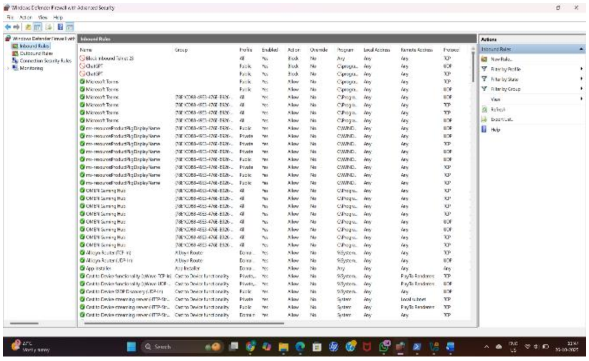
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

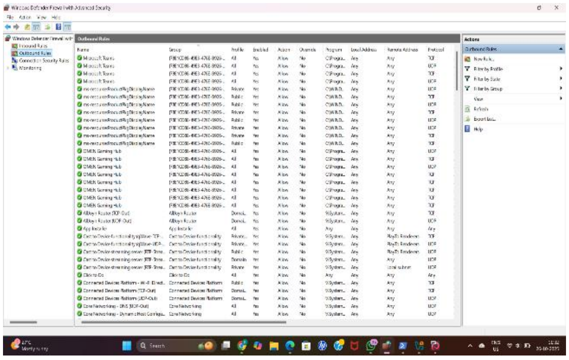
2. List current firewall rules:

- There are two types of rules Inbound and Outbound rules.
- Inbound rules: Inbound rules control traffic coming *into* your computer or network from external sources.
- Eg: The internet or another device.
- Outbound rules: Outbound rules control traffic going *out* from your computer or network to other systems.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Block inbound Telnet 23		All	Yes	Block	No	Any	Any	Any	TCP
ChatGPT		Public	Yes	Block	No	C:\progra...	Any	Any	UDP
ChatGPT		Public	Yes	Block	No	C:\progra...	Any	Any	TCP
Microsoft Teams		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Microsoft Teams		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
App Installer	App Installer	Domai...	Yes	Allow	No	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	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-St...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local subnet	TCP
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Any	TCP



Outbound Rules

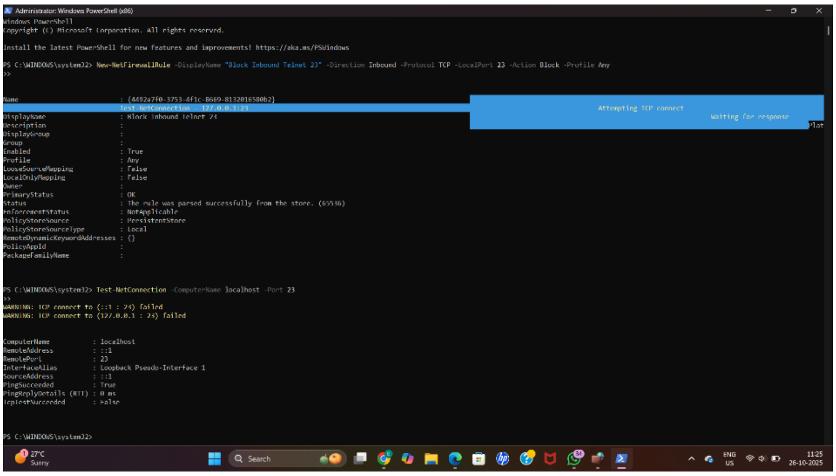
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
OMEN Gaming Hub	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP
Click to Do	Click to Do	All	Yes	Allow	No	Any	Any	Any	Any
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP

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

- To do this you can use command prompt or can be done directly through firewall settings. I have done using command prompt.
- “New-NetFirewallRule -DisplayName "Block Inbound Telnet 23" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block -Profile Any” use this command to block the telnet 23 port.

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

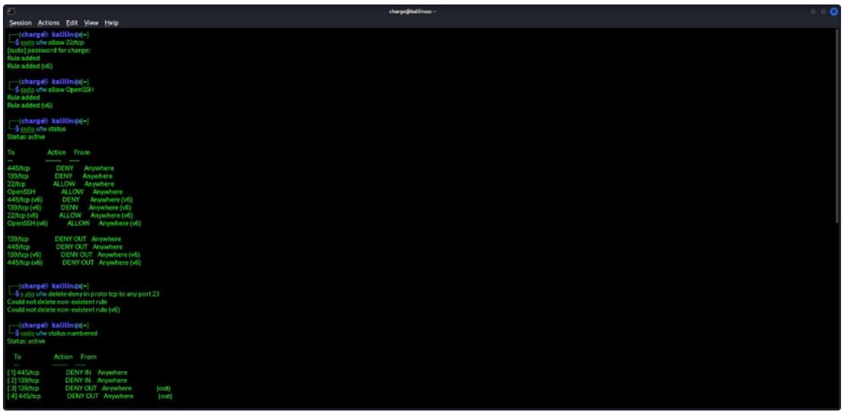
- I have tested it locally using the command “Test-NetConnection -ComputerName localhost -Port 23”



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> New-NetFirewallRule -DisplayName "Block Inbound Telnet 23" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block -Profile Any
>>

Name                          : {4492a7f0-3753-4f1c-8669-8132016580b2}
                                Test-NetConnection - 127.0.0.1:23                    Attempting TCP connect
DisplayName                   : Block Inbound Telnet 23                                           Waiting for response
Description                   :                                                                                        Plat
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :


PS C:\WINDOWS\system32> Test-NetConnection -ComputerName localhost -Port 23
>>
WARNING: TCP connect to (::1 : 23) failed
WARNING: TCP connect to (127.0.0.1 : 23) failed


ComputerName           : localhost
RemoteAddress          : ::1
RemotePort             : 23
InterfaceAlias         : Loopback Pseudo-Interface 1
SourceAddress          : ::1
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False


PS C:\WINDOWS\system32>
```

5. Add rule to allow SSH (port 22) if on Linux:

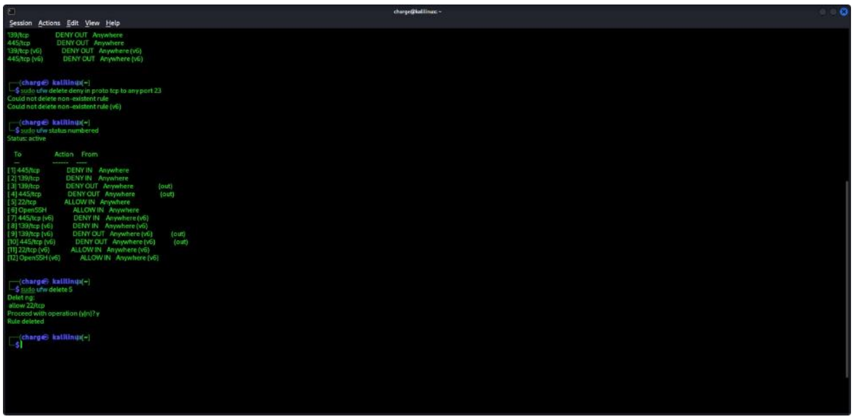
- Open linux and type the command “sudo ufw allow 22/tcp” and enter the password the rule will be added.
- Then type “sudo ufw status” to know it’s status.



```
┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw allow 22/tcp
[sudo] password for charge:
Rule added
Rule added (v6)

┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw allow OpenSSH
Rule added
Rule added (v6)

┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw status
Status: active

To                Action    From
--                ------    ----
445/tcp           DENY      Anywhere
139/tcp           DENY      Anywhere
22/tcp            ALLOW     Anywhere
OpenSSH           ALLOW     Anywhere
445/tcp (v6)      DENY      Anywhere (v6)
139/tcp (v6)      DENY      Anywhere (v6)
22/tcp (v6)       ALLOW     Anywhere (v6)
OpenSSH (v6)      ALLOW     Anywhere (v6)

139/tcp           DENY OUT  Anywhere
445/tcp           DENY OUT  Anywhere
139/tcp (v6)      DENY OUT  Anywhere (v6)
445/tcp (v6)      DENY OUT  Anywhere (v6)


┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw delete deny in proto tcp to any port 23
Could not delete non-existent rule
Could not delete non-existent rule (v6)

┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw status numbered
Status: active

     To                Action      From
     --                ------      ----
[ 1] 445/tcp           DENY IN     Anywhere
[ 2] 139/tcp           DENY IN     Anywhere
[ 3] 139/tcp           DENY OUT    Anywhere                   (out)
[ 4] 445/tcp           DENY OUT    Anywhere                   (out)
```

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

- To restore type command "sudo ufw delete deny in proto tcp to any port 23"
- Or you can also type "sudo ufw delete <rule-number>"
- To check the status type "sudo ufw status numbered"



```
139/tcp           DENY OUT  Anywhere
445/tcp           DENY OUT  Anywhere
139/tcp (v6)      DENY OUT  Anywhere (v6)
445/tcp (v6)      DENY OUT  Anywhere (v6)


┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw delete deny in proto tcp to any port 23
Could not delete non-existent rule
Could not delete non-existent rule (v6)

┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw status numbered
Status: active

     To                Action      From
     --                ------      ----
[ 1] 445/tcp           DENY IN     Anywhere
[ 2] 139/tcp           DENY IN     Anywhere
[ 3] 139/tcp           DENY OUT    Anywhere                   (out)
[ 4] 445/tcp           DENY OUT    Anywhere                   (out)
[ 5] 22/tcp            ALLOW IN    Anywhere
[ 6] OpenSSH           ALLOW IN    Anywhere
[ 7] 445/tcp (v6)      DENY IN     Anywhere (v6)
[ 8] 139/tcp (v6)      DENY IN     Anywhere (v6)
[ 9] 139/tcp (v6)      DENY OUT    Anywhere (v6)              (out)
[10] 445/tcp (v6)      DENY OUT    Anywhere (v6)              (out)
[11] 22/tcp (v6)       ALLOW IN    Anywhere (v6)
[12] OpenSSH (v6)      ALLOW IN    Anywhere (v6)


┌──(charge㉿ kalilinux)-[~]
└─$ sudo ufw delete 5
Deleting:
 allow 22/tcp
Proceed with operation (y|n)? y
Rule deleted

┌──(charge㉿ kalilinux)-[~]
└─$
```

7. Summarize how firewall filters traffic:

- **Packet filtering**: Firewalls match packets to rules based on packet headers (source IP, destination IP, protocol, ports). If a packet matches a "block" rule it's dropped or rejected.
- **Stateful inspection**: Modern firewalls track connection state (NEW, ESTABLISHED, RELATED).
- **Rule ordering & precedence**: Firewalls evaluate rules in order or by priority first match usually wins.

- **Zones & profiles**: Many systems use zones (public/private/trusted) or profiles (domain/private/public) to apply different rule sets to different network interfaces.
- **Application & service filtering**: Some firewalls allow rules by application or service name, not just port, which is more precise.
- **Logging & monitoring**: Good practice, enable logging for important rules to audit blocked/allowed traffic and troubleshoot.
- **Persistence & reload**: Some tools require extra steps to make rules persistent across reboots.