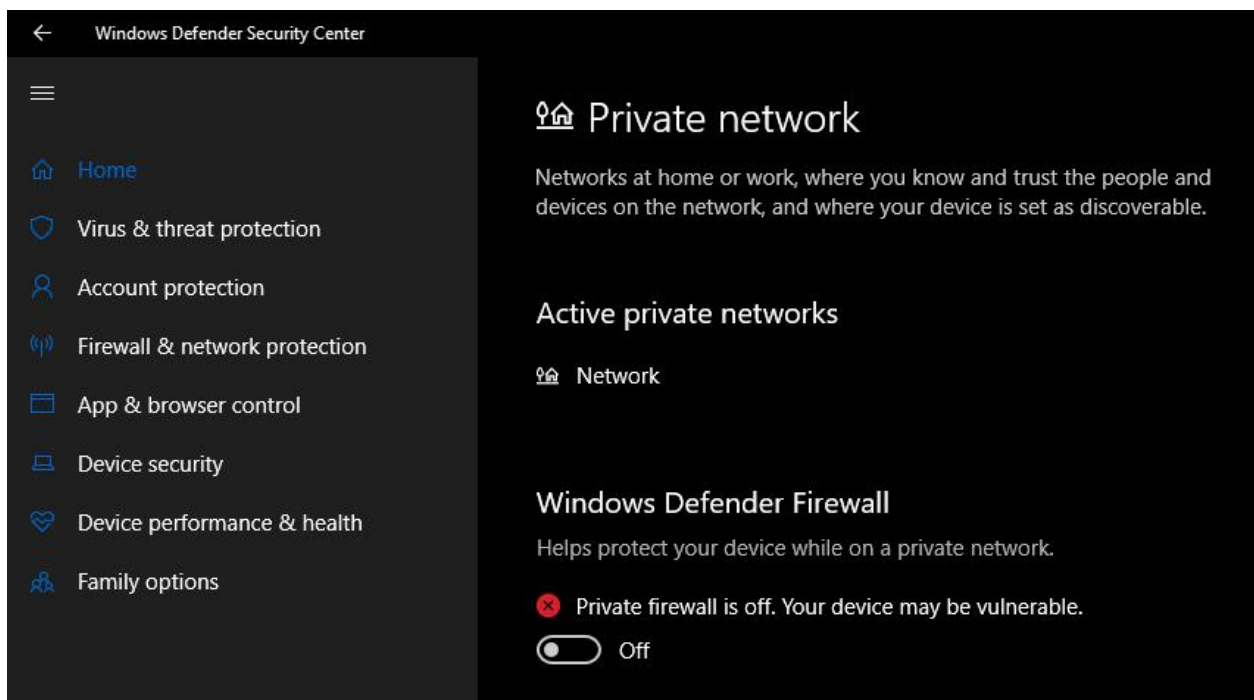


Windows 10 Private Firewall Blocks All Internet Traffic

I experience an interesting issue lately.

Sometimes when I turn on my desktop PC (Windows 10 Pro 64 bit v1803) I have no internet connection. After some searching I realized Windows' Private Firewall is on. If I turn it off, I can connect normally. *Sometimes*, when I reboot my computer the firewall is turned on again by itself and I have to turn it off to connect to the internet.



1. Is the private firewall supposed to be on or off by default?
2. Is this behavior suspicious?
3. Why is this happening?
4. How can I solve it permanently?

1. Is the private firewall supposed to be on or off by default?

- It is recommended to have the **Windows Firewall** stay *enabled always* and by default.



[Turn Windows Defender Firewall on or off](#)

"You should *always run* **Windows Defender Firewall** even if you have another firewall turned on. Turning off Windows Defender Firewall might make your device (and your network, if you have one) more vulnerable to unauthorized access."

[Learn more about protecting your PC from viruses.](#)

2. Is this behavior suspicious?

- No, because it is recommended to have the **Windows Defender Firewall** *always enabled* so having such a recommended configuration applied is not suspicious

3. Why is this happening?

- This is most likely occurring because you have a misconfiguration of a **Windows Firewall** rule that is explicitly blocking whatever access or app you are using to browse the Internet on TCP port 80 or 443 or maybe even blocking an entire subnet which is required to access the network or Internet. It is possible an application install misconfigured a rule or even something malicious but see the below section for some potentially easy solutions and workarounds.
- Since you also confirm the problem goes away when you disable the **Windows Firewall**, this further supports the issue is with a misconfiguration there being the issue.

4. How can I solve it permanently?

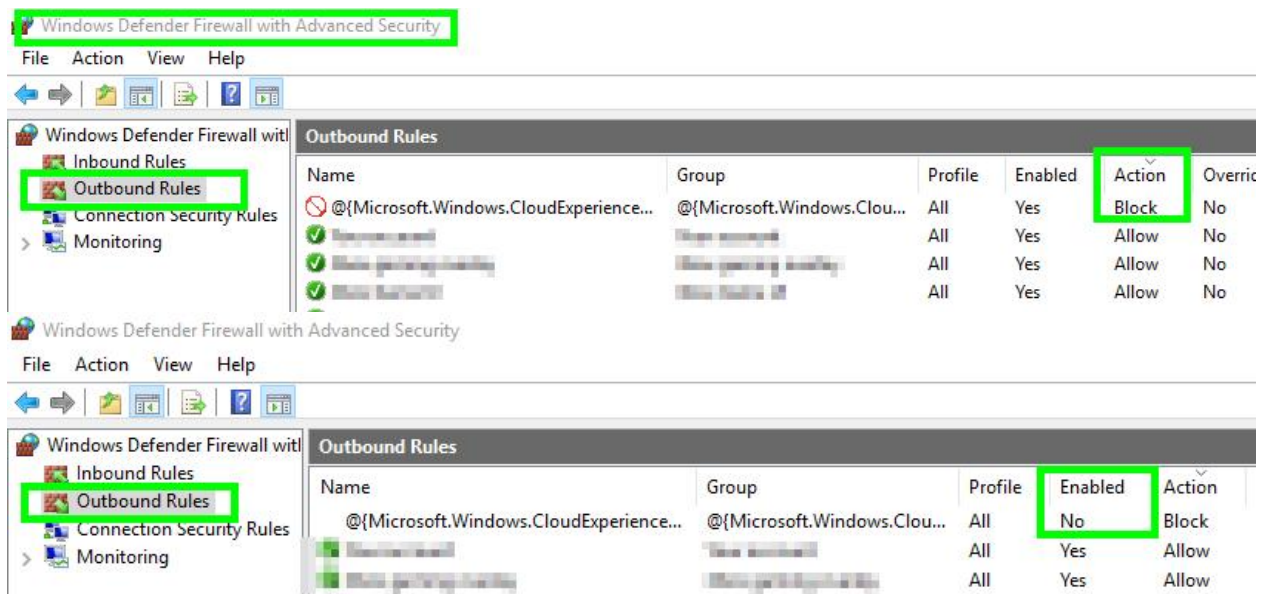
Important: It's important to use an administrator elevated command prompt for the non-GUI items listed below where applicable, and each of the items should be tried individually and in order checking after each is complete to see if it solves the issue.

1. **Reset Windows Firewall:** If you make a mistake configuring Windows Firewall, you might want to use the following netsh command to reset it back to its default settings:

```
netsh advfirewall reset
```

[source](#)

2. **Disable Explicit Deny Rules:** From `wf.msc` look in the **Outbound Rules** and sort by **Action** and try to find any rules that are set to **Block** open it to see if it could be correlated to the blocked web access you like the web browser executable file or TCP port 80, or 443. Simply right-click on any that could be blocking the web access to are related and select **Disable** which will turn the **Enabled** field value to **No**



3. **Enable and disable Windows Firewall:** It's typically a best practice to leave Windows Firewall enabled, but sometimes when you're performing testing or setting up new applications, you need to turn Windows Firewall off for a period. The following commands illustrate how to turn Windows Firewall off and then back on:

```
netsh advfirewall set allprofiles state on
netsh advfirewall set allprofiles state off
```

[source](#)

Note: This could be a solution that is run at "logon" or "startup" with a script perhaps but this is not recommended for security reasons but is a potential workaround if absolutely necessary.

4. **You could setup explicit allow rules** to allow the web browser's executable file inbound and outbound access through the **Windows Firewall**. However, this will likely not fix the blocking issue since the block rules will take precedent over the allow rules where there's any conflict as far as I know.

```
netsh advfirewall firewall add rule name="Chrome Out" dir=out action=allow
program="C:\Program Files(x86)\Google\Chrome\Application\chrome.exe" enable=yes
profile=all

netsh advfirewall firewall add rule name="Chrome In" dir=in action=allow
program="C:\Program Files(x86)\Google\Chrome\Application\chrome.exe" enable=yes
profile=all
```

Note: You simply change the program="**<value>**" variable value to be the full explicit path of the web browser executable file that is being blocked e.g. firefox.exe, iexplore.exe, etc.

Further Resources

- [Top 10: Windows Firewall Netsh Commands](#)
- [Tell Windows 10 firewall to stop prompting me to allow apps access after each reboot](#)
- [UWP icons are missing](#)
- [Malwarebytes](#)
- [Run and review the results of a Windows Defender Offline scan](#)

See if the same issue occurs in a new user profile :

1. In the *Start* button, click *Settings* and then *Accounts*
2. Click *Family & other people*
3. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click *Add someone else to this PC* and follow instructions
5. Again in *Family & other people*, choose the account you created, and then select *Change account type*.
6. Under *Account type*, select *Administrator*, then type *OK*.
7. Restart the PC and logon using the new account.

If the problem does not occur in the new profile, migrate your current profile to the new one.

For more information see the article [Troubleshoot problems with the Start menu or Cortana](#), section "Create a new local administrator account".