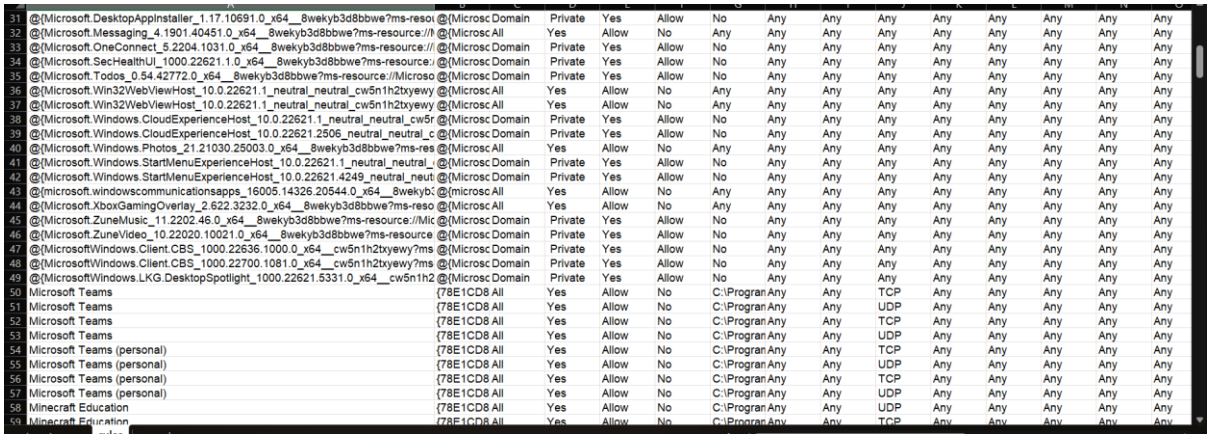
Objective: Configure and test basic firewall rules to allow or block traffic.

Step1: Open the windows defender firewall manager and exported the rules into a csv file as screenshot is not allowed in the firewall manger

Step2: screenshot of some of the rules applied.



31	@{Microsoft.DesktopAppInstaller_1.17.10691.0_x64__8wekyb3d8bbwe?ms-resou	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
32	@{Microsoft.Messaging_4.1901.40451.0_x64__8wekyb3d8bbwe?ms-resource://M	@{Microsc	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
33	@{Microsoft.OneConnect_5.2204.1031.0_x64__8wekyb3d8bbwe?ms-resource://	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
34	@{Microsoft.SecHealthUI_1000.22621.1.0_x64__8wekyb3d8bbwe?ms-resource:/	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
35	@{Microsoft.Todos_0.54.42772.0_x64__8wekyb3d8bbwe?ms-resource://Microso	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
36	@{Microsoft.Win32WebViewHost_10.0.22621.1_neutral_neutral_cw5n1h2txyewy	@{Microsc	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
37	@{Microsoft.Win32WebViewHost_10.0.22621.1_neutral_neutral_cw5n1h2txyewy	@{Microsc	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
38	@{Microsoft.Windows.CloudExperienceHost_10.0.22621.1_neutral_neutral_cw5r	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
39	@{Microsoft.Windows.CloudExperienceHost_10.0.22621.2506_neutral_neutral_c	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
40	@{Microsoft.Windows.Photos_21.21030.25003.0_x64__8wekyb3d8bbwe?ms-res	@{Microsc	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
41	@{Microsoft.Windows.StartMenuExperienceHost_10.0.22621.1_neutral_neutral_	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
42	@{Microsoft.Windows.StartMenuExperienceHost_10.0.22621.4249_neutral_neut	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
43	@{microsoft.windowscommunicationsapps_16005.14326.20544.0_x64__8wekyb3	@{microsc	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
44	@{Microsoft.XboxGamingOverlay_2.622.3232.0_x64__8wekyb3d8bbwe?ms-reso	@{Microsc	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
45	@{Microsoft.ZuneMusic_11.2202.46.0_x64__8wekyb3d8bbwe?ms-resource://Mic	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
46	@{Microsoft.ZuneVideo_10.22020.10021.0_x64__8wekyb3d8bbwe?ms-resource	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
47	@{MicrosoftWindows.Client.CBS_1000.22636.1000.0_x64__cw5n1h2txyewy?ms	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
48	@{MicrosoftWindows.Client.CBS_1000.22700.1081.0_x64__cw5n1h2txyewy?ms	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
49	@{MicrosoftWindows.LKG.DesktopSpotlight_1000.22621.5331.0_x64__cw5n1h2	@{Microsc	Domain	Private	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any
50	Microsoft Teams	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	TCP	Any	Any	Any	Any
51	Microsoft Teams	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	UDP	Any	Any	Any	Any
52	Microsoft Teams	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	TCP	Any	Any	Any	Any
53	Microsoft Teams	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	UDP	Any	Any	Any	Any
54	Microsoft Teams (personal)	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	TCP	Any	Any	Any	Any
55	Microsoft Teams (personal)	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	UDP	Any	Any	Any	Any
56	Microsoft Teams (personal)	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	TCP	Any	Any	Any	Any
57	Microsoft Teams (personal)	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	UDP	Any	Any	Any	Any
58	Minecraft Education	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	UDP	Any	Any	Any	Any
59	Minecraft Education	{78E1CD8	All	Yes	Allow	No	C:\Progran	Any	Any	TCP	Any	Any	Any	Any

Step 3: checked the connection of port using telnet

C:\Windows\System32>telnet localhost 902

Output: 220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , , NFCSSL supported/t,

Step4: added the rule

In windows defender firewall -> inbound rules -> new rule -> select port -> select TCP and mention the port -> block the connection -> choose the types of networks -> give it a name and click finish

step5: checked the connection locally which denied the connection to the port that the rule was added

C:\Windows\System32>telnet localhost 902

Output: Connecting To localhost...Could not open connection to the host, on port 902: Connect failed

step 6 : deleting the rule has restored the connection to the port

How firewall filters traffic?

A firewall filters traffic by comparing each connection or packet against a set of security rules. It blocks or allows communication based on IP, port, protocol, application, and direction, protecting your system from unauthorized access and attacks.