What is the difference between Proxy and VPN?

A proxy connects you to a remote computer and the VPN also connects you to a remote computer, so are they one? This is incorrect, let's look at the differences between them and when to use Proxy and VPN.

A proxy connects you to a remote computer and the VPN also connects you to a remote computer, so are they one? This is incorrect, let's look at the differences between them and when to use Proxy and VPN.

1. 10 common mistakes of VPN and how to fix it

Choosing the right tool is very important

In fact, the problem of encryption, data leakage, snooping, digital security is always a matter of concern. Many articles talk about the importance of enhancing the security of Internet connectivity such as using VPN (Virtual Private Network) while using public Wi-Fi in cafes. So how does the proxy server work and VPN connection work? If you intend to invest time and energy to strengthen security, make sure you choose the right tool.

Although fundamentally different, VPN and Proxy still have one thing in common: they both conceal the identity of the user, forged being connected to the Internet from another location. How VPN and Proxy perform concealment of the identity and location of users as well as the level of privacy, encryption and other functions is different.

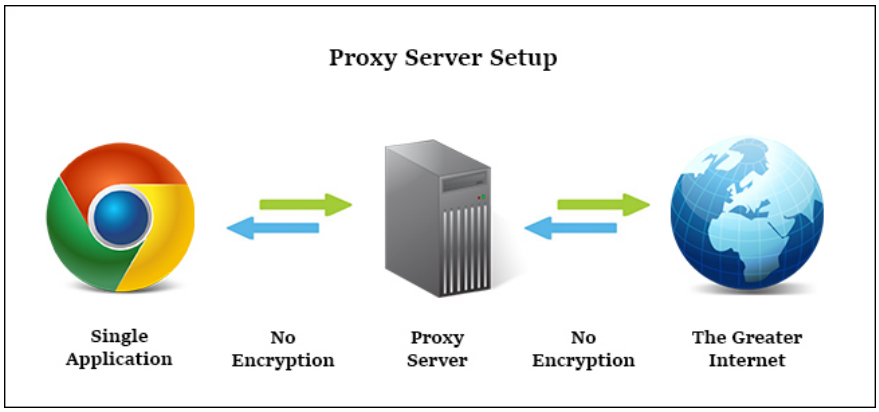
Proxy on IP address

A proxy server is a server that acts as an intermediary tool in the Internet traffic stream so the user's Internet activities seem to come from somewhere else.

Suppose, you live in New York City and want to access a site that is geographically limited to only people in the UK who can access it. You can connect to a proxy server in the UK, then visit that site. Traffic from the web browser will be from the remote computer and not your computer.

Proxies are suitable for low-level tasks such as watching YouTube videos that are limited in geography, bypassing simple content filters or bypassing IP restrictions for services.

For example, many family members of online gaming, they will receive daily bonuses by voting for game servers on a server ranking website. However, ranking websites only allow one IP to vote once in a day. Therefore, thanks to the proxy server, each person can vote and receive gifts in the game because each person's web browser seems to come from a different IP address.



However, proxy servers are not the perfect choice for high-level jobs. It only hides the IP address and acts as an intermediary in Internet traffic. It does not encrypt traffic between your computer and the proxy server, does not remove identity information from data transfer in addition to simple IP exchange and does not have built-in privacy or security options.

Anyone who has access to the data stream (ISP, government, etc.) can 'snoop on' your traffic. Furthermore, certain errors, such as malicious Flash or JavaScript elements in a web browser, can reveal your true identity. This makes proxy servers inconsistent with important tasks such as preventing the control of a malicious Wifi hotspot from stealing your data.

Finally, the proxy server connection is configured on an application basis, not on the entire computer. The user does not configure the entire computer to connect to the proxy, can only configure the web browser, BitTorrent client or application that is compatible with another proxy, suitable for using a single application connected to proxy but not appropriate when you want to redirect the entire Internet connection.

There are two most common proxy server protocols, HTTP and SOCKS.

HTTP Prox y

HTTP Proxy is the oldest type of proxy server, designed for web-based traffic. When connecting the proxy server to the web browser configuration file (or using the browser extension if the browser does not support proxy), all web traffic will be transferred via the remote proxy.

If you are using an HTTP proxy to connect to any type of service such as email or banking, you need to use a browser with SSL enabled and connected to a website that supports SSL encryption. As mentioned above, proxies do not encrypt any traffic, so the only encryption users receive is the encryption they provide themselves.

SOCKS Prox y

SOCKS proxy system is a useful extension of the HTTP proxy system, it does not care about the type of traffic passing through it. HTTP proxies can only handle web traffic, while the SOCKS server simply overcomes all traffic, such as traffic to web servers, FTP servers, or BitTorrent clients.

The downside of SOCKS proxies is that they are slower than HTTP proxies, just like HTTP proxies, it does not provide external encryption for user-defined encryption for certain connections.

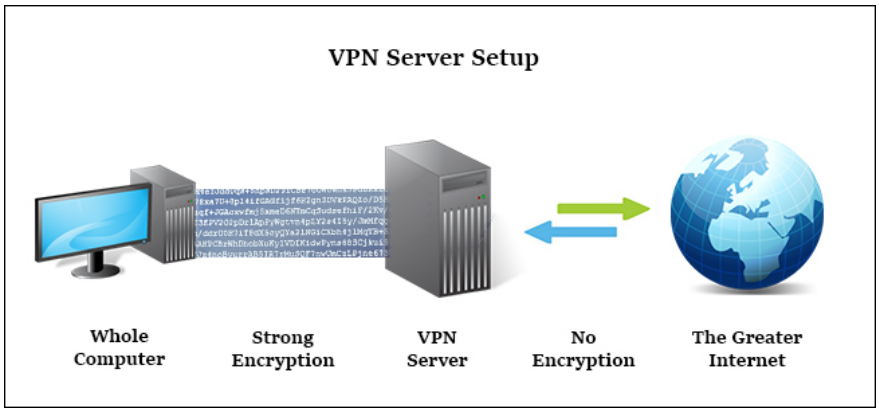
How to choose Proxy

While the Internet is flooded with thousands of free proxy servers, they are unreliable and have poor uptime. These types of services are suitable for tasks that only take a few minutes but really should not depend on free proxies from unreliable sources for important tasks. If you are looking for a quality free and secure proxy, you can find a free closed proxy server at Proxy4Free.com, a great free proxy database.

Although there are independent commercial services on the Internet like BTGuard, the increase of computers and mobile devices with faster connections (both reduce the impact of aerial encryption) has made proxies are no longer the security solution of many people, instead they switch to using high-end VPN solutions.

Network connection (VPN) is connected

Virtual private network, also known as VNP, is like a proxy that conceals a user's IP address, causing traffic to appear from a remote IP address. VPN is set up at the operating system and VPN connection level to capture the entire network connection of the configured device. This means that unlike a proxy server, simply acting as an intermediary server for a single application (like a web browser or BitTorrent client), VPN will retrieve all traffic. applications on computers, web browsers to online games and even Windows Update running in the background.



In addition, the entire process is transmitted through an encrypted tunnel between the computer and the remote network. This makes the VPN connection the most ideal solution for privacy or security protection. With VPN, ISP or any other party can access the transfer between your computer and the VPN server. For example, if you're traveling abroad and worried about logging into financial websites, email, or even securely linking to remote Home network, you can easily configure your computer. portable to use VPN.

With activating VPN, you will never have to worry about Wi-Fi network security at free coffee or Internet stores at the hotel full of security holes.

1. Find security holes on every site with Nikto

Although VPN is a great solution, they also have its disadvantages. To receive full connection encryption, you have to pay and the computer must be equipped with good hardware.

Another cost related to VPN is performance. Proxy servers simply transmit your information, there is no bandwidth cost and only a very small delay when using them. On the other hand, VPN servers handle both capacity and bandwidth. Using better VPN protocols and remote hardware, the cost you pay will be less.

Choosing a VPN seems more difficult than choosing a free proxy server. If you want a reliable and daily use VPN service, you should use Strong VPN.

1. 11 best VPN software

In short, proxies are appropriate to hide identity in low-level tasks such as "sneaking" to another country to watch sports matches, but when it comes to important tasks such as protecting you from snooping, then Please use VPN.

See also: How to make your VPN security safer?