VPN - WireGuard

WireGuard is a new, simple, and fast VPN implementation and protocol. For comparison, the older L2TP/IPsec VPNs typically will achieve about 100Mbps, but WireGuard VPNs may reach speeds upward of 300-400Mbps on the same hardware, or higher on a high-end workstation.

In addition to its speed, WireGuard has some great features such as built-in roaming (a single encrypted packet moves the tunnel to your new IP), cryptokey routing, and formal cryptographic verification.

On the other hand, it also has some challenges, such as pre-key exchange and a lack of automatic address assignment. Both of these problems require manual configuration on both ends of the tunnel. Cryptokey routing also presents its own challenges in some situations.

A WireGuard VPN is best suited for connecting single end-user devices such as laptops and phones to the mesh over the internet from a location that has no mesh access.

Routing over WireGuard

WireGuard, like other VPNs, can be used in conjunction with a routing protocol, such as OSPF which we use in NYC Mesh. However, there are some challenges with WireGuard and routing.

These challenge are highlighted on another page, as it is a longer and more technical discussion.

Please see [VPN - WireGuard + OSPF]({{ relref "vpnwireguardospf.md"}})

Device support

WireGuard implementations are being developed on a variety of platforms. The following list provides an overview, but see the WireGuard Installation instructions for further details.

- Linux: Yes!
- Android devices: Yes, some - See WireGuard website
- OpenWRT: Yes, in LEDE on latest versions, in certain builds
- Apple devices: Yes, some - See Wireguard website

- Mikrotik devices: Starting in RouterOS 7.1beta2
- Ubnt routers: No (well, technically yes, but the module has caused lots of problems, so please don't use it yet)
- Windows devices: Yes, some - See WireGuard website

Endpoints

Supernode 1:

- IPv4/6: `wgvpn.sn1.mesh.nycmesh.net:51820`
- Supported connect methods:
  - End Device
  - ~~OSPF - *Not Yet*~~
  - ~~BGP Node-Peering - *Now legacy, please do not use*~~

Supernode 3:

- IPv4/6: `wgvpn.sn3.mesh.nycmesh.net:51820`
- Supported connect methods:
  - End Device
  - OSPF Node-Peering

How To Connect

Connecting end-devices

1. Ensure WireGuard will work on your device
2. Generate a Wireguard public key, and give it to Zach. (https://www.wireguard.com/quickstart/#key-generation)
3. Zach will give you the server public key and assign you an IP address. *This will change later, but just for now to get the docs out, this is what we currently do.*

Revision #5
Created 9 December 2023 04:39:52 by Willard Nilges
Updated 23 March 2024 16:06:53 by James