Often when conducting penetration tests, there is a need to carry out full-fledged black box testing. This is where a security professional has to deal with firewalls or other restriction mechanisms on the customer’s end. This becomes an interference as penetration testers try executing checks and block them periodically by, for instance, user-agent or IP address.

If there wasn’t a gray or white box testing model and our IP is not whitelisted, what can be done to bypass the limitations regulated by the customer? There’s a possibility to evade the limitations by switching our user-agent and IP address.

When we talk about user-agent, it’s easier as you only need to install a certain plugin for your web browser, or switch agent in your script through a particular function. But what about the IP address? Let’s look at the pros and cons of some available methods that you can use to hide your IP address, mask your activities, evade firewalls and bypass bans.

**Proxy**

Proxy servers have several forms.

**HTTP** relays GET/POST request. It can add your IP address to request header and store your entire history of interaction with the site.

Pros:

* Supported by almost every browser
* Anonymity (if used properly)
* DNS query on behalf of server

Cons

* Works for HTTP protocol only
* Server history
* Can filter and replace data with proxy server

For **SOCKS Proxy**, the browser will open TCP (sometimes UDP) sockets on the server’s behalf. Depending on the browser, you can also use local DNS server and the site can track you by issuing unique name for every request and remembering the addresses from where the DNS queries come.

Pros

* Anonymity (when used correctly)
* DNS queries on server’s behalf (Chrome)
* Can forward an arbitrary TCP connection (for instance, SSH)

Cons

* DNS queries on client’s behalf (Firefox)
* Server history
* Can filter and replace data with proxy server

**Virtual Private Network**

A VPN allows a user to send and receive any data across public or shared networks. Hence, applications that run on a device across a Virtual Private Network can take advantage from the security, management and functionality of the private network. When using VPN, the most common solution is an OpenVPN. It provides many features such as the possibility to work through UDP, undergoing NAT using SSL/TLS, and much more. You can change your machine’s IP address as well.

Pros

* More reliable
* Higher capability
* Better encryption
* Can be used as a VPN inside a VPN
* Easier to use with a large number of tools

Cons

* One IP for everything
* Takes longer to connect
* Hard to switch IPs

TOR

Tor network is an anonymising technology to help you get access to Tor network along with hiding your real IP address. You can either install the Tor browser or run your Tor service on a remote server used as a proxy.

You can switch your IP by using the option provided in your browser or by restarting your server’s Tor service

Pros

* Free
* Easy to use
* Quick with changing locations and IPs

Cons

* Anyone on the exit node is able to monitor your traffic
* You cannot use Tor the same way as proxy. It’s more like the VPN method

Whether you are looking for a whitebox or blackbox assessment, Aardwolf security can fulfill your requirement. Get in touch today to find out more.