Why You Probably Don't Need a Third-Party Firewall App on Windows

Firewalls are your Windows system's first line of defense against online threats, but is Windows Defender Firewall up to the task?

Firewalls are your Windows system's first line of defense against online threats, but is Windows Defender Firewall up to the task? Or will you need to use third-party firewall applications? Let's find out.

What is a firewall? How does it work?

A firewall is a security barrier between an internal network and an external network, such as the Internet. It is often part of a security system that monitors and filters incoming and outgoing network traffic based on established security rules.

In simple terms, a firewall is a network security system, which can be hardware or software based, that uses rules to control traffic entering and leaving the system. A firewall acts as a barrier between a secure network and an insecure network. It controls access to network resources through an active control model. That is, only traffic that matches the policy defined in the firewall is allowed to access the network, all other traffic is denied.

As mentioned, firewalls can be software, hardware, or even a combination of both. There are several different types of firewalls. However, the basic principle of operation will be based on an allowlist and blocklist (formerly known as 'whitelist' and 'blacklist'), where networks, IP addresses, domains, and applications are added to either list, to allow access to resources or deny access. They not only monitor and filter traffic, but also log traffic and all security events over a certain period of time.

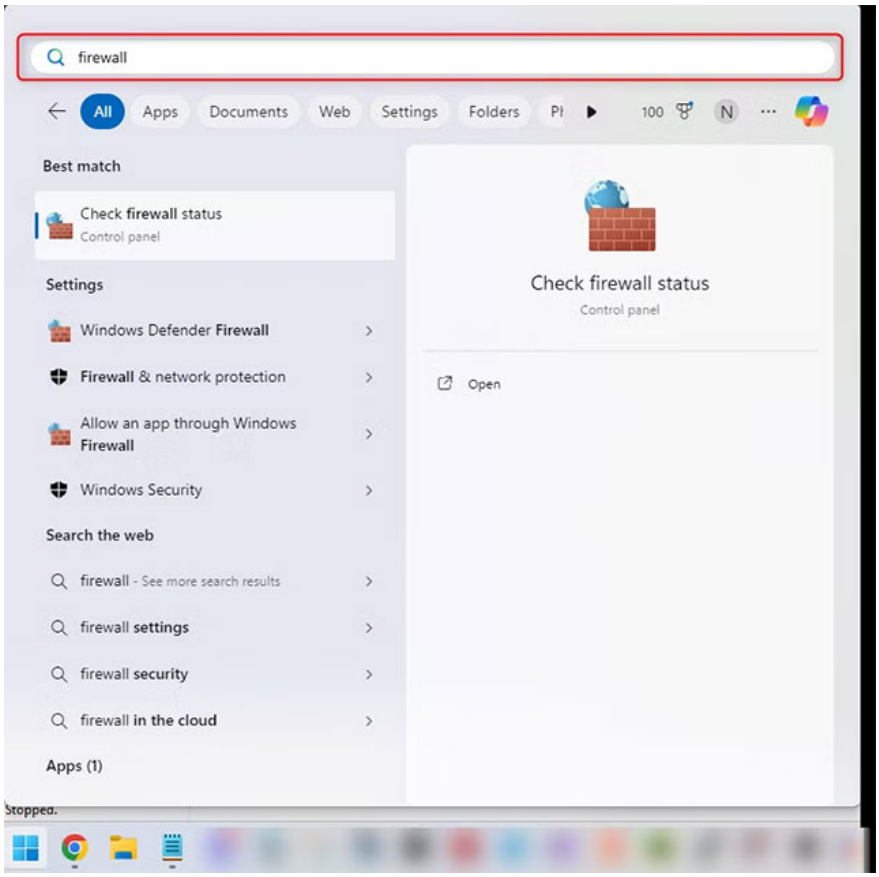
What if you don't have a firewall?

Windows Defender Firewall protects your Windows system from network-based threats, such as Denial of Service (DoS) attacks, malware, etc. By acting as gatekeepers, firewalls can block unauthorized users and potential hackers from accessing private networks.

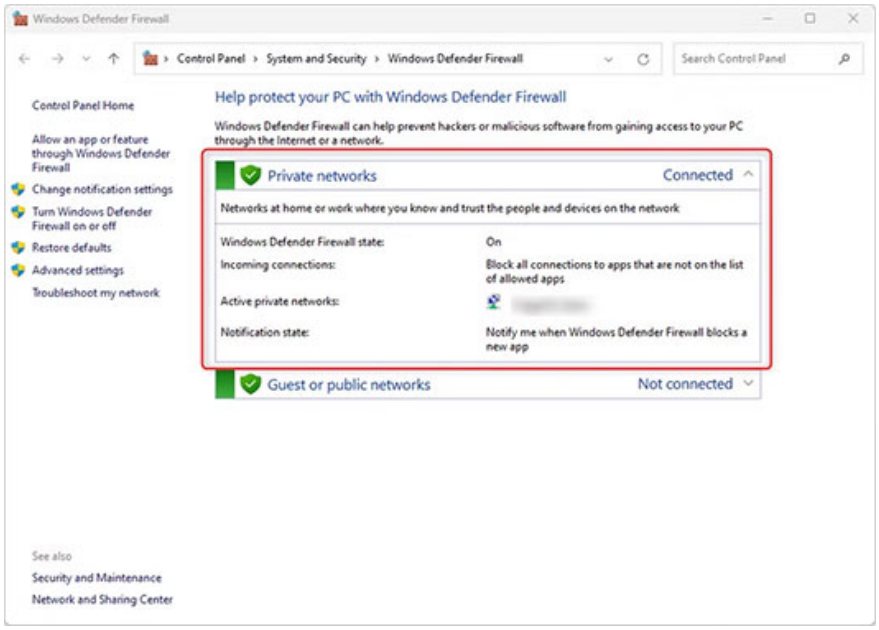
Without a firewall, hackers can more easily access your system and your private and confidential data, and it also makes it easier for many types of malware to infect your system, including viruses, worms, and even ransomware. Firewalls also play an essential role in maintaining data privacy by controlling what information can enter or leave your network, which can protect against data theft.

Windows Firewall is enabled by default and should remain enabled unless you have manually disabled it or installed a third-party firewall.

To check if Windows Defender Firewall is connected, click the Start menu (or press Windows key+i) and search for Firewall:



Press Enter and a window will appear:



If Windows Defender Firewall is connected, the system will display the status "Connected" as shown above. However, if it is not connected, click "Use Recommended Settings" to enable it.

Is Windows Defender Firewall enough?

Windows Defender Firewall is basically enough for the average internet user and most of them do not need an additional firewall. It has minimal impact on system performance and Microsoft regularly updates it to address new threats. Since it is developed by Microsoft, it integrates seamlessly with the Windows operating system. It is user-friendly compared to many other third-party firewall tools and does not require extensive configuration.

Windows Defender Firewall includes an interface with advanced firewall configuration where you can create advanced firewall rules. It is accessible through the Windows Defender Firewall with Advanced Security interface.

It can be a bit time-consuming, as there are sometimes multiple requests from a single application connection that can trigger multiple pop-ups. However, it does give you more power and control as a user. If you want a little more control without using a third-party firewall, fortunately, Windows Defender Firewall actually offers more features than you might expect.

However, a firewall is just one aspect of security, and hackers have many other ways to gain access or launch attacks. It's important to keep your Windows computer up to date and be aware of common online scams that are on the rise.

Who might need to use a third-party firewall?

For casual Windows users who primarily browse the web, play games, and shop online, Windows Defender Firewall alone is sufficient. As long as you use Windows Security along with Windows Defender Firewall and follow good security practices. On the other hand, remote workers and those who handle sensitive corporate data will benefit from an additional firewall.

Many Fortune 500 companies use Windows Security, but they also benefit from additional firewalls, as do small and medium-sized businesses (SMBs). Firewalls are also required for compliance to help organizations meet regulatory requirements for data protection and network security.

Additional firewalls are beneficial to businesses, as they not only protect the business from data breaches and theft, but can also improve employee productivity by blocking access to non-work related websites, and reduce the risk of reputational damage caused by security incidents.

One of the biggest differences between Windows Security and more advanced firewalls, such as Next-Generation Firewall (NGFW), is that it can be used for threat detection because it can monitor, identify, and alert administrators to potential security threats, which is especially useful for security teams. NGFW can also perform proactive actions such as intrusion prevention and application control.

Firewalls also work well with VPNs to facilitate secure remote access, where the VPN encrypts the user's IP address and data through a secure tunnel and the firewall filters traffic. This provides another layer of security, allowing for a more secure connection for remote workers.

Ultimately, Windows Defender Firewall does its job well, but a little extra security from a third party doesn't hurt either!