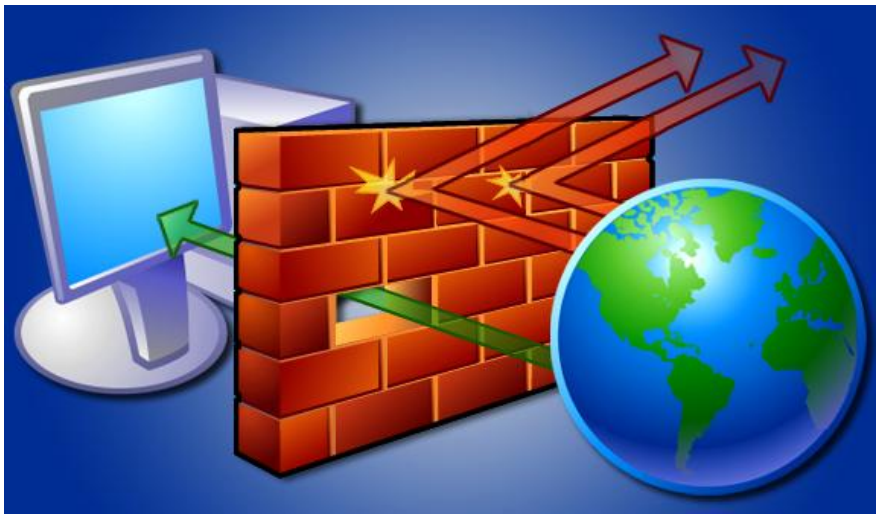
How does the firewall work?

Experts agree that there are three types of 'backbone' software to set up personal computer security: antivirus, firewall and password management. However, though extremely important, firewalls are often least remembered.

Experts agree that there are three types of 'backbone' software to set up personal computer security: antivirus, firewall and password management. However, though extremely important, firewalls are often least remembered.



The faintness of firewalls in the eyes of users results from Windows already integrating a firewall, so there is less and less need to find third-party options. However, for those interested How to protect yourself and want to know about the firewall's activities is an article you should not ignore.

The first session of the firewall

The phrase ' *firewall* ' originating from real-life walls was built to prevent fire. They still exist in buildings today, when there is fire, the wall will prevent the fire from escaping from the dangerous area and destroy the rest of the building. Technology experts applied the term in the late 1980s to describe any software or hardware capable of protecting the system or network from Internet hazards. After **Morris Worm** (January 2, 1988) - the first malicious code spread over the internet, potentially causing serious damage to the system, of course individuals and organizations began to find ways to protect themselves. from similar malware.

Types of common firewalls today.

Packet Filter - Packet Filter

The first firewall can only read packet headers such as source and destination addresses. The action is then performed based on the information obtained. This type is often effective and fast but vulnerable. For example, counterfeit attacks can resist effective packet filtering. Upgraded versions of packet filters store packet data in memory and can change behavior based on events occurring on the network. They are also called stateful firewalls and dynamic firewalls.

Gateway - Circuit Gateway

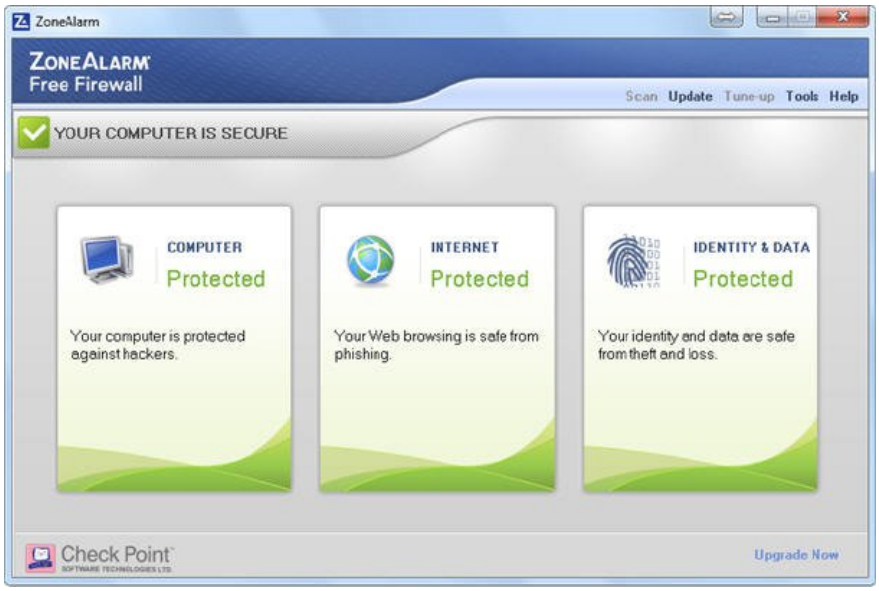
This is the next development of the firewall, Circuit Gateway not only handles the packet header data but also ensures a valid connection to the packet. To do this, the Circuit Gateway takes care of the data packet, looking for changes such as the source IP address or abnormal port (port). If the specified connection is invalid, it will be closed. This type of firewall can also automatically reject specific information sent by users within it.

Application portal - Application Level Gateway

This type of firewall shares the characteristics of the ring port, but delves into the information sent through the firewall and examines the relevance to the specific application, service, and website. For example, an application port can ' *look* ' into web traffic transmission packets and determine where web traffic comes from. The firewall will then block data from the site if the administrator wants it.

The firewall software

The firewall installed on the computer is mostly an application firewall. It has the ability to control each application to access the internet and block specific or unknown applications trying to receive or send information.



Personal firewalls are also a firewall software. That means all its features are controlled by the code installed on the computer. The advantage of this is that you can easily change the firewall settings as needed and access the interface without logging in to any particular device.

However, the firewall software is vulnerable because it will be affected if the installation system fails. If your computer is affected by malicious code regardless of firewall or other security methods, malicious code can very likely be programmed to break or change the firewall's settings. Therefore, the firewall software is never completely safe.

Hardware firewall and home use

To address this vulnerability, large organizations often use firewalls with hardware besides firewall software. Usually they are sold as part of a large security system from enterprise security solutions companies such as Cisco. These devices are often unrealistic for home users, but you still have alternatives. For example, every broadband router acts as an intermediate firewall between the computer and the internet, and the connections sent from the computer to the internet are not sent directly, but through the router first, then the router decides. where information is needed. This is why sometimes you should install ' *port fowarding* ' in the router to make sure the firewall function works. However, routers are not true firewalls because they cannot investigate packets. It is simply a two-sided effect of the router.

If you want a real firewall, you can buy Cisco 'Netgear' ' *router for small businesses* ' - small sized devices featuring an internal firewall, designed to connect a small number. computer with internet. Such devices always use packet filters or ring ports, so it is not easy to be *'bypassed* ' by any malicious software on the computer network.

In addition, basic firewall devices are also useful if you run the server, help with denial of service (DDoS) control and other intrusion actions.

Conclude

Firewall software always plays an important role in ensuring the safety of home computer systems. Windows has integrated the firewall from the XP version, but third-party firewall applications still exist in parallel. If you have a router and use firewall software, you can be confident of being well protected. Keep in mind that the main path to compromising a computer is to download malware programmed to break the system, including a firewall. If you have antivirus software and do not disable the **User Account Control feature** on Windows, the attacks will be blocked.