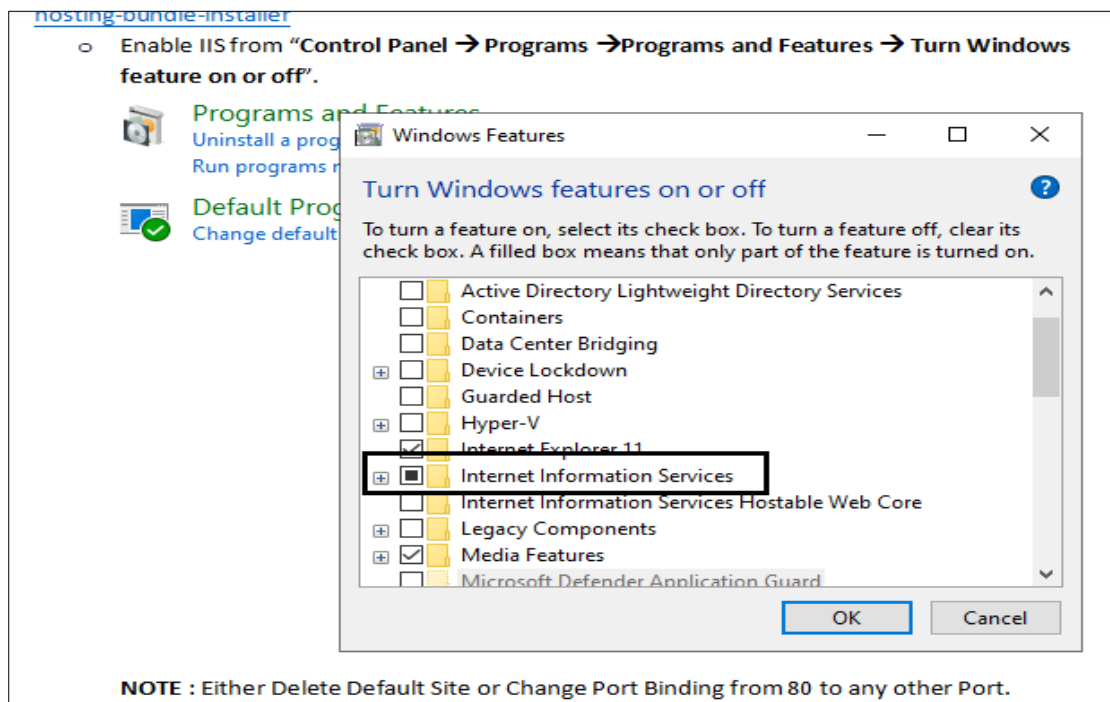


BACKEND SOFTWARE INSTALLATION PROCEDURE FOR MOBIVUE PMMS:-

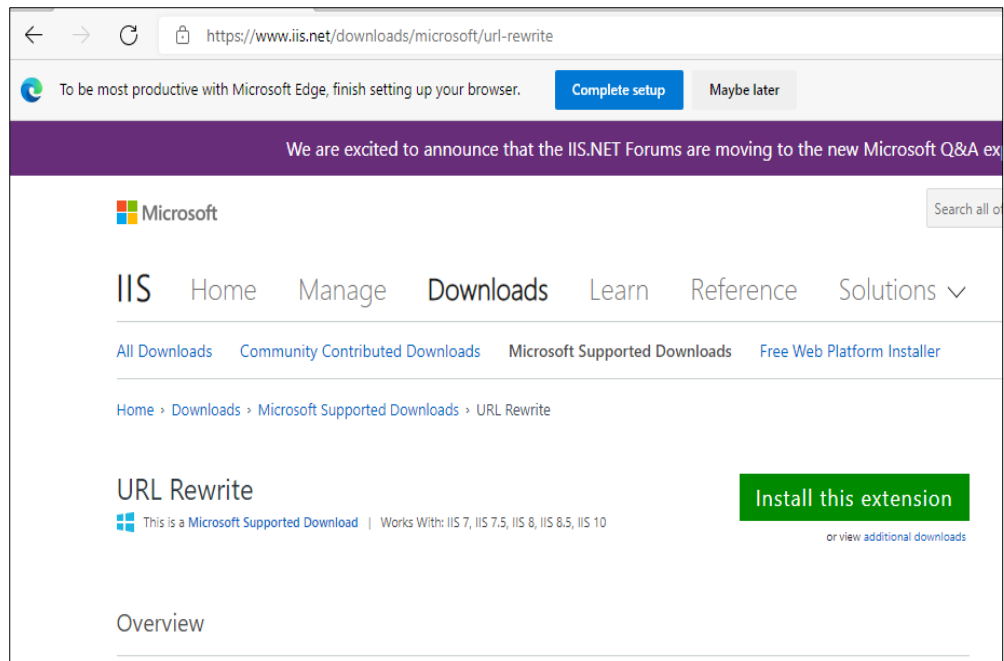
1. Install the .net framework which is compatible to IIS
.Net Core 3.1
2. After this we need to configure the IIS same as follow in the below screen shot



3. "URL Rewrite" IIS extension using below URL:

<https://www.iis.net/downloads/microsoft/url-rewrite>

Annexure No. -I



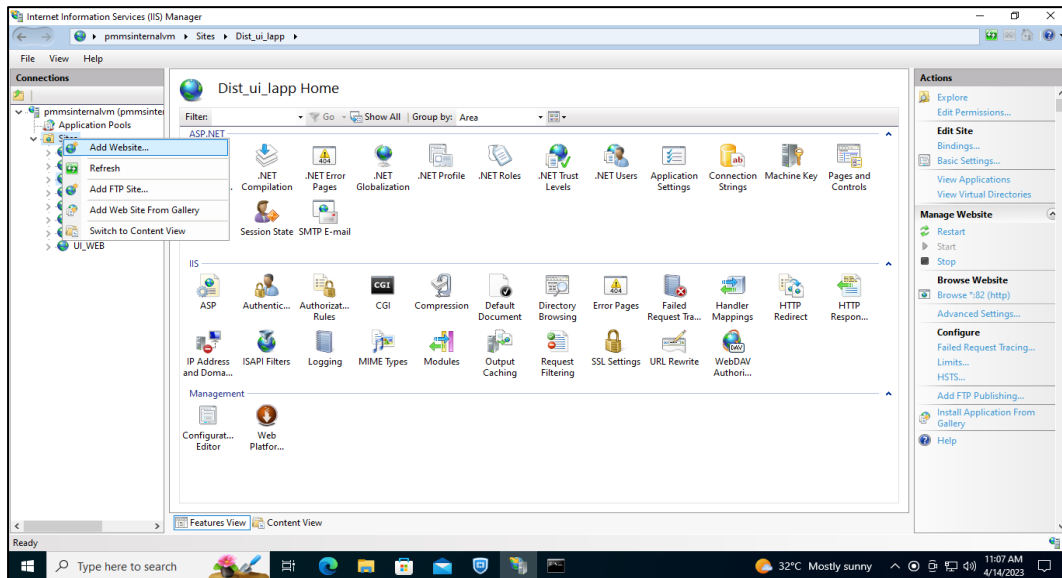
4. Node.js windows installer 64-bit using below URL:

<https://nodejs.org/en/download/>

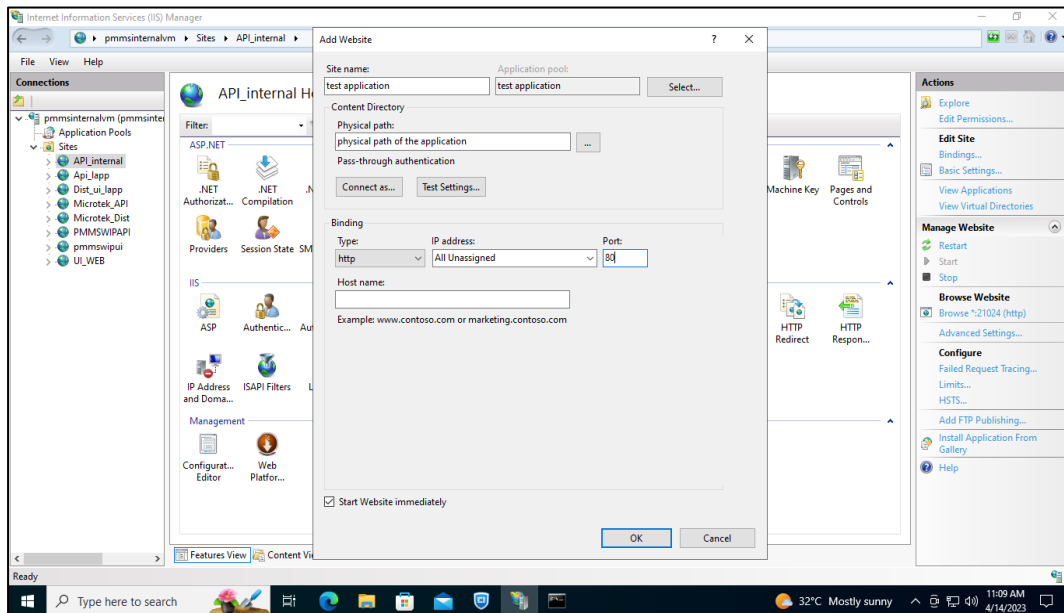
Annexure No. -I

Procedure for application pool/link creation:

1. Hosting an application in IIS (In Ajanta) with IIS version: IIS 10.0 version is the latest version of Internet Information Services (IIS) for Windows Server 2019
2. Creating pools: Right click on the sites it shows add website click on add web site.

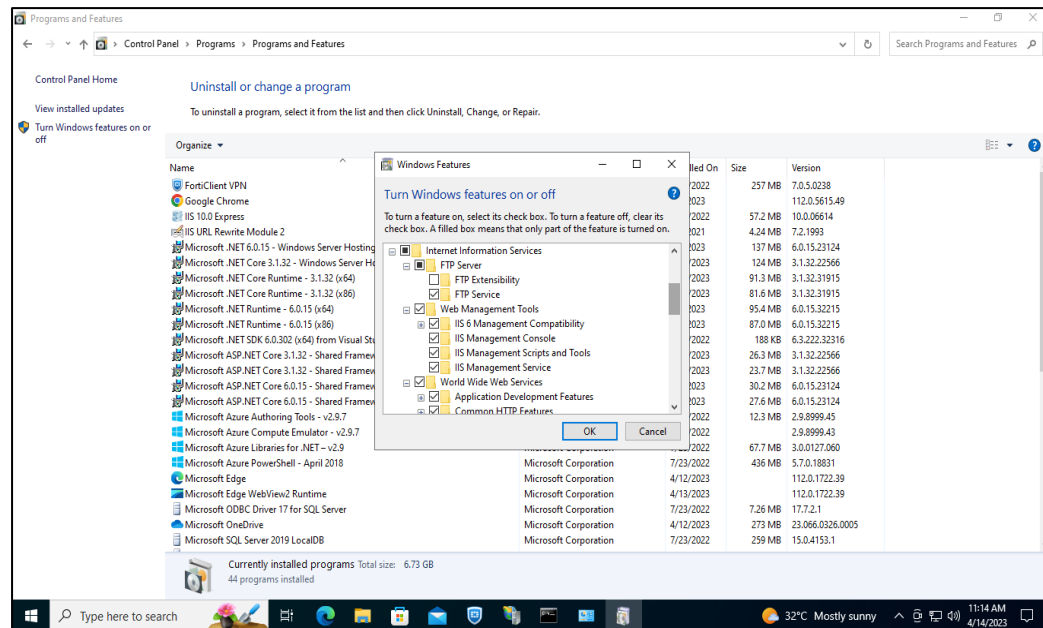


3. Here we add application pool name, Physical path of the application and Assign the port number as well



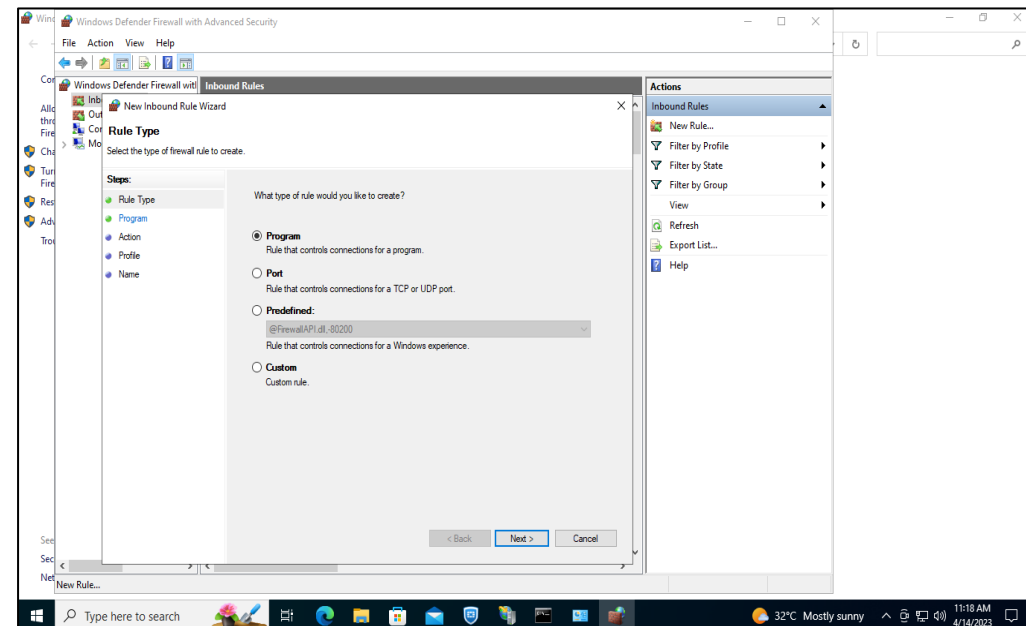
Annexure No. -I

4. Setting basic things in IIS: We should enable all the prerequisites which is shown in the image below.

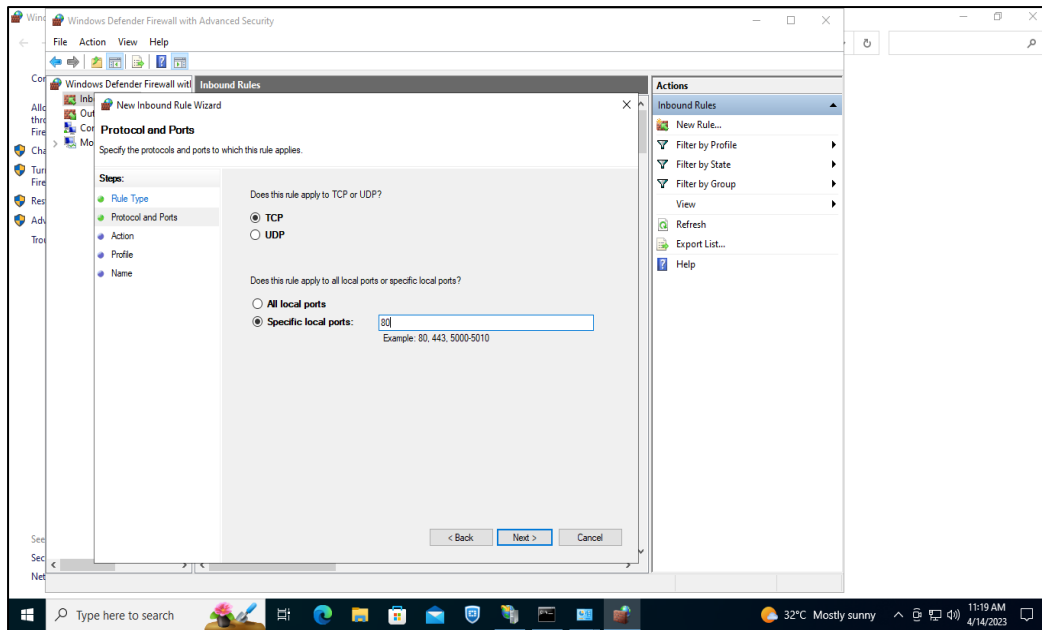


- Setting port if required: In the firewall section of the server go to advanced settings add inbound and outbound rule of the specific port.

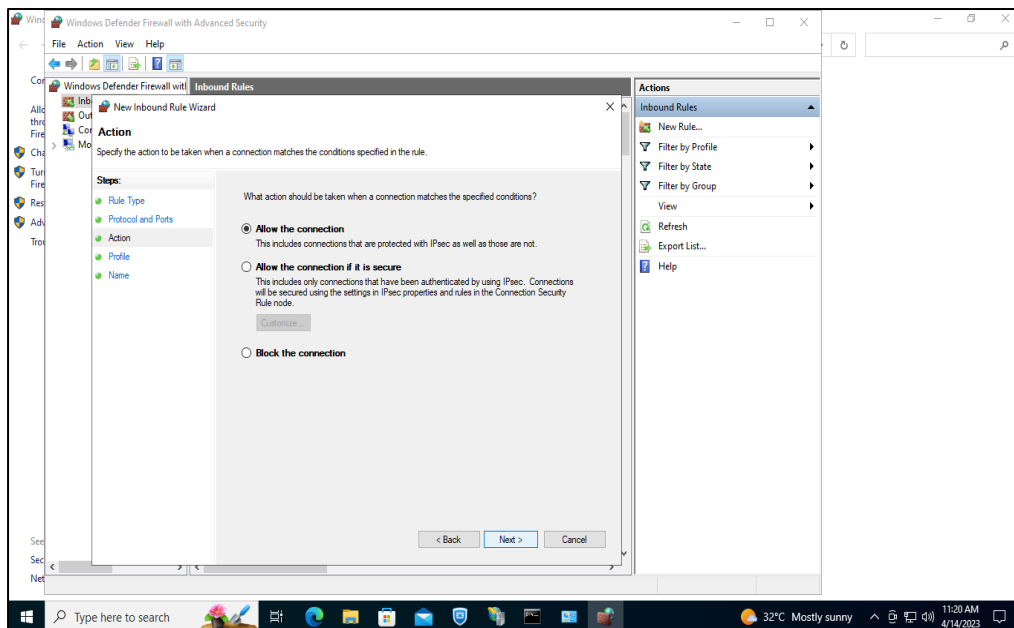
Inbound port:



Annexure No. -I



6. Click on Next



Then finish the setup with default settings.

Outbound rules: This one also same as the inbound port rules.

7. Enable site: We can allow the specific ports which are assigned to the application that port into the DNS entry from Ajanta side then the application browse externally.

Application will **always use API** to make any transaction. The **connection of DB will be in the API**.

There will be a file in APIs called "appsettings.json" where we will give DB connection. The DB should be accessible to the IP where Application is hosted.

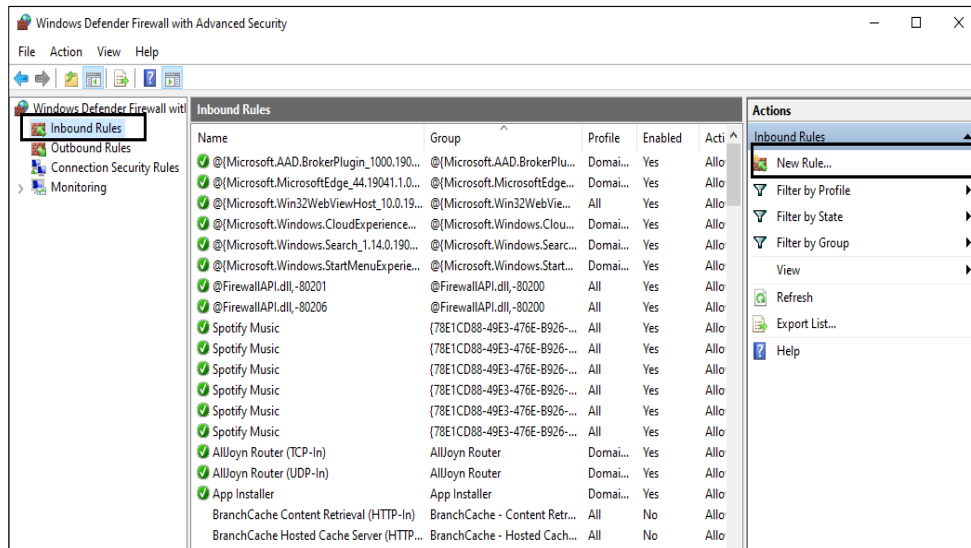
Annexure No. -I

The application will work on the browser of android device. Hence no installation required

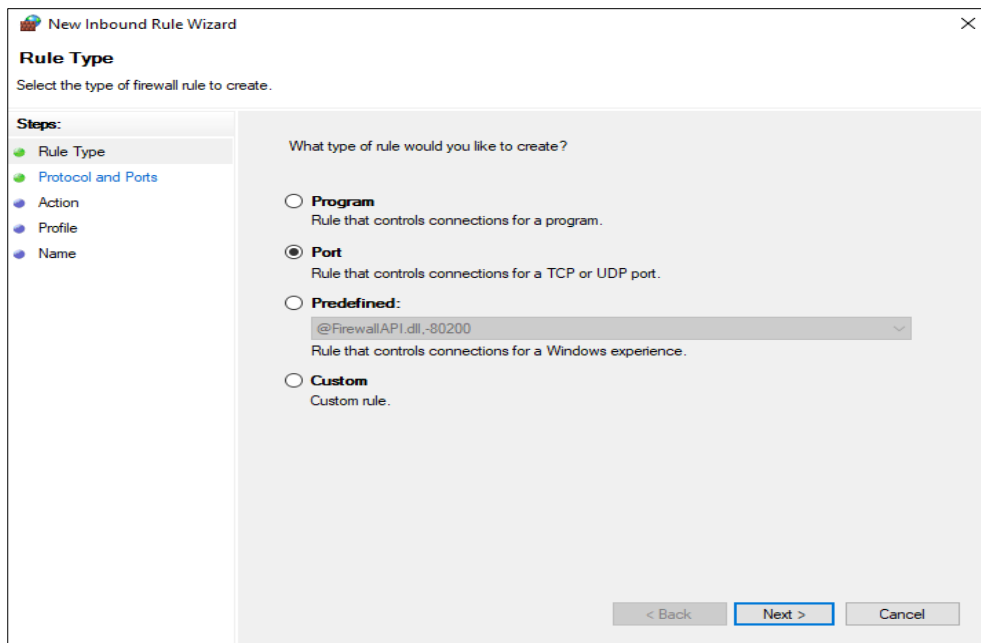
Add Rules in Firewall

1. Add Inbound Rules

a. Navigate to Windows Firewall → Advance Settings

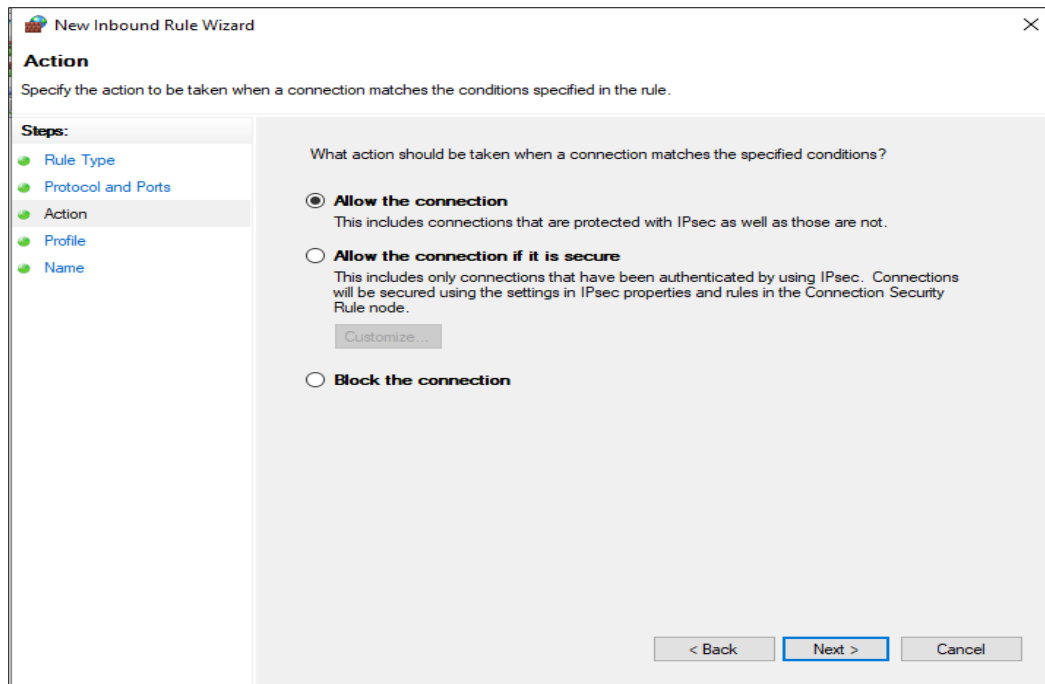


2. Select Port:



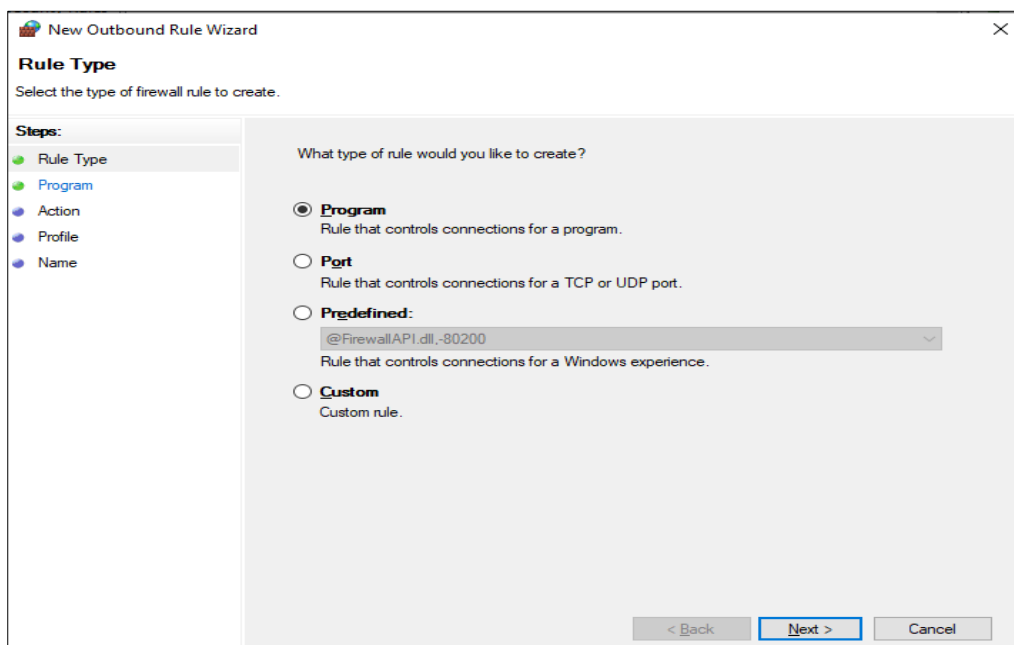
3. Click Next → Select "Allow the Connection" → Click Next

Annexure No. -I



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: '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.' Below this is a 'Customize...' button. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

4. Enter Rule Name "Port_UI_80" and Click Finish.
5. Repeat Add InBound Rules Steps for Port "21021".
6. Add OutBound Rules:
 - a. Navigate to Windows Firewall → Advance Settings
 - b. Select OutBound Rules and Click on Create Rule and Select Port



The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Rule Type' step. The title bar reads 'New Outbound Rule Wizard'. The left sidebar lists the steps: Rule Type (selected), Program, Action, Profile, and Name. The main area asks 'What type of rule would you like to create?'. There are four radio button options: 'Program' (selected), 'Port', 'Predefined:', and 'Custom'. The 'Program' option has a description: 'Rule that controls connections for a program.' The 'Port' option has a description: 'Rule that controls connections for a TCP or UDP port.' The 'Predefined:' option has a dropdown menu showing '@FirewallAPI.dll,-80200' and a description: 'Rule that controls connections for a Windows experience.' The 'Custom' option has a description: 'Custom rule.' At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

Annexure No. -I

c. Enter Specific port as “80” → Next

The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP. The second question is 'Does this rule apply to all remote ports or specific remote ports?' with radio buttons for All remote ports and Specific remote ports (selected). A text box next to 'Specific remote ports' contains the value '80'. Below the text box is an example: 'Example: 80, 443, 5000-5010'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted), and 'Cancel'.

d. ==> Select Allow the connection → Click Next → Click Next

The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: '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.' and a 'Customize...' button. At the bottom right are three buttons: '< Back', 'Next >' (highlighted), and 'Cancel'.