Basically, you are very well protected with the use of a VPN service. We nevertheless advise countermeasures against IP Leaks due to WebRTC (Web Real-Time Communication). You can see if you are vulnerable from this problem with our WebRTC Leak check.

**IP Leak**

In conjunction with WebRTC, private IP addresses can be read out via JavaScript via a VPN connection. The example Firefox Hello closes computers behind a firewall and with private IP addresses. Therefore, a website with JavaScript can ask a STUN server for the actual IP address. As a result, anonymisation services no longer fulfill their purpose and can no longer provide protection against an IP leak.

**Countermeasures**

There are two approaches to protecting against an IP leak. One option in Chrome is to install WebRTC Leak Prevent add-ons / plugins to manage potential IP leaks. Also available since the end of 2016 is the extension Easy WebRTC Block, which also exists in a version for Opera.

The other option is to change the settings in the browser.

In Firefox, about: config can set the value `media.peerconnection.enabled` to false, which prevents an IP leak.

**More about WebRTC**

at: [https://en.wikipedia.org/wiki/WebRTC](https://en.wikipedia.org/wiki/WebRTC)
Prevent IP Leak through WebRTC

SpyOFF Support