

5 reasons why you should use a firewall

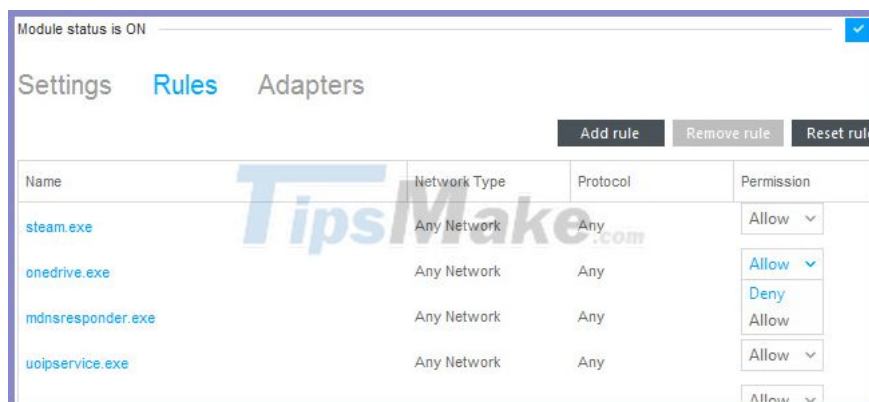
What is the firewall used for? Can you be safe without it? Keep reading to find out why you really need a firewall.

Chances are you are using a firewall at the moment. If your computer is running a modern operating system, a firewall is usually built in. Or you may also be using an installed third-party firewall.

But what is the firewall used for? Can you be safe without it? Keep reading to find out why you really need a firewall.

1. Firewalls help prevent unauthorized remote access

One of the worst things that can happen to a computer is when someone tries to take over remote control. Sure, you don't want that intruder to usurp your digital 'kingdom', by taking control of the data in the machine.



Firewalls help prevent unauthorized remote access

With a correctly configured firewall (and a modern operating system), it's a good idea to disable remote desktop access. This will prevent hackers from sneaking over your computer

Note, however, that this does not block remote control applications from being used by scammers, in the name of supporting Windows technology. These apps are browser-based, and scammers trick you into allowing them to work.

Illegal copies of Windows found on the Bittorrent network often come with malware (Trojan, keylogger, backdoor) pre-installed in the disk image. If you are running one of these applications, even with a firewall installed, you may experience security issues.

Also understand that firewalls block the access of applications - possibly software you trust - from unauthorized Internet access.

2. The firewall can protect old PCs in the short term

Incredibly there are still people using Windows XP and Windows 7, even though they were released in 2001 and 2009 respectively. Worse yet, some of them are using these operating systems without any firewall.

The Internet has a lot of malicious code going through cyberspace, waiting to attack unprotected computers. While the ISP can help prevent this, the ISP's intervention is limited.

So those Windows 7 users out there (14% as of June 2019) help yourself out by installing a third-party firewall.

Once you're done, start the upgrade process. Upgrade to Windows 10 if possible or even to Linux, or simply buy a new computer capable of running a secure, modern operating system.

Because right now, you are an easy, direct target of hackers.

3. Firewalls make online gaming safer



Online gaming is one of the most important activities on the Internet, but it also poses a security risk. Various malware has been developed that target online gamers, which exist on recent unsecured or compromised game servers.

While game publishers often pay attention to security on their servers, it's smart to use a firewall. All attempts by hackers to use malware to enter the system will be stopped, making your system secure.

In most cases, the firewall will configure itself based on the game's requirements, using the information provided in the metadata.

Note that security suites usually come pre-installed with "**Gaming Mode**" or some other similar option. Use this to optimize your PC before launching your favorite game and ensure the best available performance. If there is a problem, you can consult the game's support pages and edit the firewall application settings.

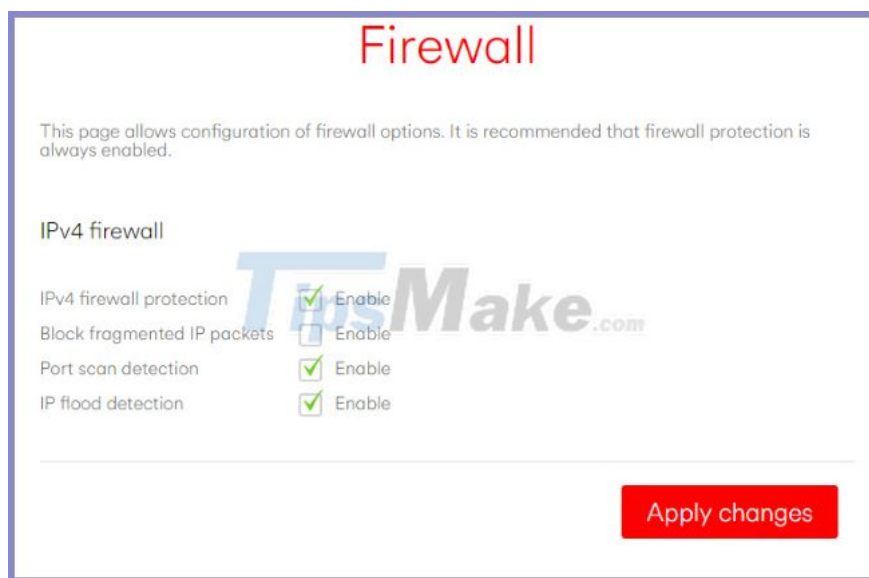
Console players can take advantage of hardware firewalls or routers if required to tweak settings. For even more security, consider a VPN for online gaming.

4. Firewalls can block inappropriate content

Up to now, the article has mainly talked about blocking hackers and other types of malware from remotely accessing it. However, a firewall is much more likely than that. Firewall applications often also have the option to block specific online destinations, including "adult" websites.

Content filtering is commonly found in parental control applications, but is increasingly being introduced into firewalls. In some countries, ISPs may manage content blocking.

5. A firewall can be either hardware or software



As noted above, firewalls are not necessarily software. Hardware firewalls are found in most homes, built into routers.

Accessing these firewall settings requires admin login credentials for the router (make sure you've changed the default password). Once logged in, you will be able to review the options and change them as needed.

Sometimes you'll need to make some tweaks, especially to play online games using a game console. For example, changing the NAT type on PlayStation 3 and PlayStation 4 is a common fix for online gaming connection problems.

Make sure to check the documentation for your router to familiarize yourself with the settings before saving any changes!

You finished reading the article "**5 reasons why you should use a firewall**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
