ZeroTier

The zero trust SD-WAN

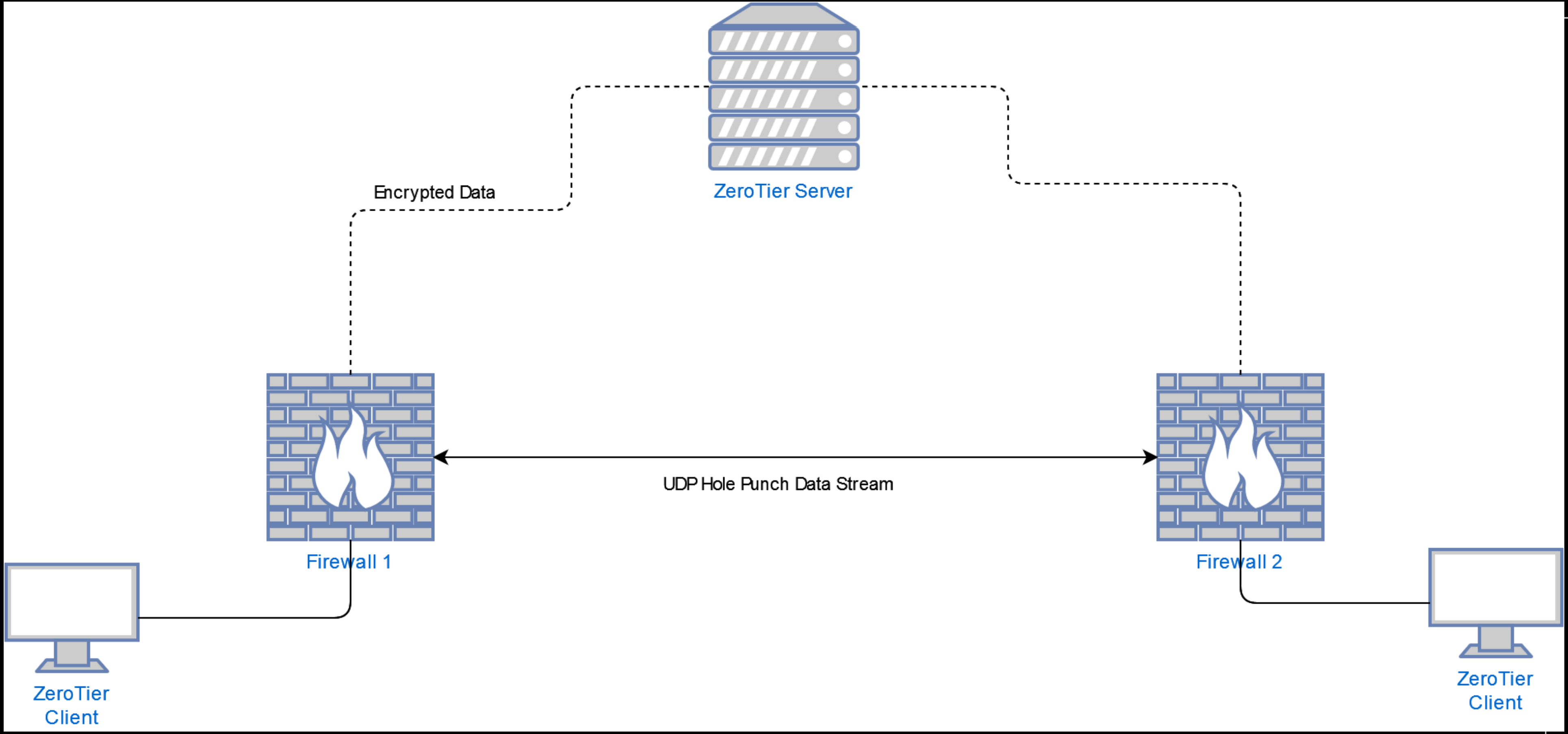
What is it?

- Free & Open Source
- A network connection that combines the capabilities of a VPN[1] and SD-WAN[2].
- Devices are connected to each other over the ZeroTier network (P2P[3] mesh). Decentralized, zero trust networking, NAT traversal.
- Uses Asymmetric public key encryption: Curve25519/Ed25519 (256-bit elliptic curve)
- White Paper: https://docs.zerotier.com/zerotier/manual
- Available on the following platforms:

Windows MacOS Android iOS Linux FreeBSD NAS

[1] Virtual Private Network
[2] Software Defined-Wide Area Network
[3] Peer-to-Peer

How does it work? Pt 1



How does it work? Pt 2

- ZeroTier is installed on each client

- Each client sends data up to the ZeroTier servers.

- ZeroTier then attempts to do a NAT[1] Traversal behind each firewall.

- Once each device is located a UDP[2] Hole Punch Data Stream keeps the connection alive behind each firewall and data is no longer sent to the ZeroTier server until connection needs to be re-established.

Note: *You can host your own ZeroTier server and you do not have to use their cloud offerings. The code is open source https://github.com/zerotier*

1. Network Address Translation
2. User Datagram Protocol

Common Applications

- Connecting ATAK devices together without a central server such as TAK, FTS, TAKY, etc.
- Private Gaming LAN
- Route to a remote subnet
- Access devices or services on a home network without configuring firewall rules or port forwarding.
  - Using Pi-Hole or PFSense NGBlocker you can configure ZeroTier to use your local DNS server when routing back to your home network. This will block all ads/trackers on your mobile device.

Pros

- No firewall configuration (*usually*[1])
- Fast and simple to setup
- Can be self hosted
- End-To-End Encryption
- Available across multiple different devices and operating systems
- It just works
- No networking skills required

1. Some firewalls block the port ZeroTier uses to connect through.