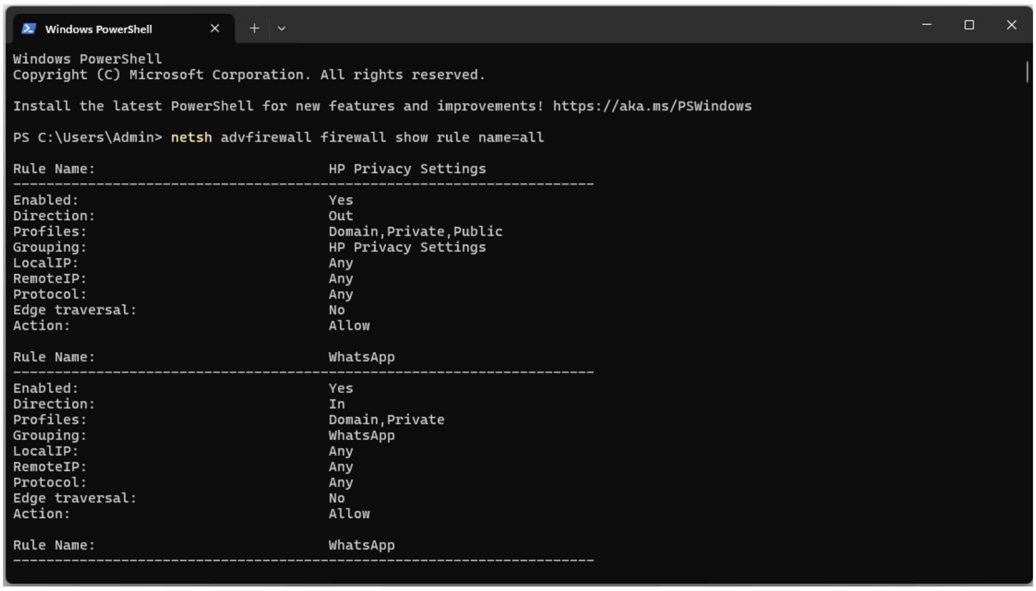
Task 4 – Setup and Use a Firewall (Windows)

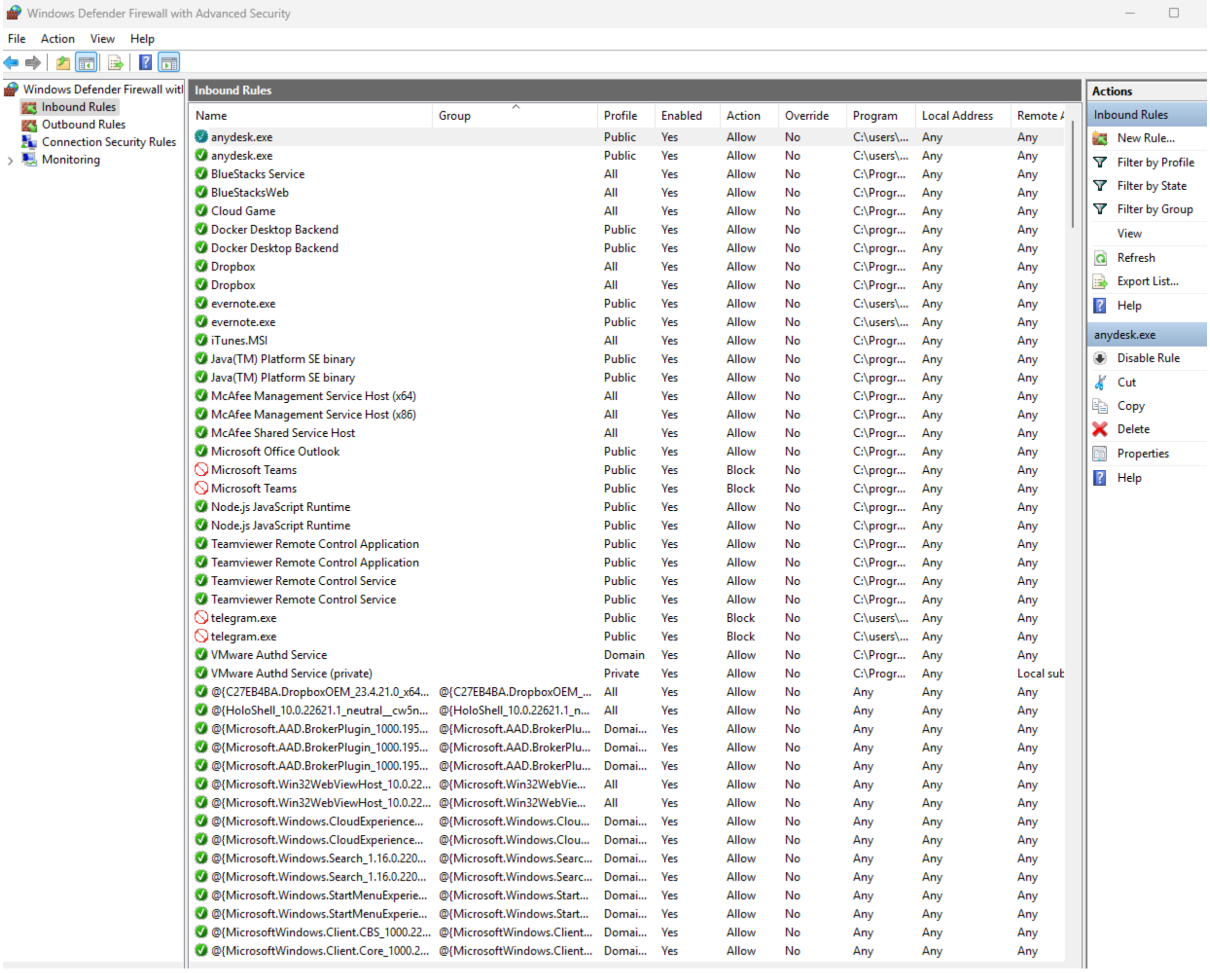
Objective

Configure and test basic firewall rules to allow or block traffic, demonstrating basic firewall management skills.

List Of Current Firewall Rules



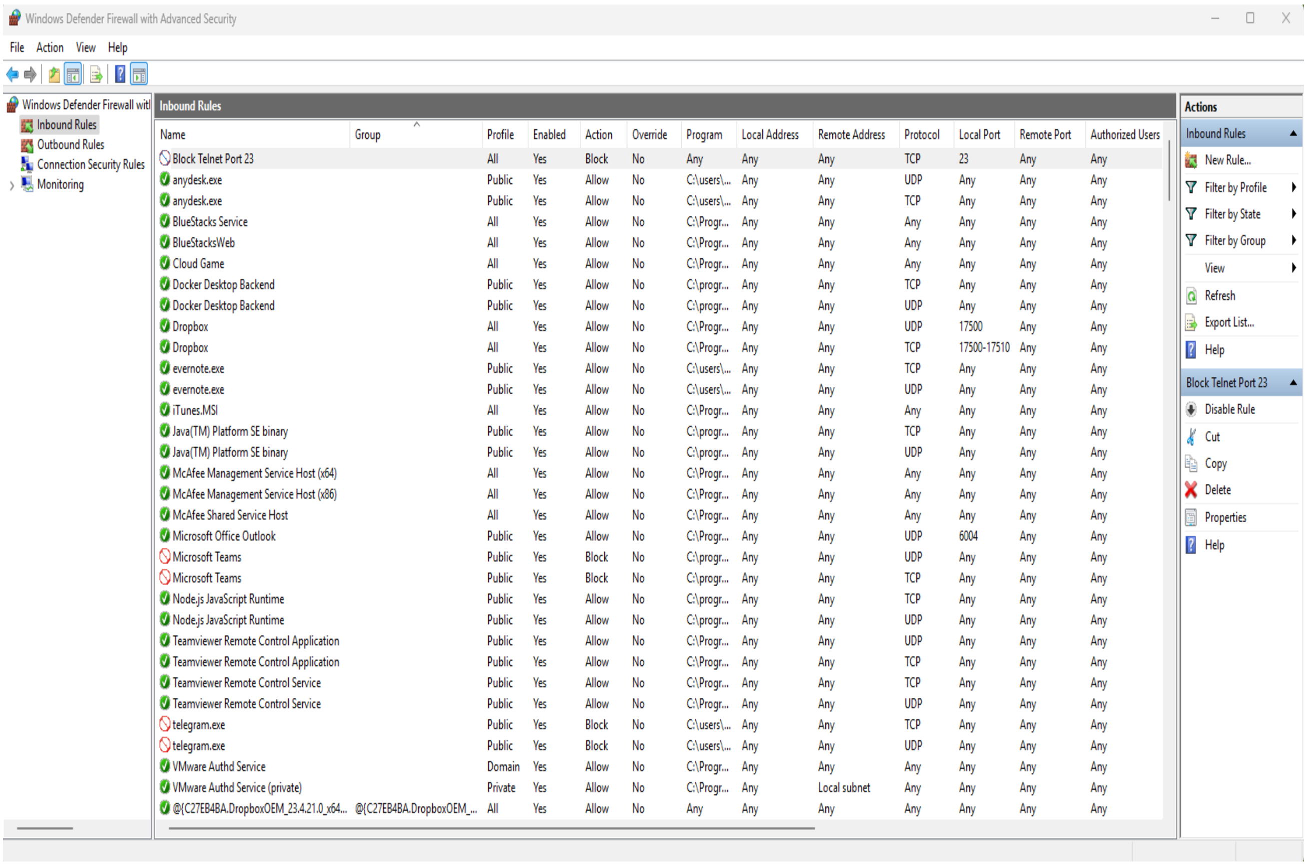
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\Admin> netsh advfirewall firewall show rule name=all

Rule Name:                            HP Privacy Settings
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:                             HP Privacy Settings
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            WhatsApp
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private
Grouping:                             WhatsApp
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            WhatsApp
----------------------------------------------------------------------
```



Inbound Rules

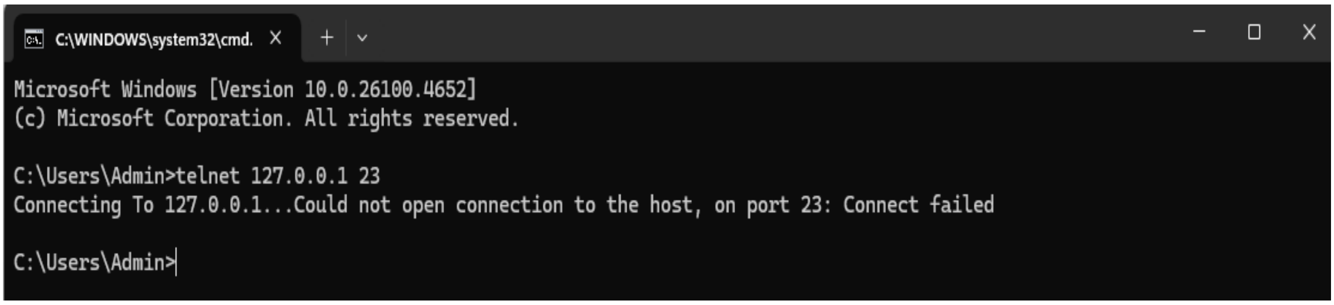
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote A
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any
Cloud Game		All	Yes	Allow	No	C:\Progr...	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
iTunes.MSI		All	Yes	Allow	No	C:\Progr...	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any
McAfee Management Service Host (x64)		All	Yes	Allow	No	C:\Progr...	Any	Any
McAfee Management Service Host (x86)		All	Yes	Allow	No	C:\Progr...	Any	Any
McAfee Shared Service Host		All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any
VMware Authd Service		Domain	Yes	Allow	No	C:\Progr...	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progr...	Any	Local sub
@{C27EB4BA.DropboxOEM_23.4.21.0_x64...	@{C27EB4BA.DropboxOEM_...	All	Yes	Allow	No	Any	Any	Any
@{HoloShell_10.0.22621.1_neutral__cw5n...	@{HoloShell_10.0.22621.1_n...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.Client.CBS_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.Client.Core_1000.2...	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any	Any

Block Inbound Traffic on Port 23 (Telnet)



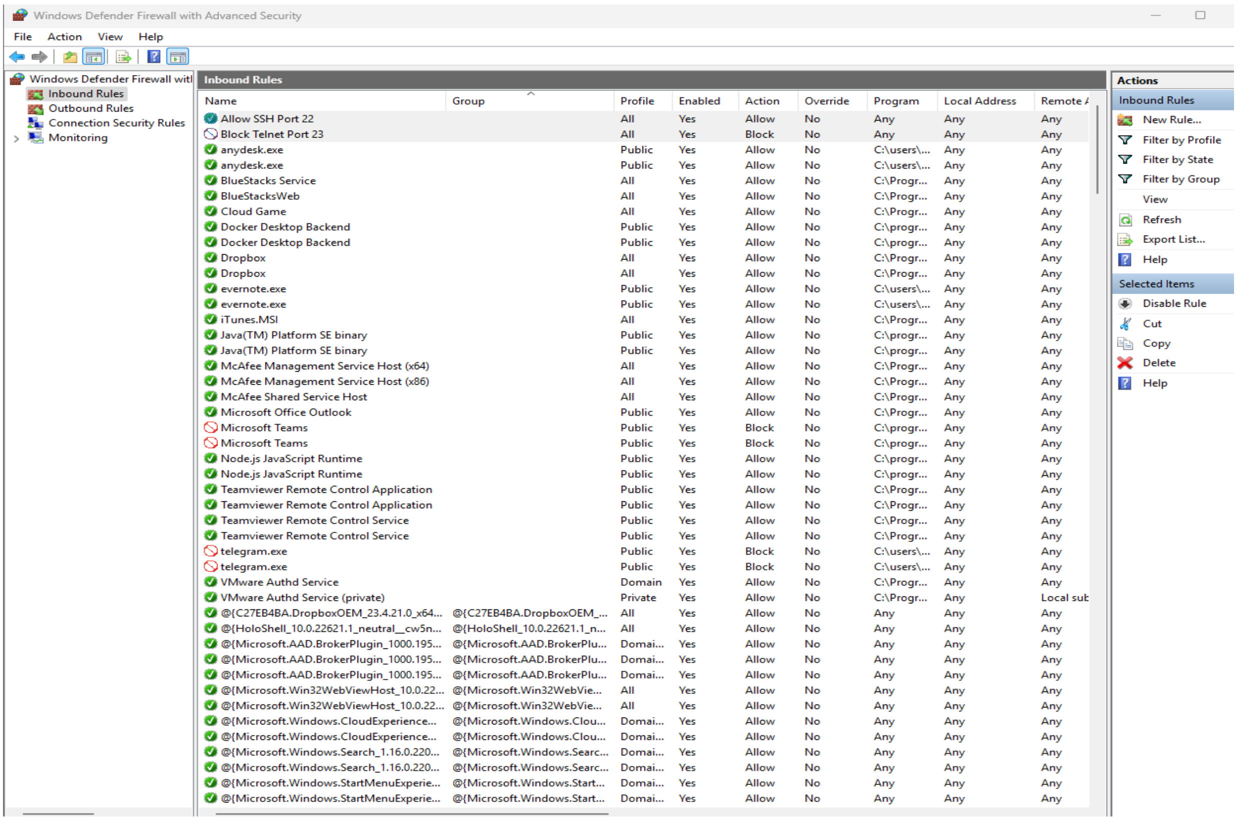
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users
Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any	TCP	23	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	UDP	Any	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP	Any	Any	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
Cloud Game		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	17500	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	17500-17510	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	TCP	Any	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any	UDP	Any	Any	Any
iTunes.MSI		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any
McAfee Management Service Host (x64)		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
McAfee Management Service Host (x86)		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
McAfee Shared Service Host		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any	UDP	6004	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any	UDP	Any	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any	TCP	Any	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any	TCP	Any	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any	UDP	Any	Any	Any
VMware Authd Service		Domain	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progr...	Any	Local subnet	Any	Any	Any	Any
@{C27EB4BA.DropboxOEM_23.4.21.0_x64...	@{C27EB4BA.DropboxOEM_...	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any

Test the Rule



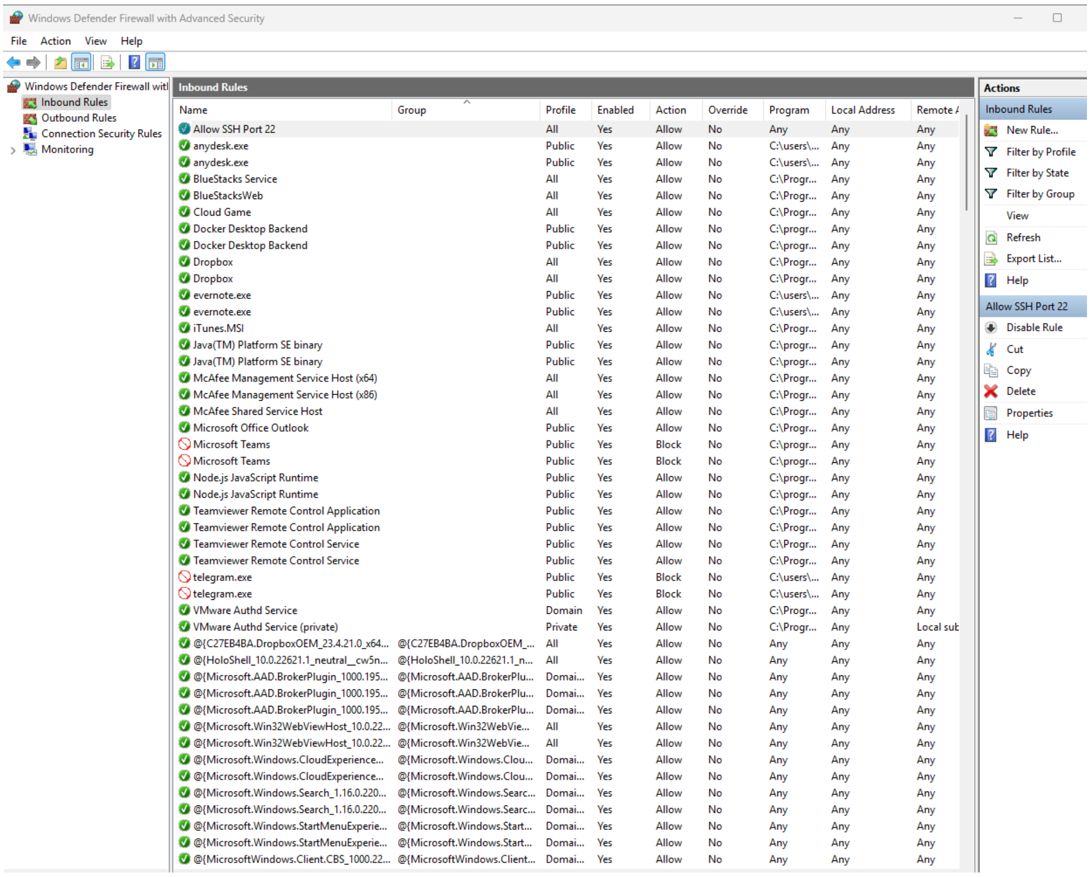
```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>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:\Users\Admin>
```

Allow SSH (Port 22)



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote A
Allow SSH Port 22		All	Yes	Allow	No	Any	Any	Any
Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any
Cloud Game		All	Yes	Allow	No	C:\Progr...	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
iTunes.MSI		All	Yes	Allow	No	C:\Progr...	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any
McAfee Management Service Host (x64)		All	Yes	Allow	No	C:\Progr...	Any	Any
McAfee Management Service Host (x86)		All	Yes	Allow	No	C:\Progr...	Any	Any
McAfee Shared Service Host		All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any
VMware Authd Service		Domain	Yes	Allow	No	C:\Progr...	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progr...	Any	Local sub
@{C27EB4BA.DropboxOEM_23.4.21.0_x64...	@{C27EB4BA.DropboxOEM_...	All	Yes	Allow	No	Any	Any	Any
@{HoloShell_10.0.22621.1_neutral__cw5n...	@{HoloShell_10.0.22621.1_n...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any

Remove Test Block Rule



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote A
Allow SSH Port 22		All	Yes	Allow	No	Any	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
anydesk.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any
Cloud Game		All	Yes	Allow	No	C:\Progr...	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any
Docker Desktop Backend		Public	Yes	Allow	No	C:\progr...	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any
Dropbox		All	Yes	Allow	No	C:\Progr...	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
evernote.exe		Public	Yes	Allow	No	C:\users\...	Any	Any
iTunes.MSI		All	Yes	Allow	No	C:\Progr...	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any
Java(TM) Platform SE binary		Public	Yes	Allow	No	C:\progr...	Any	Any
McAfee Management Service Host (x64)		All	Yes	Allow	No	C:\Progr...	Any	Any
McAfee Management Service Host (x86)		All	Yes	Allow	No	C:\Progr...	Any	Any
McAfee Shared Service Host		All	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any
Microsoft Teams		Public	Yes	Block	No	C:\progr...	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progr...	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Application		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any
Teamviewer Remote Control Service		Public	Yes	Allow	No	C:\Progr...	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any
telegram.exe		Public	Yes	Block	No	C:\users\...	Any	Any
VMware Authd Service		Domain	Yes	Allow	No	C:\Progr...	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progr...	Any	Local sub
@{C27EB4BA.DropboxOEM_23.4.21.0_x64...	@{C27EB4BA.DropboxOEM_...	All	Yes	Allow	No	Any	Any	Any
@{HoloShell_10.0.22621.1_neutral__cw5n...	@{HoloShell_10.0.22621.1_n...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.AAD.BrokerPlugin_1000.195...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Win32WebViewHost_10.0.22...	@{Microsoft.Win32WebVie...	All	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	Domai...	Yes	Allow	No	Any	Any	Any
@{MicrosoftWindows.Client.CBS_1000.22...	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	No	Any	Any	Any

Summary

1) **A firewall works as a protective barrier between a computer or network and external connections.**
2) **It examines all incoming and outgoing data packets and matches them against a set of security rules.**
3) **These rules can be based on factors like the packet's source and destination address, the port number, the protocol being used, and whether the connection is new or already established.**
4) **If a packet meets the allowed conditions, it is permitted through; if not, it is blocked or dropped.**
5) **This process ensures that only trusted and necessary traffic can pass, reducing the risk of unauthorized access or malicious activity.**