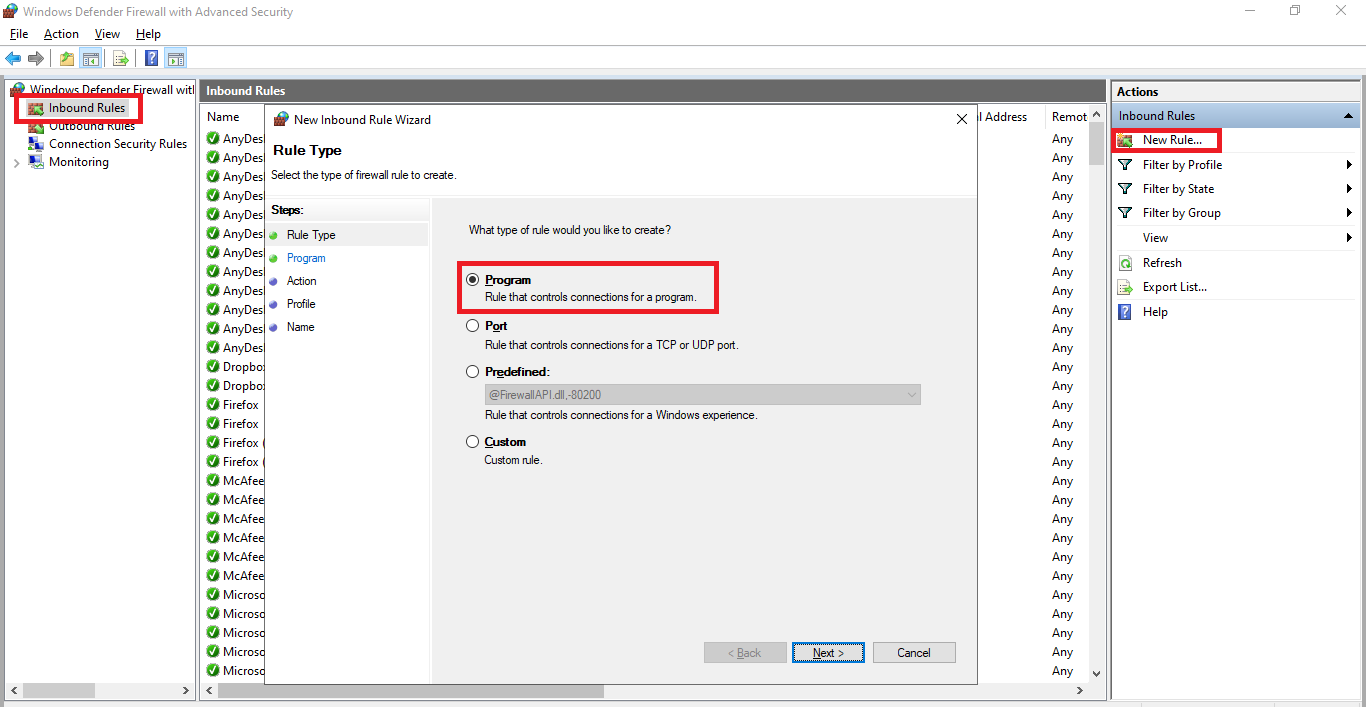
**How to add SQL Server to Windows Firewall Exception**

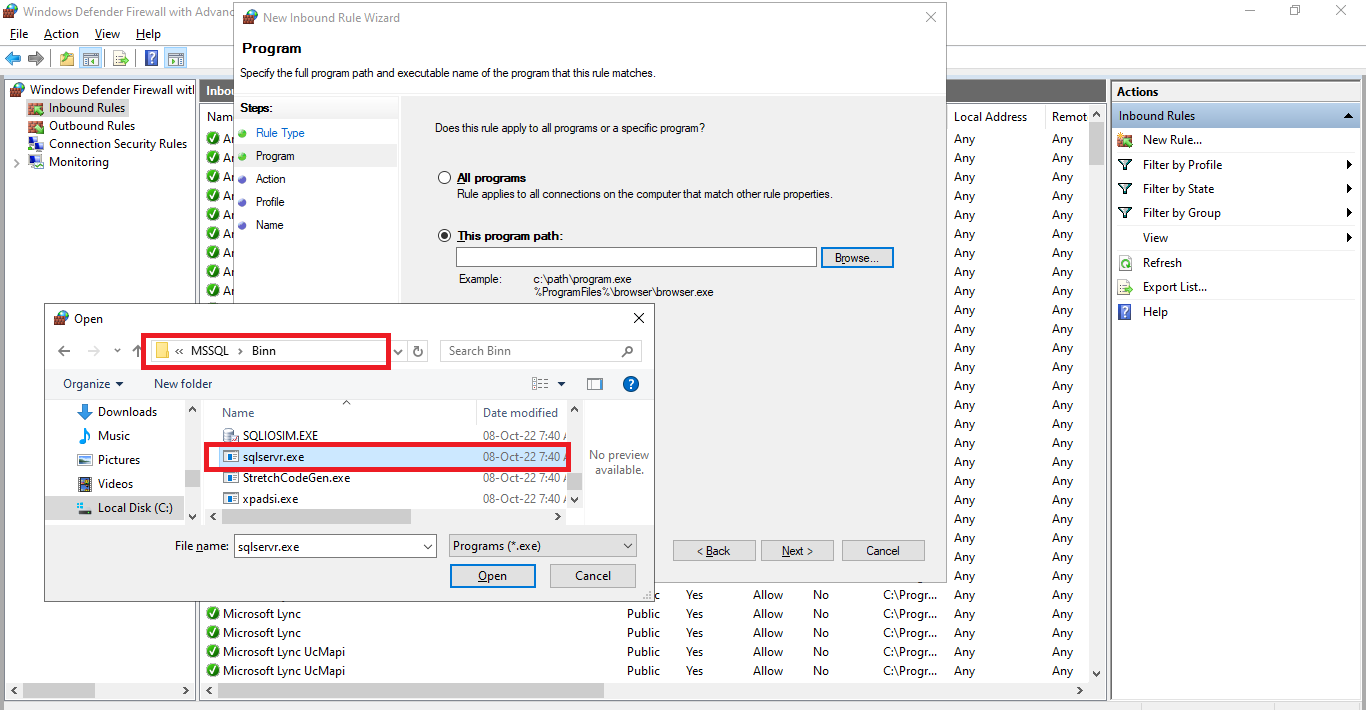
1. Open Windows Defender Firewall with Advance Security. (Using windows key and type).

* **Adding sqlsvr.exe**
  1. Create New Inbound Rule, Select Rule Type as ‘Program’, click on Next button.

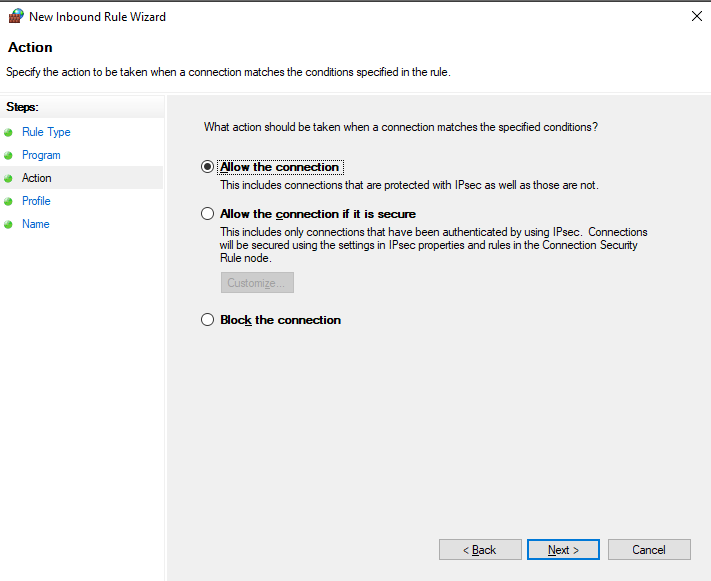


* 1. Click the "Browse" button and then navigate to you SQL Server installation path and click next. I.e:  ‘C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2014\MSSQL\Binn\’

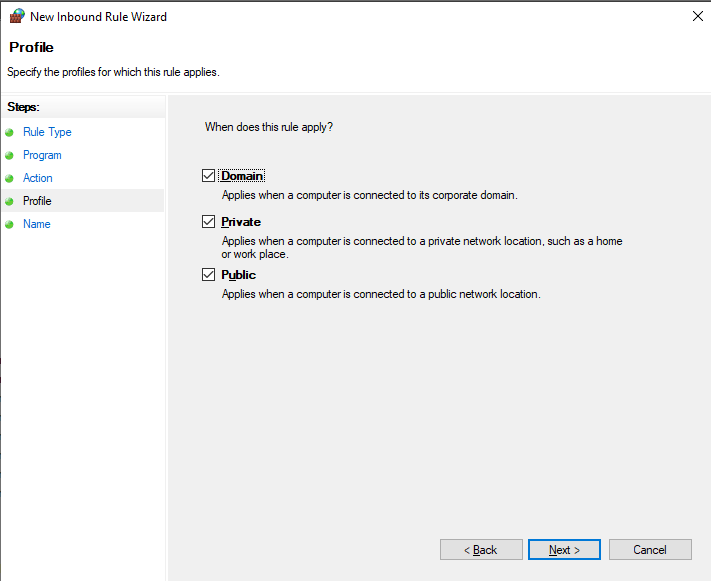
Here, choose the file called sqlservr.exe and add it. The navigate to:



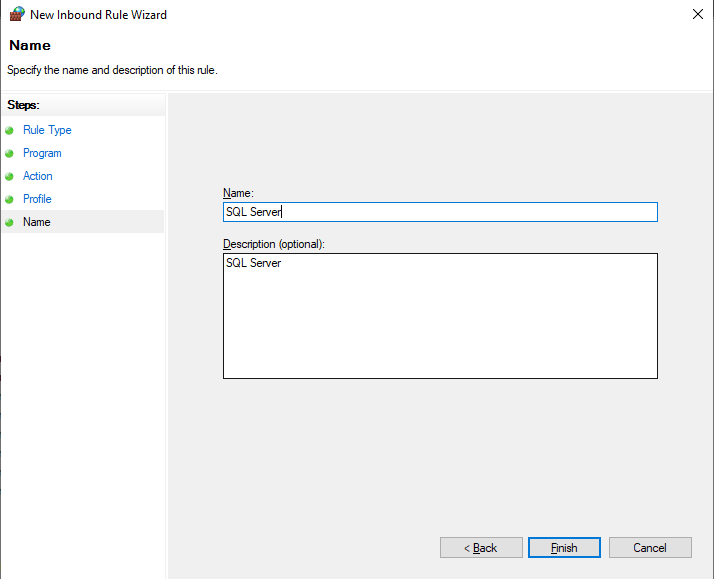
* 1. Allow the connection for Action, click next.



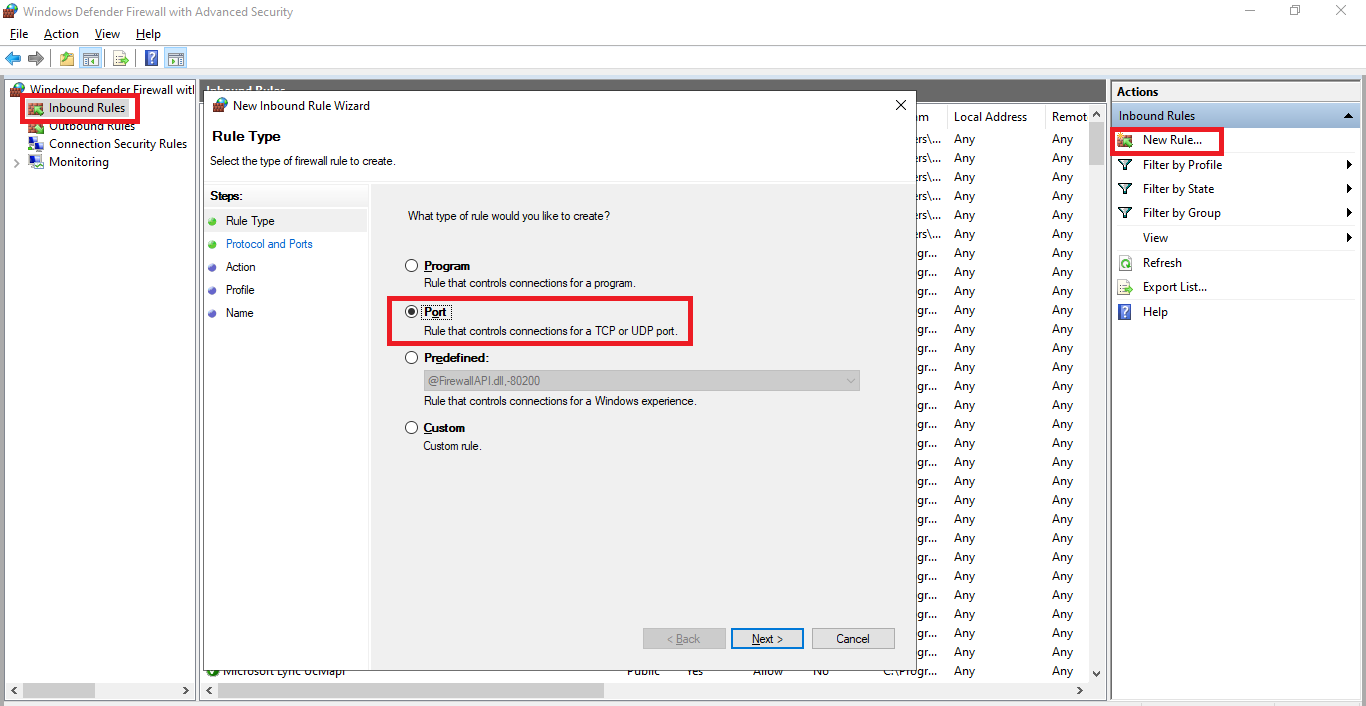
* 1. Specify all the profiles for which the rules applies, click next.



* 1. Give an appropriate name for the rule, click finish.

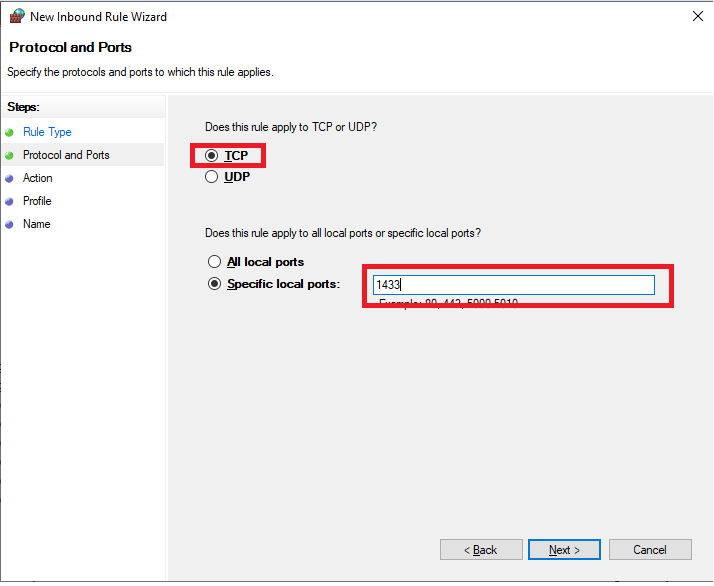


* **Adding Inbound Rules for TCP PORT.**
  1. Create New Inbound Rule, Select Rule Type as ‘Port’, click next button.

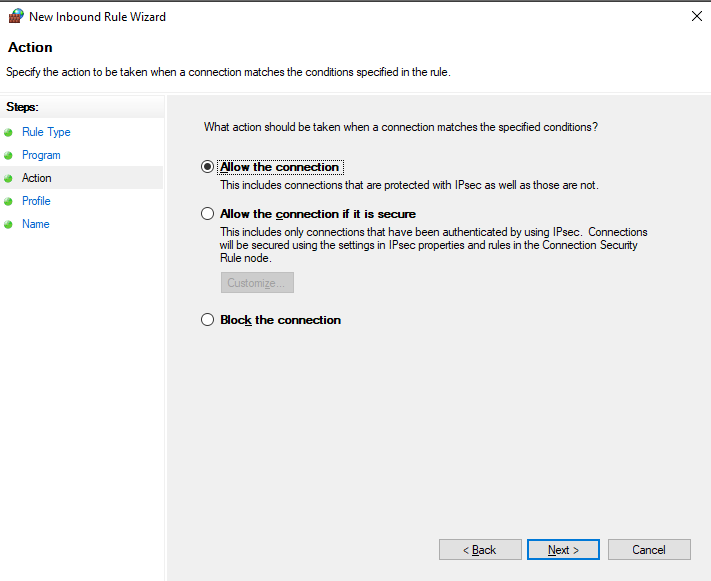


* 1. Select port as ‘TCP’ and Specific local port as ‘1433’, click next.

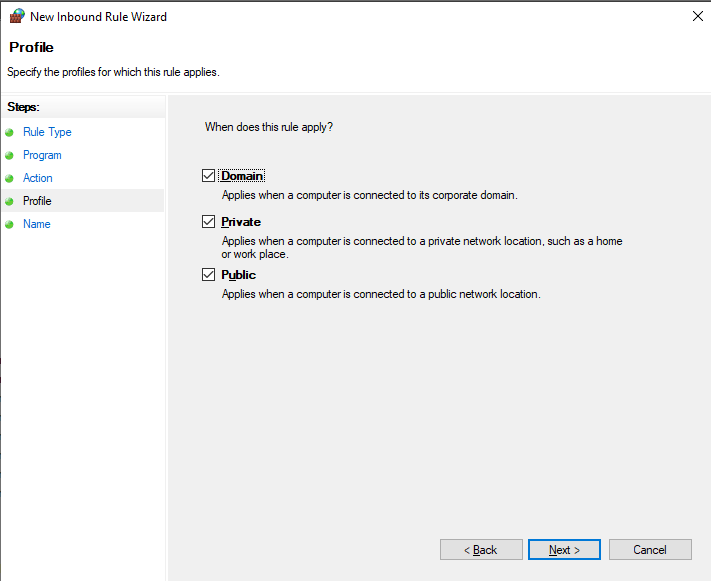
(Generally local ports ‘1433' will be the same in most cases. If it is not same then it should require to check in the sql server configuration manager.)



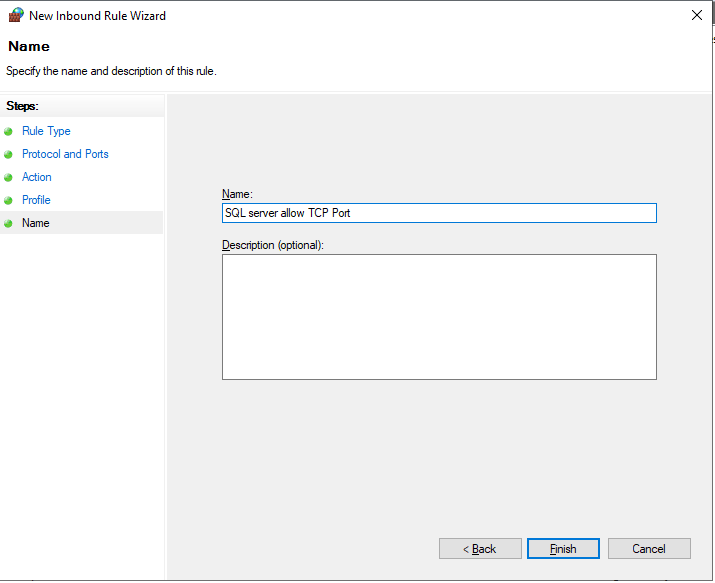
* 1. Allow the connection in Action and click next.



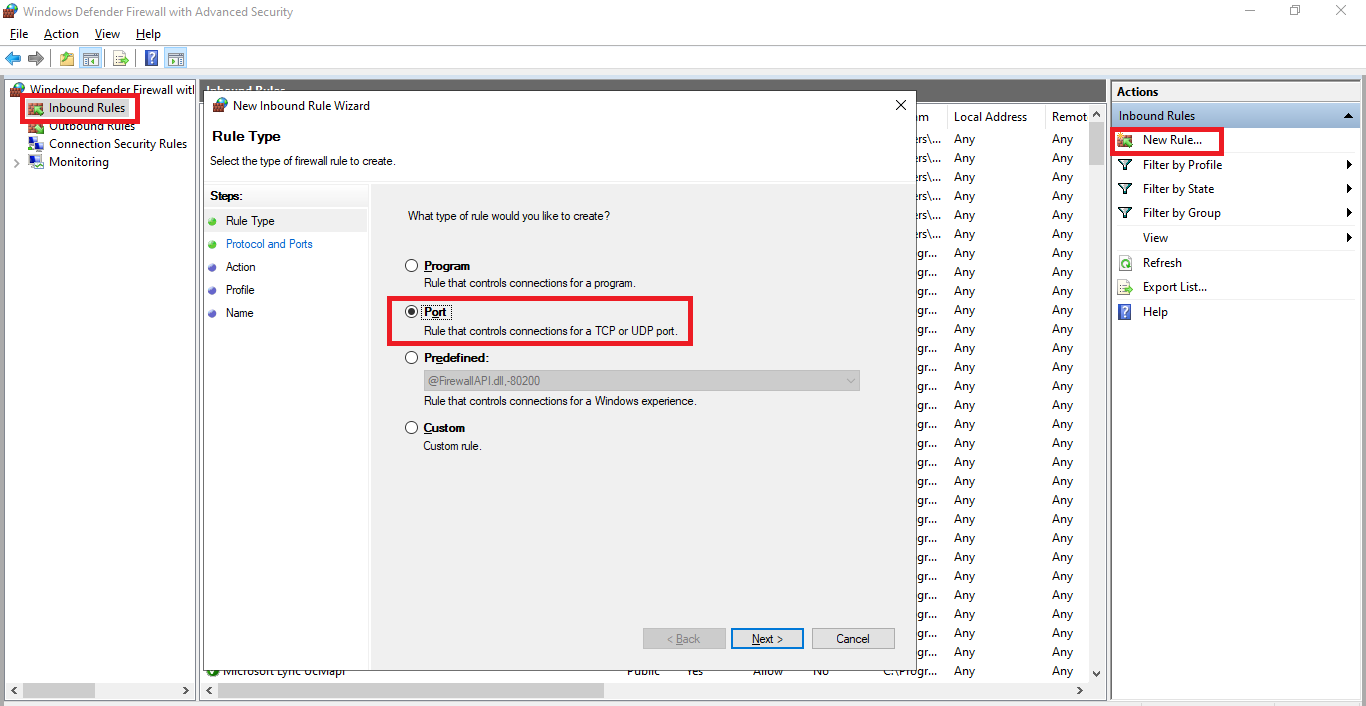
* 1. Specify all the profiles for which the rules applies, click next.



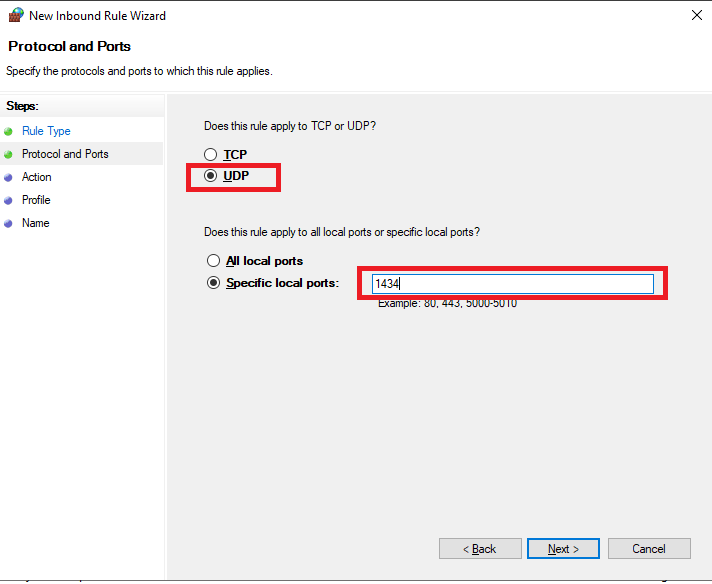
* 1. Give an appropriate name for the rule, click finish.



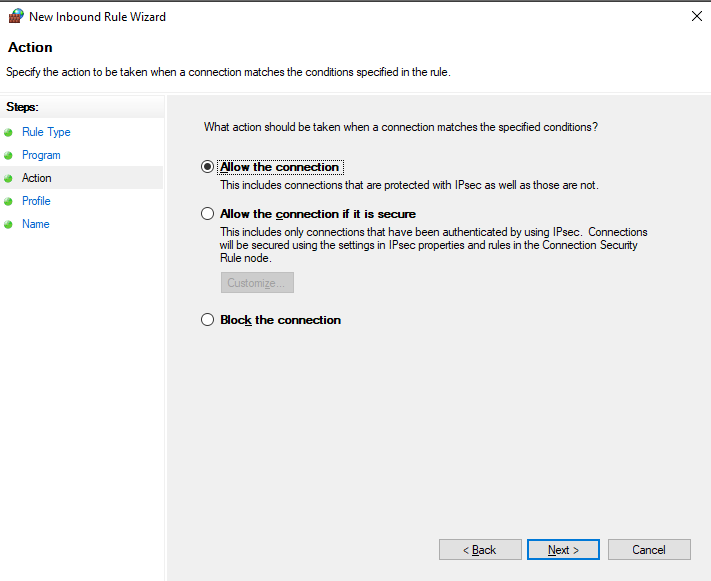
* **Adding Inbound Rules for UDP PORT.**
  1. Create New Inbound Rule, Select Rule Type as ‘Port’, click next button.



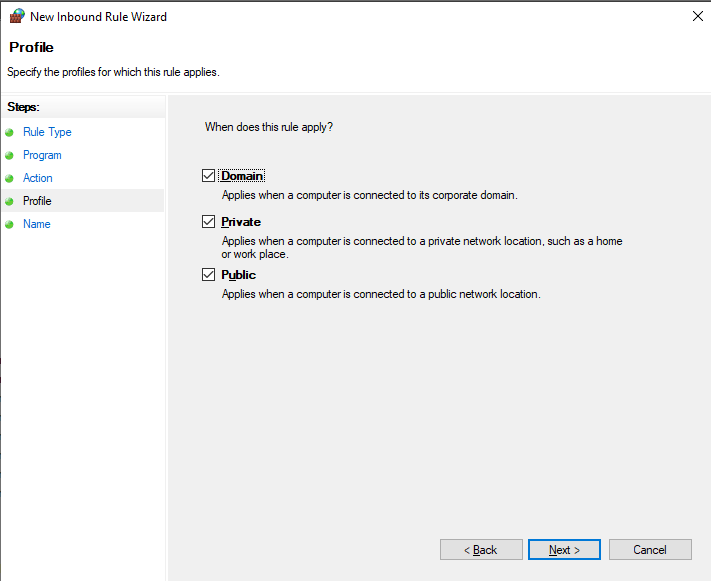
* 1. Select port as ‘UDP’ and Specific local port as ‘1434’, click next.



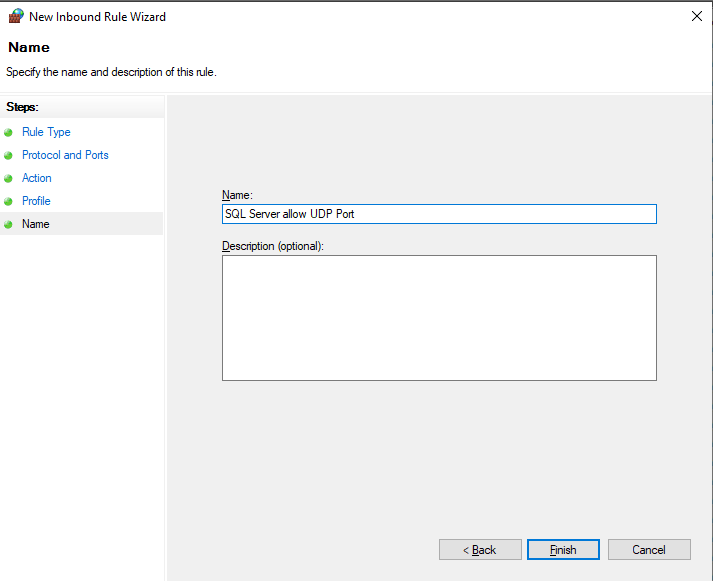
* 1. Allow the connection in Action and click next.



* 1. Specify all the profiles for which the rules applies, click next.



* 1. Give an appropriate name for the rule, click finish.



* Once finished all the settings, test the database connection between the server computer and the client/bridge computer.