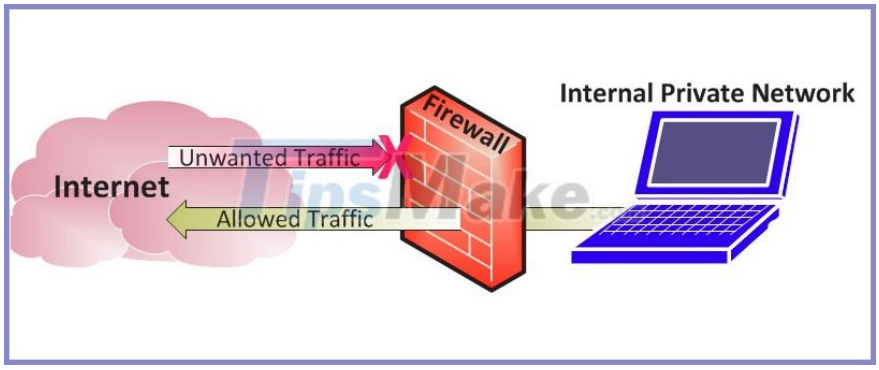
# How to turn off firewall on Windows 7,8,10

How to turn off firewall is one of the keywords that are searched a lot. So what is a firewall? Why turn it off and how to turn it off? Watch now

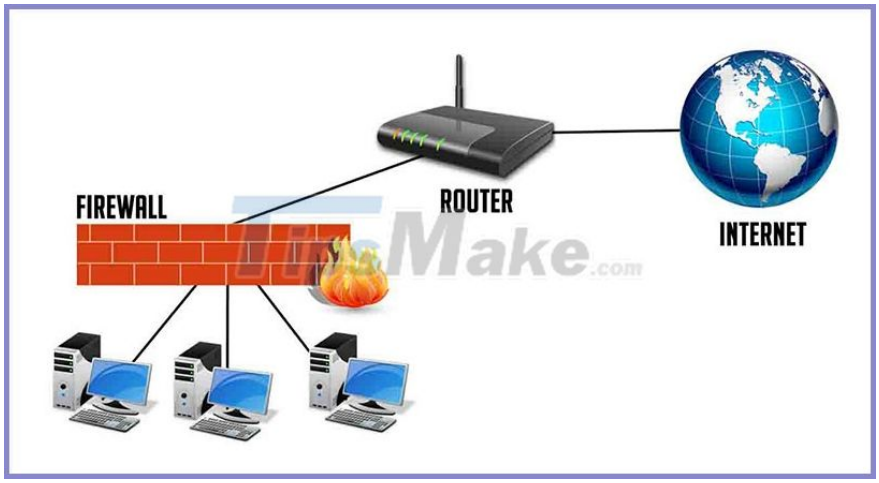
Before you begin, you must understand that disabling the firewall ( ***Windows Firewall*** ) and disabling **Window Defender** ( *the Windows antivirus* ) are two completely different concepts.

## I. What is a firewall?




A firewall, also known as **Windows Firewall** , is a network security tool that monitors incoming and outgoing network traffic, allowing the transmission or interception of data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and traffic coming from outside sources (such as the internet) to block malicious traffic like viruses and hackers.

### How does a firewall work?



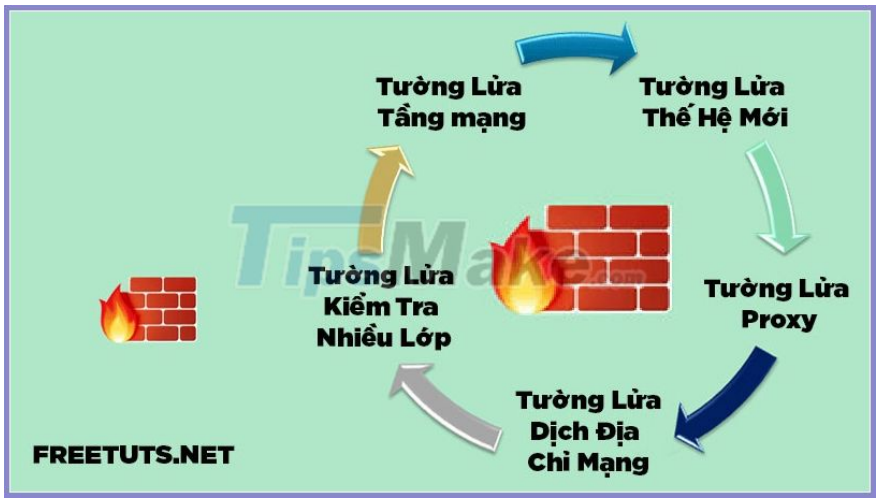
Firewalls carefully analyze download traffic based on predefined rules, filtering traffic coming from unsafe or suspicious sources to prevent attacks.

A firewall protects traffic at a computer's entry point, called a gateway, where information is exchanged with external devices. For example: 'Source address 172.18.1.1 is allowed to destination 172.18.2.1 via port 22. "

Think of the IP address as home and the port number for the room in the house. Only trusted people (source address) are allowed in the home (destination address). It is then further filtered so that people in the house are only allowed access to certain rooms (destination gate).

Depending on whether they are the owner or not, the owner is allowed in any room (any gate), while children and guests are allowed to enter a certain group of rooms (specific gate) .

## Firewall classification




A firewall can be either software or hardware, although it's best to have both. A software firewall is a program that is installed on each computer and regulates traffic through the number of ports and applications, while a physical firewall is a piece of equipment installed between your network and your gateway. .

### 1. Network layer firewall

The most common type of firewall is the 'Packet-filtering firewalls', which checks the packets and prohibits them from passing if they do not match the established security rules. This type of firewall checks the source and destination IP address of the data packet. If the packet conforms to the 'allowed' rule on the firewall then it is 'trusted' to enter the network.

Packet filtering firewalls are divided into two categories: stateful and stateless. Stateless firewalls examine packages independently of each other, and many experts think it's easy for hackers to bypass. In contrast, a state firewall remembers information about previously transmitted packets and is considered to be much more secure.

With two types of packet filtering firewall, it seems quite effective, but there are many security holes, for example, they cannot determine whether the content of the request being sent has an adverse effect on the response. to which it is approaching or not. If the malicious packet is allowed from the source address will result in the database deletion, the packet-filtering firewall has no way of knowing it.

That's why next-generation firewalls and proxy firewalls are more equipped to detect such threats.

**2. New generation firewall**

Next-generation firewalls (Next-generation firewalls) combine traditional firewall technology with additional functions, such as encrypted traffic monitoring, intrusion prevention systems, antivirus, etc

Most notably, it includes in-depth packet inspection (DPI). Whereas the basic firewall considers only the packet header, in-depth packet inspection examines the data inside the package itself, allowing users to effectively identify, classify, or prevent packets with malicious data. than.

**3. Proxy Firewall**

A proxy firewall filters network traffic at the application level. Unlike basic firewalls, proxies act as an intermediary between the two end systems. The client has to send a request to the firewall, where it is then evaluated against a set of security rules and then allowed or blocked. Most notably, the proxy firewall monitors traffic for seven-layer protocols like HTTP and FTP, and uses both stateful and intensive packet inspection to detect malicious traffic.

**4. Network address translation (NAT) Firewalls**

This firewall allows multiple devices with independent network addresses to connect to the internet with a single IP address, keeping individual IP addresses hidden.

As a result, attackers scan the network for IP addresses that cannot capture specific details, providing greater security against attacks. NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and external traffic.

**5. Stateful multilayer inspection (SMLI) firewalls**

Multiple layers of inspection during application transport compare them with known reliable packets. Like the NGFW firewall, SMLI also checks all packets and allows them to pass only after filtering each individual layer. These firewalls check packets to determine the state of the communication (hence the name) to ensure all initiated communication takes place only with reliable sources.

## Why turn off the firewall?

With the main purpose born to be security, the firewall is an indispensable tool for any device accessing the Internet.

However, not so that the firewall is always trusted by everyone. Let's take a look at the cases where you should turn off the firewall to make the machine work better.

As mentioned about the effect of a firewall, like a security guard of an agency or a department, Windows Firewall will monitor all data sent and received to your computer, thus causing it takes time in the "check-in process" and certain confusion cannot be avoided.

There are quite a few different types of firewalls, but in this article we are talking about the built-in firewall (Windows Firewall) of Windows operating systems. Most computer users believe that the benefit of a firewall is less than the harm it does.

Specifically, here are two cases where the firewall (Windows Firewall) is not useful, annoying the user:

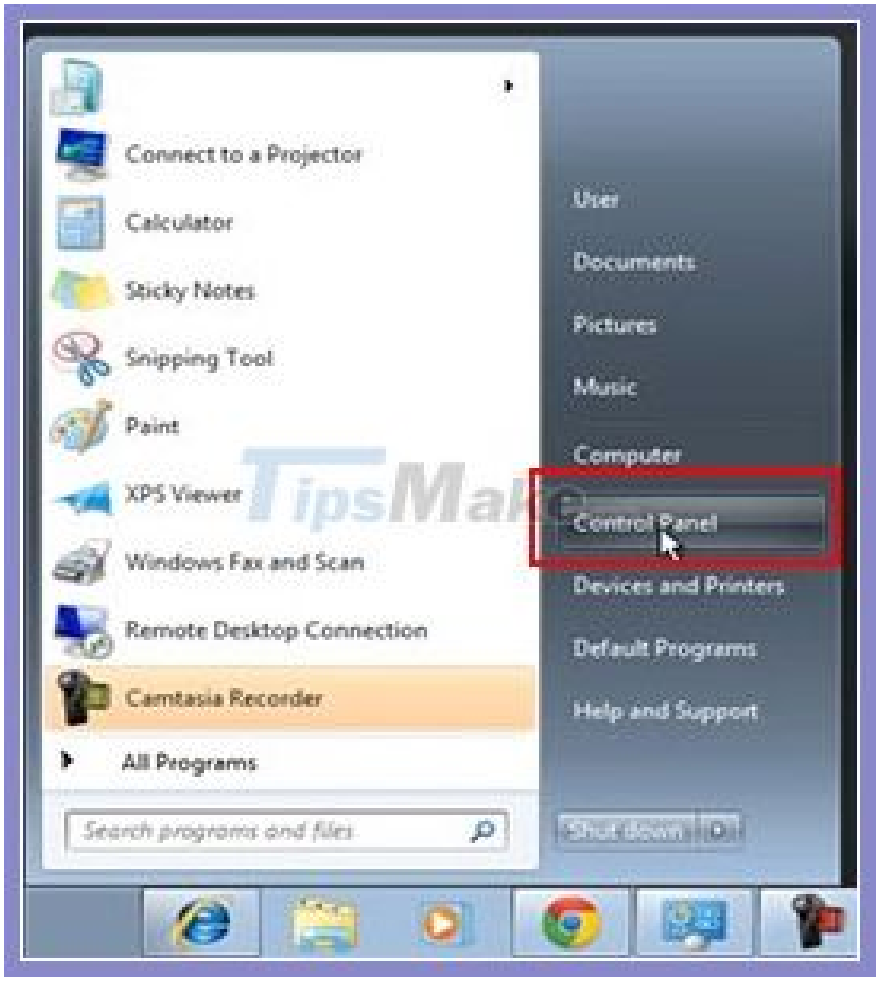
1. Fake Alarm: Like other programs, the firewall can malfunction and misunderstand some information as "dangerous", leading to blocking access or even deleting the data you download! For example, blocking a regular secure website. Especially in the case of using LAN / Wifi to transfer data between computers in the network, it will be very difficult to turn on the firewall.
2. The firewall becomes useless when you install the firewall from 3rd party software, at this point you should also turn off the Windows firewall to save resources.

If you have not installed any 3rd party firewalls, you can consult a list of the best antivirus software available today. With advanced firewall feature - smart will definitely do much better than the existing Windows firewall a lot.

# 2. How to turn off firewall on Windows 7

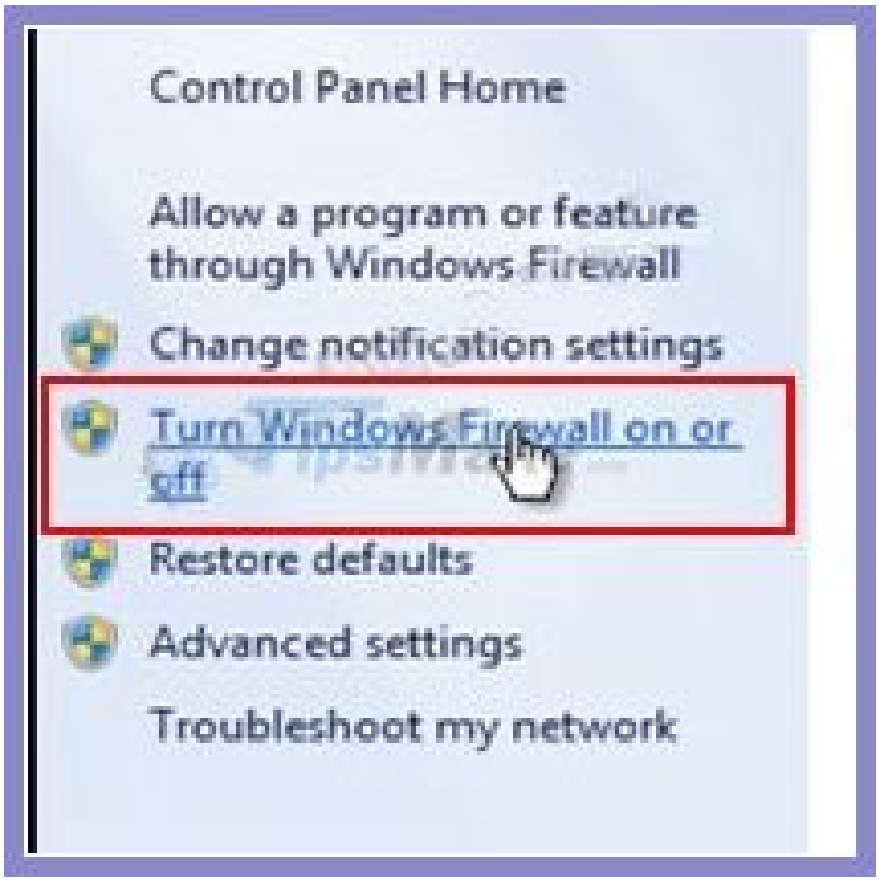
To disable Firewall on Win 7, you do the following:

**Step 1:** Click **Start Menu** in the lower left corner of the screen and then click **Control Panel.**



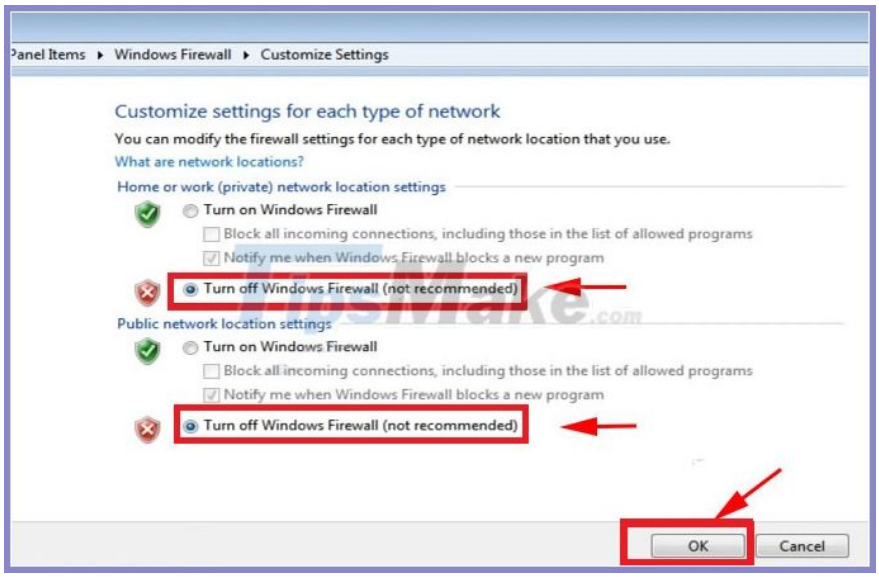

**Step 2:** In the **Control Panel** window , click **Windows Firewall.**


**Step 3:** Left-click on the option **Turn Windows Firewall on or off.**



**Step 4:** You switch to the following option in both items to turn off the firewall: **Turn off Windows Firewall (not recommended).**

Then click **OK** to complete disabling the firewall for Windows 7 computers.

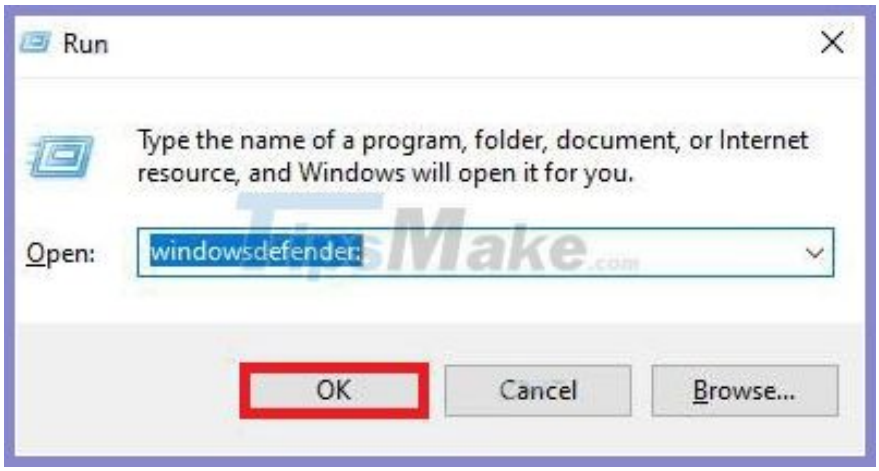



# 3. How to turn off firewall on Windows 8 - 10

In this article, I am instructing to turn off the firewall on Windows 10. Please do the same on Windows 8 and 8.1.

**Step 1:** Press the key combination `Windows + R`to open the **Run** dialog box **.**

1. -> Enter: *windowsdefender:*
2. -> Click **OK.**




**Step 2:** In the **Windows Securit** y window , then left-click on **Firewall & network protection.**

Next, click on **Domain network.**

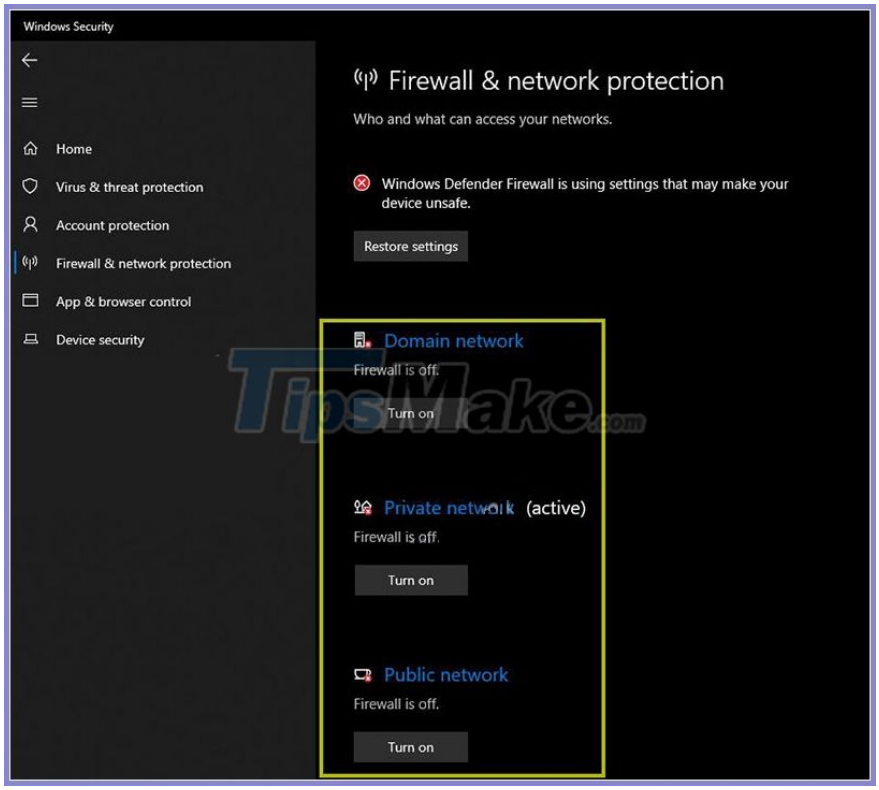

**Step 3:** Click the switch to switch **Windows Defender Firewall state** to **Off** -> **Turn off firewall.**


**Step 4:** Click the back button ( *Back* ) and then click on **Private network.**


**Step 5:** Click on disable firewall similar to step 3.


**Step 6:** You should also turn off the firewall in the **Public network section.**


You will disable the firewall (Windows Firewall) for your Windows 10 computer completely after turning off the firewall in all 3 sections: **Domain network, Private network, Public network** .




# 4. Summary

Surely through the article you have a clear understanding of what a firewall is and how to easily disable this function on Windows. Turning off the firewall is not difficult, anyone can turn off the Windows Firewall very quickly. However, you should be aware of the reasons for turning off your firewall, only turn off the firewall when absolutely necessary.

If your friends or colleagues want to turn off the firewall but do not know how, please share this article with them right away.

Good luck !