Task 4 – Setup and Use a Firewall (Windows)

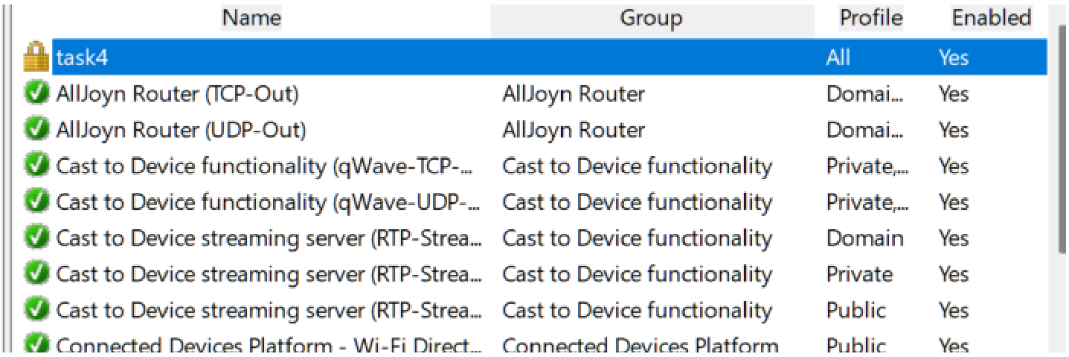
Objective: Configure and test basic firewall rules to allow or block traffic using Windows Defender Firewall with Advanced Security.

Tool Used	Windows Defender Firewall with Advanced Security
OS	Windows 10/11
Firewall Type	Stateful Packet Filtering
Date	2025-08-08

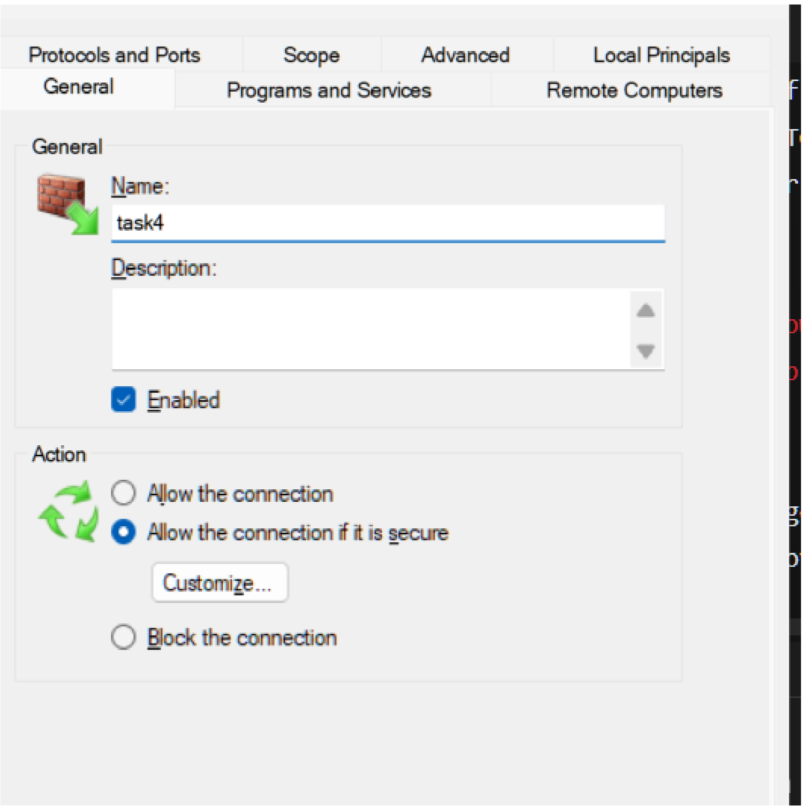
Execution Steps

1. Opened Windows Defender Firewall with Advanced Security using `wf.msc`.
2. Navigated to Inbound Rules to create a new firewall rule.
3. Named the rule **task4** for tracking purposes.
4. Configured the rule to allow the connection only if it is secure.
5. Set Protocol to **TCP** and applied it to **All Local Ports** with remote port set to **118**.
6. Saved and enabled the rule.
7. Verified the rule in the firewall rules list.

Screenshots



Name	Group	Profile	Enabled
task4		All	Yes
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes



General

Name: task4

Description:

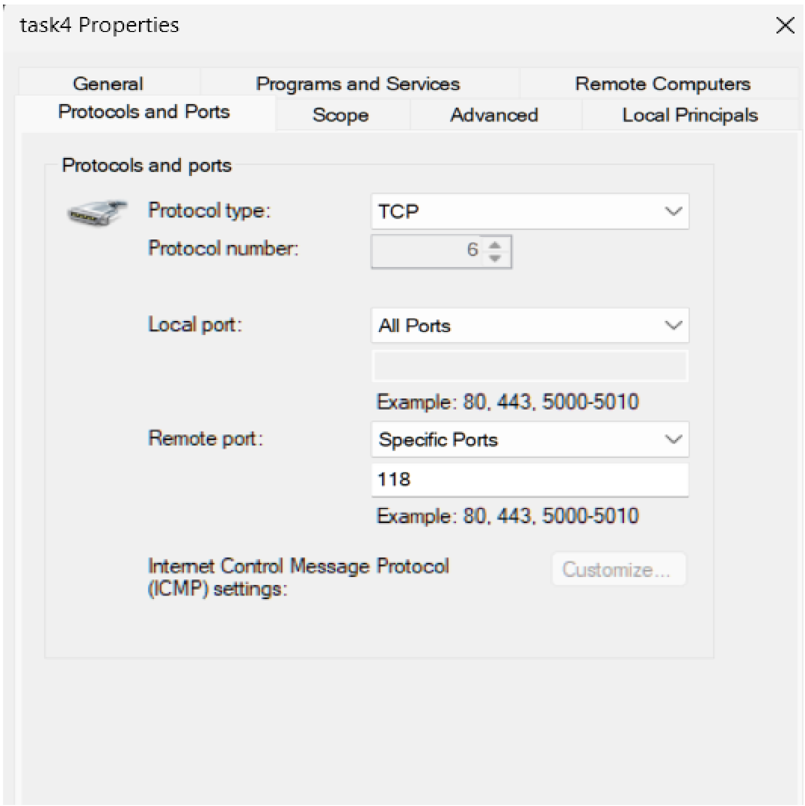
☑ Enabled

Action

○ Allow the connection

● Allow the connection if it is secure

○ Block the connection


task4 Properties

Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: Specific Ports

118

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

Summary

The firewall rule named 'task4' was successfully created and configured to allow secure TCP connections on remote port 118 from any local port. This configuration demonstrates how Windows

Firewall can be used to control network access based on protocol, port, and security requirements. Such rules are vital in reducing the attack surface and ensuring that only authorized, secure connections are permitted.