https://www.varonis.com/blog/what-is-a-proxy-server/

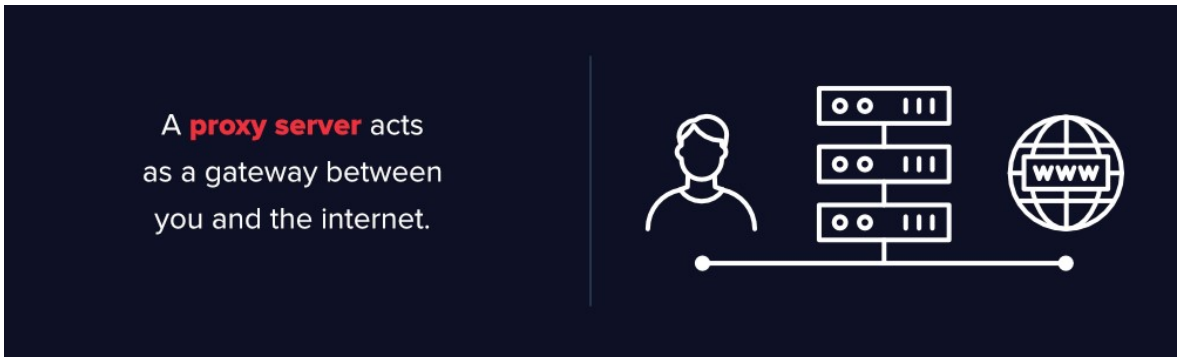
The actual nuts and bolts of how the internet works are not something people often stop to consider. The problem with that is the inherent danger of data security breaches and identity theft that come along with the cute dog pictures, 24-hour news updates, and great deals online.

But what actually happens when you browse the web? You might be using a proxy server at your office, on a Virtual Private Network (VPN) or you could be one of the more tech-savvy who always use a proxy server of some kind or another.

What's a Proxy Server?

A proxy server is any machine that translates traffic between networks or protocols. It's an intermediary server separating end-user clients from the destinations that they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

If you're using a proxy server, traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.



If that's all it does, why bother with a proxy server? Why not just go straight from to the website and back?

Modern proxy servers do much more than forward web requests, all in the name of data security and network performance. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. Lastly, proxy servers can provide a high level of privacy.

How Does a Proxy Server Operate?

Every computer on the internet needs to have a unique Internet Protocol (IP) Address. Think of this IP address as your computer's street address. Just as the post office knows to deliver your mail to your street address, the internet knows how to send the correct data to the correct computer by the IP address.

A proxy server is basically a computer on the internet with its own IP address that your computer knows. When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.

When the proxy server forwards your web requests, it can make changes to the data you send and still get you the information that you expect to see. A proxy server can change your IP address, so the web server doesn't know exactly where you are in the world. It can encrypt your data, so your data is unreadable in transit. And lastly, a proxy server can block access to certain web pages, based on IP address.

What are Forward Proxies

A forward proxy server sits between the client and an external network. It evaluates the outbound requests and takes action on them before relaying that request to the external resource.

Most proxy services that you're likely to encounter are forward proxies. Virtual Private Networks and Web content filters are both examples of forward proxies.

What are Reverse Proxies

A reverse proxy server sits between a network and multiple other internal resources. A large website might have dozens of servers that collectively serve requests from a single domain. To accomplish that, client requests would resolve to a machine that would act as a load balancer. The load balancer would then proxy that traffic back to the individual servers.

Some popular open source reverse proxies are:

- Varnish
- Squid

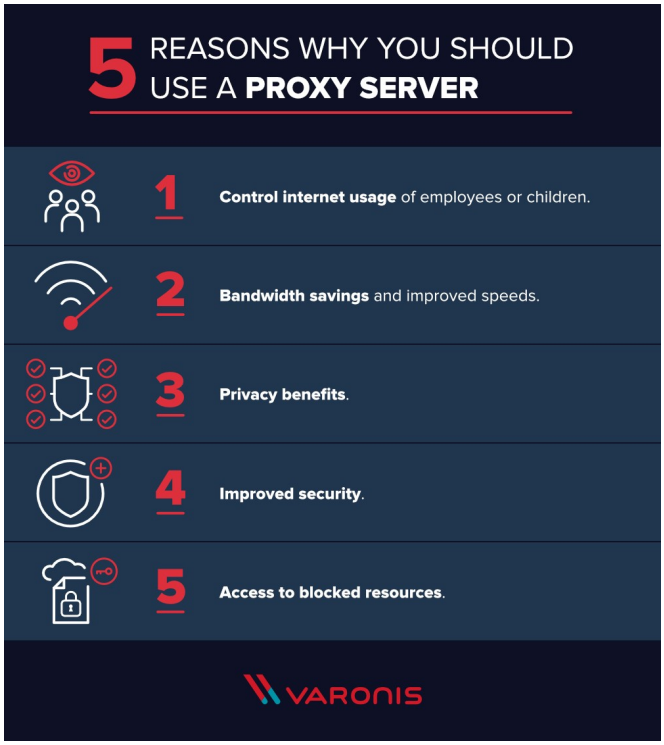
Why Should You Use a Proxy Server?

There are several reasons organizations and individuals use a proxy server.

- **To control internet usage of employees and children:** Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet. Most

organizations don't want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites, instead redirecting you with a nice note asking you to refrain from looking at said sites on the company network. They can also monitor and log all web requests, so even though they might not block the site, they know how much time you spend cyberloafing.

- **Bandwidth savings and improved speeds:** Organizations can also get better overall network performance with a good proxy server. Proxy servers can cache (save a copy of the website locally) popular websites – so when you ask for www.varonis.com, the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy. What this means is that when hundreds of people hit www.varonis.com at the same time from the same proxy server, the proxy server only sends one request to varonis.com. This saves bandwidth for the company and improves the network performance.
- **Privacy benefits:** Individuals and organizations alike use proxy servers to browse the internet more privately. Some proxy servers will change the IP address and other identifying information the web request contains. This means the destination server doesn't know who actually made the original request, which helps keeps your personal information and browsing habits more private.
- **Improved security:** Proxy servers provide security benefits on top of the privacy benefits. You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server. Additionally, organizations can couple their proxy server with a Virtual Private Network (VPN), so remote users always access the internet through the company proxy. A VPN is a direct connection to the company network that companies provide to external or remote users. By using a VPN, the company can control and verify that their users have access to the resources (email, internal data) they need, while also providing a secure connection for the user to protect the company data.
- **Get access to blocked resources:** Proxy servers allow users to circumvent content restrictions imposed by companies or governments. Is the local sportsball team's game blacked out online? Log into a proxy server on the other side of the country and watch from there. The proxy server makes it look like you are in California, but you actually live in North Carolina. Several governments around the world closely monitor and restrict access to the internet, and proxy servers offer their citizens access to an uncensored internet.



Now that you have an idea about why organizations and individuals use a proxy server, take a look at the risks below.

Proxy Server Risks

You do need to be cautious when you choose a proxy server: a few common risks can negate any of the potential benefits:

- **Free proxy server risks**
  - You know the old saying "you get what you pay for?" Well, using one of the many free proxy server services can be quite risky, even the services using ad-based revenue models.
  - Free usually means they aren't investing heavily in backend hardware or encryption. You'll likely see performance issues and potential data security issues. If you ever find a completely "free" proxy server, tread very carefully. Some of those are just looking to steal your credit card numbers.
- **Browsing history log**
  - The proxy server has your original IP address and web request information possibly unencrypted, saved locally. Make sure to check if your proxy server logs and saves that data – and what kind of retention or law enforcement cooperation policies they follow.
  - If you expect to use a proxy server for privacy, but the vendor is just logging and selling your data you might not be receiving the expected value for the service.

- **No encryption**
  - If you use a proxy server without encryption, you might as well not use a proxy server. No encryption means you are sending your requests as plain text. Anyone who is listening will be able to pull usernames and passwords and account information really easily. Make sure whatever proxy server you use provides full encryption capability.

Types of Proxy Servers

Not all proxy servers work the same way. It's important to understand exactly what functionality you're getting from the proxy server, and ensure that the proxy server meets your use case.

Transparent Proxy

- A transparent proxy tells websites that it is a proxy server and it will still pass along your IP address, identifying you to the web server. Businesses, public libraries, and schools often use transparent proxies for content filtering: they're easy to set up both client and server side.

Anonymous Proxy

- An anonymous proxy will identify itself as a proxy, but it won't pass your IP address to the website – this helps prevent identity theft and keep your browsing habits private. They can also prevent a website from serving you targeted marketing content based on your location. For example, if CNN.com knows you live in Raleigh, NC, they will show you news stories they feel are relevant to Raleigh, NC. Browsing anonymously will prevent a website from using some ad targeting techniques, but is not a 100% guarantee.

Distorting proxy

- A distorting proxy server passes along a *false* IP address for you while identifying itself as a proxy. This serves similar purposes as the anonymous proxy, but by passing a false IP address, you can *appear* to be from a different location to get around content restrictions.

High Anonymity proxy

- High Anonymity proxy servers periodically change the IP address they present to the web server, making it very difficult to keep track of what traffic belongs to who. High anonymity proxies, like the TOR Network, is the most private and secure way to read the internet.

Proxy servers are a hot item in the news these days with the controversies around Net Neutrality and censorship. By removing net neutrality protections in the United States, Internet Service Providers (ISP) are now able to control your bandwidth and internet traffic. ISPs can potentially tell you what sites you can and cannot see. While there's a great amount of uncertainty around what is going to happen with Net Neutrality, it's possible that proxy servers will provide some ability to work around an ISPs restrictions.

Varonis analyzes data from proxy servers to protect you from data breaches and cyber attacks. The addition of proxy data gives more context to better analyze user behavior trends for abnormalities. You can get an alert on that suspicious activity with actionable intelligence to investigate and deal with the incident.

For example, a user accessing GDPR data might not be significant on its own. But if they access GDPR data and then try to upload it to an external website, it could be an exfiltration attempt and

potential data breach. Without the context provided by file system monitoring, proxy monitoring, and Varonis threat models, you might see these events in a vacuum and not realize you need to prevent a data breach.