Run a VPN with global exit nodes with fly.io, tailscale and github!

README.md

fly-tailscale-exit

This repo shows how to run tailscale on fly, specifically to run exit nodes. If you want to add tailscale to a fly.io application, follow this guide instead: https://tailscale.com/kb/1132/flydotio/

Did you ever need a wormhole to another place in the internet? But you didn't trust the shady VPN providers with ads all over YouTube? Well, why not run it "yourself"? This guide helps you to set up a globally distributed and easily sharable VPN service for you and your friends.

- Instantly scale up or down nodes around the planet
- Choose where your traffic exits to the internet from 20 locations.
- Enjoy solid connections worldwide
- Bonus: the setup and the first 160GB of traffic each month are gratis

Sounds too good to be true. Well that's probably because it is. I compiled this setup as an excercise while exploring the capabilities of fly.io and tailscale. This is probably not what you should use as a serious VPN replacement. Go to one of the few trustworthy providers. For the reasons why this is a bad idea, read below.

Machines

All | External

Search machines...

MACHINE	IP	OS	LAST SEEN
fly-cdg patte@github Exit Node	100.64.233.113	Linux 1.12.3	Connected
fly-fra patte@github Exit Node	100.121.148.79	Linux 1.12.3	Connected
fly-hkg patte@github Exit Node	100.122.241.41	Linux 1.12.3	Connected
fly-sin patte@github Exit Node	100.66.119.94	Linux 1.12.3	Connected
fly-sjc patte@github Exit Node	100.99.49.112	Linux 1.12.3	Connected
fly-syd patte@github Exit Node	100.127.84.39	Linux 1.12.3	Connected
fly-yyz patte@github Exit Node	100.119.217.81	Linux 1.12.3	Connected

▶ Video of tailscale on iOS changing exit nodes.

Setup

1. Have a GitHub account

Create a GitHub account if you don't have one already: https://github.com/signup

2. Have a GitHub organization

Let's create a new github org for your network: https://github.com/organizations/plan

- Choose a name for your network: eg. `banana-bender-net`
- Plan: free

3. Have tailscale

Install tailscale on your machine(s):

- Instal it on your notebook and mobile phone: https://tailscale.com/download
- Login with github, choose the github organization created before (eg. `banana-bender-net`).

- Check your network and keep this tab around: https://login.tailscale.com/admin/machines

4. Setup DNS in tailscale

In order to use tailscale for exit traffic you need to configure a public DNS. Go to https://login.tailscale.com/admin/dns and add the nameservers of your choice (eg. cloudflare: `1.1.1.1, 1.0.0.1, 2606:4700:4700::1111, 2606:4700:4700::1001`)

5. Create a tailscale auth key

Create a reusable auth key in tailscale: https://login.tailscale.com/admin/settings/authkeys

A ephemeral key would be better for our use case, but it's restricted to IPv6 only by tailscale, which doesn't work so well as a VPN exit node.

6. Have a fly.io account and cli

Install the fly-cli to your machine and login with github: https://fly.io/docs/hands-on/installing/

7. Have a fly.io organization

- Create an org on fly (technically there is no requirement to name it the same). `flyctl orgs create banana-bender-net`
- Go and enter your credit card at https://fly.io/organizations/banana-bender-net. It's only going to be charged if you use more than the free resources.

8. Setup fly

Give the app the name you want. Don't deploy yet.

```
git clone https://github.com/patte/fly-tailscale-exit.git

cd fly-tailscale-exit

flyctl launch

? fly.toml file already exits would you like copy its configuration : (yes/no) yes

? App Name (leave blank to use an auto-generated name) tailwings

? Select organization: banana-bender-net-test (banana-bender-net-test)

? would you like to deploy postgressql for the app: (yes/no) no

? would you like to deploy now : (yes/no) no
```

9. Set the tailscale auth key in fly

```
flyctl secrets set TAILSCALE_AUTH_KEY=[see step 4]
Secrets are staged for the first deployment
```

10. Deploy

```
flyctl  deploy
```

11. Enable exit node in tailscale

Wait for the node to appear in the tailscale machine overview. Enable exit routing for the nodes https://login.tailscale.com/admin/machines (see tailscale docs on how to do it)

12. Connect with your local machine or smartphone

On iOS, choose "use exit node" and there you go.

On linux, just run

```
tailscale up --use-exit-node=fly-fra
```

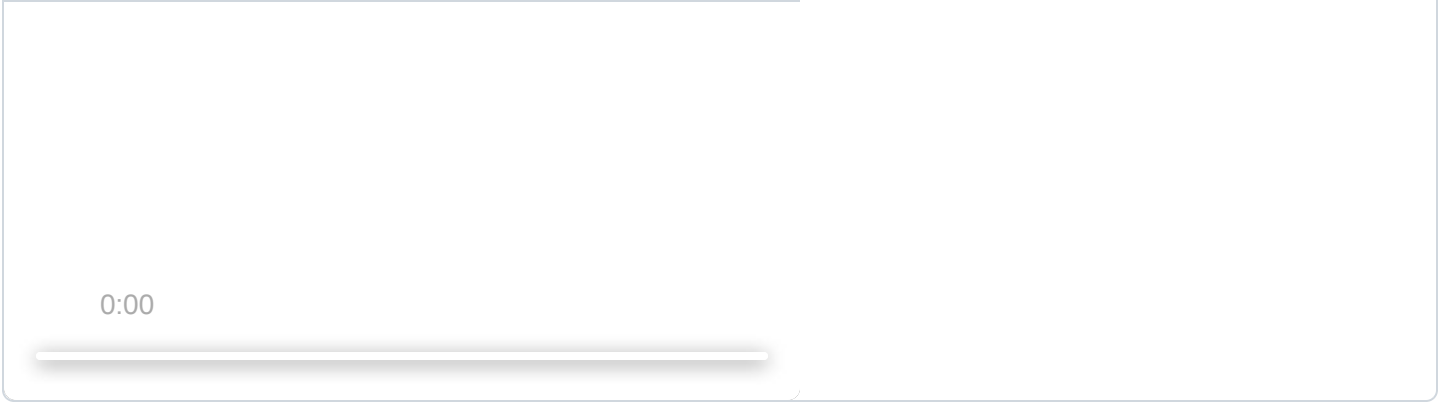
13. Regions

To add or remove regions just type:

```
flyctl scale count --region hkg 1
flyctl scale count --region fra 1
```

Wait for the node to appear in tailscale, confirm it to be a legit exit node (step 11), choose it in your client boom! In less than 5 minutes you access the internet from another place. Note: Scaling up also reinitializes the existing nodes. Just use the newly created one and delete the old. Note: It seems not all fly regions have their own exit routers and some use another for egress traffic. This needs further investigation.

Screencast.mp4



14. halt

In case you want to stop:

```
sudo systemctl stop tailscaled
flyctl suspend
```

15. remove

In case you want to tear it down:

```
flyctl orgs delete banana-bender-net
```

I think there is no way to delete a tailscale org.

Invite your friends

All you need to do to invite friends into your network is to invite them to the github organization, have them install tailscale and login with github. They immediately see the available exit nodes and can use whichever they please. Easiest VPN setup ever!!

Why this probably is a bad idea

- Dirty egress traffic for fly.io.
  Usually traffic exiting fly machines is upstream API traffic not dirty users surfing the web. If too many people do this and use it for scraping or worse fly's traffic reputation might suffer.
- Increased traffic on tailscale derp servers.
  Usually tailscale is used for internal networks. If everybody uses this as their everyday VPN the traffic the derp servers might increase beyond what's forseen.

- Tailscale teams is supposed to cost money.
  ~~Tailscale lists teams to cost $5 per user per month but creating and using a github org in the way described above doesn't count as team but as personal account. I didn't find a way to upgrade an org created this way into a paying org. Please let me pay ;)~~ It seems you can pay at tailscale for a github team now, so go there and do that if you use this together with others: https://login.tailscale.com/admin/settings/billing/plans This makes this VPN approach being fully paid.

> You'll never be stopped from spinning up more devices or subnet routers, or trying out ACL rules. We encourage you to play around, find what works best for you, and update your payment settings after-the-fact.

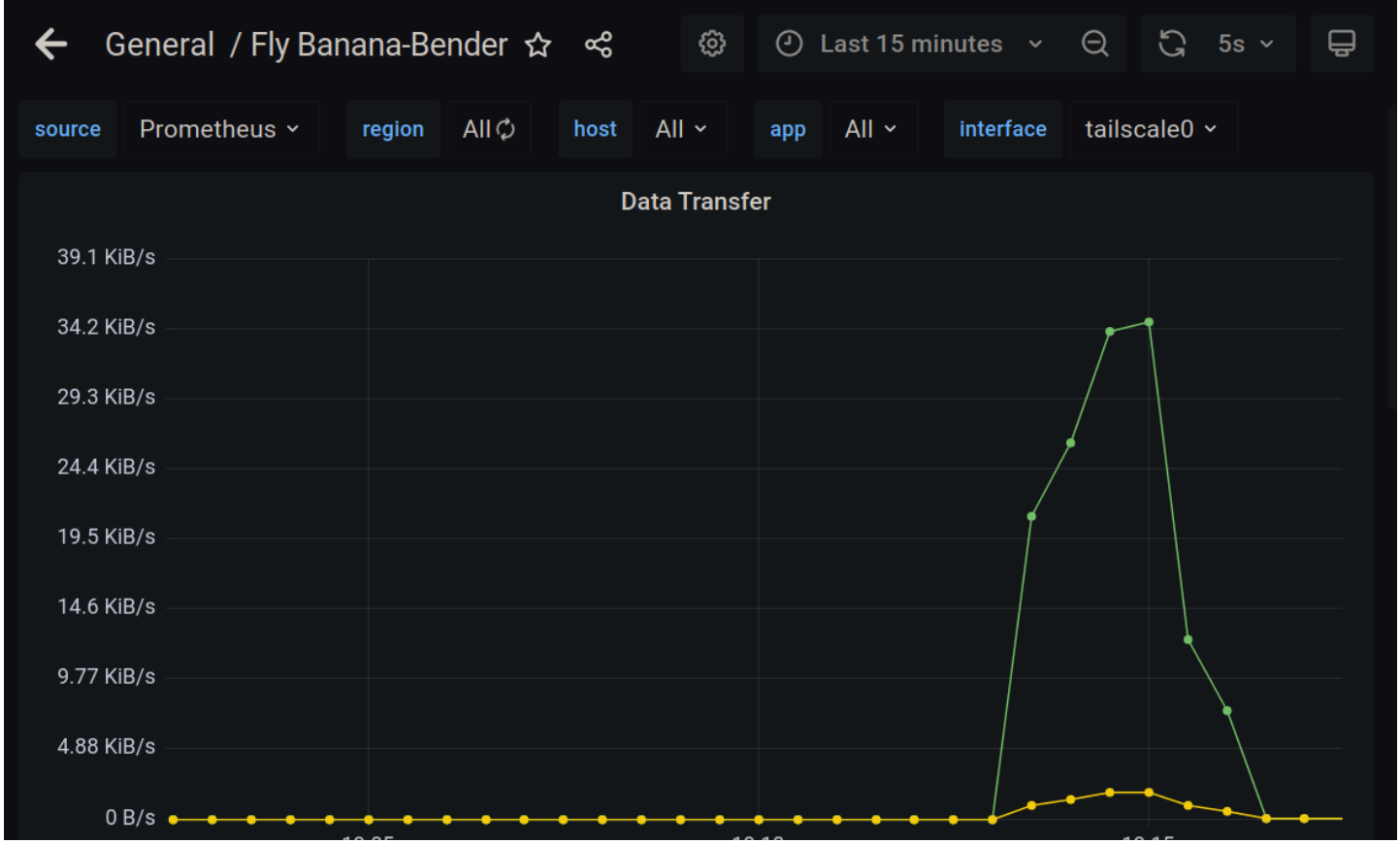
source Kudos to tailscale for using soft-limit, IMHO this makes for a great user experience and I'd expect it to simplify some code parts as well.

Love Letter

Just enjoy the magnificence, the crazyness of the house of cards that the modern cloud is. I seriously enjoyed setting this up with fly and tailscale. I think both are mind blowingly awesome.

I mean tailscale... just look at it. The already awesome wireguard set up to a mesh by an open-source client that does all sorts of NAT wizardry, provided servers to route through if P2P doesn't work and a nice web-ui. It's just great. If I could wish for anything it would be to be able to run the server part myself (I know about headscale and I'll give it a try next) . Not because I don't want to pay the company money, the contrary is the case, but because I just don't feel comfortable having my (bare-metal) machines trusting a network interface for which I can't fully control who is connected to the other end. Tailscale could auth a machine into my network and I'd have no possibility to reliably find out.

What gets me most about fly is the approach to turn Dockerfiles into microVMs. Imagine docker but with `--privileged --net=host` . This is what makes this example so simple in comparison to other cloud providers: Just a neat Dockerfile and start script but you can use tailscale as if it would run on a real linux host, because it does. No need to run tailscaled with `--tun=userspace-networking --socks5-server=localhost:1055` , the tailscale interface get's added to the VM and everything just works. This includes that the metrics gathered by fly automatically include the `tailscale0` interface and you can view it's traffic chart in grafana easily.



This plus anycast, interapp vpn, persistent storage, locations all over the world, an open-source client and being a chatty crew with the mindset "Go Nuts" have me left in awe.

Contributors 5

Languages

- **Shell** 60.4%
- **Dockerfile** 39.6%