

Setup and Use a Firewall on Windows

Objective:

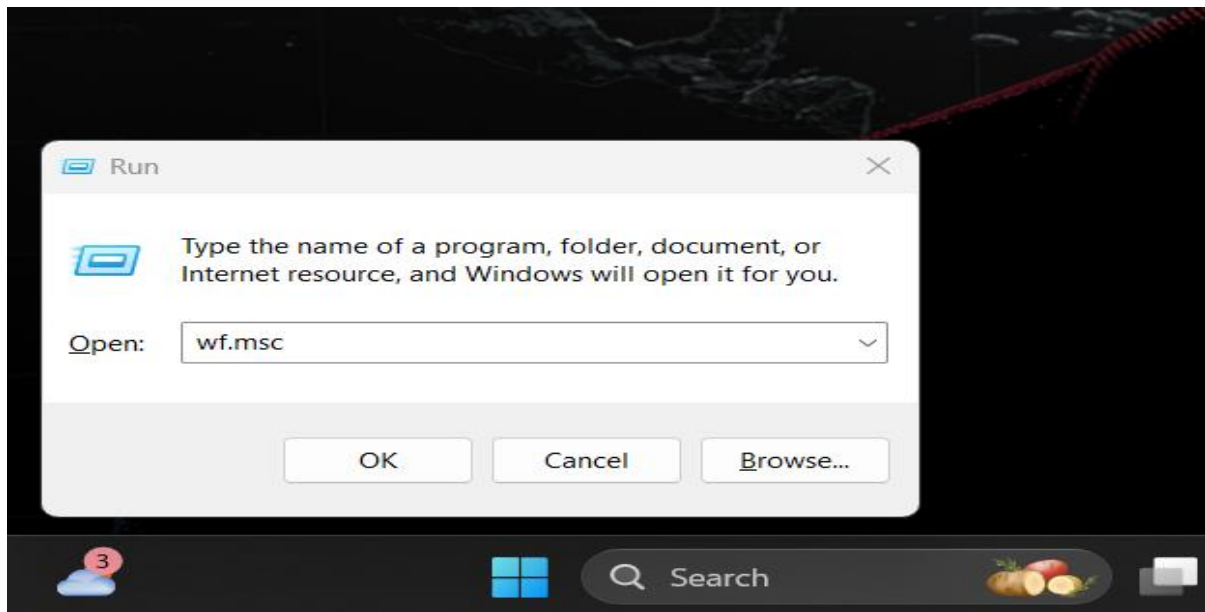
To set up and check simple firewall rules that either allow or block network traffic. This helps control what kind of data can enter or leave a computer or network, making it more secure by letting in safe traffic and blocking unwanted or harmful traffic.

Tools:

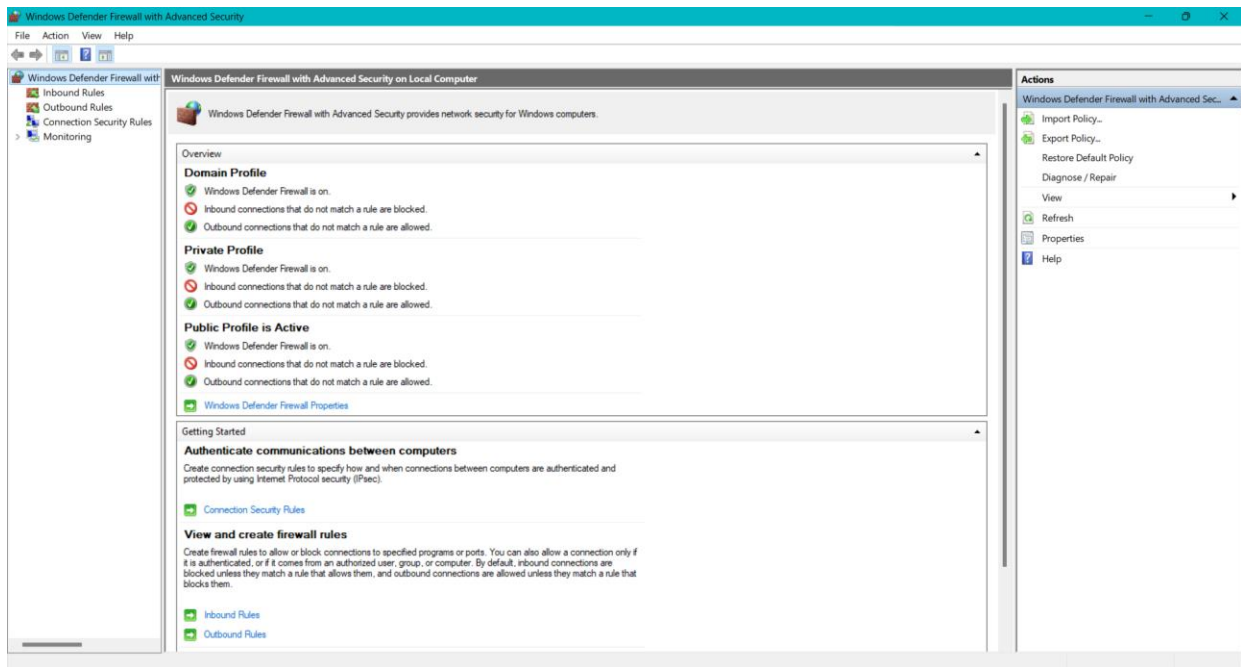
We will use Windows Firewall for Windows and UFW for Linux. These tools help us allow or block network traffic to keep the system safe.

Step 1: Open Windows Firewall Advanced Settings

Press **Win + R**, type **wf.msc**, and hit Enter, This opens Windows Defender Firewall with Advanced Security.



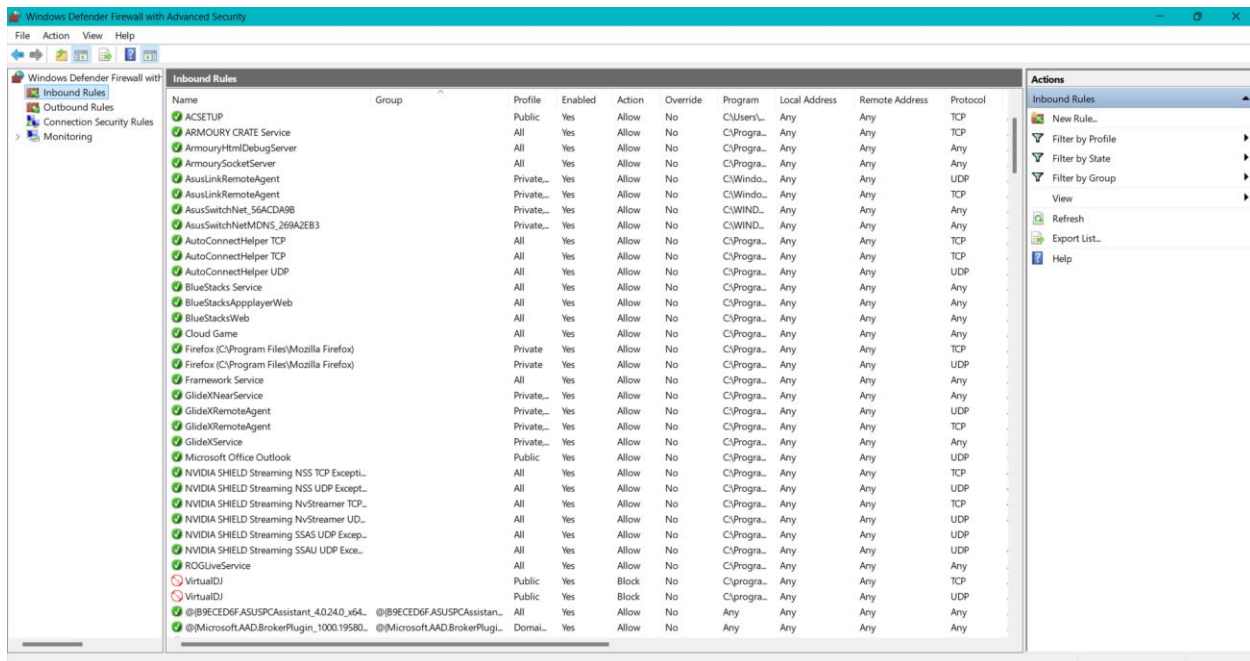
This opens Windows Defender Firewall with Advanced Security.



Step 2: View Current Firewall Rules

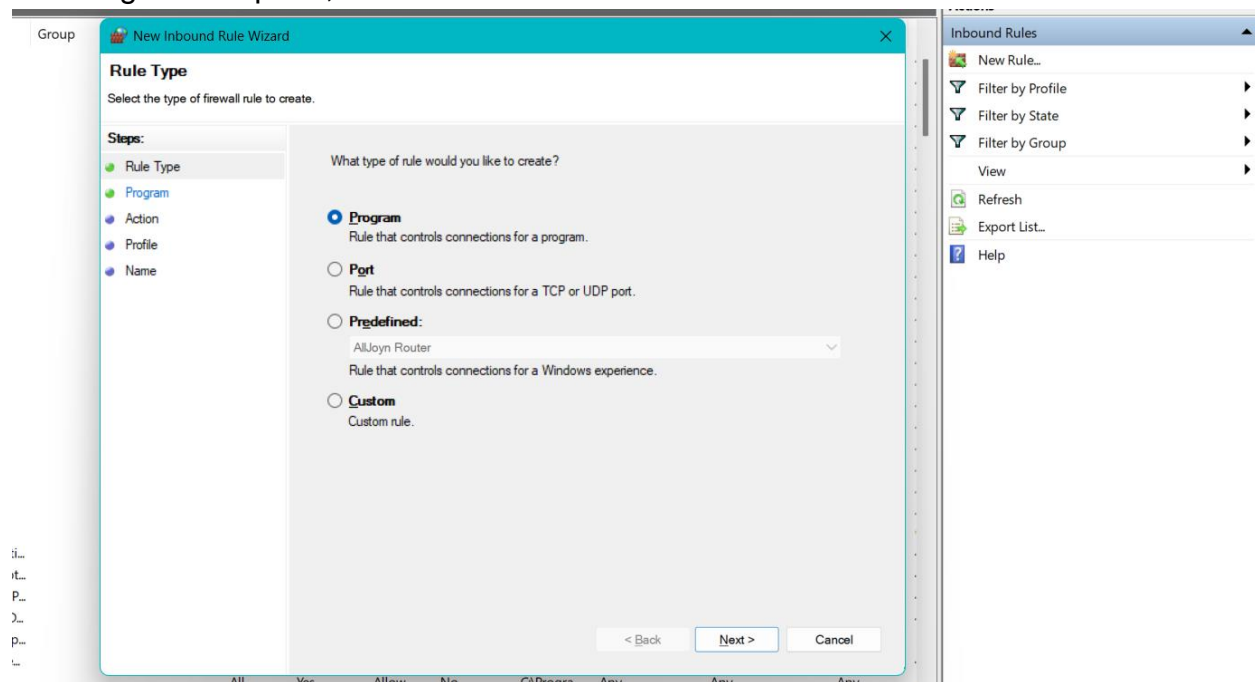
On the left, click "Inbound Rules" to view existing rules.

Scroll through to see current port rules like Remote Desktop, File Sharing ,etc..

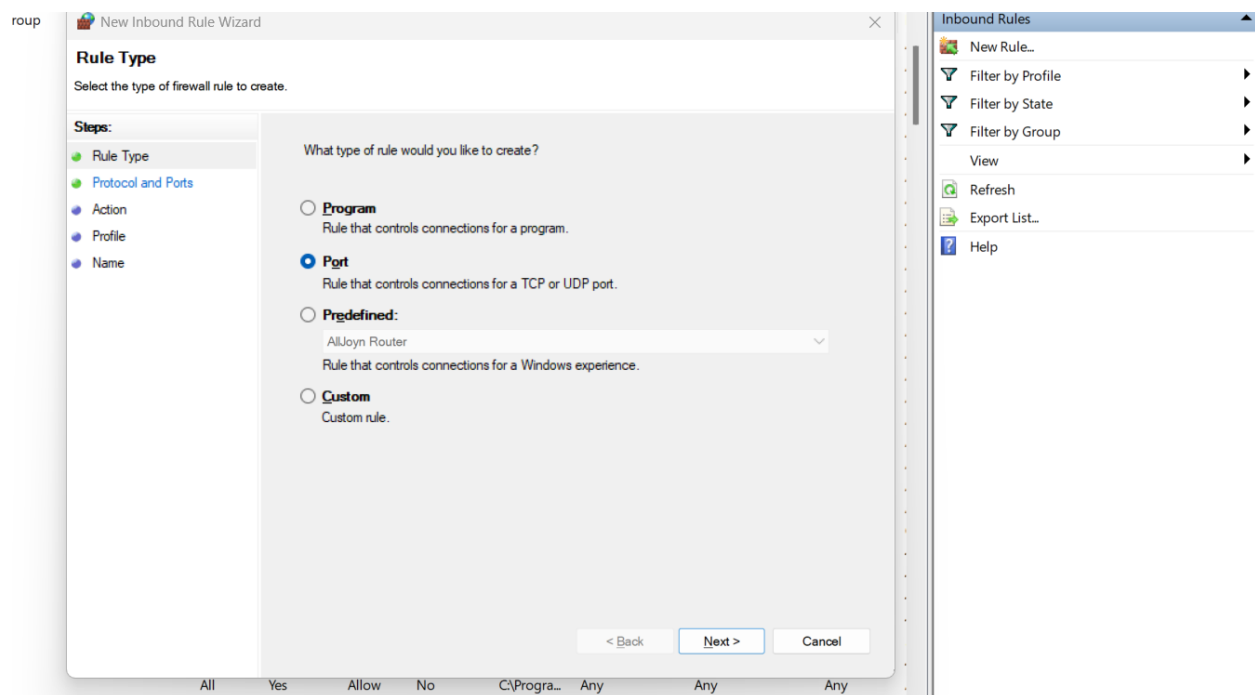


Step 3: Block Inbound Traffic on Port 23 (Telnet)

In the right-hand pane, click "New Rule..."



Select **Port** → Click **Next**.



Select TCP and enter 23 in the “specific local ports” field → Click **Next**

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP

☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

Choose **Block the connection** → Next.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP

☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

Apply it to **Domain, Private, and Public** → Next.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

Name the rule something like **Block Telnet Port 23.**

Steps:














- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
Block Telnet Port 23.

Description (optional):

< Back Finish Cancel

Click **Finish.**

Actions	
Inbound Rules	▲
 New Rule...	
 Filter by Profile	▶
 Filter by State	▶
 Filter by Group	▶
View	▶
 Refresh	
 Export List...	
 Help	
Block Telnet Port 23.	▲
 Disable Rule	
 Cut	
 Copy	
 Delete	
 Properties	
 Help	

Step 4: Test the Rule (Optional but Recommended)

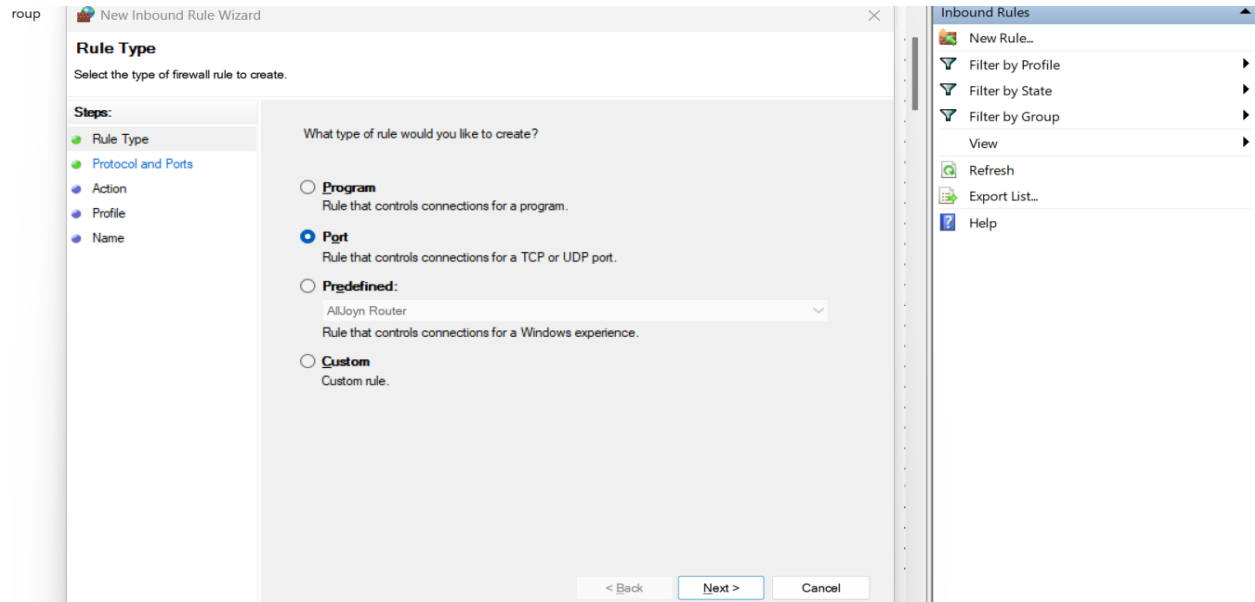
Open Command Prompt, Type **telnet localhost 23**

If it says "Connecting to localhost..." followed by a failure, the rule works.

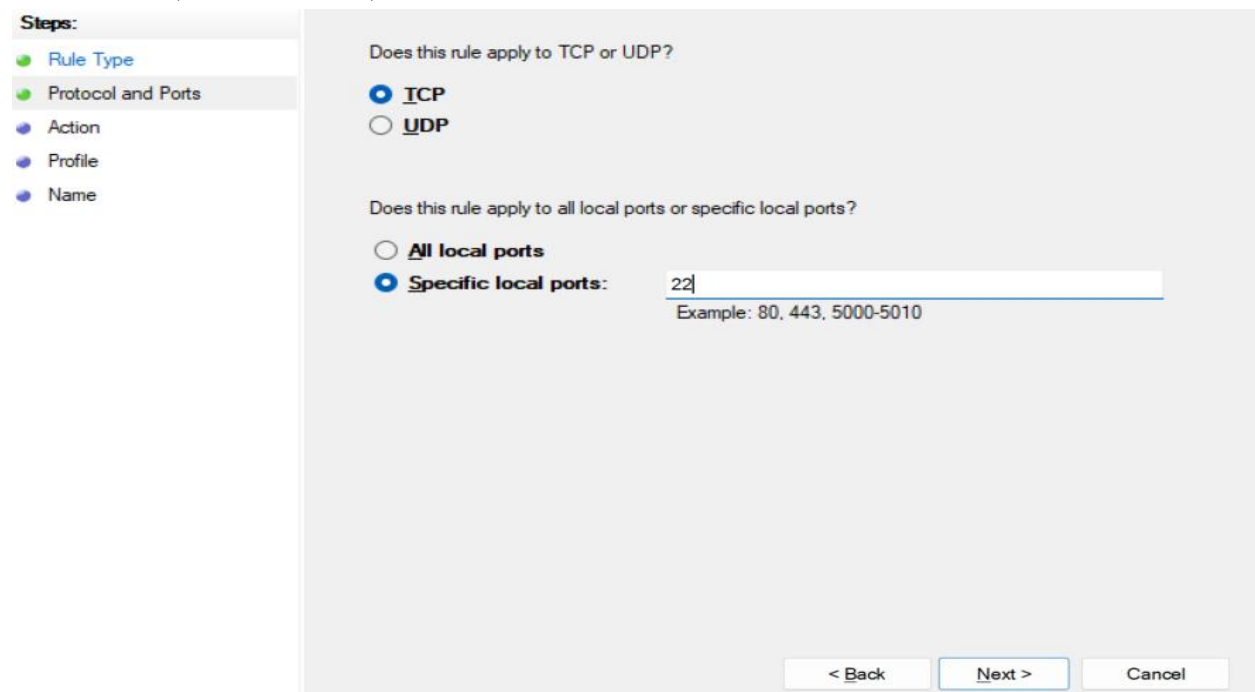
```
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed
```

Step 5: Allow Port 22 (SSH) Rule

Create a new inbound rule like before.



Select **Port**, choose **TCP**, and enter **22**.



Choose "**Allow the connection**".

● Rule Type
● Protocol and Ports
● Action
● Profile
● Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

< Back Next > Cancel

Apply to all profiles.

Steps:

● Rule Type
● Protocol and Ports
● Action
● Profile
● Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

Name it **Allow SSH Port 22**.

Name:

SSH Port 22.

Description (optional):

|

Click Finish.



Step 6: Remove the Block Rule

Go to Inbound Rules, Find your **Block Telnet Port 23** rule.

Inbound Rules									
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
✓ SSH Port 22.		All	Yes	Allow	No	Any	Any	Any	TCP
✗ Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any	TCP
✓ 360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
✓ 360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP

Right-click → Click **Delete**.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
SSH Port 22.		All	Yes	Allow	No	Any	Any	Any	TCP
Block Telnet Port 23		All	Yes	Block	No	Any	Any	Any	TCP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
360TsLiveUpd.exe		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
360TsLiveUpd.exe		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AacAmbientLighting		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
AacAmbientLightingLowercase		All	Yes	Allow	No	C:\progra...	Any	Any	Any
ACSETUP		Public	Yes	Allow	No	C:\Users\...	Any	Any	TCP

Disable Rule
Cut
Copy
Delete
Properties
Help

DELETED

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
SSH Port 22.		All	Yes	Allow	No	Any	Any	Any	TCP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
360 Total Security		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
360TsLiveUpd.exe		Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
360TsLiveUpd.exe		Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AacAmbientLighting		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
AacAmbientLightingLowercase		All	Yes	Allow	No	C:\progra...	Any	Any	Any
ACSETUP		Public	Yes	Allow	No	C:\Users\...	Any	Any	TCP
ACSETUP		Public	Yes	Allow	No	C:\Users\...	Any	Any	UDP
ARMOURY CRATE Service		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
ArmouryHtmlDebugServer		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
ArmourySocketServer		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
AsusLinkRemoteAgent		Private...	Yes	Allow	No	C:\Windo...	Any	Any	UDP
AsusLinkRemoteAgent		Private...	Yes	Allow	No	C:\Windo...	Any	Any	TCP
AsusSwitchNet_56ACDA9B		Private...	Yes	Allow	No	C:\WIND...	Any	Any	Any
AsusSwitchNetMDNS_269A2EB3		Private...	Yes	Allow	No	C:\WIND...	Any	Any	Any
AutoConnectHelper TCP		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AutoConnectHelper TCP		All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AutoConnectHelper UDP		All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Block Telnet Port 23.		All	Yes	Block	No	Any	Any	Any	TCP
Block Telnet Port 23.		All	Yes	Block	No	Any	Any	Any	TCP
BlueStacks Service		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
BlueStacksAppplayerWeb		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
Cloud Game		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Framework Service		All	Yes	Allow	No	C:\Progra...	Any	Any	Any
GlideXNearService		Private...	Yes	Allow	No	C:\Progra...	Any	Any	Any
GlideXRemoteAgent		Private...	Yes	Allow	No	C:\Progra...	Any	Any	UDP
GlideXRemoteAgent		Private...	Yes	Allow	No	C:\Progra...	Any	Any	TCP
GlideXService		Private...	Yes	Allow	No	C:\Progra...	Any	Any	Any