AnonVPN

Project Details (home)

We Protect You Against Your ISP

Like all VPN’s, we encrypt traffic between your VPN client and our VPN servers, but in most VPN’s, if the ISP knows where the server is, then they can tell that you are connecting to the VPN. With our VPN, the ISP will only see the middle hop, one of tens-of-thousands of possible computers around the world, and not the true VPN service IP address.

In addition to that, we use the I2P network to transport your communication, and in doing so, we inherit the I2P network’s Censorship-Resistance properties. The communication itself will be obfuscated and “Unclassifiable” to known Deep-Packet Inspection devices, and connections will be made using peers in the I2P network which, once bootstrapped, is self-sustaining.

As a result of all this, it is very unlikely that your ISP will even be able to tell that you are using our VPN.

We Protect You Against Us

All other commercial VPN’s require you to trust that the VPN provider will not undermine the security of your connection, share your account information, or be subverted by attack. We take steps to minimize what account information we can possibly collect by anonymously routing your connection to and from our servers.

This anonymous routing is enforced from both the client and the server side, with each choosing a single hop from a network with tens-of-thousands of nodes. Both the client and the server are only addressable by self-authenticating, end-to-end encrypted, and DPI-Unclassifiable tunnels, and never by a public IP address. As a result, even if we were compromised, we could not provide account information linking you to a real identity.

We are, of course, Free Software and only depend on Free Software. We have also chosen to license our server components under the GNU Affero General Public License 3.0. in order to require that derivatives of this software also be Free Software. Someone could make a non-free clone of this software, but they will have to do it without our help.

Recommended Software

Web Browser

Of course, just like Tor and I2P, we can only protect you with the software we write on the network we design. Once you exit to the internet, your traffic will appear to be coming from our servers, but you should also make sure to use HTTPS-Everywhere in your web browser, or use a web browser which enforces TLS usage on it’s own.

Firefox

Firefox is a community web browser developed in the interest of a healthier, respectful web. Firefox should be combined with the “HTTPS Everywhere” extension and an ad-blocker of your choice.

Brave Browser

Brave Browser is a new Chrome-based web browser which has integrated privacy enhancements.