Blocking an IP address on Windows using the Command Prompt involves creating a rule in the Windows Firewall. Here's a step-by-step guide to do this:

Using Command Prompt to Block an IP Address

1. **Open Command Prompt as Administrator:**
   - Press 'Win + S', type 'cmd', and then right-click on "Command Prompt" and select "Run as administrator".

2. **Create a New Firewall Rule to Block the IP Address:**
   - Use the 'netsh' command to create a new rule. The syntax is as follows:

   ```shell
   netsh advfirewall firewall add rule name="Block IP Address" dir=in action=block remoteip=<IP_ADDRESS> enable=yes
   ```

   Replace '<IP_ADDRESS>' with the IP address you want to block. For example, to block the IP address '192.168.1.100', the command would be:

   ```shell
   netsh advfirewall firewall add rule name="Block 192.168.1.100" dir=in action=block remoteip=192.168.1.100 enable=yes
   ```

3. **Verify the New Rule:**
   - To make sure your rule has been added, you can list all the firewall rules using:

   ```shell
   netsh advfirewall firewall show rule name=all
   ```

   - Look for the rule you just created in the list.

4. **Remove the Rule (if needed):**
   - If you need to remove the rule later, use the following command:

   ```shell
   netsh advfirewall firewall delete rule name="Block IP Address"
   ```

   Replace '"Block IP Address"' with the name of the rule you created if it's different.

Additional Notes

- **Scope:** The above command blocks incoming traffic from the specified IP address. If you want to block outgoing traffic, replace 'dir=in' with 'dir=out'.

- **Rule Name:** Ensure the rule name is unique if you plan to add multiple rules. This helps in managing and identifying them later.

- **Windows Firewall Profile:** By default, the rule applies to all profiles (Domain, Private, Public). If you need to specify a profile, add 'profile=<profile>' to the command, where '<profile>' can be 'domain', 'private', or 'public'.

If you need a more advanced setup or multiple IP addresses, consider using the Windows Firewall with Advanced Security GUI or PowerShell for greater flexibility and scripting capabilities.

To unblock an IP address that you previously blocked using the Windows Firewall, you need to remove the firewall rule that was set up. Here's how to do it:

Unblocking an IP Address Using Command Prompt

1. **Open Command Prompt as Administrator:**
   - Press 'Win + S', type 'cmd', and then right-click on "Command Prompt" and select "Run as administrator".

2. **Delete the Firewall Rule:**
   - Use the 'netsh' command to delete the firewall rule you created earlier. The syntax is:

     ```shell
     netsh advfirewall firewall delete rule name="Rule_Name"
     ```

     Replace 'Rule_Name' with the exact name of the rule you created. For example, if the rule was named '"Block 192.168.1.100"', the command would be:

     ```shell
     netsh advfirewall firewall delete rule name="Block 192.168.1.100"
     ```

3. **Verify the Rule is Deleted:**
   - To confirm that the rule has been removed, list all the firewall rules using:

     ```shell
     netsh advfirewall firewall show rule name=all
     ```

   - Check the list to ensure that the rule is no longer present.

Additional Notes

- **Rule Name:** Ensure that you use the exact name of the rule as it was when created. If you've forgotten the exact name or if there are multiple similar rules, you might need to review the list of rules carefully to find the one you need to delete.

- **Advanced Firewall Management:** If you prefer a more graphical approach or if you're managing multiple rules, you might use the Windows Firewall with Advanced Security GUI. You can access it by searching for "Windows Defender Firewall with Advanced Security" in the Start menu and then navigating to the "Inbound Rules" or "Outbound Rules" sections to find and delete the specific rule.

If you have further questions or need additional help, feel free to ask!