how do I ensure that the firewall on the host machine allows that will inbound traffic on the port I've exposed.

To ensure that your host machine's firewall allows inbound traffic on the port you've exposed, you need to configure firewall rules to permit access to that port. Here's how you can do it depending on your operating system:

For Windows:

1. **Open Windows Defender Firewall**:
    - Press Win + R, type control, and hit Enter.
    - Select **Windows Defender Firewall**.
2. **Allow an App or Feature Through Windows Firewall**:
    - On the left sidebar, click **Allow an app or feature through Windows Defender Firewall**.
    - Scroll through the list and check if **Docker** is already allowed for **Private** and **Public** networks. If not, follow the next steps.
3. **Create a New Inbound Rule**:
    - In the left sidebar, click **Advanced settings**. This will open **Windows Defender Firewall with Advanced Security**.
    - On the left, click **Inbound Rules**, then on the right side, click **New Rule**.
4. **Configure the Rule**:
    - Choose **Port** and click **Next**.
    - Select **TCP** (since most web traffic uses TCP) and specify the port you're exposing (e.g., 80). Click **Next**.
    - Choose **Allow the connection**.
    - Ensure the rule applies to **Private** networks (assuming you're on a trusted home or work Wi-Fi) and click **Next**.
    - Give the rule a name (e.g., "Docker Website Port 80") and click **Finish**.
5. **Test the Connection**: Once the rule is created, test the connection by accessing the website from another machine on the network.

For macOS:

1. **Open Firewall Settings**:
    - Go to **System Preferences** > **Security & Privacy** > **Firewall**.
    - If the firewall is turned off, you don’t need to configure anything. If it's on, click the **Firewall Options** button.
2. **Add Docker or the Port**:
    - Click the **+** button to add an application or a port exception.
    - Select **Docker** (if visible) or manually add the application hosting the Docker container.

- Alternatively, you can create a specific port rule using pfctl, but the GUI method is simpler for most users.

3. **Test the Connection**: After making these changes, test the connection from another machine.

For Linux (Using iptables):

1. **Check if ufw (Uncomplicated Firewall) is Active**:
    - Run the following command in a terminal:

bash

Copy code

sudo ufw status

    - If the firewall is active, proceed with the following steps.

2. **Allow Traffic on the Specific Port**:
    - To allow traffic on port 80 (or any other port you've exposed):

bash

Copy code

sudo ufw allow 80/tcp

    - If you're using a non-default port, replace 80 with the appropriate port number.

3. **Reload and Check Status**:
    - Reload the firewall to apply the changes:

bash

sudo ufw reload

    - Then verify the rule has been added:

bash

sudo ufw status

Once the firewall is configured, try accessing the website again from another device on the same LAN. If everything is set up correctly, the connection should go through.