

What is a firewall? Overview of Firewall

What is a firewall Overview of a firewall. A firewall, also known as a firewall, is a technique that is integrated into the network to prevent unauthorized access, to protect internal information sources and prevent unwanted intrusion into the system. Fire

The Internet is currently a large information portal where you will learn and gather a lot of important news, information, documents along with valuable social networking. However, there are also many bad guys who take advantage of that and want to steal information or have malicious intent to access your computer. But to do that, you must first pass an invisible shield called Firewall. So what is a firewall? Let's TipsMake.com learn Firewall Overview offline!

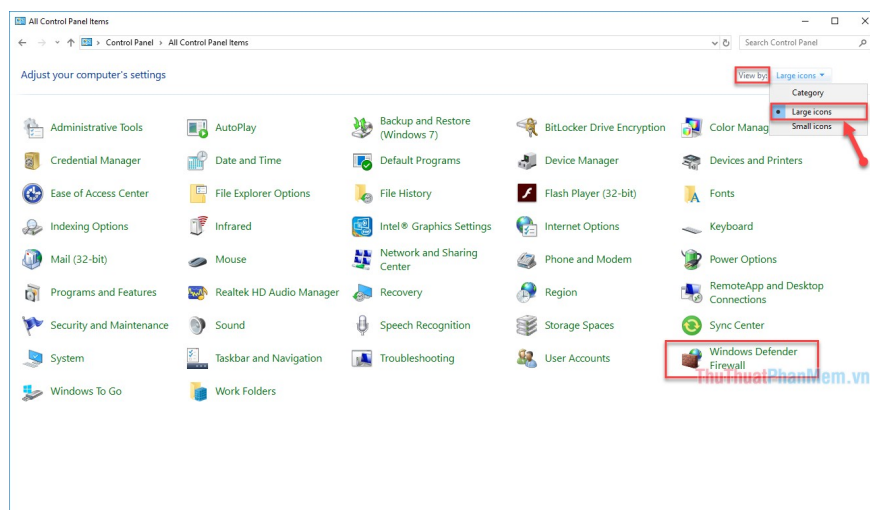


What is a firewall?

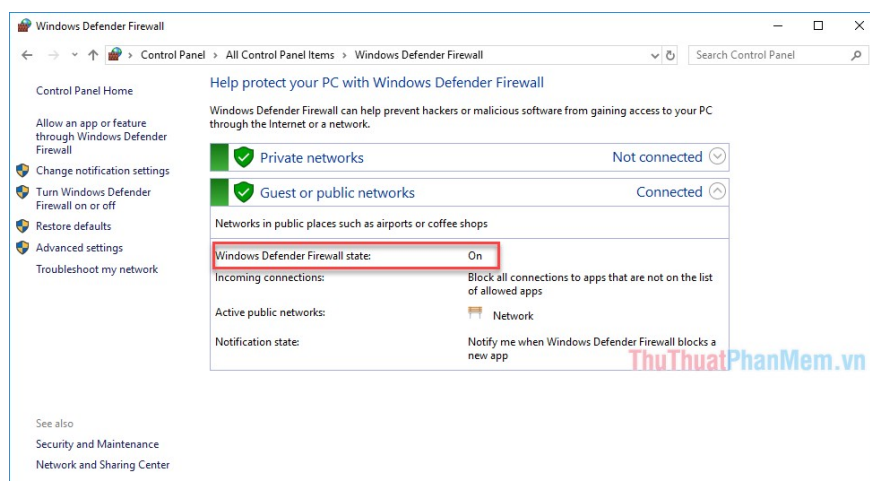
A firewall, also known as a firewall, is a technique that is integrated into the network to prevent unauthorized access, to protect internal information sources and prevent unwanted intrusion into the system. Firewall uses rules to control inbound and outbound traffic that acts as a barrier between secure and unsafe networks. It controls access to network resources through an active control model. That is, only traffic that conforms to the policy defined in the firewall is allowed to access the network, all other traffic will be denied.

Firewall is usually activated automatically, TipsMake.com will show you how to check if the computer has a firewall enabled.

Click **Start (Windows)** ? find **Control Panel** . Normally Control Panel will display as a summary, to display all the search functions you hover on ' **View by** ' and select ' **Large icons** '. Then you can easily see the icon of Firewall / Firewall.



Click on ' **Windows Defender Firewall** ' to check. If ' **On** ' is displayed, your computer has a firewall enabled.



Overview of Firewall

Any computer that uses the Internet needs a firewall, which helps to manage what is allowed into the network and what is allowed out of the network. Having such a 'guardian' to oversee everything happens is important for two reasons:

- **Firstly** , any computer with a network connection is usually permanently connected to the Internet.
- **Secondly** , each online computer has its own digital signature, called the Internet Protocol address (also known as an IP address): Without a firewall, it is no different than opening and waiting for someone. burglar into.

A properly configured Firewall will prevent this from happening and will effectively 'hide' the computer, allowing users to freely enjoy what the online world has to offer. A firewall is not the same as an antivirus program. Instead, it works in conjunction with these tools to ensure that the computer is protected from most common malicious attacks. Every firewall must have at least two network interfaces, one for the network it protects, and the other for the external network. A firewall can be a gateway or a link between two networks, usually a private network and a public network such as the Internet. The first firewalls are simple routers.



Firewall function

The main function of the Firewall is to control the flow of information between the Intranet and the Internet. Establish a mechanism for controlling the flow of information between an internal network (Intranet) and the Internet.

- Allow or prohibit outbound access services.
- Allowing or banning services from outside.
- Monitor network data flow between Internet and Intranet.
- Control access address, ban access address
- User control and user access.
- Control the content of information circulating on the network.

A firewall checks all information flows between two networks to see if it is up to standard. If it reaches, it is routed between networks, otherwise it fails. A firewall filter filters both incoming and outgoing traffic. It can also manage external access to internal network resources. It can be used to record all attempts to enter a private network and give quick alerts when an enemy or unauthorized person enters. Firewalls can filter packets based on their source, destination and port numbers. This is called address filtering. Firewalls can also filter special types of network traffic. This is called protocol filtering because decision making for forwarding or denying traffic depends on the protocol used.

Some firewalls have an interesting and advanced function, deceiving intruders that they have broken the security system. Basically, it detects an attack and takes over it, leading the attacker to follow it with a 'hall of mirrors' approach. If an attacker believes he or she has gained access to a part of the system and has further access, the attacker's activity can be recorded and monitored. If it is possible to keep the perpetrator for a while, the administrator can trace their tracks. For example, you can use the finger command to track an attacker or create a 'bait' file so that it takes a long time to transfer, and then track the file transfer to the attacker's location over an Internet connection.



Advantages and limitations of Firewall

Advantages:

- Protect the system by attacks (inside, outside).
- Filter connections based on data content.
- Implement NAT.
- Combined with IDS / IPS system.
- Composition of defense solutions in depth.

Limit:

- Application layer attacks may be ignored.
- Connections: Dial-up, VPN can bypass firewall.
- Operation management is relatively complicated.
- There exist intrinsic weaknesses.
- Affect connection speed.

For users, the Windows Firewall may still be inadequate because it does not block outbound connections. So if any malware finds a way into the computer, there is no way to prevent its destructive activity. TipsMake.com recommends downloading additional free Firewall software and installing it to use in parallel with Windows Firewall.

With the above information, you probably understand a little about the firewall, its function and its advantages and disadvantages. If you find the article useful, please share your knowledge to everyone. Thank you for watching!

You finished reading the article "**What is a firewall? Overview of 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.

