Tailscale

A Mesh VPN system I dearly wish had existed a few years prior.

Authentication & Authorisation

Currently using the official control server with an MSOL account. Single tenant, not very pleased about it, but they won't give me a single-user enterprise account.

SSH

Honestly one of the best things about Tailscale. In use on all machines that support it.

ACLs

- ICMP is allowed from anywhere to anywhere
- DNS lookups are allowed from anywhere to udp/53 on any machine tagged `nameserver`
- Any traffic is allowed from machines tagged `permit-tx` to machines tagged `permit-rx`
- SSH is allowed from machines tagged `permit-tx` or `permit-tx-ssh` to machines tagged `permit-rx` on tcp/22
- HTTP is allowed from machines tagged `permit-tx` or `permit-tx-web` to machines tagged `permit-rx` on tcp+udp/80 and tcp+udp/443
- Traffic is allowed from machines tagged `logsender` to machines tagged `logserver` on tcp+udp/514, tcp+udp/1514 and tcp+udp/12201

Plans

- Add ACLs for FTP, SMB and maybe others
- Figure out how to integrate it with docker
    - Ideally this would be just a network driver, but Tailscale doesn't appear to support being used as a docker network driver, so no dice.
    - Common option seems to be to use TS as a sidecar; does this work with docker swarm mode?
    - Option that -would- work with swarm mode is to build a custom container that runs both tailscale and also something else, but that's.. intellectually expensive.
    - Other suggested option is subnet router, but for the number of docker hosts I have in swarm mode, this would be wildly impractical
    - Maybe just use a tailscale-aware load balancer and stick with good old DNS for service ID?
- Get DNS working properly (maybe write a script/daemon that updates a DO zone with IPs for each machine/endpoint?)
    - Idea for a science-based naming system (SBNS) (listen to Kill James Bond!)
        - TLD .tail

        - tag.tail - returns A and AAAA records for all hosts with the given tag
        - hostname.tail - returns A and AAAA for a host
        - hostname.tag.tail - as with hostname.tail - might be useful if two hosts have the same name? does TS allow that?
        - service.tail - it'd be cool to have some kind of declarative thing so you can say like, grafana.tail and it goes to a web loadbalancer for grafana somewhere on your tailnet, though that's more of a consul thing i guess
    - DNS resolution is working over TS.
        - Because I run AdGuard Home inside docker using macvlan, i would have to have ran tailscale inside the AGH container in order to do it “properly”. instead: DNAT time
        - AGH has an internal address used for host-to-container resolution because traffic can't go from a host to a macvlan'd container using a routed address, which is useful for DNAT

iptables-save output

```
-A PREROUTING -i tailscale+ -p udp -m udp --dport 53 -j DNAT --to-destination 172.21.0.53
-A PREROUTING -i tailscale+ -p tcp -m tcp --dport 53 -j DNAT --to-destination 172.21.0.53
-A POSTROUTING -s 172.21.0.53/32 -o tailscale+ -m mark --mark 0x40000 -j MASQUERADE
```

- VoIP!