Understanding the WireGuard Protocol

Kaneesha D. - 2021-03-16 - Application & Features

Private Internet Access is happy to announce that we now offer Wireguard as a connection protocol across all platforms.

> Note: WireGuard currently does not work on Ubuntu 16.04, our development team is working to address this issue. However, there is no ETA as to when this will be addressed. Additionally please be aware that Windows 7 does not support WireGuard to use this feature requires Windows 8 or later.

WireGuard connectivity in PIA works by sending an HTTPS request to the server to request an IP address and connection information, then we send UDP WireGuard traffic to the server. A WireGuard connection, therefore, requires connectivity to both TCP 1337 and UDP 1337 on the VPN server.

Currently, within the desktop application, you can utilize the "Small Packets" feature should you find yourself in need of additional speed on top of the speeds that Wireguard currently provides. Additional features that can be utilized with Wireguard will be implemented in the future, but as it is currently in preview mode, we are unable to provide a timeline for additional options or settings.

Installation and utilization of Wireguard is very straightforward on all devices with the exception of Linux which requires Linux Kernel implementation. In some cases, this will require you to perform the kernel installation manually using the Wireguard’s download page which can be found here:

https://www.wireguard.com/install/

If you are unable to locate your distribution in the link above, but you have the application installed, you may be able to compile the kernel directly from the source (you must have git installed on your system) via the following link:

https://www.wireguard.com/compilation/

> NOTE: As both methods require installation outside of the functionality of our application, we are unable to provide support for installation errors that may occur when installing the kernel.

Should you experience any issues with Wireguard on any platform, within our scope of support, please feel free to reach out to us with a support ticket, here

About Wireguard

WireGuard is an open-source and relatively new VPN protocol that promises to offer advantages over previous options, written and developed by Jason A. Donenfeld. WireGuard aims to be highly effective and easy to use with less going on behind the scenes. Compared to other VPN protocols such as OpenVPN (600,000) and IPsec (400,000), WireGuard is made up of a fraction of the amount of code, under 4,000 lines. This results in security audits and identifying bugs to be faster and easier to remedy, with fewer lines of code to comb through.

A big advantage here is the use of modern technology. With less overhead and current encryption ciphers, WireGuard looks to reduce the issues of easy disconnects and the time to negotiate connections. This is all done while having a more secure and stable tunnel with a faster connection sending IP packets over UDP. All these features also aim to provide cell phones with faster connect times, improved battery life, and an overall more reliable connection.

The following list of protocols and primitives used by WireGuard can be found below as well as more detailed information from the official website.

- ChaCha20 for symmetric encryption, authenticated with Poly1305, using RFC7539's AEAD construction
- Curve25519 for ECDH
- BLAKE2s for hashing and keyed hashing, described in RFC7693
- SipHash24 for hashtable keys
- HKDF for key derivation, as described in RFC5869