What is a Proxy Server? How They Work + Security Risks

A [proxy server](https://www.upguard.com/glossary/proxy-server) is an intermediary(միջնորդ) server that retrieves data from an Internet source, such as a webpage, on behalf of a user. They act as additional [data security](https://www.upguard.com/blog/data-security) boundaries protecting users from malicious activity(վնասակար գործողություններ) on the internet.

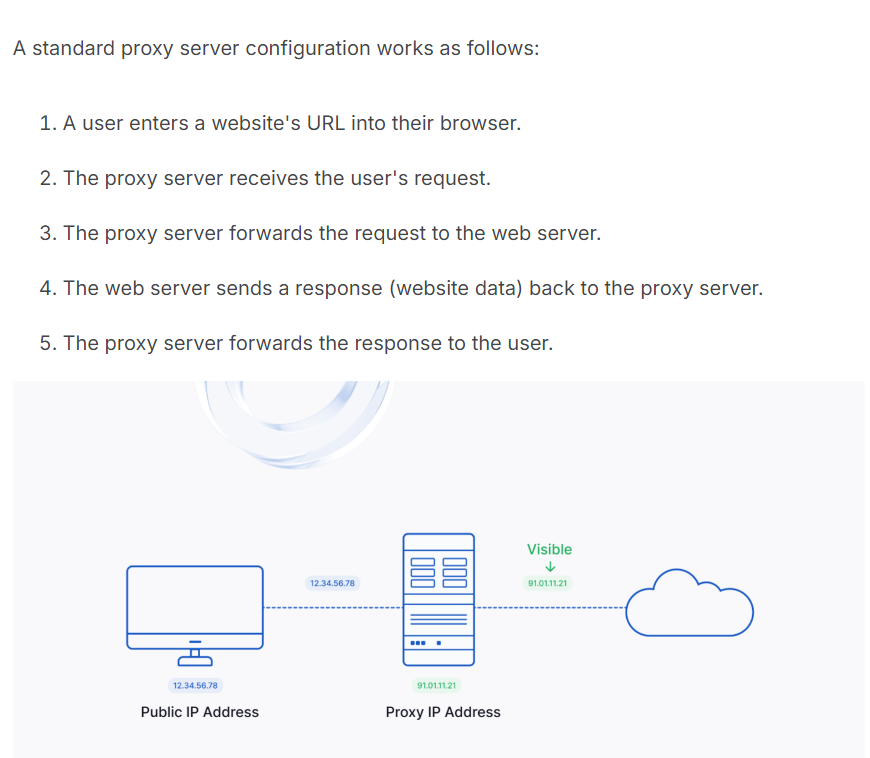
Proxy servers have many different uses, depending on their configuration and type. Common uses include facilitating anonymous Internet browsing, bypassing geo-blocking, and regulating web requests.

Proxies operate by intercepting the client’s requests and forwarding them to the destination server. The response from the server is then received by the proxy and relayed back to the client. Depending on the configuration and purpose, proxies can modify, filter, or cache data before sending it to the client or server.

Like any device connected over the Internet, proxies have associated [cybersecurity risks](https://www.upguard.com/blog/cybersecurity-risk) 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.



#### **Common Use Cases for Proxies**

* **Improving Security:** Proxies can filter malicious content, block access to dangerous websites, and protect internal servers from direct exposure to the internet.
* **Enhancing Performance:** Through caching and load balancing, proxies can reduce latency and distribute traffic more efficiently across servers.
* **Ensuring Anonymity:** Proxies can hide users' IP addresses, making it harder for third parties to track online activities.
* **Bypassing Restrictions:** Proxies can allow users to access content that might be blocked in their region or organization.
* **Monitoring and Logging:** Organizations can use proxies to monitor and log user activity for compliance and security purposes.

Types of Proxy Servers

### **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(?).**

< What is firewall?

*a firewall is protection technology that separates areas of a network from one another. In practical terms, this generally means that it keeps an eye on all incoming and outgoing data packets. It is a kind of digital gatekeeper and checks that these data packets are only sent in and out when they are actually permitted to. When doing so, the firewall works according to predefined rules to open, block and monitor the inbound and outbound access points (ports) as needed. >*

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.

(important)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](https://www.upguard.com/blog/what-is-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'.

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.

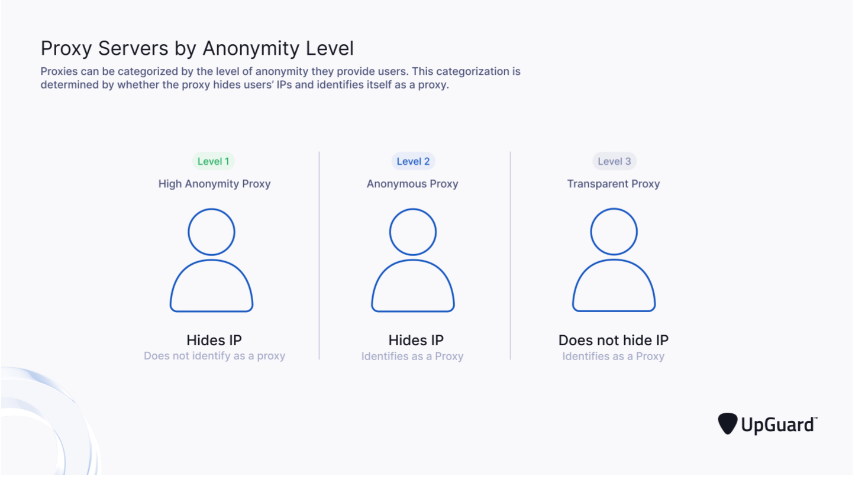
If the proxy denies the user's request, it sends the user an error or redirect message.

### **3. Anonymous Proxy Servers**

#### **High Anonymity Proxy Server (Level 1)**

#### **Anonymous Proxy Server (Level 2)**

#### **Transparent Proxy Server (Level 3)**



### **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.

#### **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://www.upguard.com/blog/what-is-https). HTTPS websites are already [encrypted through SSL certificates](https://www.upguard.com/blog/ssl-certificate), 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.

***And so on …***

### **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](https://www.upguard.com/blog/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](https://www.upguard.com/blog/revisiting-the-perils-of-wifi-on-planes).

#### **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.

### Conclusion

*Server proxies, whether forward or reverse, play a crucial role in modern networking by enhancing security, performance, and privacy. Understanding the different types of proxies and their use cases is essential for designing and managing networks effectively.*