

[Theory] What is Proxy Server?

Probably a lot of people have heard from Proxy, or Server Proxy, or Proxy Server! So do you know exactly what it is? In the article below, TipsMake.com will introduce you to this Proxy concept.

Probably a lot of people have heard from Proxy, or Server Proxy, or Proxy Server! So do you know exactly what it is? In the article below, TipsMake.com will introduce you to this Proxy concept.

Learn about Proxy Server

1. What is Proxy Server?
2. Features of Proxy Server
 1. Firewall and Filtering
 2. Share connection with Proxy Server
 3. Proxy Server and Caching
3. How the proxy server works
4. Why should you use a proxy server?
5. Proxy server risk
6. Types of proxy servers
 1. Transparent Proxy (Transparent Proxy)
 2. Anonymous proxy
 3. Distorting proxy (Distorting proxy)
 4. High anonymous proxy (High Anonymity proxy)

What is Proxy Server?

Proxy Server acts as a gateway between users and the Internet. This is an intermediary server between the end user and the website they visit. Proxy servers offer different functions, security and privacy depending on your needs or company policy.

If you are using a proxy server, Internet traffic will pass through the proxy server along its route to the address you require. After that, this request will return to the same proxy server (also the exception to this rule) and that proxy server forwards the data received from the website to the user.

Some network administrators use both firewalls and proxy servers to work together. To do so, they must install both firewall software and proxy server software on a gateway server.

Because of reopening the Application layer, the filtering function of proxy servers can be considered as a normal router. For example, a Web server proxy can check the URL of requests sent to web pages by inspecting HTTP GET and POST messages. Using this feature, network administrators can prevent access and in the domain illegally but allow access to other sites. Common firewalls, which cannot see Web domains within messages. With incoming data traffic, regular routers can filter by port number or network address, but proxy servers can also filter based on the application content within the notification.

Share connection with Proxy Server

Many software products for connection sharing on home networks have appeared in recent years. However, in medium and large size networks, proxy servers are still the solution that provides scalability and efficiency in Internet access. Instead of assigning each client a direct Internet connection, in this case, all internal connections can be passed through one or more proxies and in turn connect out.

Proxy Server and Caching

Web caching can improve the service quality of a network in three ways. First, it can preserve network bandwidth, increase scalability. Next, it is possible to improve responsiveness for clients. For example, with an HTTP proxy cache, Web pages can load faster in a web browser. Finally, proxy server caches can increase service availability. Web pages or other lines in the cache are still accessible even if the original source or intermediate network link is offline.

How the proxy server works

Every computer on the Internet must have a unique IP address. Think of this IP address as your home address. Just like the post office needs to know your street address to send mail, the Internet also needs to know the computer's IP address to send data to the right computer.

Proxy server is basically a computer on the Internet with its own IP address that your computer knows. When sending a web request, it will go to the first proxy server. Then the proxy server will perform your web request, collect feedback from the web server and forward the site data so that you can see the web page in the browser.

When the proxy server forwards the user's web request, it can change that data and still retrieve the information requested. The proxy server can change your IP address, so that the web server doesn't know your location. It can encrypt data so no one can read it during transport. And finally the proxy server can block access to specific websites based on IP addresses.

Why should you use a proxy server?

There are many reasons organizations and individuals should use proxy servers.

1. **To control Internet usage of employees and children:** Organizations and parents set up proxy servers to control and monitor employees or children using the Internet. Most organizations do not want their

employees to view specific websites during working time and they can configure proxy servers to deny access to specific websites, navigate you with a love note. Please do not view these websites on the corporate network. They can monitor and record all web requests, so even though they do not block the website, they still know the time you spend on jobs other than work.

2. **Save bandwidth and improve speed:** Organizations can also get better overall network performance when using a proxy server. Proxy servers can be cached (save a local site copy) of websites that are accessed. Therefore, when requesting TipsMake.com, the proxy server will check for the latest copy of this site and then send you a saved copy. This means that when hundreds of people access TipsMake.com at the same time from the same proxy server, this server only needs to send a request to TipsMake.com. This saves corporate bandwidth and improves network performance.
3. **Privacy :** Individuals and organizations also use proxy servers to browse the Internet more privately. Some proxy servers will change IP addresses and other identity information. This means that the destination server does not know who actually made the initial request, helping to keep your personal information and browsing habits more private.
4. **Improve security :** You can configure the proxy server to encrypt web requests so that no one can read your transaction. In addition, users can also avoid malicious websites through proxy servers. Organizations can connect their proxy servers to Virtual Private Networks (VPNs), so that remote users can access the Internet through the company's proxy. VPNs connect directly to the corporate network to be able to control and verify their users have access to the resources they need (email, internal data) and also provide secure connections for people. used to protect company data.
5. **Access to blocked resources :** Proxy servers allow users to circumvent content restrictions imposed by companies or some organizations. If access to the site is blocked, you can log in to the proxy server elsewhere and view it from there. Proxy servers make you look like you are in the US but you're actually in Vietnam.

5 REASONS WHY YOU SHOULD USE A PROXY SERVER



1

Control internet usage of employees or children.



2

Bandwidth savings and improved speeds.



3

Privacy benefits.



4

Improved security.



5

Access to blocked resources.



Proxy server risk

Be careful when choosing a proxy server, here are some risks when using a proxy server.

1. **Risks from free proxy server** . Using the server for free can be risky even for advertising based model services. Free usually means they don't invest heavily in hardware or auxiliary coding. You can see performance issues and potential data security issues. If you are using a completely free proxy server, be careful, some of them only seek to steal your credit card number.
2. **Diary of browsing history** . The proxy server has your original IP address and web request information, so be sure to check the proxy server logs and save that data.
3. **No coding** . If you use a proxy server without encryption, that means you are sending your request in plain text. Anyone can see your username, password and account information. Make sure the proxy server you use has encryption features.

Types of proxy servers

Not all proxy servers work the same way. It is important to understand exactly the functionality of each type of proxy server and make sure it meets your usage needs.

Transparent Proxy (Transparent Proxy)

The transparent proxy will tell the site that it is a proxy server and it still uses your IP address, determine the web request. Businesses, public libraries and schools often use transparent proxies to filter content because they are easy to set up client and server names.

Anonymous proxy

An anonymous proxy will identify itself as a proxy, but it will not transfer your IP address to the site - this helps prevent identity theft and keeps your browsing habits private. . They may also prevent a website from serving targeted marketing content based on your location. Browsing anonymously will prevent the site from using some ad targeting techniques, but not 100% guaranteed.

Distorting proxy (Distorting proxy)

A proxy server performs the same function as an anonymous server, but by sending the wrong IP address to the web server, you can appear from another location to access blocked content. .

See also: [Accessing websites blocked by ISP](#)

High anonymous proxy (High Anonymity proxy)

High anonymous anonymous proxy servers periodically change the IP addresses they appear on web servers, making it difficult to track who the traffic belongs to. High anonymous proxies, like the TOR network, are the most secure and private way to use the Internet.

See more:

1. [What is the difference between Proxy and VPN?](#)
2. [Summary of several ways to access blocked websites](#)
3. [The difference between Proxy and SOCKS](#)

You finished reading the article "[Theory] **What is Proxy Server?**" 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.