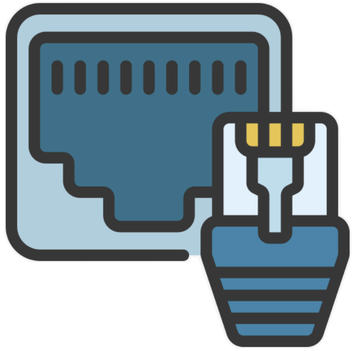
Securely accessing self-hosted services remotely.

Remote access is easy.
Port forwarding is dangerous.

Alex Kretzschmar

Remote access is easy.

Just open a port.



What is a port?

Apartment Block

Apartment Number

192.168.1.10:**80**

What is a port?

IP Address

Port

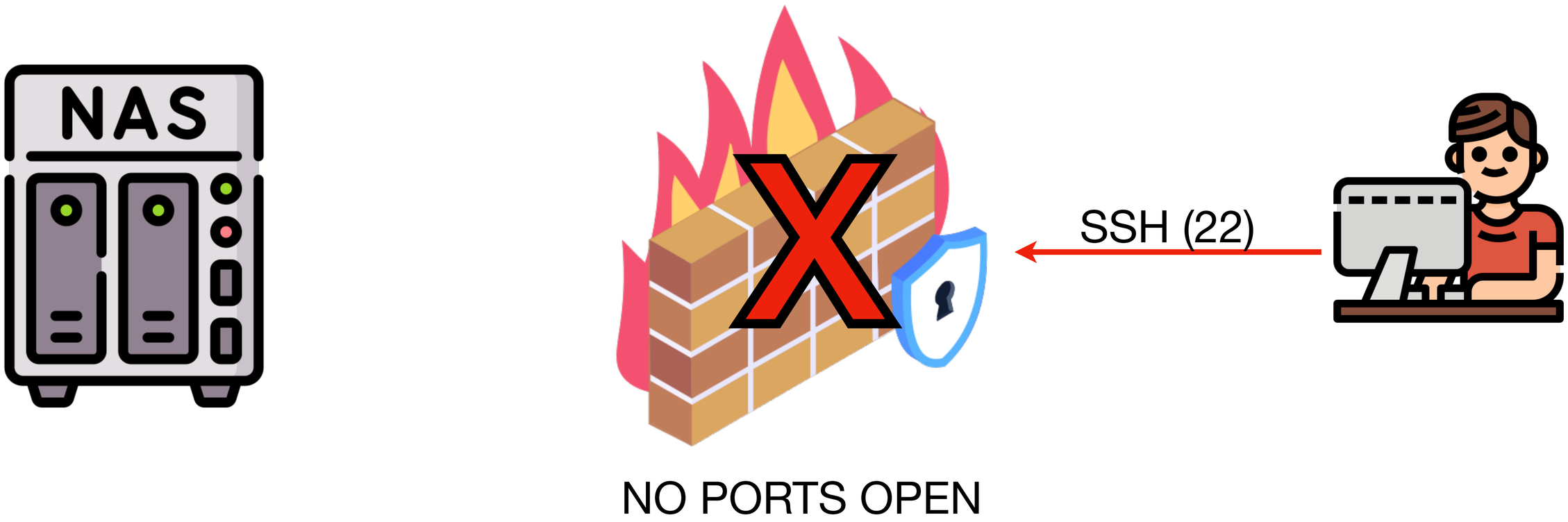
192.168.1.10:**80**

SSH	22
DNS	53
HTTP	80

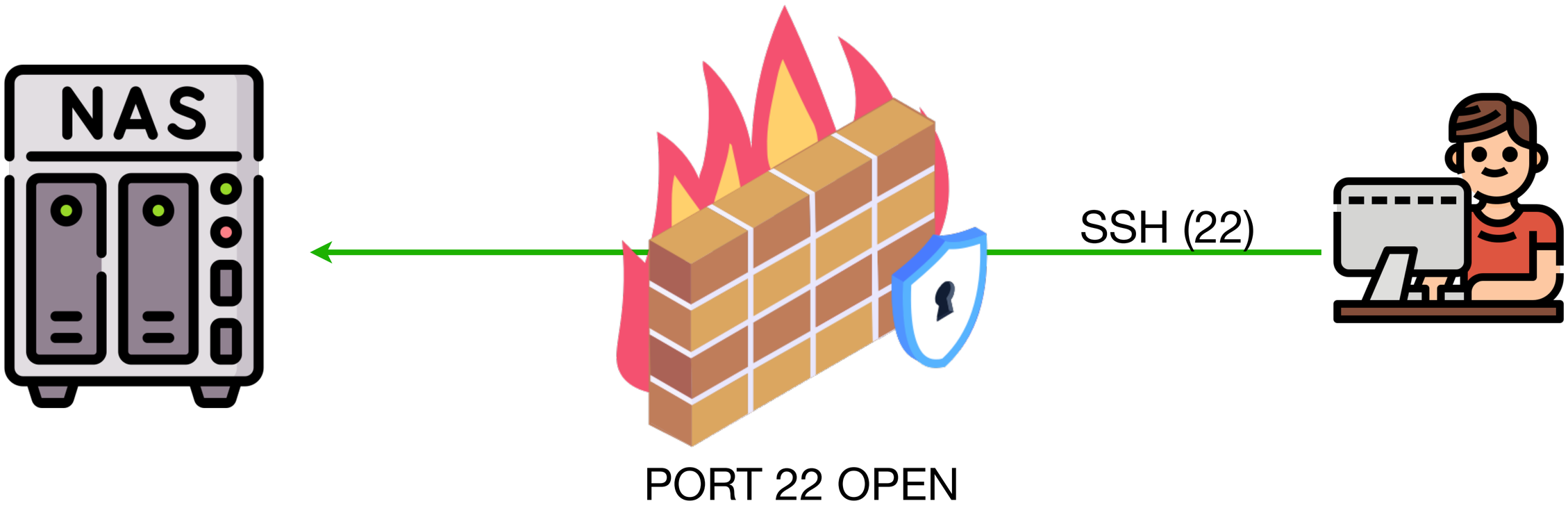
Port forwarding

is dangerous.

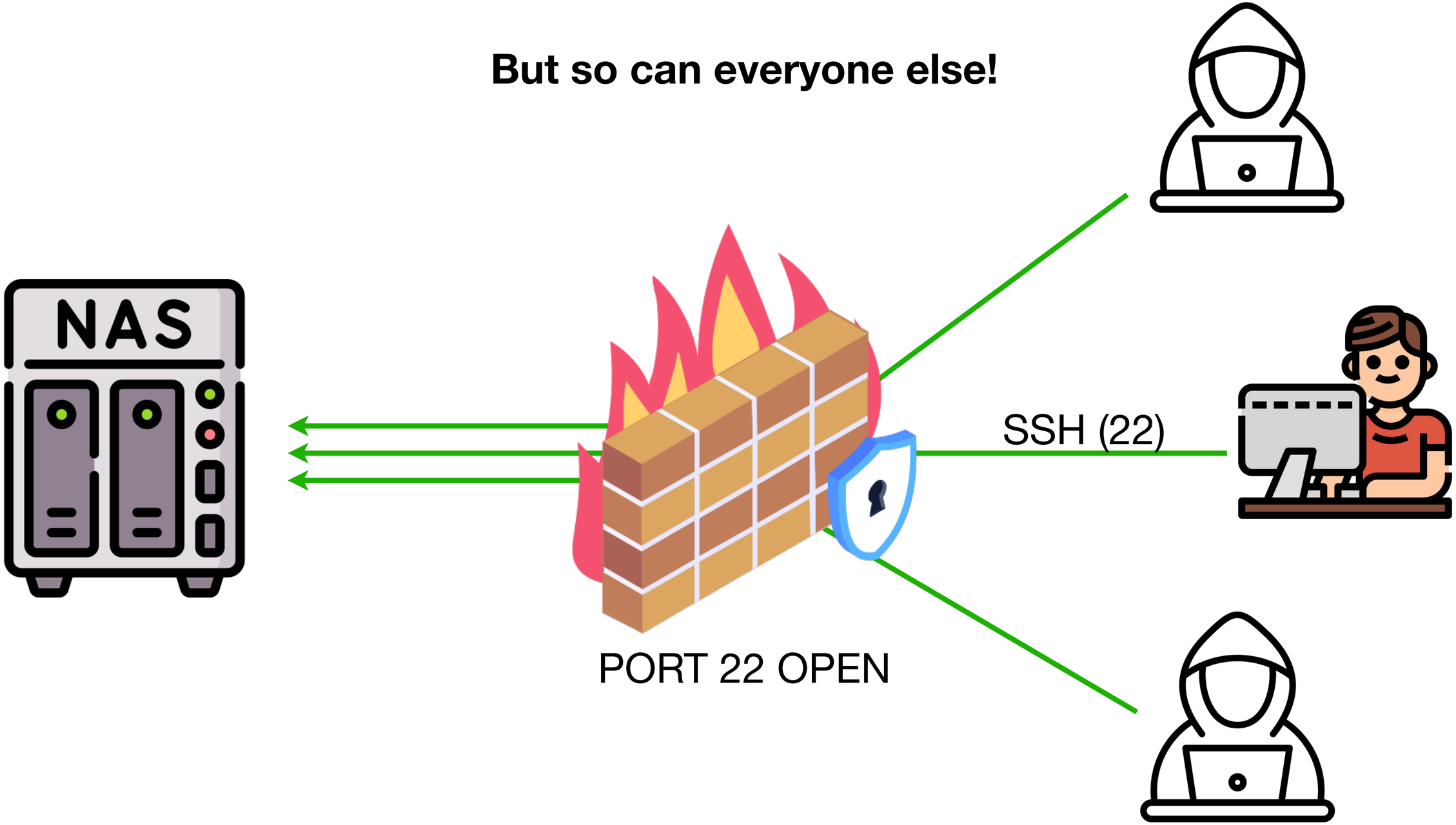
No-one can connect

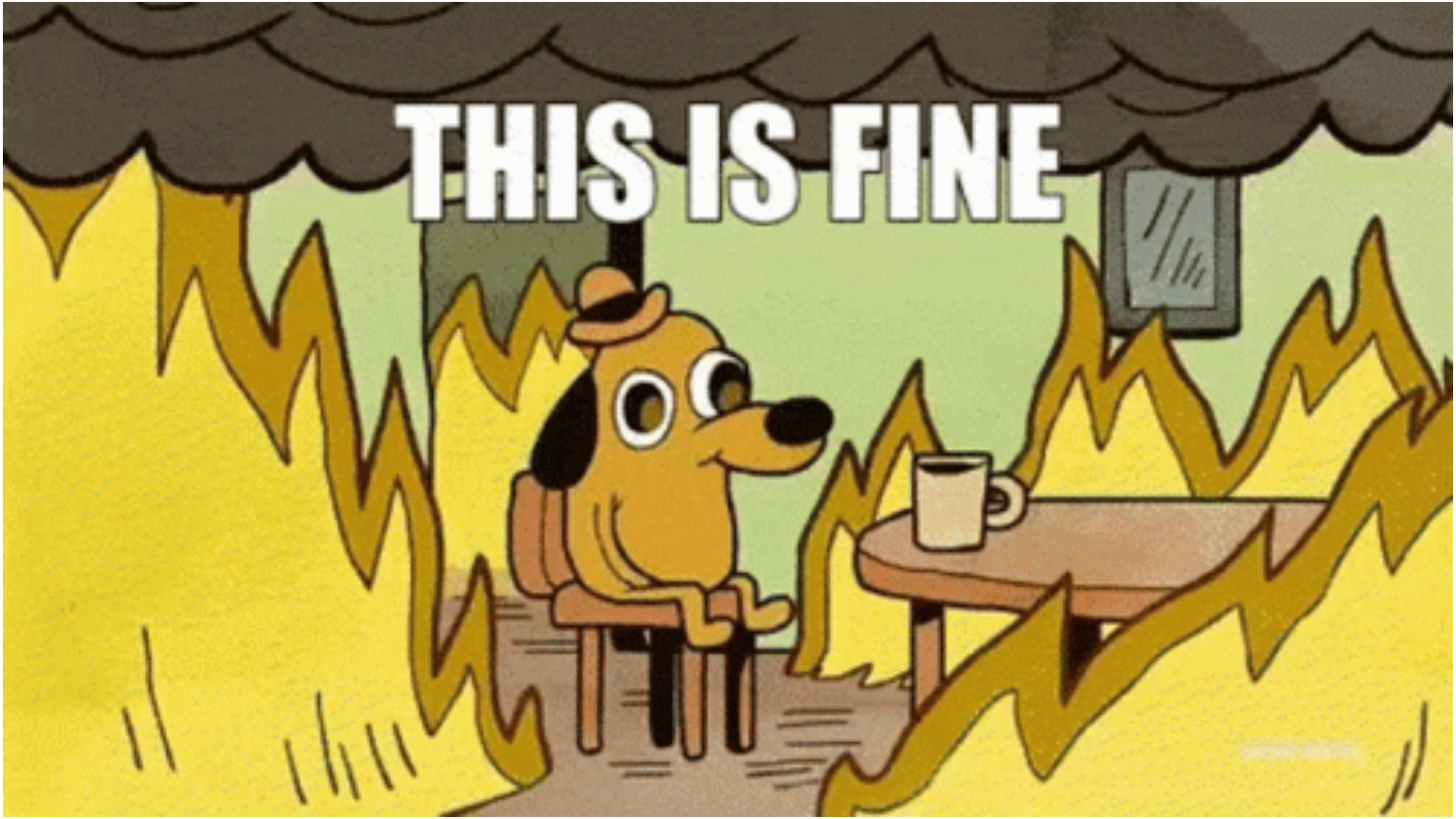


Now you can connect!



But so can everyone else!




THIS IS FINE

Firewall rules suck

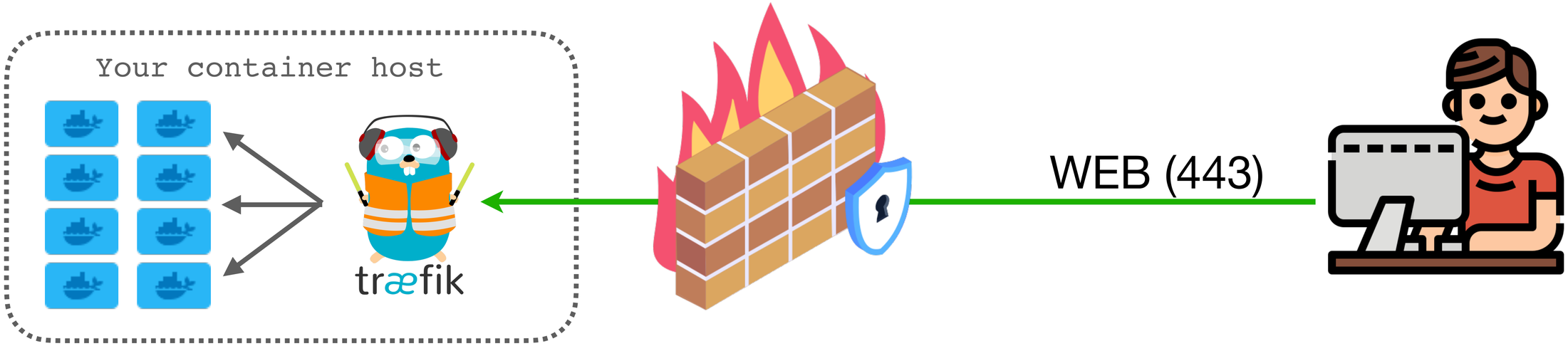
- Rules must become very restrictive
  - Limit based on source IP
  - Limit based on protocol (TCP / UDP / ICMP)
  - Must always go to a fixed destination
    - Such as a hardened bastion server or jump box
    - Quite inflexible
- Rules don’t scale particularly well
- Inbound / Outbound rules get confusing

Remote access is easy.

What’s my IP address again?

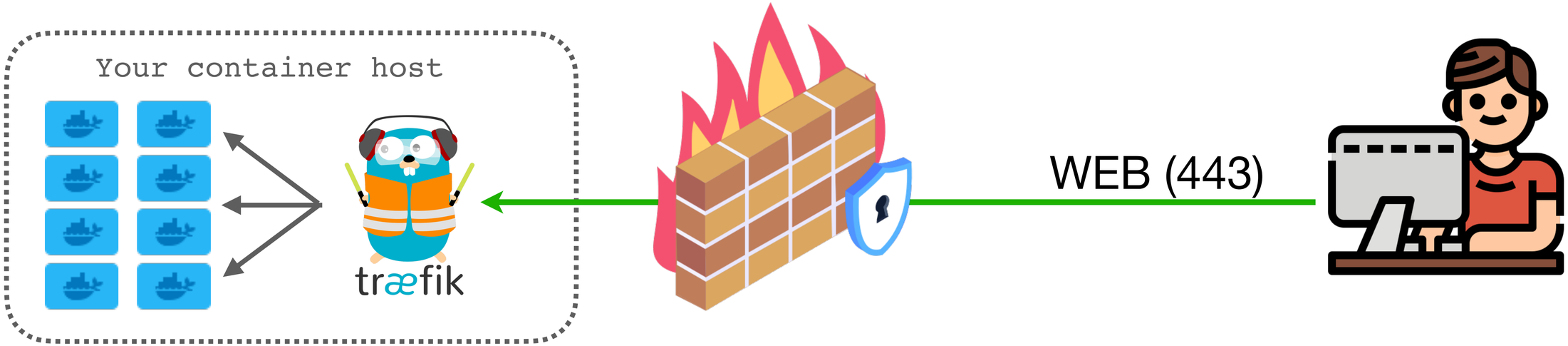
What about VMs and containers?

We can use VMS and containers to limit the blast radius



We can use VMS and containers limit the blast radius

But island hopping is still a thing



Containers help a bit

- They create isolation via Linux kernel namespaces
- Many containers attach to one kernel
  - Efficient
  - But more risky than the entire encapsulation provided by a VM
- Containers are Linux only
- With care, more than good enough for most people self-hosting at home

There’s a better way.

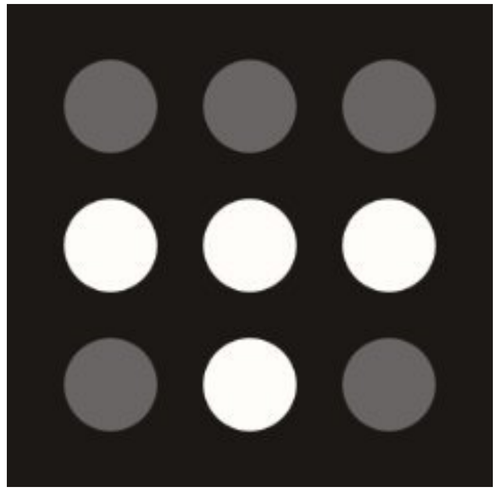
What if we could just
(mostly) ignore the firewall altogether?

Today’s agenda

- ~~Why port forwarding is dangerous~~
- Using a mesh VPN to “tunnel through” your firewall securely
- docker compose basics
  - And how to run self-hosted services
  - Including some reverse proxy tips with Traefik and Caddy
- Move on to some DNS trickery
  - Cloudflare
  - Tailscale MagicDNS
- The big reveal!

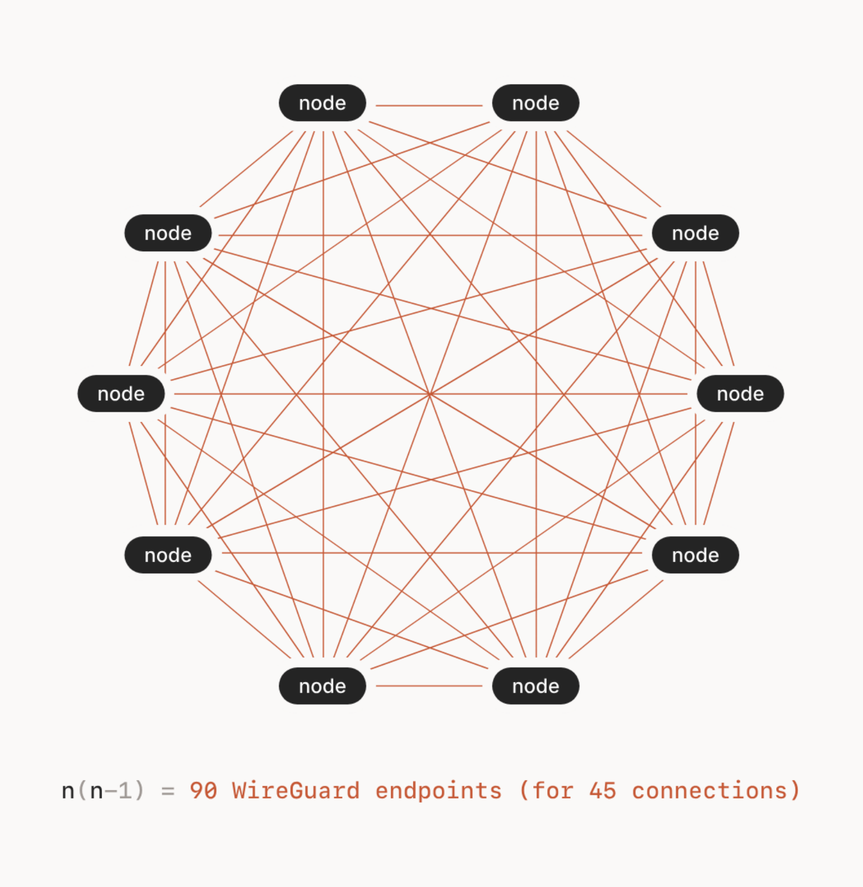
Use a mesh VPN

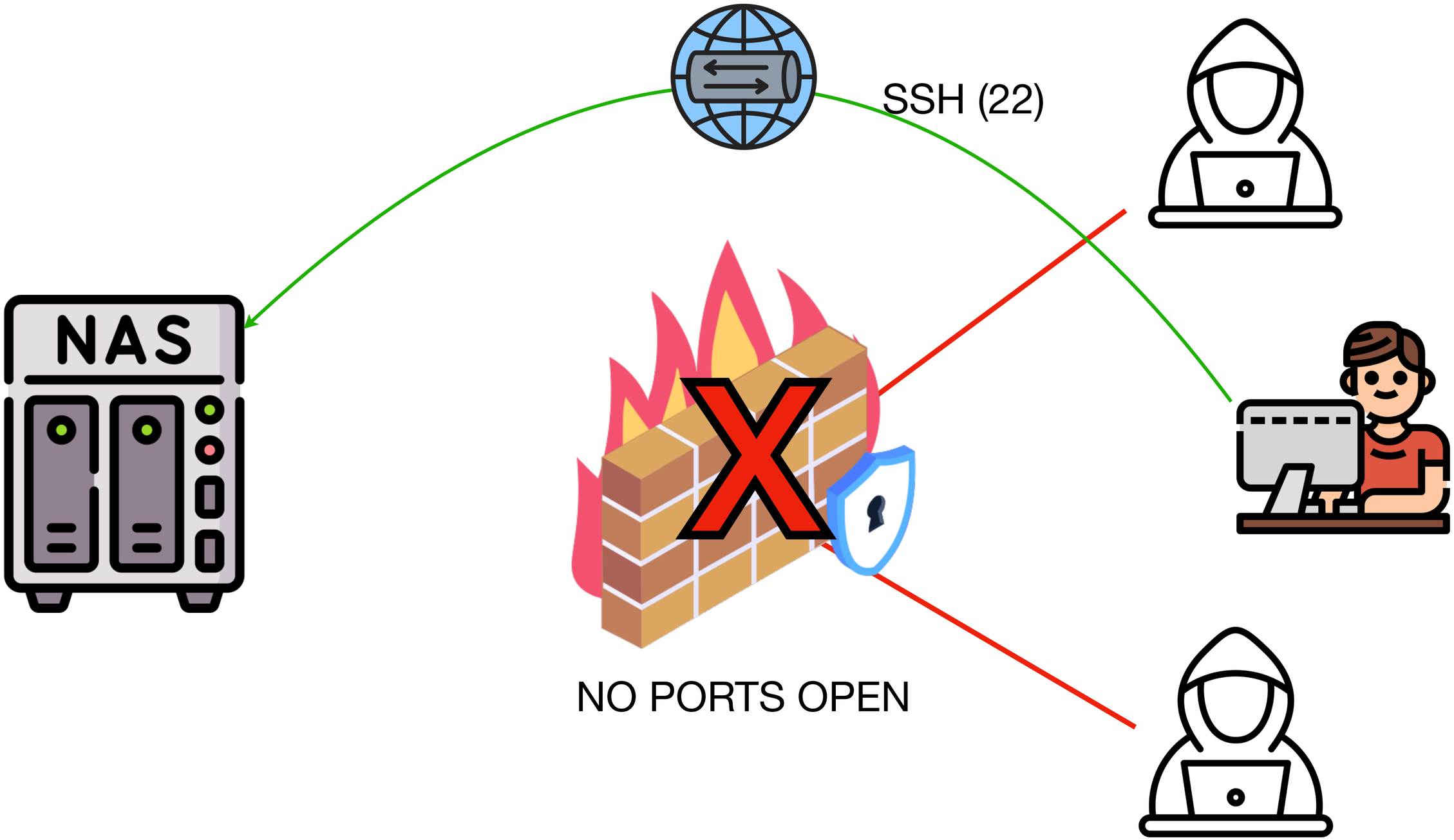
Disclaimer time!

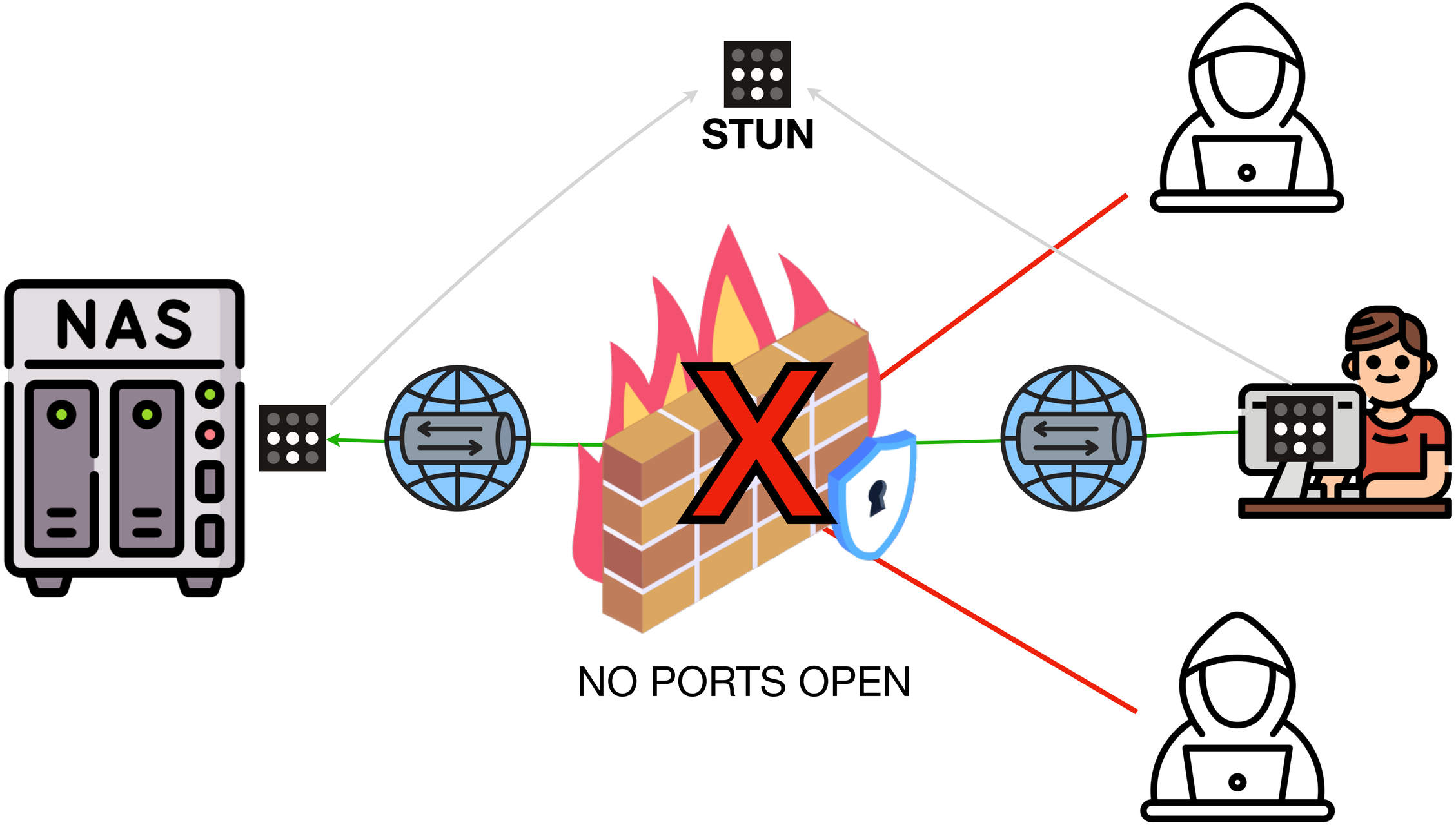


Moving beyond the firewall

- Every device can talk to every other device
  - (And avoid the hub and spoke VPN model)
- Traverse NAT and complex network topologies
- Encrypt traffic
- We need a way to establish identity
  - Only allowing trusted users access to even attempt to connect to services
  - No more port forwarding!

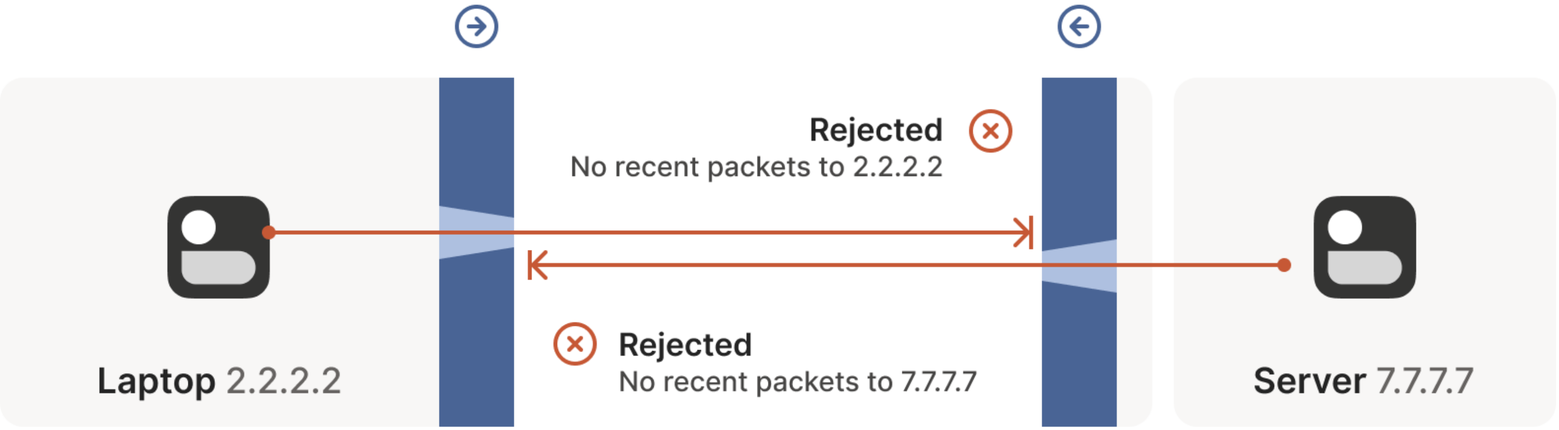



SSH (22)
NAS
NO PORTS OPEN


STUN
NAS
NO PORTS OPEN

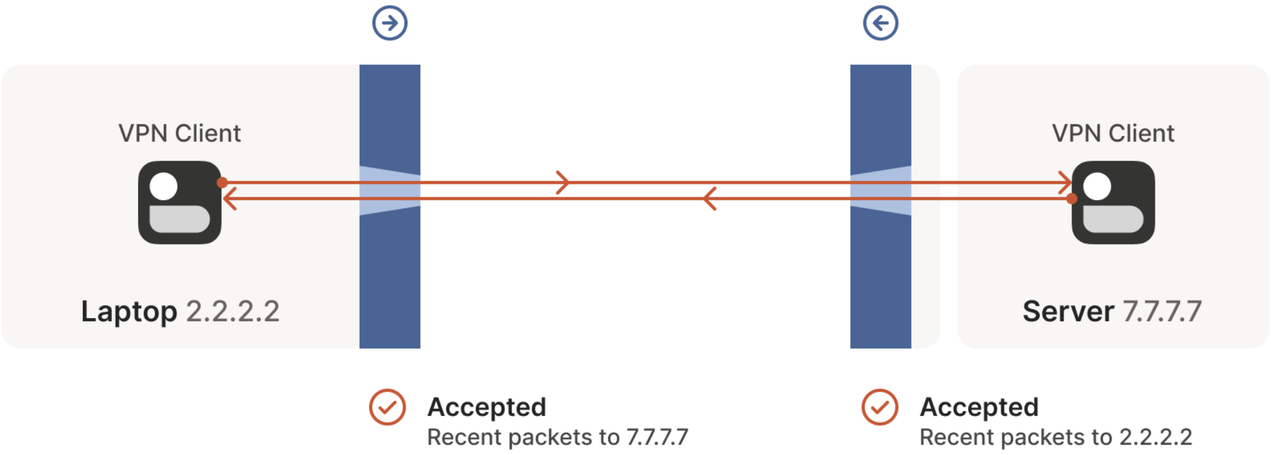
Direct connections

- Using NAT Traversal any device can directly connect to any other device securely no matter the network topology
- Tailscale uses a combination of external STUN and co-ordination servers
  - They handle the mapping of NAT addresses to UDP ports
  - Allowing devices behind stateful firewalls to connect directly to each other



Direct connections

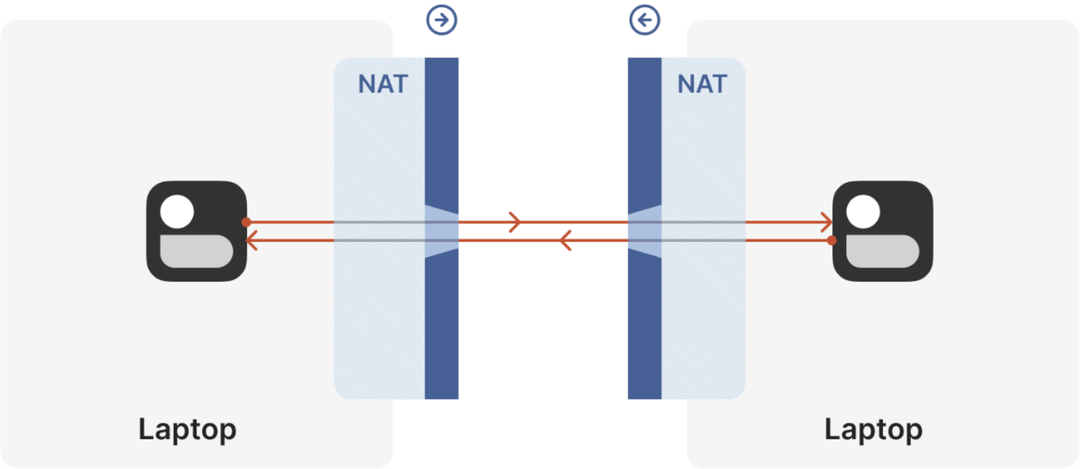
- Using NAT Traversal any device can directly connect to any other device securely no matter the network topology
- Tailscale uses a combination of external STUN and co-ordination servers
  - They handle the mapping of NAT addresses to UDP ports
  - Allowing devices behind stateful firewalls to connect directly to each other



How NAT traversal works

August 21 2020 David Anderson

We covered a lot of ground in our post about *How Tailscale Works*. However, we glossed over how we can get through NATs (Network Address Translators) and connect your devices directly to each other, no matter what's standing between them. Let's talk about that now!



https://tailscale.com/blog/how-nat-traversal-works

Let's start with a simple problem: establishing a peer-to-peer connection

So what?

Today’s agenda

- ~~Why port forwarding is dangerous~~
- ~~Using a mesh VPN to “hop over” your firewall securely~~
- Discuss a bit about docker compose
  - And how to run self-hosted services
  - Including some reverse proxy tips with Traefik and Caddy
- Move on to some DNS trickery
  - Cloudflare
  - Tailscale MagicDNS
- The big reveal!

Running local services

Using docker compose

Self-hosting is fun!

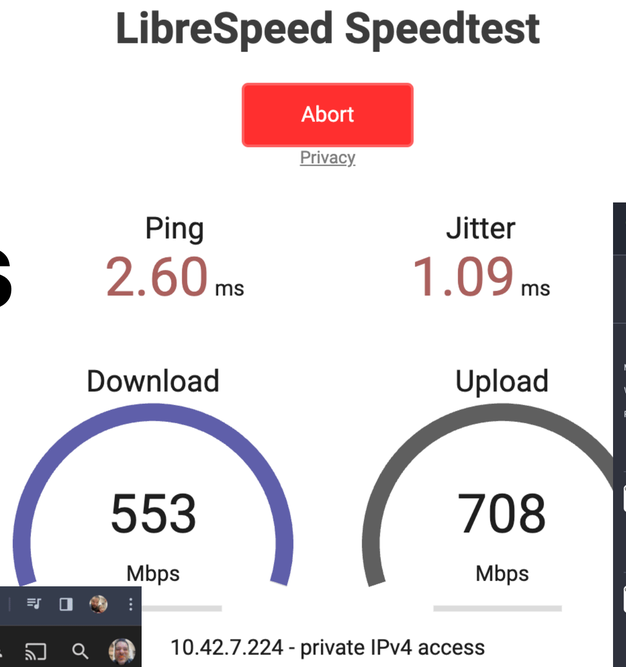
Honest.

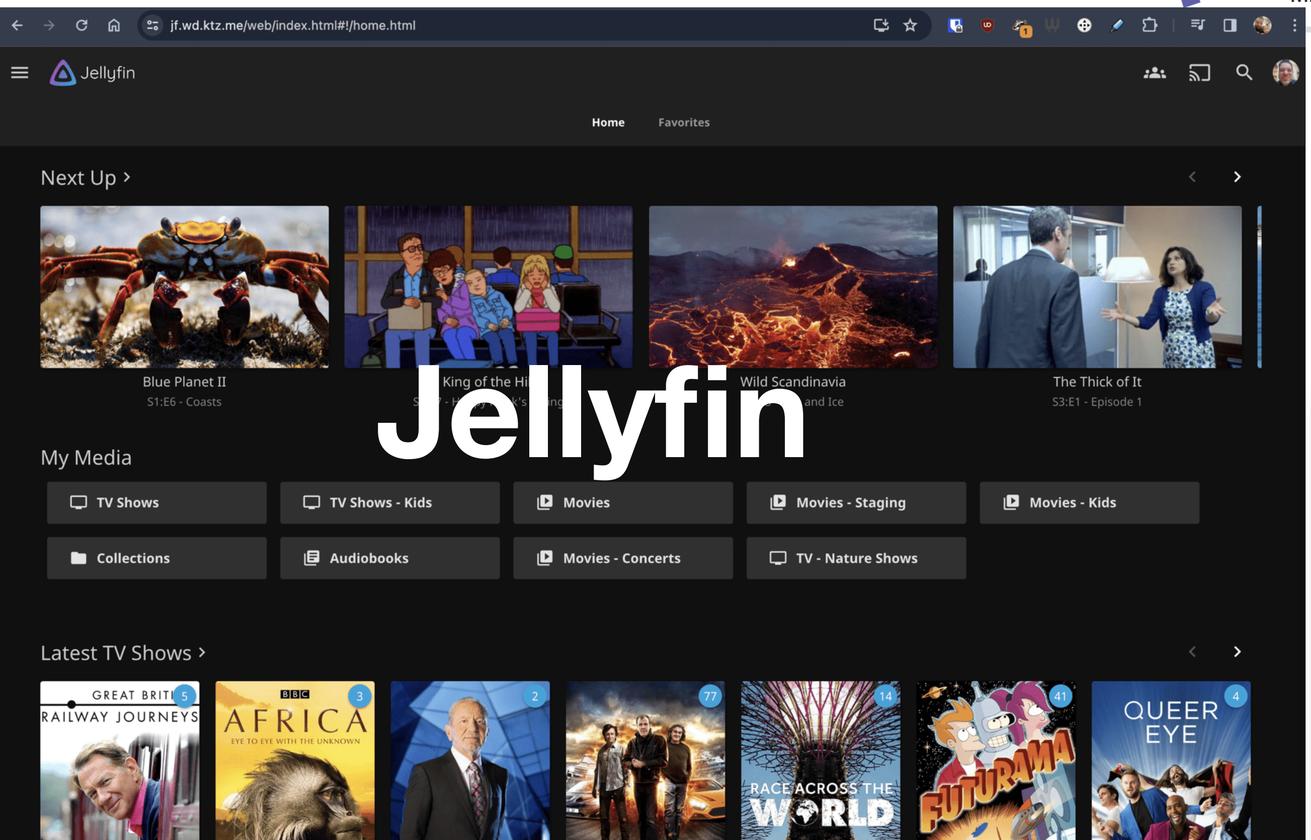
- You own your data.
  - You can lose data, and it's your fault!
  - And the outages too!
- Build a solution piece by piece
- Considered project selection means you can build solutions to last a lifetime with real craftsmanship and care
- There is no business model to feed (except an open source developer)

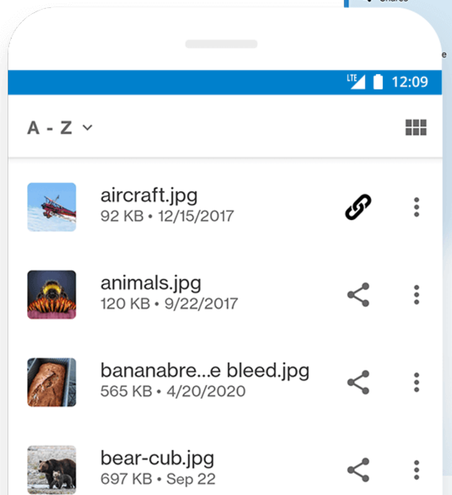
SELFHOSTED

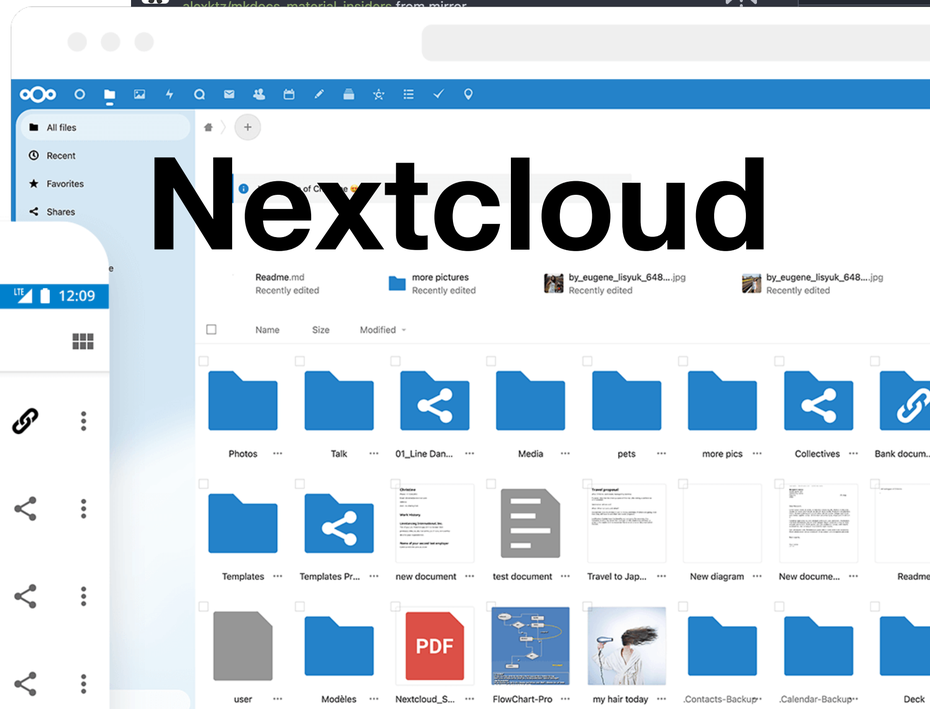
https://selfhosted.show

Self-hosted app picks









immich

Self-hosted photo and video management solution

Self-hosting basics

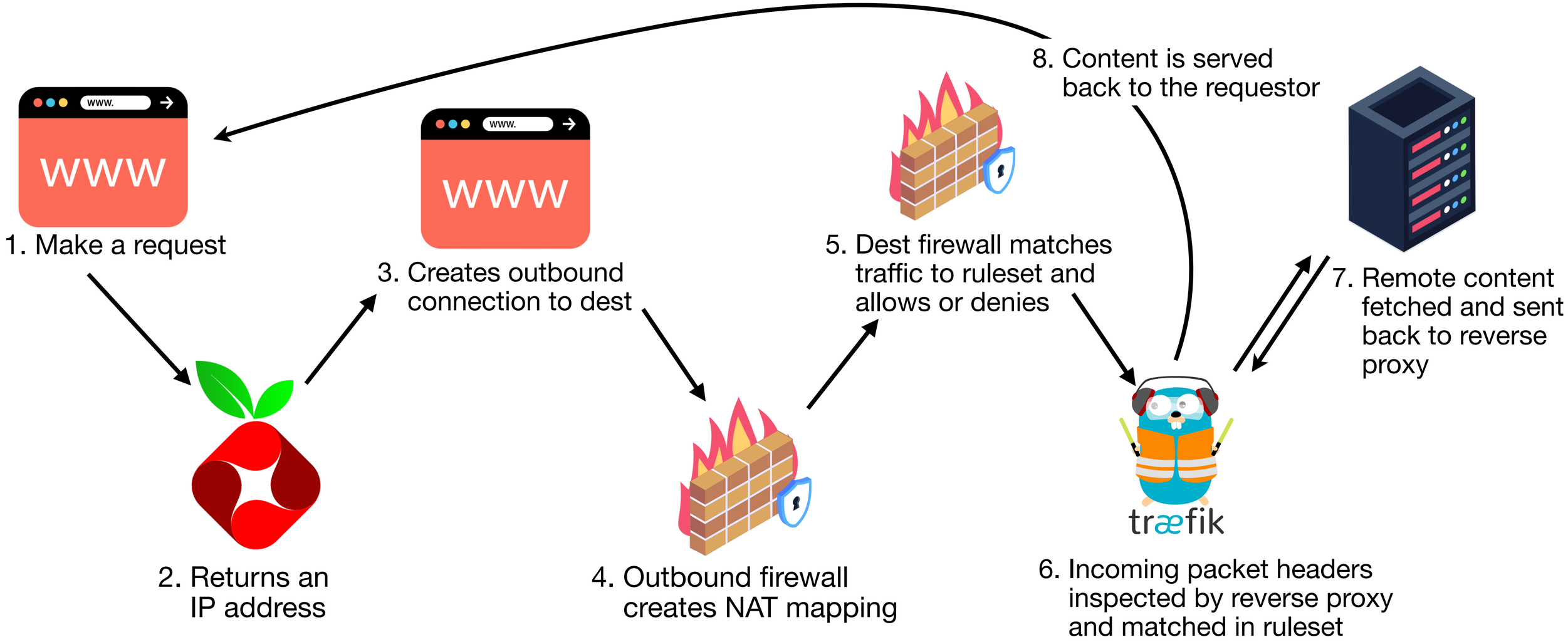
- Docker compose is a YAML based declarative way to deploy containers

```yaml
abs:
  image: advplyr/audiobookshelf
  container_name: abs
  volumes:
    - /mnt/bigrust18/media/audiobooks/library:/audiobooks:ro
    - /mnt/bigrust18/media/audiobooks/library2:/audiobooks2:ro
    - /mnt/bigrust18/media/audiobooks/podcasts:/podcasts
    - /mnt/appdata/mediaservers/audiobookshelf/metadata:/metadata
    - /mnt/appdata/mediaservers/audiobookshelf/config:/config
  labels:
    - traefik.enable=true
    - traefik.http.routers.audiobookshelf.rule=Host(`abs.wd.ktz.me`)
  ports:
    - 2284:80
  restart: unless-stopped
```

- `docker compose up -d`

What happens?

- If I type “https://abs.wd.ktz.me" into a browser - what happens?



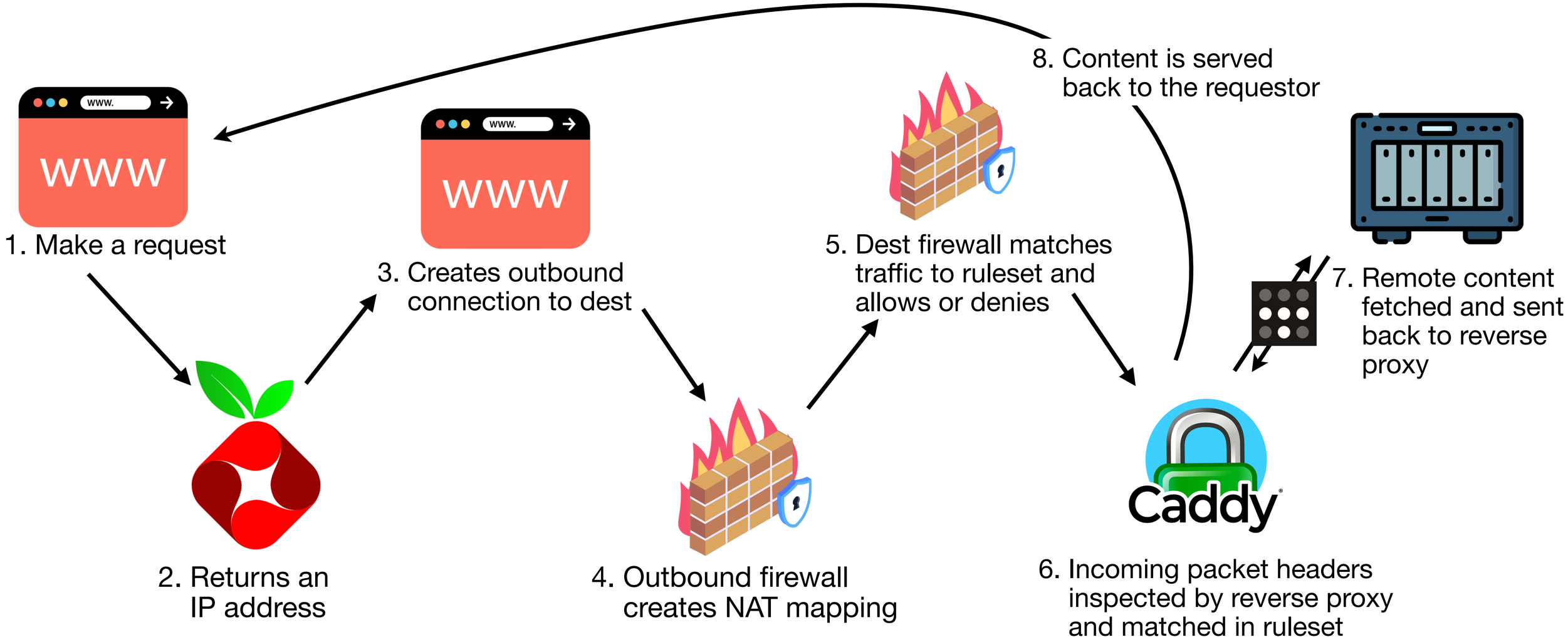
Pihole specifics

- I want each site locally to work as a standalone entity
  - without internet or Tailscale involved
- I run a Pihole in each location as a local DNS server
- I place an A record for `192.168.1.10` resolving to `abs.wd.ktz.me`
- Feel free to sub Pihole (which is really just dnsmasq in a fancy frock) for AdGuard Home, Unbound or any other DNS server you like

```
root@pihole:~# cat /etc/dnsmasq.d/03-dns-overrides.conf
# Ansible managed
address=/wd.ktz.me/10.42.0.252
address=/opnsense.wd.ktz.me/10.42.0.252
address=/zoidberg.wd.ktz.me/10.42.0.252
address=/hass.ktz.me/10.42.1.99
address=/nc.ktz.cloud/10.42.1.42
address=/git.ktz.me/10.42.1.42
address=/unifi/10.42.0.250
address=/inform.unifi.wd.ktz.me/10.42.0.250
address=/opnsense.firewall.wd.ktz.me/10.42.0.254
address=/z.wd.ktz.me/10.42.0.42
```

Tailscale madness

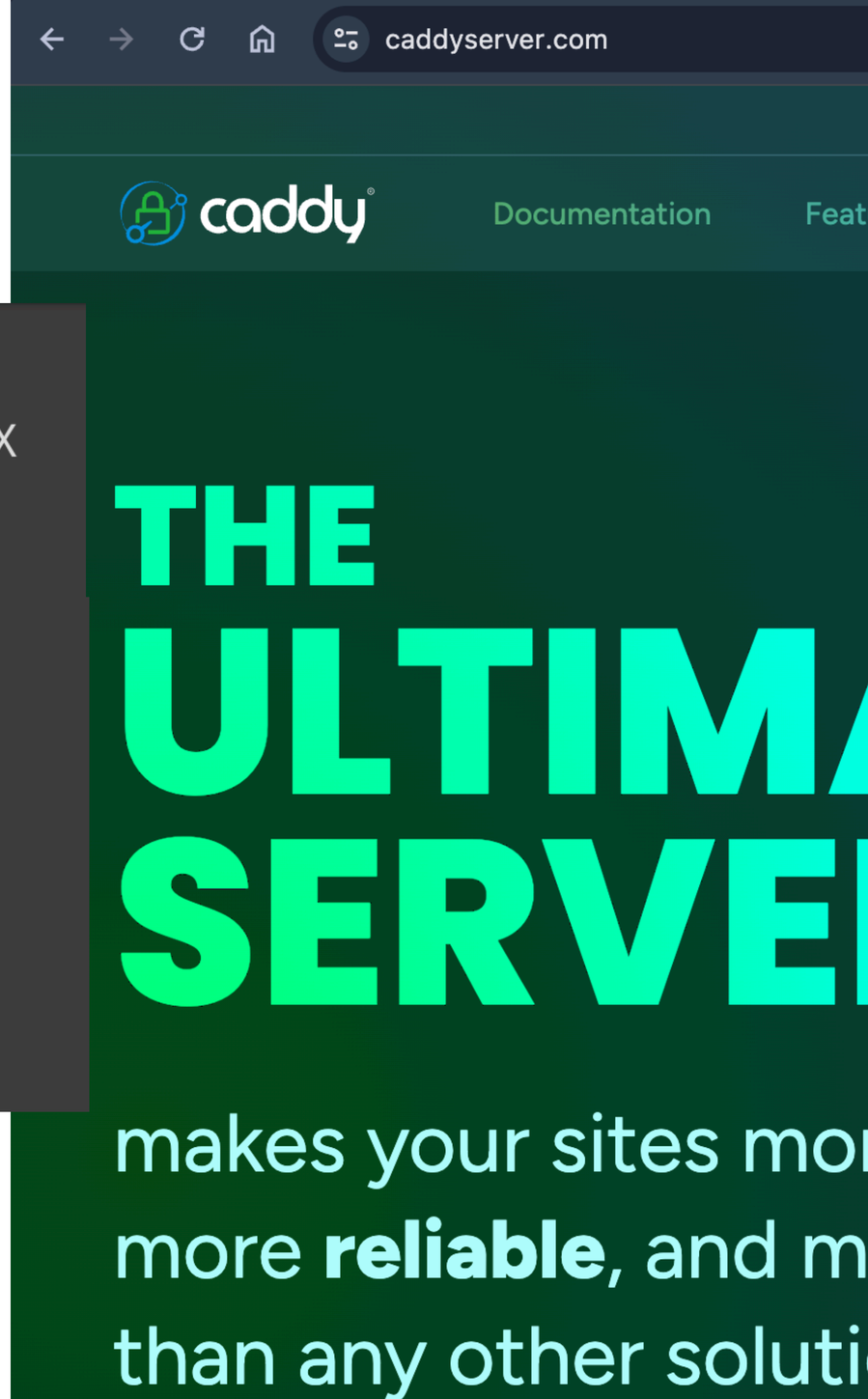
- What if step 6 and 7 were in totally different physical locations?



Caddy is stupidly simple

```
(cloudflare) {
  tls {
    dns cloudflare vC4s[redacted]fX
  }
}

# abs
abs.wd.ktz.me {
  reverse_proxy http://10.42.1.10:2284
  import cloudflare
}
```

/etc/caddy/Caddyfile



Fun with Caddy

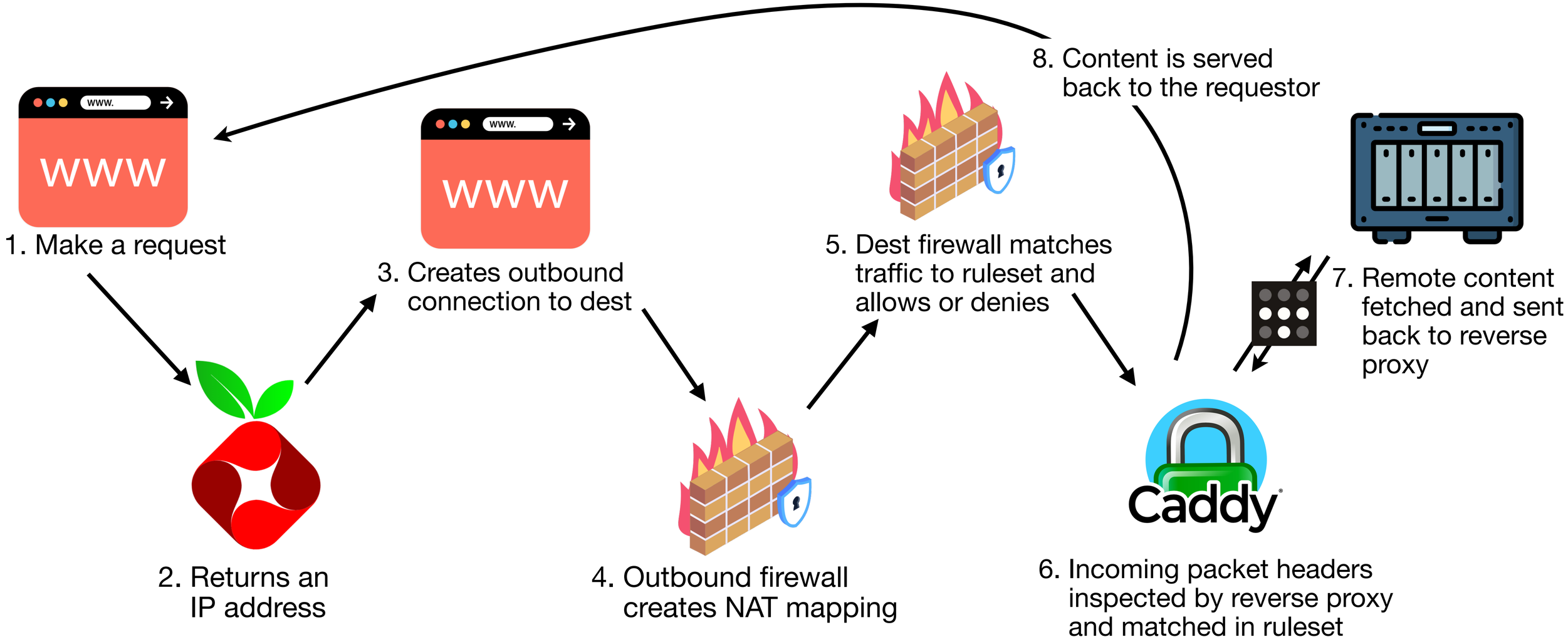
awesomo alexktz@gmail.com	100.89.87.143
caddy alexktz@gmail.com Shared out +3 SSH	100.118.52.61
cat-laptop alexktz@gmail.com	100.93.152.121
deepthought alexktz@gmail.com Shared out +1 SSH	100.109.58.127
synology alexktz@gmail.com	100.99.254.122

```
(cloudflare) {
  tls {
    dns cloudflare vC4s[redacted]fX
  }
}

dsm.wd.ktz.me {
  reverse_proxy https://100.99.254.122:5001 {
    transport http {
      tls_insecure_skip_verify
    }
  }
  import cloudflare
}



# abs
abs.wd.ktz.me {
  reverse_proxy http://10.42.1.10:2284
  import cloudflare
}
```

/etc/caddy/Caddyfile

Tailscale madness

- What if step 6 and 7 were in totally different physical locations?

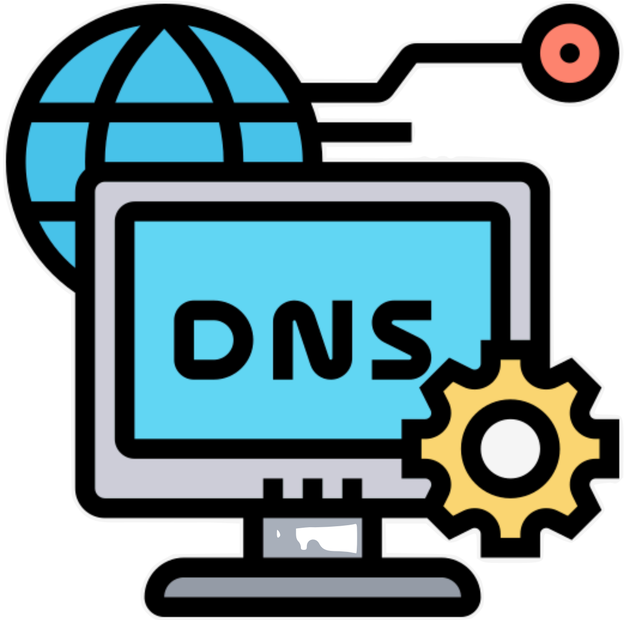


Agenda (time check!)

- ~~Why port forwarding is dangerous~~
- ~~Using a mesh VPN to “hop over” your firewall securely~~
- ~~Discuss a bit about docker compose~~
  - ~~And how to run self-hosted services~~
  - ~~Including some reverse proxy tips with Traefik and Caddy~~
- Move on to some DNS trickery
  - Cloudflare
  - Tailscale MagicDNS
- The big reveal!

Cloudflare CNAME trickery

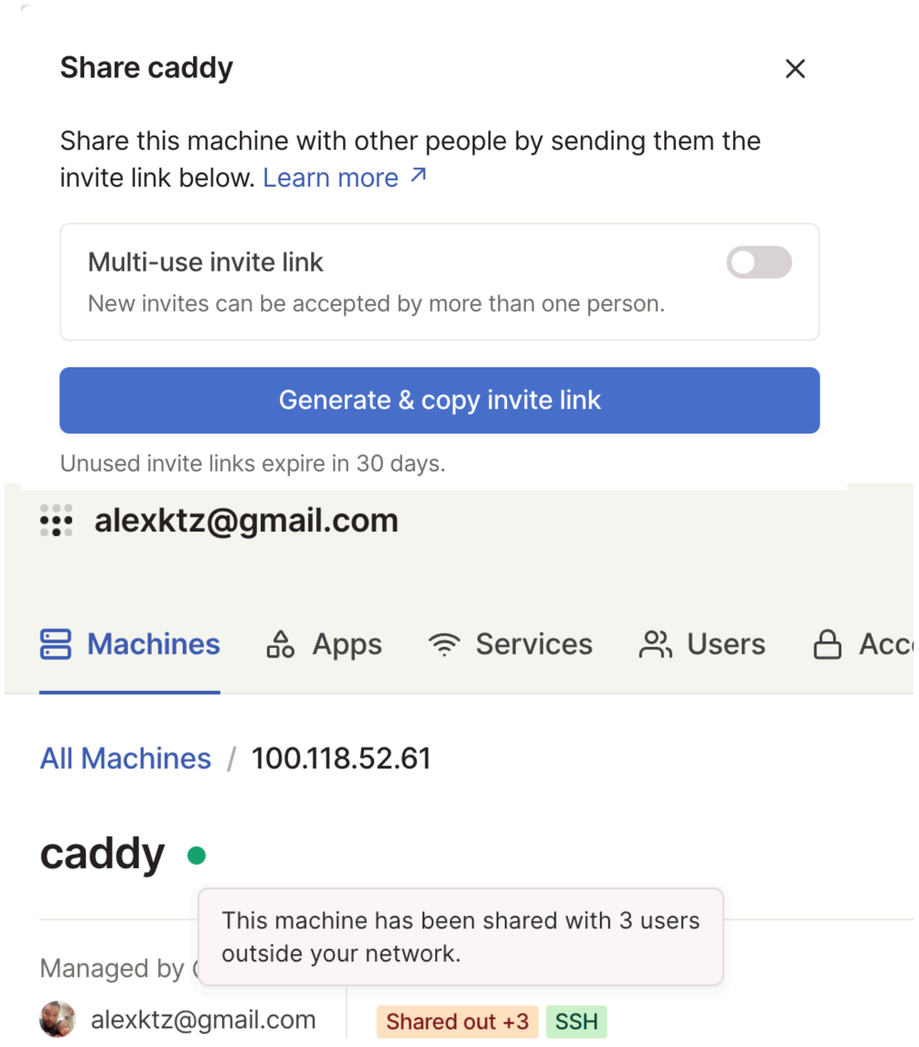
It’s always DNS



How to securely share services

with others and other Tailnets

- Make sure your reverse proxy is a dedicated node on your Tailnet
- Share it out using node sharing to a friend or relative
- Place a CNAME into a public DNS provider pointing to that node



DNS management for **dotsandstuff.dev**

Review, add, and edit DNS records. Edits will go into

Type	Name	Content	Proxy status	TTL	Actions
CNAME	*.rdu	caddy.velociraptor-noodlefis...	DNS only	1 min	Edit

Type: CNAME

Name (required): *.rdu

Use @ for root

Target (required): caddy.velociraptor-noodlefish.ts.net

E.g. www.example.com

Proxy status: DNS only

TTL: 1 min

Record Attributes

Documentation

The information provided here will not impact DNS record resolution and is only meant for your reference.

Comment

Enter your comment here (up to 100 characters).

Delete

Cancel

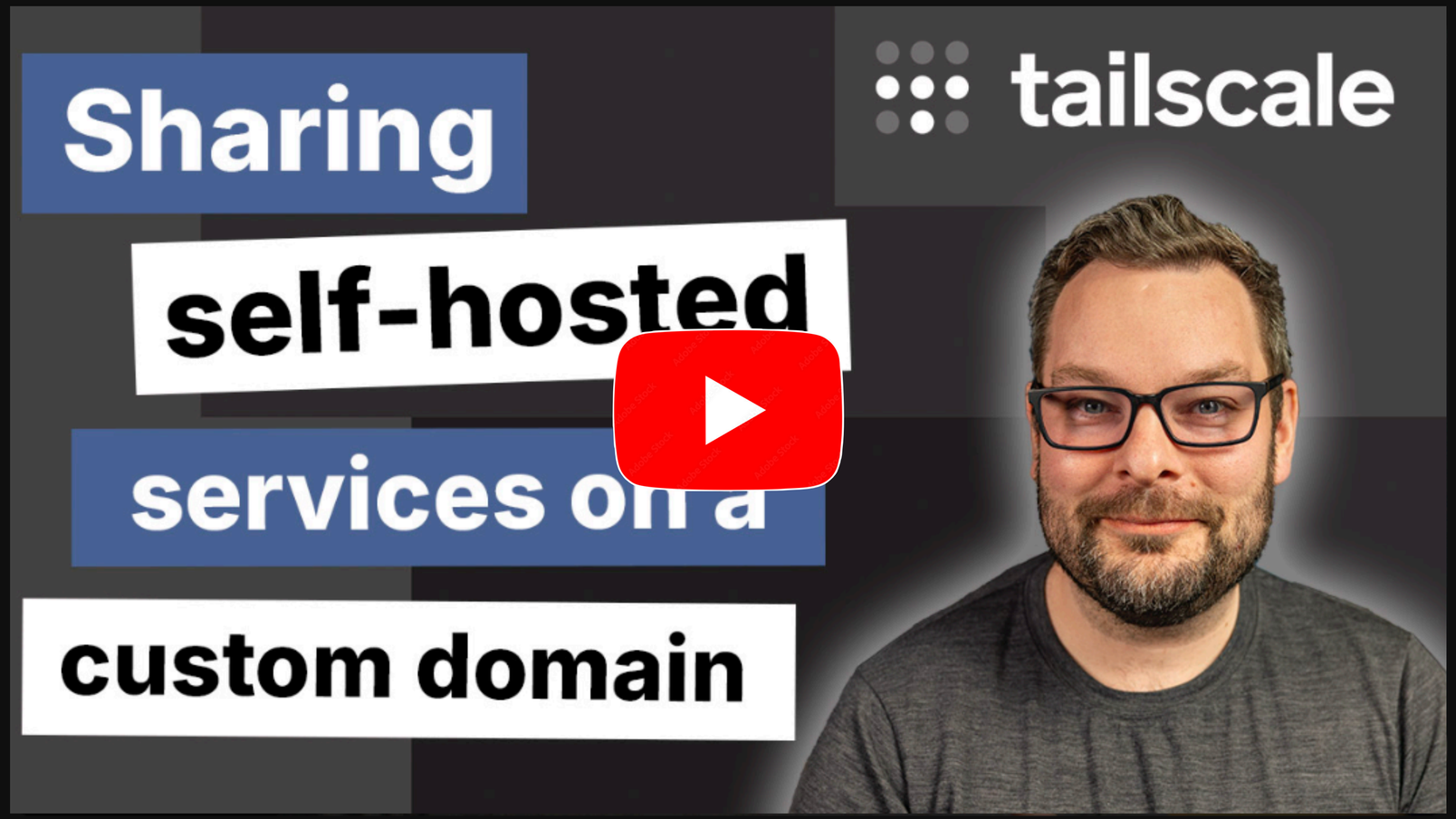
Save

```
alex@magrathea ~ % dig test.rdu.dotsandstuff.dev

; <<>> DiG 9.10.6 <<>> test.rdu.dotsandstuff.dev
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 26572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;test.rdu.dotsandstuff.dev.     IN      A

;; ANSWER SECTION:
test.rdu.dotsandstuff.dev. 60   IN      CNAME   caddy.velociraptor-noodlefish.ts.net.

;; AUTHORITY SECTION:
ts.net.                 300     IN      SOA     ns1.dnsimple.com. admin.dnsimple.com. 1616222330 86400
7200 604800 300

;; Query time: 189 msec
;; SERVER: 100.100.100.100#53(100.100.100.100)
;; WHEN: Tue Apr 09 18:27:34 EDT 2024
;; MSG SIZE  rcvd: 162
```

```
alex@magrathea ~ % dig test.rdu.dotsandstuff.dev

; <<>> DiG 9.10.6 <<>> test.rdu.dotsandstuff.dev
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 26572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;test.rdu.dotsandstuff.dev.     IN      A

;; ANSWER SECTION:
test.rdu.dotsandstuff.dev. 60   IN      CNAME   caddy.velociraptor-noodlefish.ts.net.

;; AUTHORITY SECTION:
ts.net.                 300     IN      SOA     ns1.dnsimple.com. admin.dnsimple.com. 1616222330 86400
7200 604800 300

;; Query time: 189 msec
;; SERVER: 100.100.100.100#53(100.100.100.100)
;; WHEN: Tue Apr 09 18:27:34 EDT 2024
;; MSG SIZE  rcvd: 162
```

YouTube

Search



Remotely access and share your self-hosted services

Tailscale
8.11K subscribers

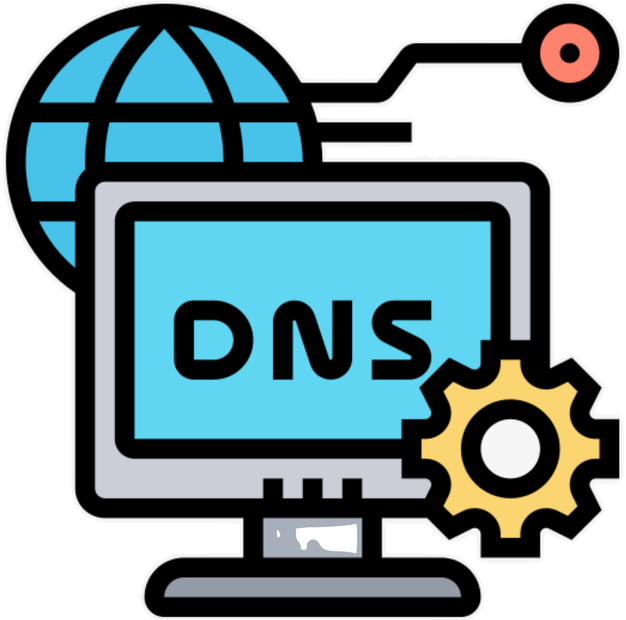
Analytics | Edit video | 968 | Share | Promote | ···

32K views 1 month ago

We're going to use Tailscale and the reverse proxy Caddy to share self-hosted services on your Tailnet with friends and family.

In today's video we focus on Immich - a self-hosted photo backup tool, Audiobookshelf - an audiobook server, and Jelly ...more

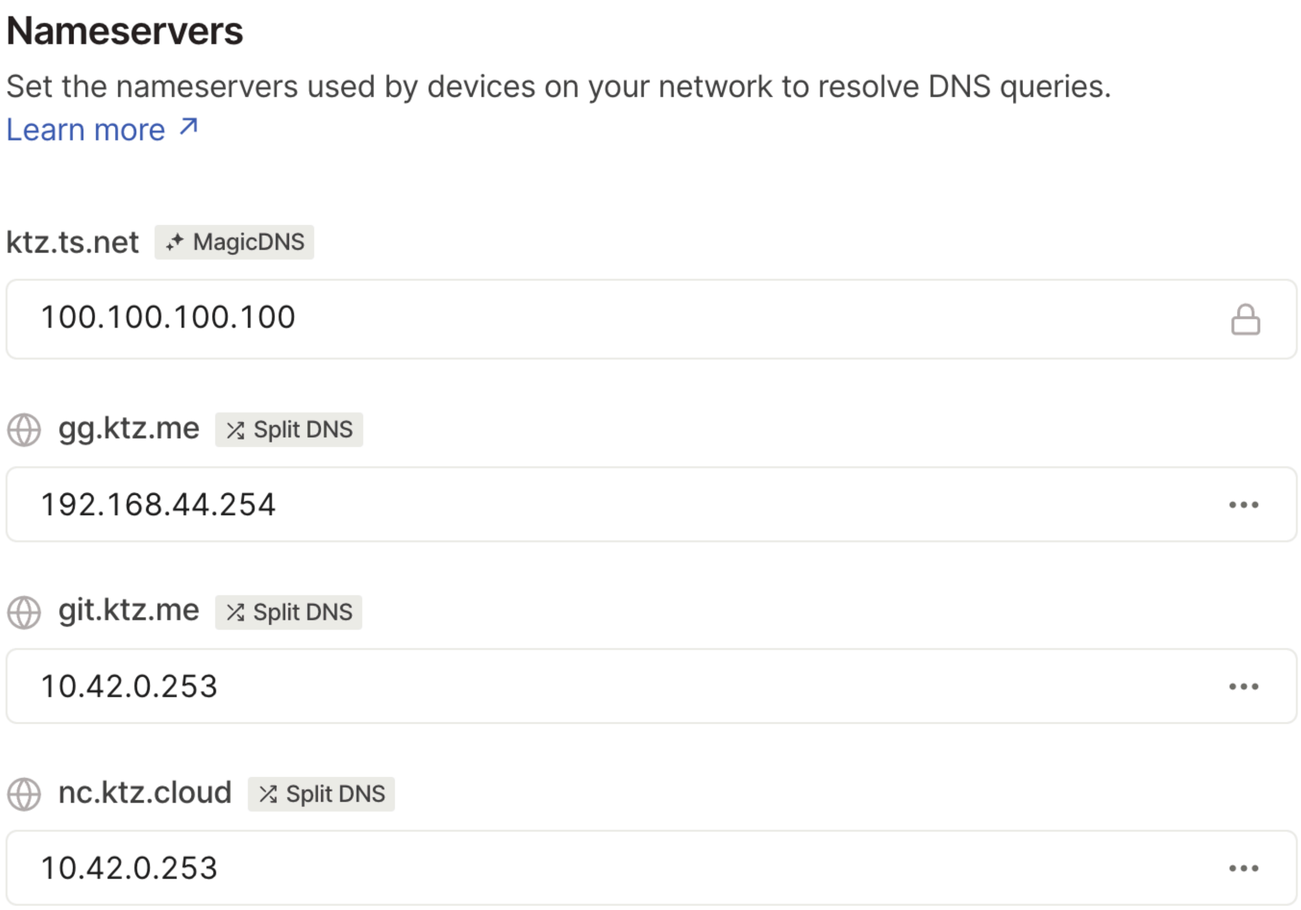
MagicDNS tricks



Or if it’s just your Tailnet

Use MagicDNS

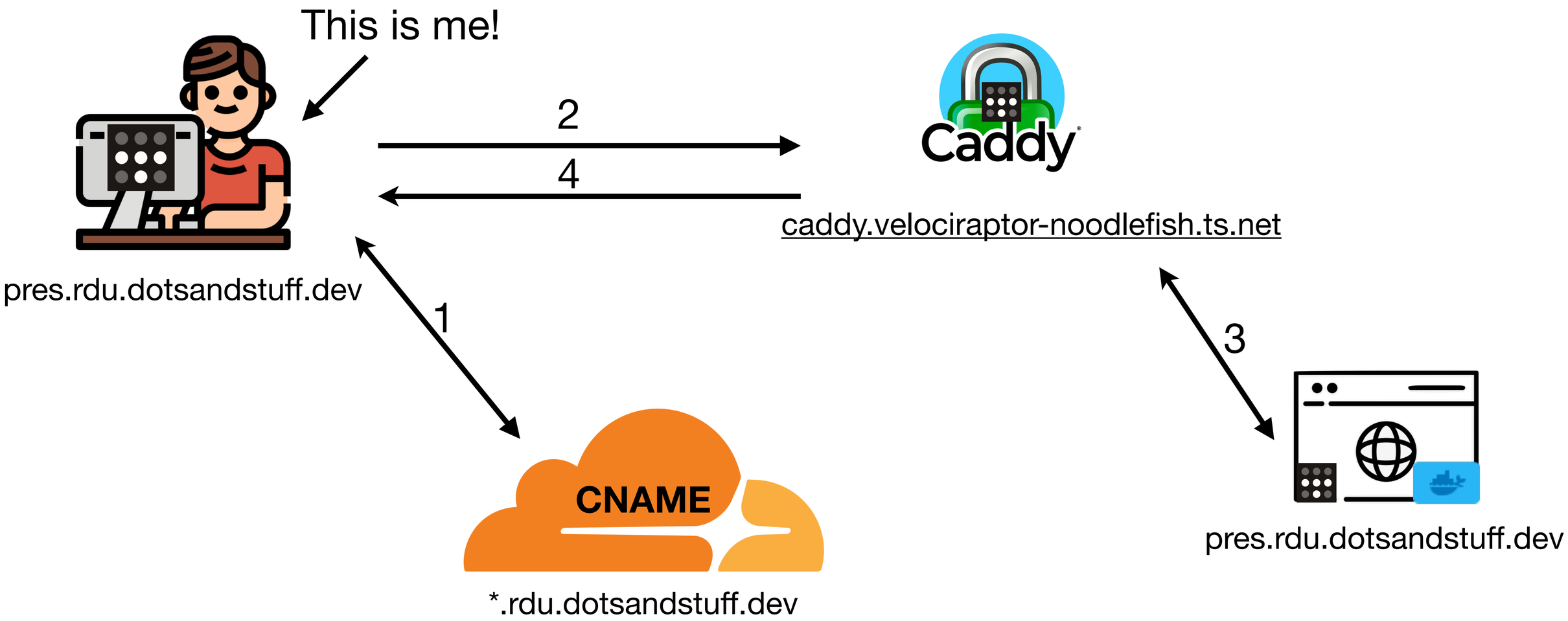
- Use SplitDNS to route arbitrary requests wherever you’d like
- This works for ts.net domains
- And for any custom domain you’d like to go somewhere unusual



The big reveal!

It’s turtles all the way down.

It’s turtles all the way down.



KTZ Systems

SELF HOSTED

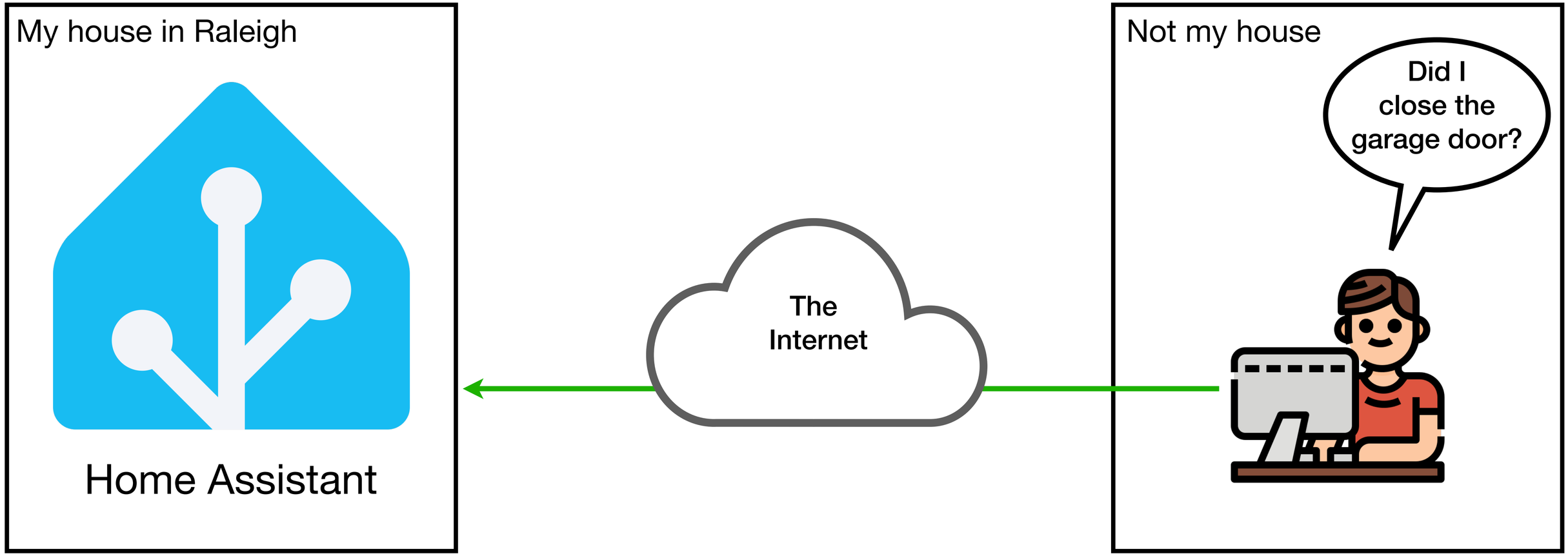
Alex Kretzschmar

🖥️ https://alex.ktz.me
📽️ YouTube - KTZ Systems
🎙️ https://selfhosted.show
🦣 mastodon techhub.social/@ironicbadger
📓 https://blog.ktz.me
💾 https://perfectmediaserver.com
👨🏽‍💻 https://github.com/ironicbadger

Death Valley at Sunset

fin.

ide


My house in Raleigh
Home Assistant
The Internet
Not my house
Did I close the garage door?

A real domain name

Garage door