What is a Proxy Server?

A proxy server is an intermediary server that retrieves data from an Internet source, such as a webpage, on behalf of a user. They act as additional data security boundaries protecting users from malicious activity on the internet.

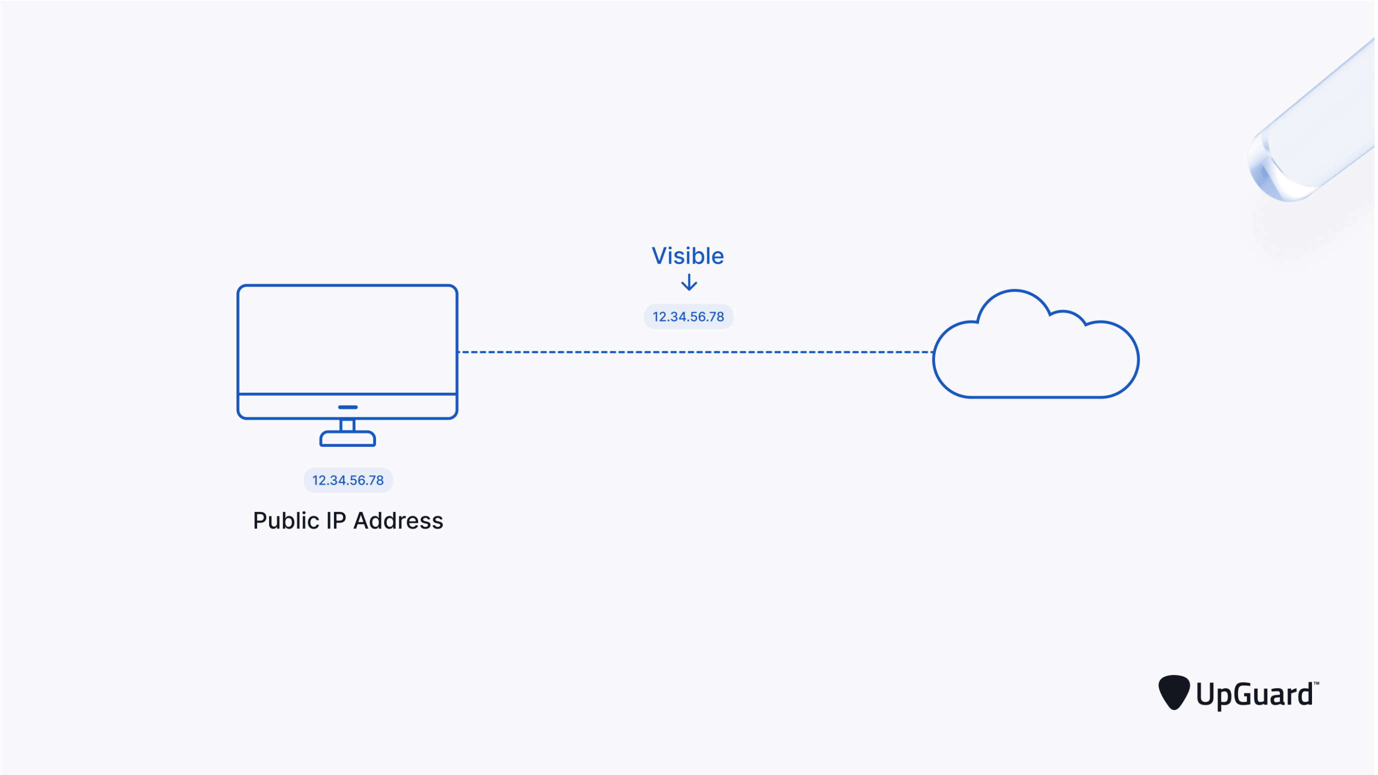
Proxy servers have many different uses, depending on their configuration and type. Common uses include facilitating anonymous Internet browsing, bypassing geo-blocking, and regulating web requests.

Like any device connected over the Internet, proxies have associated cybersecurity risks that users should consider before use.

How Does a Proxy Server Work?

Proxy servers work by facilitating web requests and responses between a user and web server.

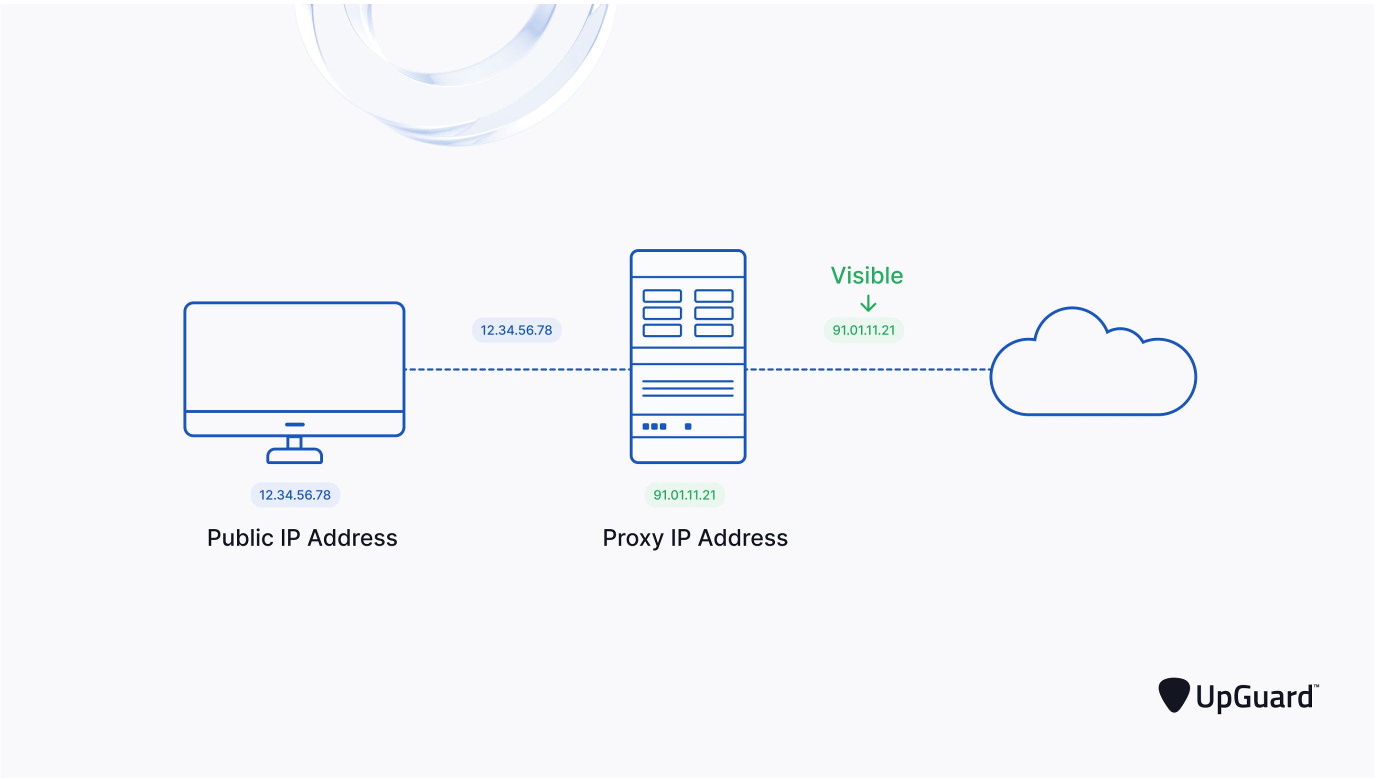
Typically, a user accesses a website by sending a direct request to its web server from a web browser via their IP address. The web server then sends a response containing the website data directly back to the user.



A proxy server acts as an intermediary between the user and the web server. Proxy servers use a different IP address on behalf of the user, concealing the user's real address from web servers.

A standard proxy server configuration works as follows:

1. A user enters a website's URL into their browser.
2. The proxy server receives the user's request.
3. The proxy server forwards the request to the web server.
4. The web server sends a response (website data) back to the proxy server.
5. The proxy server forwards the response to the user.



Types of Proxy Servers

There are many different types of proxy servers, categorized by traffic flow, anonymity level, application, service, IPs, and accessibility.

Below is a classification of some of the different types of proxy servers f

1. Forward Proxy Server

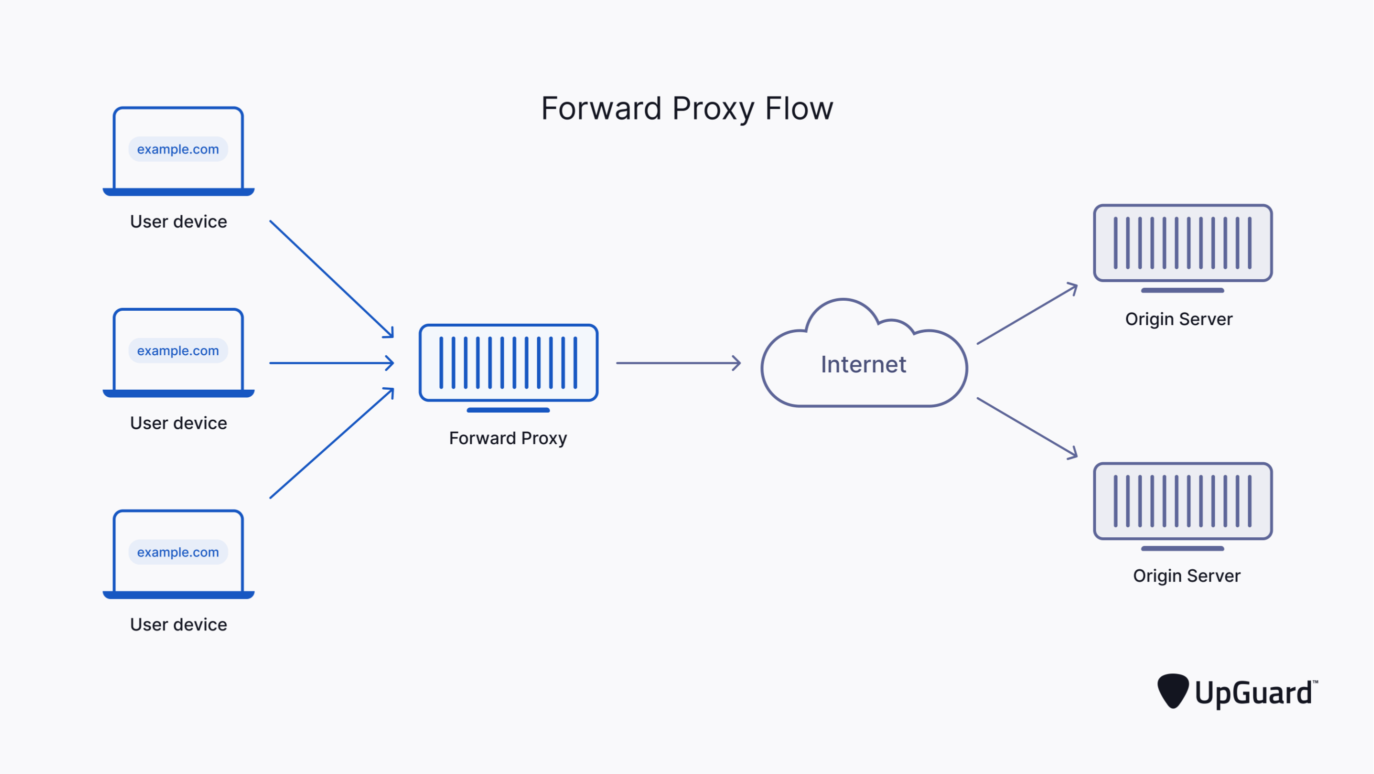
A forward proxy (commonly known as a ‘proxy') is a type of proxy server that typically passes requests from users in an internal network to the Internet via a firewall.

Forward proxies are configured to either ‘allow' or ‘deny' the user's request to pass through the firewall to access content on the Internet.

If the proxy allows the user's request, it forwards it to the web server through the firewall. The web server sends its response to the proxy. The proxy then sends this response back to the user.

A forward proxy will first check if the user's requested information is cached before retrieving it from the server. The proxy stores cached information itself, eliminating the need to request it from the server. If the requested information is cached, the proxy will send it directly to the user.

If the proxy denies the user's request, it sends the user an error or redirect message.



2. Reverse Proxy Server

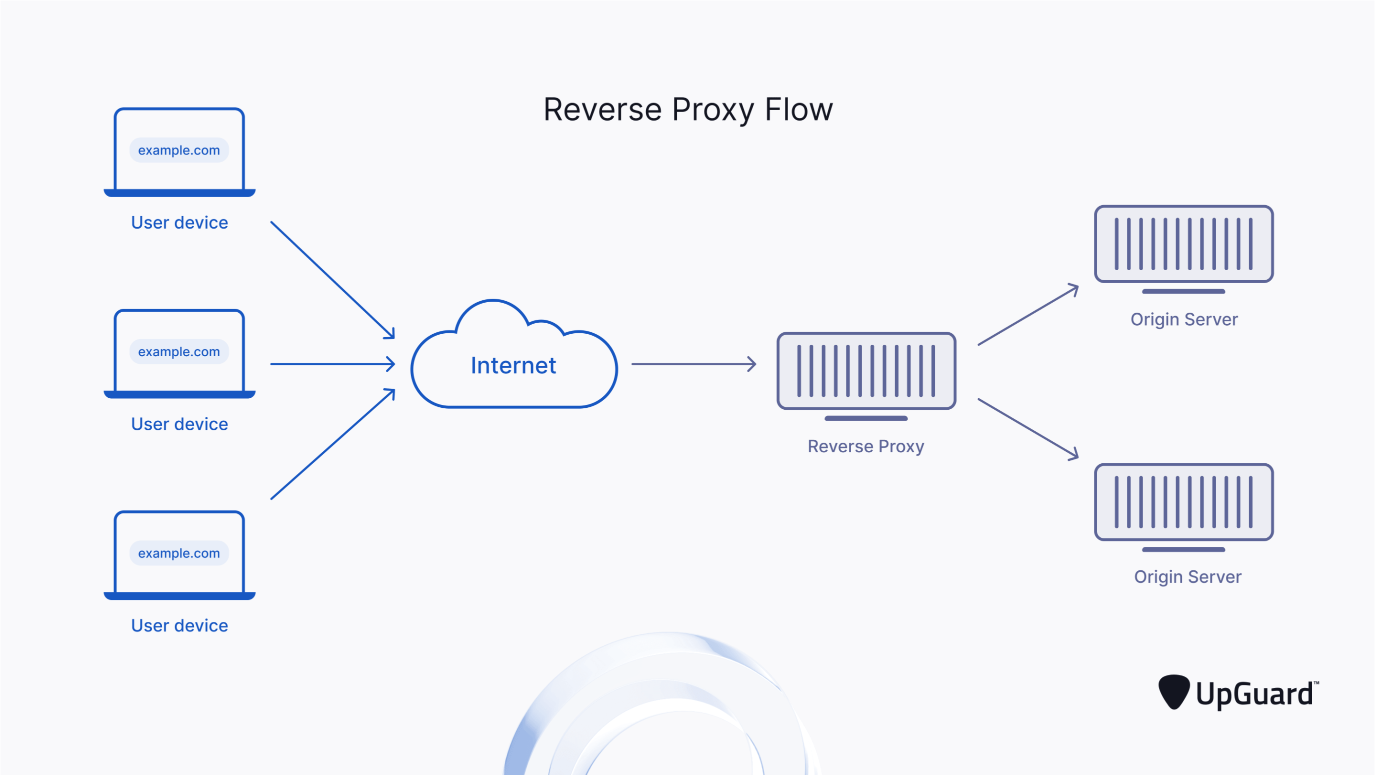
A reverse proxy is a type of proxy server that typically passes requests from the Internet through to users in an internal network via a firewall; essentially, a forward proxy in ‘reverse'.

Reverse proxies are configured to restrict and monitor users' access to web servers containing sensitive data. User requests are passed through the Internet via a firewall to the reverse proxy.

If the proxy allows the user's request, it retrieves this information from the web server and responds to the user.

A reverse proxy will first check if the user's requested information is cached before retrieving it from the server. The proxy stores any cached information, eliminating the need to request it from the server. If the requested information is cached, the proxy will send it directly to the user.

If the proxy denies the user's request, it sends the user an error or redirect message.



3. Anonymous Proxy Servers

High Anonymity Proxy Server (Level 1)

High anonymity proxies offer the most security to a user. They conceal the user's IP address and do not identify themselves as proxies to web servers (unlike anonymous proxies). These proxies routinely change IP addresses when making requests to web servers, allowing a high level of privacy.

Anonymous Proxy Server (Level 2)

An anonymous proxy (also called a distorting proxy) conceals a user's real IP address when they visit a website. The proxy server ‘distorts' its own IP address by changing its geolocation to the web server. Anonymous proxies identify as proxies in web server requests.

Anonymous proxies are one of the most commonly used proxies. They can be used to hide geographical location, avoid targeted marketing, or access sites that are censored in the user's actual location.

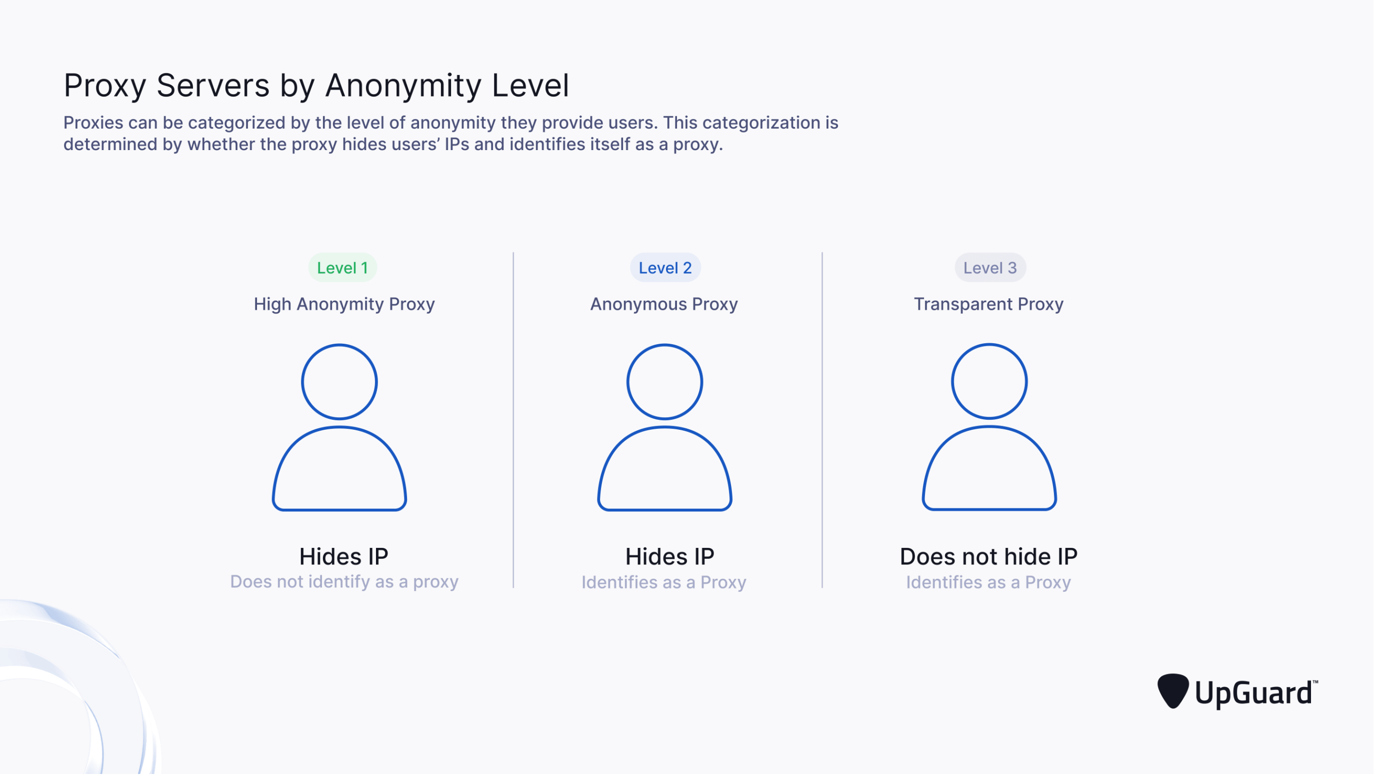
TOR (The Onion Router) is a free, open-source web browser that routes users' internet traffic through a network of volunteer servers to provide anonymity. TOR helps remove visibility over Internet activity by encrypting, decrypting, and re-encrypting web requests many times before they reach the destination server - a process known as ‘onion routing'.

An anonymous proxy is the opposite of a transparent proxy.

Transparent Proxy Server (Level 3)

A transparent proxy is the opposite of an anonymous proxy. As its name suggests, transparent proxies do not conceal any identifying information about the user.

They send a request to the web server that shows as coming directly from the user. Transparent proxies are set up by a network operator or website, not the user, and are commonly used by organizations, public libraries, and schools for website content filtering purposes. Transparent proxies are one the easiest proxies to set up.



Proxy Servers by Anonymity Level

Proxies can be categorized by the level of anonymity they provide users. This categorization is determined by whether the proxy hides users' IPs and identifies itself as a proxy.

Level 1	Level 2	Level 3
High Anonymity Proxy	Anonymous Proxy	Transparent Proxy
Hides IP	Hides IP	Does not hide IP
Does not identify as a proxy	Identifies as a Proxy	Identifies as a Proxy

4. Protocol Proxy Servers

HTTP Proxy Server

HTTP proxies use the HTTP protocol and are not configured by the user. Instead, they are either configured by the browser or within the website's interface. The HTTP proxy works exclusively with web content and cannot be used for any other data types.

HTTP proxies allow users to browse the web with a different IP address but do not offer any additional privacy or security. All user activity is still visible over the Internet, the same as without a proxy.

While some HTTP proxies allow users to connect to HTTPS websites, enabling encrypted internet connections, this is not always the case. HTTP proxies may completely filter out HTTPS connections or only allow users to connect to unsecured versions of a website, even if it also allows secure connections.

Many HTTP proxies are free and monetize their services by injecting ads into the unsecured connection. Users should exercise caution when accessing HTTP proxies.

HTTPS Proxy Server

The HTTPS proxy (also called SSL Proxy) works similarly to the HTTP proxy but differs in that it establishes secure connections. The HTTPS proxy works exclusively with web content and cannot be used for any other data types.

HTTPS proxies encrypt all web traffic using the HTTPS protocol. HTTPS websites are already encrypted through SSL certificates, offering users private and secure connections. If a user connects to an HTTPS website via an HTTPS proxy, their connection is doubly secured.

SOCKS Proxy Server

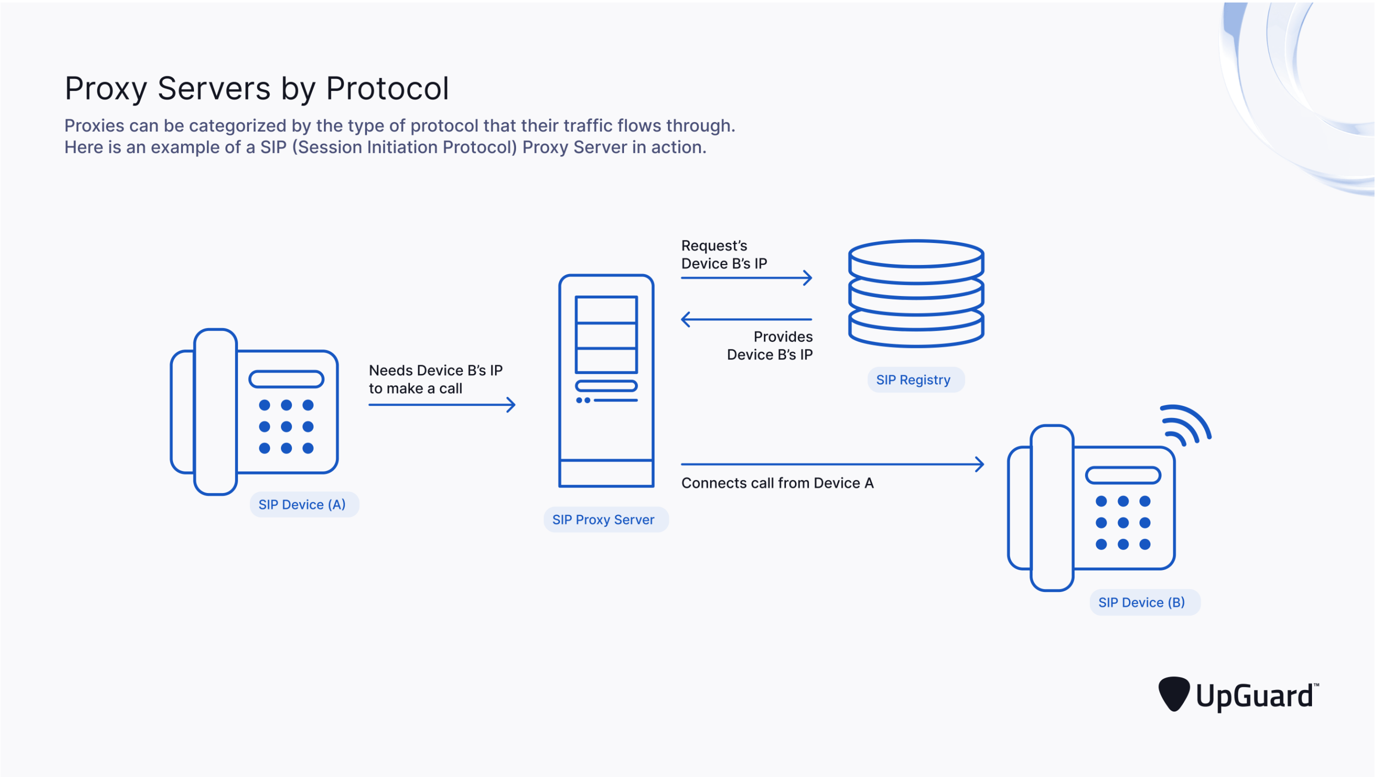
The SOCKS (SOCKets Secure) proxy allows any type of traffic that is compatible with the SOCKS5 protocol. The SOCKS5 protocol routes users' traffic through a third-party server - SOCKS proxy server - via TCP (Transmission Control Protocol).

SOCKS proxies do not offer their own encryption. They can only operate through secured connections if the website/app they are working with uses encryption itself.

Most SOCKS proxy servers support SHH, which enables secure connections with apps that also support SHH. It's important to note that even with SHH enabled, SOCKS proxies do not guarantee anonymity.

SIP Proxy

A SIP (Session Initiation Protocol) proxy works as an intermediary between SIP devices (e.g. telephones) through the SIP protocol. SIP proxies control calls within a network by requesting information from the SIP registry and directing calls accordingly.


Proxy Servers by Protocol
Proxies can be categorized by the type of protocol that their traffic flows through.
Here is an example of a SIP (Session Initiation Protocol) Proxy Server in action.
Request's Device B's IP
Provides Device B's IP
SIP Registry
Needs Device B's IP to make a call
SIP Device (A)
SIP Proxy Server
Connects call from Device A
SIP Device (B)
UpGuard

SMTP Proxy Server

An SMTP (Simple Mail Transfer Protocol) proxy works as an intermediary for mail transfer through the SMTP protocol. The proxy is configured to allow or deny incoming and outgoing emails based on factors, such as source address, the sender's server, and even the content of the email.

As SMTP does not provide an authentication method, it does not protect users from cybercrimes like email spoofing. Organizations need to implement additional email security measures to authenticate incoming emails, such as Sender Policy Framework (SPF) filtering, Domain Key Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC).

SMTP proxies can also be used to:

- Filter spam and inappropriate content
- Protect users from cyber attacks such as phishing attacks and malware
- Load balance SMTP traffic

FTP Proxy Server

An FTP (File Transfer Protocol) proxy works as an intermediary between all traffic through the FTP protocol. FTP is a protocol used for exchanging files over the Internet and internal networks.

FTP proxies allow or deny file transfers based on factors, such as source/destination IP addresses and user authentication.

FTP proxies can also be used to:

- Regulate the quantity and frequency of file transfers
- Filter certain senders/receivers from file transfers
- Limit the size of transferred files
- Authenticate users/receivers before file transfer begins

DHCP Proxy Agent

The DHCP (Dynamic Host Configuration Protocol) proxy agent is a network management tool that works as an intermediary between DHCP devices and requests through the DHCP protocol.

DHCP servers send network configuration to devices within a network.

Sometimes, devices connected to a subnetwork via a router cannot send configuration requests to the DHCP server. A DHCP proxy agent forwards such devices' requests to the server, receives the response, and relays this back to the device.

DNS Proxy Server

A DNS proxy forwards DNS (Domain Name System) requests from the user to a DNS server. DNS is a system that allows users to enter a domain name (e.g. http://google.com) into their browser rather than its IP address.

When a user enters a domain name, DNS will choose which of the domain's servers will complete the user's request. DNS servers can either allow access to a domain or block requests from an IP based on several factors, such as authentication or geolocation restrictions.

DNS proxies can also be used to:

- Load balance DNS Security Extensions (DNSSEC)-aware servers
- Protect servers from domain hijacking and DNS spoofing
- Speed up the domain lookup process and performance
- Cache and forward DNS requests between DNS servers

Smart DNS Proxy Server

A Smart DNS proxy enables users to bypass DNS restrictions such as geo-location restrictions. Unlike regular proxy servers, Smart DNS proxies only divert one part of a user's internet traffic - DNS requests.

DNS servers will usually connect users to the closest web server in their geo-location. Certain online content, such as video streaming services and news platforms, restrict their content based on location.

Smart DNS proxies work around these restrictions by directing DNS requests to specific servers that allow access to such content. For example, if an Australian user wants to access US content, the Smart DNS proxy will divert the DNS request to a US-based server.

CGI Proxy Server

A CGI (Common Gateway Interface) proxy is a type of web proxy server that allows users to access websites anonymously via a web form. As CGI proxies are web-based, they allow users to access the proxy's services on devices or networks that do not allow proxy configurations.

5. Access Proxy Servers

Public Proxy Server

A public proxy (also called an open proxy or shared proxy) is available for use by any Internet user, free of charge. The proxy allows users to browse the Internet anonymously by providing access to its IP address.

Public proxies are ideal for cost-sensitive users but not for those with data security and speed concerns. As many users are drawn in by the free service of public proxies, they are prone to lagging. The open nature also puts users at higher risk of compromising sensitive data if they share personal information through the proxy, much like public wi-fi networks.

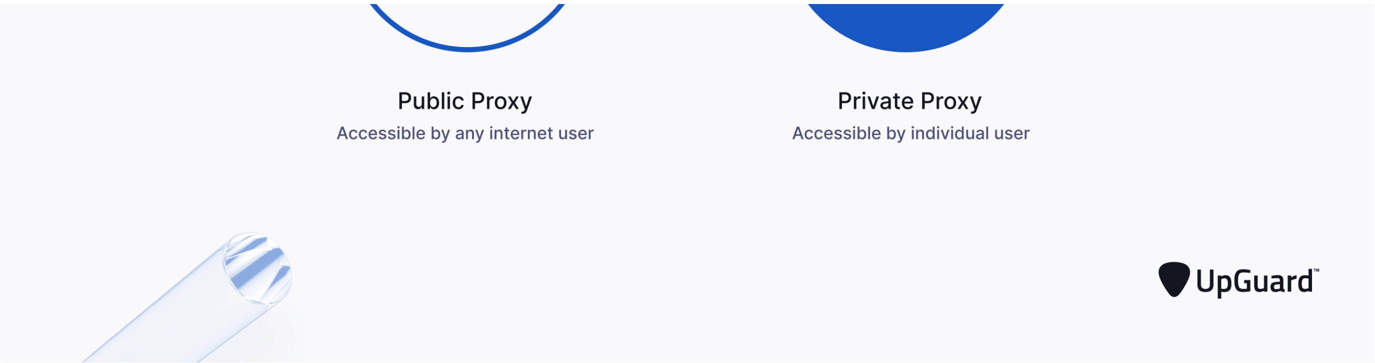
Private Proxy Server

A private proxy (also called a dedicated proxy) provides individual users access exclusive access to a provided IP address.

As the IP address is allocated exclusively to a specific user, it is much safer to use than a public proxy.

Private proxies are ideal for users who value greater privacy over the Internet and are willing to invest in the higher costs required to access their services.

Proxy Servers by Accessibility
Proxies can be categorized by their accessibility to users.


Public Proxy
Accessible by any internet user
Private Proxy
Accessible by individual user
UpGuard

6. IP Location/Source Proxy Servers

Data Center Proxy Server

A data center proxy is not affiliated with an Internet Service Provider (ISP). Data center proxies create artificial IP addresses, providing users with anonymity on the Internet.

While these proxies are cheaper and faster to run than residential proxies, they are also less reliable. Web servers can easily identify data center proxies and quite often block their access to websites.

Residential Proxy Server

A residential proxy is affiliated with an ISP. Residential proxies provide users with real IP addresses from a physical location to enable anonymous Internet activity.

Residential proxies are costlier than data center proxies but are more reliable. As they use real residential addresses, web servers are more trusting of residential proxies and are less likely to flag them.

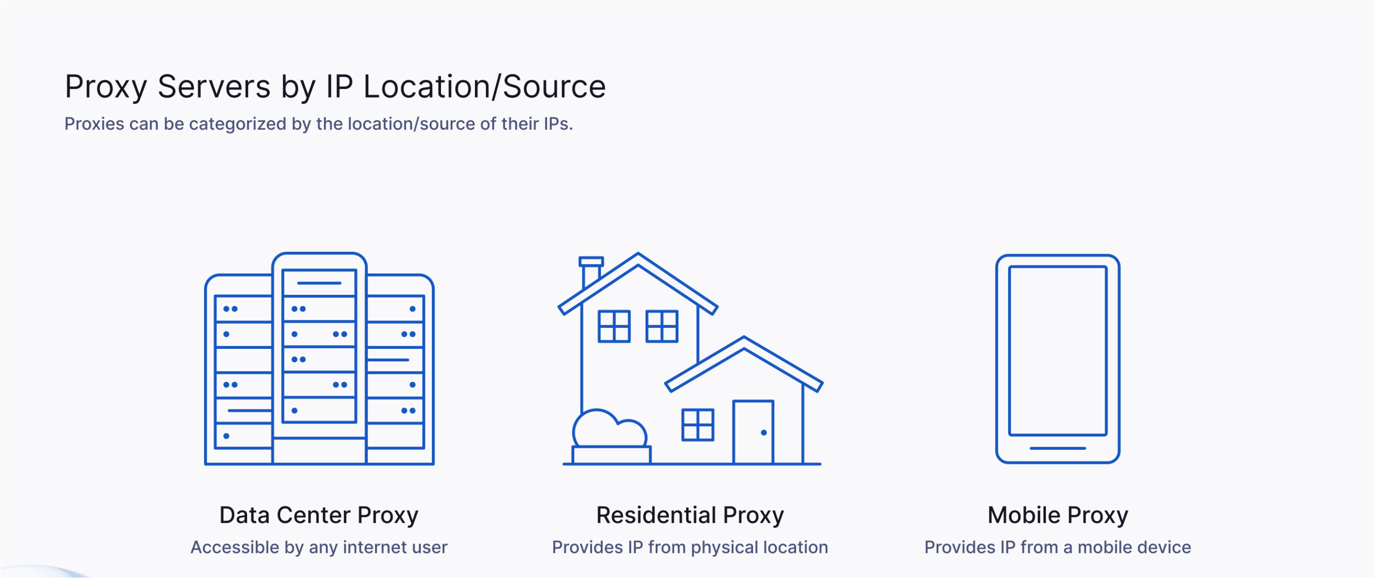
There are two types of residential proxy servers:

- **Static Proxy Server:** A static proxy server assigns users with a single residential IP address. Static proxies are often less secure than rotating proxies as hackers can easily access them. They are also easier to trace than rotating proxies, as they operate through a single source.
- **Rotating Proxy Server:** A rotating proxy server assigns users with a different IP from a pool of proxy IP addresses each time they make a new connection. Rotating proxies are more secure than static proxies as their changing nature makes them harder to trace.

Mobile Proxy Server

A mobile proxy uses IP addresses from devices that use mobile data (through 3G, 4G, or 5G), e.g. smartphones and tablets. Desktop device users can use mobile proxies to appear as mobile devices in web server requests.

Mobile proxies help users with ad and app testing, UX, and other product development purposes.


Proxy Servers by IP Location/Source
Proxies can be categorized by the location/source of their IPs.
Data Center Proxy
Accessible by any internet user
Residential Proxy
Provides IP from physical location
Mobile Proxy
Provides IP from a mobile device

What is the Difference Between a Proxy Server and a VPN?

While proxy servers and VPNs (Virtual Private Networks) share some common features, their differences far outweigh their similarities.

Proxy servers and VPNs both act as an intermediary between the user and a website. Proxies and VPNs forward the user's request to the web server and conceal location and connection information by changing their IP addresses.

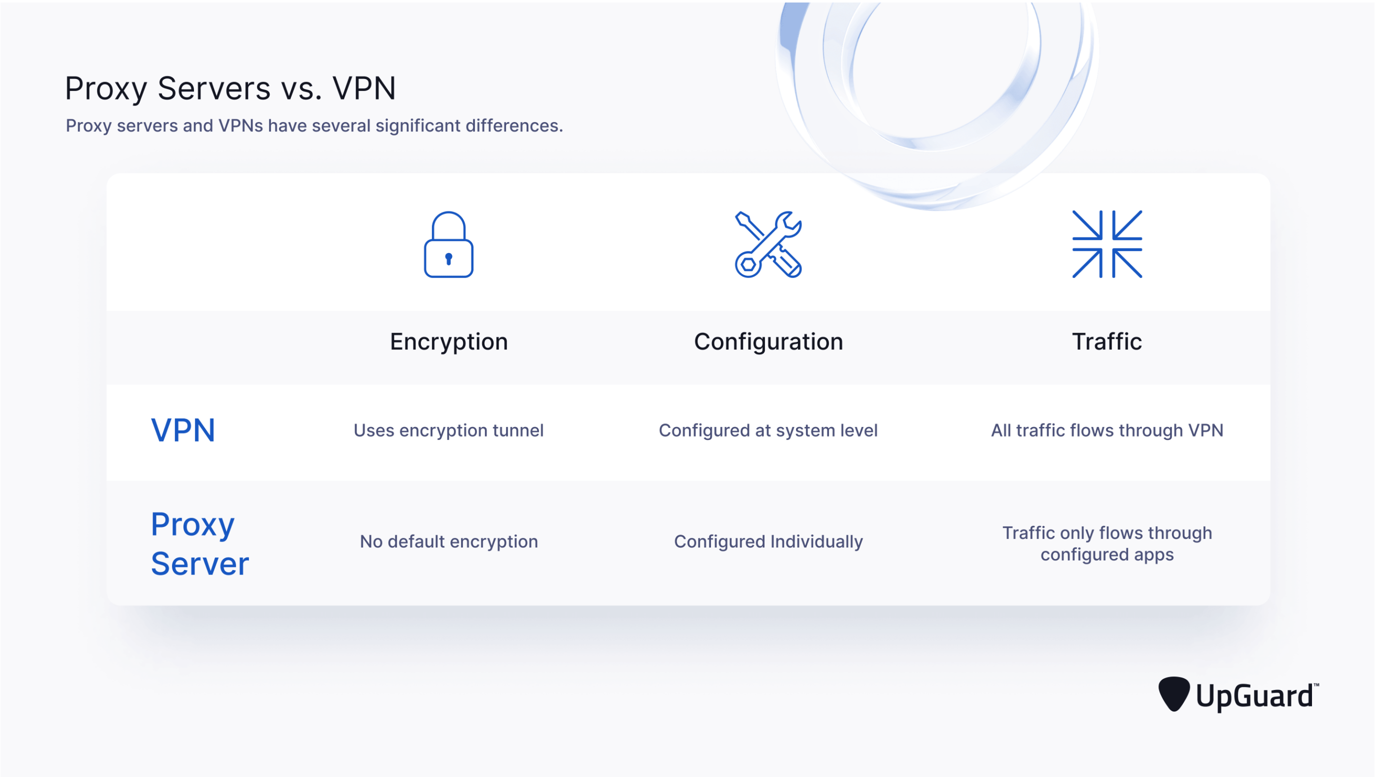
The key differences between proxy servers and VPNs are how they work and which protocols they support, which affects their privacy and security capabilities.

VPNs are typically configured at a system level, allowing all traffic to pass through them, e.g., web browsing, music streaming, file sharing, gaming. Many VPN software solutions allow users to exclude selected apps from operating through the VPN, but the default settings usually direct all traffic through them.

Proxy servers are typically configured individually, meaning users must configure their proxy connection settings separately to direct traffic through the proxy. Until a user has configured the proxy on an app, it will remain unaffected by the proxy's existing connections on the same device.

Generally, VPNs are more secure than proxy servers due to the way they operate. VPNs create an encrypted tunnel between a user's device and the outside network. The tunnel allows users to browse the web without sharing their IP address and other identifying connection data.

Proxy servers work differently from VPNs in this sense - the level of security they provide depends on which protocol they are using, as each protocol offers a differing level of network security.



Proxy Servers vs. VPN

Proxy servers and VPNs have several significant differences.

	Encryption	Configuration	Traffic
VPN	Uses encryption tunnel	Configured at system level	All traffic flows through VPN
Proxy Server	No default encryption	Configured Individually	Traffic only flows through configured apps

Proxy Server vs. VPN Summary

Proxy servers are often cheaper and faster than VPNs because they usually do not offer secure connections.

VPNs can be used across an entire system as most apps can't recognize when they are connected through an encrypted VPN tunnel. Proxies need to be configured individually across apps.

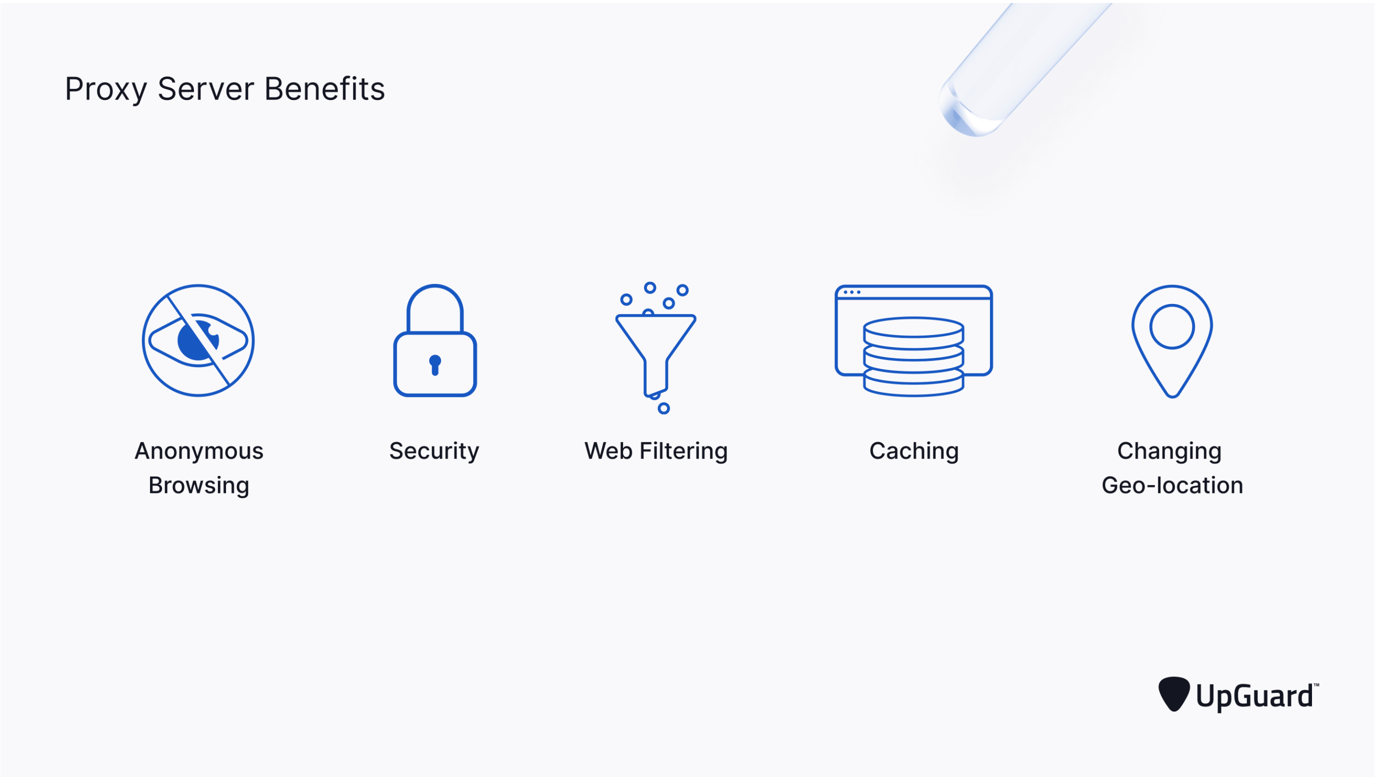
Web-based proxies are advantageous over VPNs on devices where users can't change software settings if privacy is not a significant concern. Users should be careful not to share personally identifiable information (PII), or login credentials like usernames and passwords, over web-based proxies.

A proxy server can't encrypt data on its own; it just changes a user's IP address. VPNs change a user's IP address and encrypt the data transfers between the device and Internet, allowing private and secure web browsing.

What are the Benefits of Using a Proxy Server?

Proxy servers offer several benefits to users. It is important to note that these benefits are dependent on the proxy's type and configuration. Users should always find out the specific capabilities of a proxy before using it.

- **Anonymous Browsing:** Anonymous proxies allow users to browse the web anonymously by concealing their IP addresses.
- **Security:** Some proxy server types (e.g., HTTPS proxies) can be configured to provide secure connections through encryption. Organizations can use transparent proxies to block certain websites that are flagged as malware. SMTP proxies can block malicious emails, such as phishing attacks, from reaching employee inboxes. Reverse proxies are effective at helping organizations prevent Distributed Denial of Service (DDoS) attacks and man-in-the-middle (MITM) attacks by blocking suspicious and repeated requests.
- **Web filtering:** Organizations often use transparent proxies to restrict employees from accessing certain websites. Transparent proxies also log user activity, allowing organizations to monitor employees' Internet use at work.
- **Web acceleration:** Proxy servers can speed up data transfer and conserve bandwidth by caching popular websites. When a user requests data from a server via a proxy, the proxy will first check if a cached copy is available in its database. Cached data reduces the number of web requests from the proxy server, making data retrieval much faster for the user. Reverse proxy servers are often used for load balancing, which spreads user requests evenly across servers to improve speeds.
- **Changing Geo-Location:** Organizations can use rotating proxies for Internet-based marketing activities where data is dependent on geo-location. Such activities could include price aggregation, web scraping, market research, and SEO.



What Security Risks are Associated with Using a Proxy Server?

Like any third-party service operating over the Internet, proxy servers are not without their cyber risks. Users should understand the common risks associated with proxies to decide if they are fit-for-purpose.

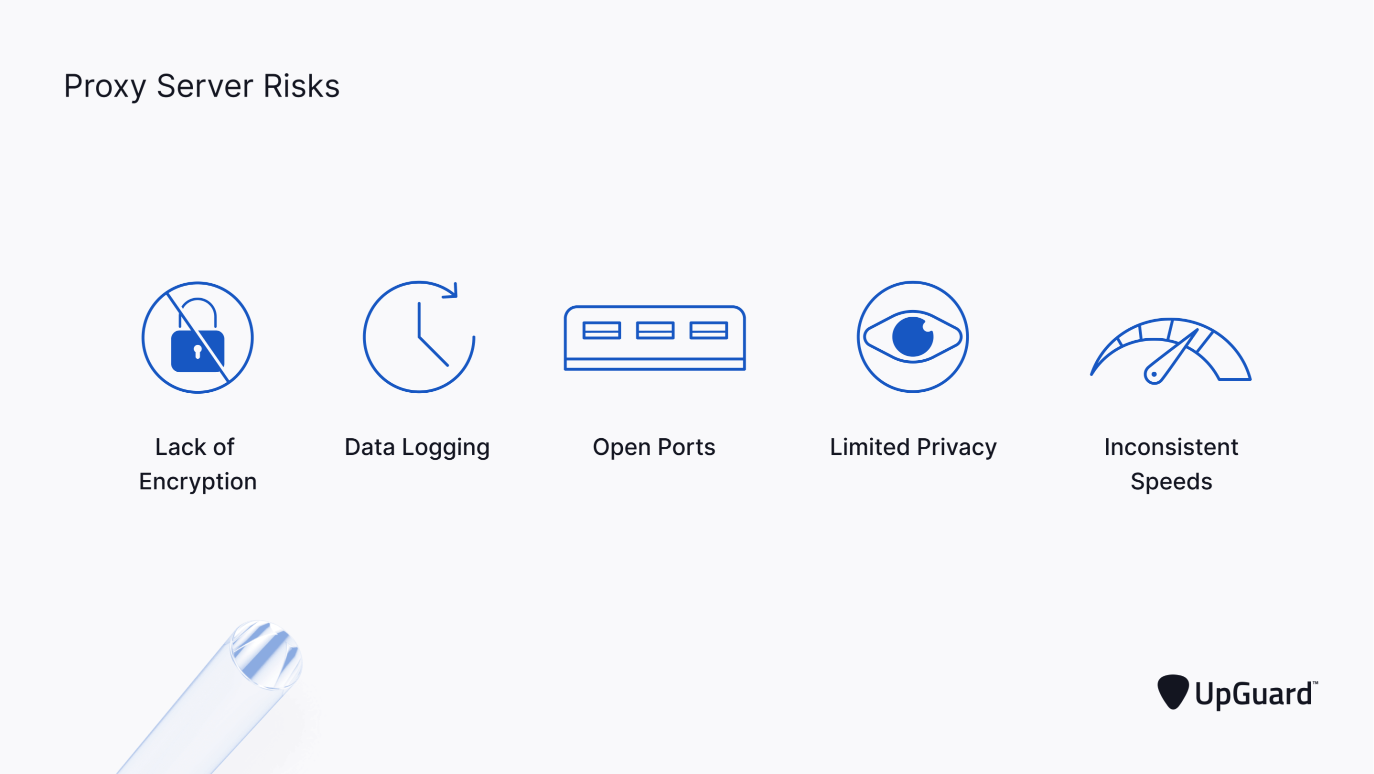
- **Lack of encryption:** Unless a proxy is configured with encryption, it will operate through an unsecured connection. Attackers can easily intercept communications over unsecured proxies, meaning any sensitive data like usernames and passwords are at risk of being compromised. Unsecured connections also put users at high risk of data breaches, such as identity theft. Users should ensure they are using encrypted proxies to maximize network security.

- **Data logging**: Proxy servers store users' IP addresses along with their web request data. Some proxies do not encrypt this information and, depending on the service, may even sell the data to other parties - once again, putting users at risk of data breaches. Users should always read the terms and conditions before using a proxy.

- **Open ports**: Most proxies run on open ports, which can be exploited through security vulnerabilities. Open ports also increase security risks as they increase an organization's total number of attack vectors.

- **Limited privacy:** While proxy servers conceal users' IP addresses, this privacy does not necessarily extend beyond web requests. Free proxies often operate over unsecured networks and ad-based revenue models. Not only does this mean that anyone can ‘listen' to user traffic, but these ads are often injected with viruses or other types of malware, which can easily infiltrate devices.

- **Inconsistent speed:** Free proxies are susceptible to traffic overload. Servers often do not have the necessary bandwidth to serve thousands of users at once with maintained speeds and are prone to lagging.



Are Proxy Servers Safe to Use?

The safety of a proxy ultimately comes down to proxy type and server configuration. Users must understand how the specific proxy they are using operates before engaging in Web activity through it.

While proxy services offer some privacy to the user by concealing their IP address, the proxy itself logs this information, along with browsing history. Depending on the type of proxy, this data could be forwarded to external parties, causing a data breach.

Some proxies are not configured with encryption, meaning the user's online activity is available in plain text for anyone to see. Users should assume a proxy is not encrypted unless the proxy server settings state otherwise, and use unencrypted proxies at their own risk.

Private proxies are safer than public proxies as they provide exclusive access to users instead of being open for use by anyone on the Internet.

Generally, free proxies are the least safe to use as they have open access and are often unencrypted.

How Do I Set Up a Proxy Server?

Proxy settings vary across operating systems and web browsers.

You will need to find the Local Area Network (LAN) settings for your operating system or browser, enter the proxy server's address, port number, and other related information.

Mac Operating on macOS

Proxy configuration settings for Wi-Fi or Ethernet can be found in **System Preferences**.

Click here for full instructions for setup on MacOS.

Apple iPhone Operating on iOS

Proxy configuration settings can be found in **Wi-Fi Settings**.

Click here for full instructions on setup for iOS.

Microsoft Windows 10

Proxy configuration settings can be found in **Internet Options** > **Connections** > **LAN Settings.**

Click here for full instructions for setup in Windows 10.

Safari

Proxy configuration settings can be found in the Safari app's **System Preferences**.

Click here for full instructions for setup in Safari.

Mozilla Firefox

Proxy configuration settings can be found in Firefox's **Network Settings.**

Click here for full instructions for setup in Firefox.

Google Chrome

Proxy configuration settings can be found in **Devices > Networks.**

Click here for full instructions for setup in Google Chrome.

FAQs about Proxy Servers

What's the definition of a Proxy Server?

A proxy server is a server situated between users and the internet. It acts as a filter or compression zone for cyber cyberattack attempts.

How does a Proxy Server Work?

When a website is accessed, the connection request is routed through a proxy server to the website's server. The web server then responds by connecting to the IP address of the proxy server, which then forwards the response to the user. The proxy server establishes and maintains every connection between the user and a web server.

What is a Proxy Server Used For?

Proxy servers are primarily used for cybersecurity purposes. Because they sit between users and the internet, proxy servers can stop cyber criminals from connecting to a private network.

Is a VPN the Same as a Proxy Server?

No, a VPN is different from a proxy. VPNs route all internet traffic through an encryption tunnel, but Proxy servers only operate with single apps or websites.

What are some Examples of a Proxy Server?

Some popular examples of proxy servers include:

- Forward proxy servers
- Reverse proxy servers

- Anonymous proxy servers
- Protocol proxy servers
- Access proxy servers
- IP location proxy servers

What are the Benefits of a Proxy Server?

There are many benefits to implementing a proxy server. With a proxy server, you can:

- Improve web browsing security
- Browse the web anonymously
- Filter unwanted web content
- Prevent staff from accessing inappropriate or unproductive websites