Proxy

A proxy is **an intermediary server that acts as a gateway between a user's device and the internet**. When you use a proxy, your internet traffic is routed through this server, which forwards your requests to websites or services on your behalf. The website you are accessing sees the IP address of the proxy server instead of your actual IP address, **providing a level of anonymity and security**.

Common Types of Proxies

1. **HTTP Proxy**: Designed to handle web traffic (HTTP/HTTPS). It only works for websites and web-based applications.
2. **SOCKS Proxy**: A lower-level proxy that can handle any type of traffic, not just HTTP. SOCKS proxies are **more versatile but generally slower than HTTP proxies**.
3. **Transparent Proxy**: It **forwards requests without modifying the data** but doesn't hide the fact that it's a proxy. The **client's IP address can still be detected by the destination**.
4. **Anonymous Proxy**: **Hides your IP address** from the website you're accessing, but may still disclose that you are using a proxy.
5. **Elite/High Anonymity Proxy**: **Provides the highest level of anonymity** by not revealing that a proxy is in use and effectively hiding your IP address.

Why People Use Proxies

- **Anonymity**: By hiding your real IP address, proxies provide some degree of online privacy.
- **Bypassing Geolocation Restrictions**: Proxies can be used to access region-locked content by making it appear as though the user is in a different country.
- **Improved Security**: Proxies can help **protect sensitive data by acting as a buffer** between the user and potentially harmful websites.
- **Network Performance**: Some proxies **cache frequently accessed data**, speeding up load times for users.