

# CYBER SECURITY INTERNSHIP - TASK 4

## Task Title: Set Up and Use a Firewall on Windows

**Objective:** Set up and test default firewall rules for allowing or blocking traffic by using Windows Defender Firewall.

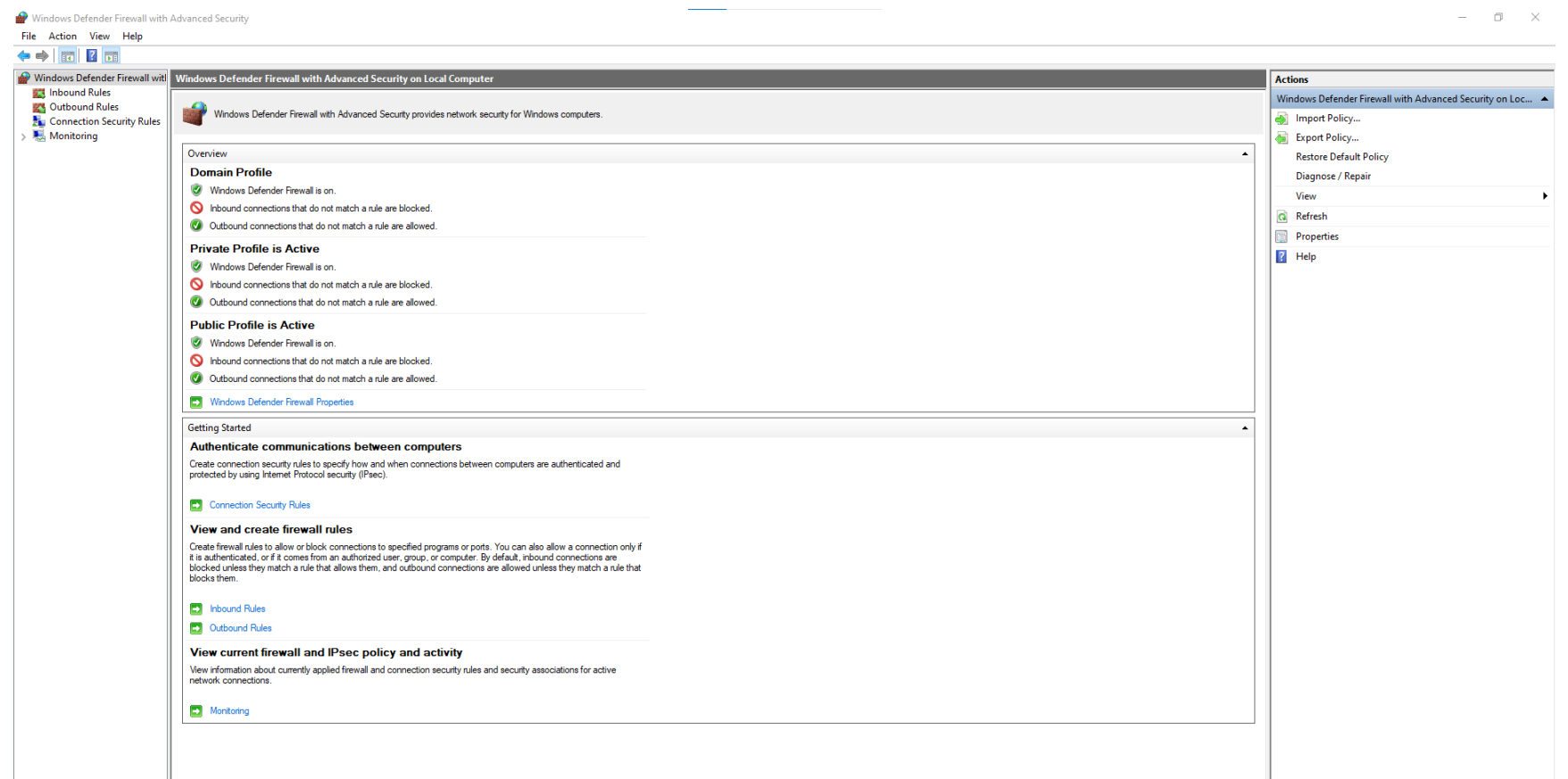
**Tool Used:** Windows Defender Firewall with Advanced Security

Here’s what I did :

### Step 1: Open Firewall Configuration Tool

Visited Windows Defender Firewall > Advanced Settings.

Opened "Inbound Rules" section to handle traffic.



Screenshot 1: Windows Firewall Advanced Settings main window.

### Step 2: List Current Firewall Rules

Reviewed system default inbound rules already installed on the system.

Windows Defender Firewall with Advanced Security

FileActionViewHelp

Windows Defender Firewall with Advanced Security

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc
Bitdefender Network OS Helper Process		All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	67	68	Any	Any
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any
BlueStacksAppplayerWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any
Cloud Game		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any	UDP	53	Any	Any	Any
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any	UDP	53	Any	Any	Any
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any	UDP	53	Any	Any	Any
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any	TCP	53	Any	Any	Any
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any	TCP	53	Any	Any	Any
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any	TCP	53	Any	Any	Any
PixelSee		All	Yes	Allow	No	C:\Users\...	Any	Any	Any	Any	Any	Any	Any
@FirewallAPI.dll - 80201	@FirewallAPI.dll - 80200	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	554, 8554-...	Any	Any	Any
@FirewallAPI.dll - 80206	@FirewallAPI.dll - 80200	All	Yes	Allow	No	%System...	Any	Local subnet	UDP	5000-5020	Any	Any	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	9955	Any	Any	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any
App Installer	App Installer	Domai...	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any	Any
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP	3702	Any	Any	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any	Any
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any	Any
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any	UDP	PlayTo Dis...	Any	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local subnet	TCP	10246	Any	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Any	TCP	10246	Any	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	10246	Any	Any	Any
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	TCP	23554, 235...	Any	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	23554, 235...	Any	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	TCP	23554, 235...	Any	Any	Any
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP	2869	Any	Any	Any
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Connected Devices Platform (TCP-In)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any
Connected Devices Platform (UDP-In)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547	Any	Any
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any	Any
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any	Any	Any

Screenshot 2: Default inbound rules list.

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

Added a new inbound rule:

Type: Port

Protocol: TCP

Port: 23

Action: Block the connection

Profile: Domain, Private, Public

Name: "Block Telnet"

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:

Block Telnet

Description (optional):

< Back

Finish

Cancel

Screenshot 3: Port 23 blocking rule added.

Step 4: Add Rule to Allow SSH (Port 22)

Added another inbound rule:

Type: Port

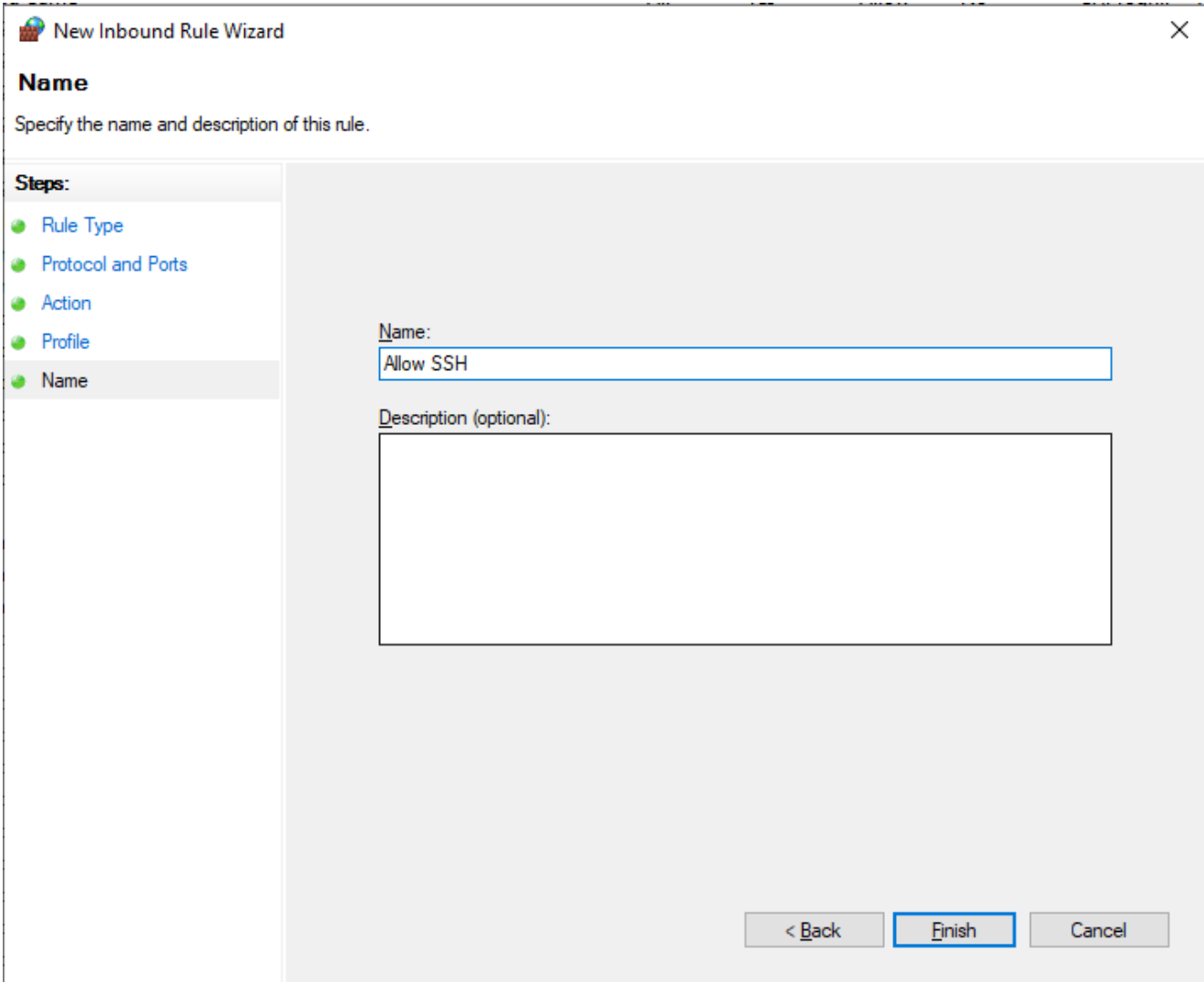
Protocol: TCP

Port: 22

Action: Allow the connection

Profile: Domain, Private, Public

Name: "Allow SSH"



Screenshot 4: New rule for port 22 added.

Inbound Rules													
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc ^
Allow SSH		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any	Any	Any
Block Telnet		All	Yes	Block	No	Any	Any	Any	TCP	23	Any	Any	Any
Bitdefender Network OS Helper Process		All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	67	68	Any	Any

Screenshot 5: Rules list showing both Telnet block and SSH allow

Step 5: Delete the Telnet Rule

Deleted the previously made "Block Telnet" rule to return original state of firewall.

Inbound Rules														Action
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc	
Allow SSH		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any	Any	Any	
Block Telnet		All	Yes	Block	No	Any	Any	Any	TCP	23	Any	Any	Any	
Bitdefender Network OS Helper Process		All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	67	68	Any	Any	
BlueStacks Service		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any	
BlueStacksAppplayerWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any	
BlueStacksWeb		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any	
Cloud Game		All	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any	Any	Any	
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any	UDP	53	Any	Any	Any	
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any	UDP	53	Any	Any	Any	
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any	UDP	53	Any	Any	Any	
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any	TCP	53	Any	Any	Any	
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any	TCP	53	Any	Any	Any	
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any	TCP	53	Any	Any	Any	
PixelSee		All	Yes	Allow	No	C:\Users\...	Any	Any	Any	Any	Any	Any	Any	
@FirewallAPI.dll, -80201	@FirewallAPI.dll, -80200	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	554, 8554-...	Any	Any	Any	
@FirewallAPI.dll, -80206	@FirewallAPI.dll, -80200	All	Yes	Allow	No	%System...	Any	Local subnet	UDP	5000-5020	Any	Any	Any	
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any	
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any	
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	Any	Any	Any	Any	
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	Any	Any	Any	Any	
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No				TCP	9955	Any	Any	Any	
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No				UDP	Any	Any	Any	Any	
App Installer	App Installer	Domai...	Yes	Allow	No				Any	Any	Any	Any	Any	
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No				TCP	80	Any	Any	Any	
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No				TCP	80, 443	Any	Any	Any	
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No				UDP	3702	Any	Any	Any	
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any	Any	
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any	Any	
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any	UDP	PlayTo Dis...	Any	Any	Any	

Windows Defender Firewall with Advanced Security

Are you sure you want to delete these rules?

YesNo

Screenshot 6: Confirmation of rule deletion.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc
Allow SSH		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any	Any	Any
Bitdefender Network OS Helper Process		All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	67	68	Any	Any

Screenshot 7: after deletion of telnet rule.

### Summary

This activity taught me how to set up inbound traffic rules in the Windows Firewall with GUI tools. I blocked Telnet, which is insecure and obsolete, and opened SSH, a secure remote access protocol. These rules were added successfully, confirmed, and then reset to the original system configuration.