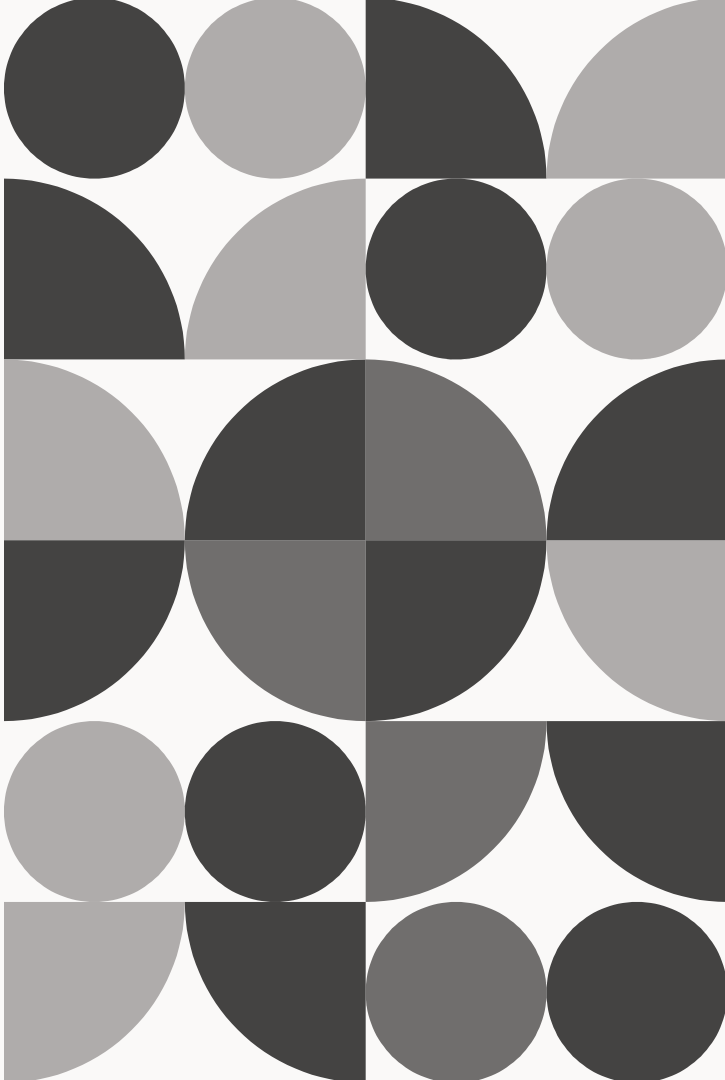
SCALE 23X

Punching Through Firewalls Without Punching Holes

03.08.2026

tailscale




Not Alex Kretzschmar
Howard

I’m Kevin Purdy, here’s how I got here

ANNOUNCEMENTS

Five Lists of Five Things I Learned at Lifehacker

BY KEVIN PURDY

Share +1 Like

Today is my last day as the "morning guy" at Lifehacker. I wrote approximately 5,883 posts in slightly less than three and a half years. Some, I hope, were notable. Some make me cringe. I've pulled out a few posts

GET OUR TOP STORI
FOLLOW LIFEHACK

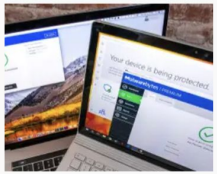
Like 343,179 pe

The Best Toilet Brush

Updated January 22, 2026

You Can Build an Ebike. Yes,

Updated June 24, 2022



You Don’t Need to Buy Antiv

Updated April 21, 2020

I RESPECT YOU TECHNICALLY

As the Kernel Turns: Rust in Linux saga reaches the “Linus in all-caps” phase

Torvalds: You can avoid Rust as a C maintainer, but you can’t interfere with it.

KEVIN PURDY – FEB 21, 2025 1:55 PM | 224

Lifehacker

Ask me about blogging before proxy-Hulk-Hogan took it down

Wirecutter

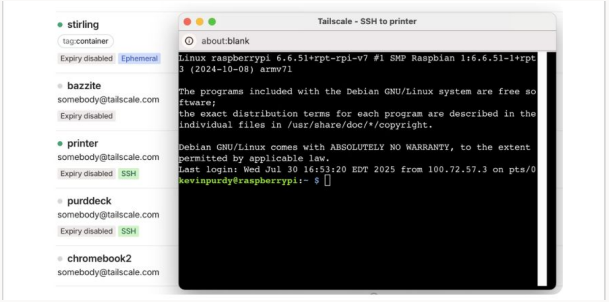
Ask me about mattresses. Or recycled toilet paper. Or cutting boards.

Ars Technica

Ask me about … the Linux Kernel Mailing List?

Insights December 01, 2025

Let's put Tailscale on a jailbroken Kindle



Insights November 04, 2025

Why you should mail your parents a Tailscale node

Set up a VPN, remote tech support, file sharing, and other useful things by mailing a little Tailscale to your friends and family.

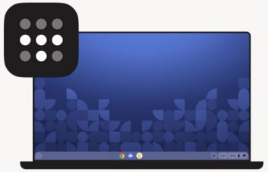
Kevin Purdy

Insights September 22, 2025

Upgrade your travel kit with a tiny, Tailscale-friendly router

I'll be on vacation when this post is published. It's not a tropical, cultural, or adventure vacation, but a kind of remote staycation, in a big rented house, with...

Kevin Purdy



And now I do this!

Homelab

Education! Refurbishment! Unpaid labor! Backups of ... your Linux ISOs, yes.

But really, anything is a homelab

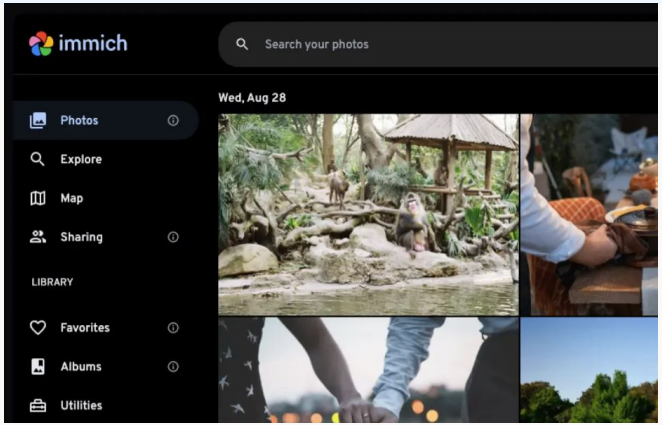
(Except an iPad)

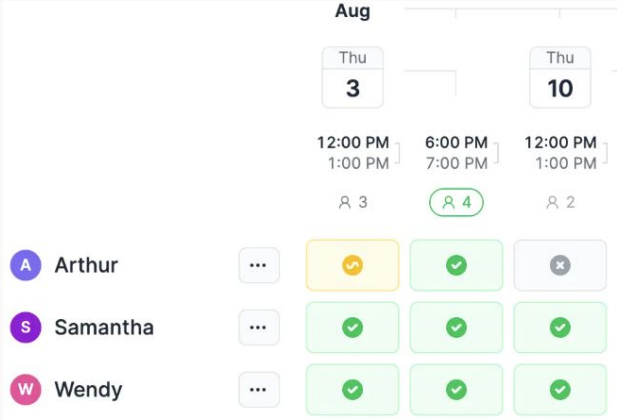
- Raspberry Pi
- Mac mini
- NUC from a dentist’s office
- Laptop w/ or w/o screen

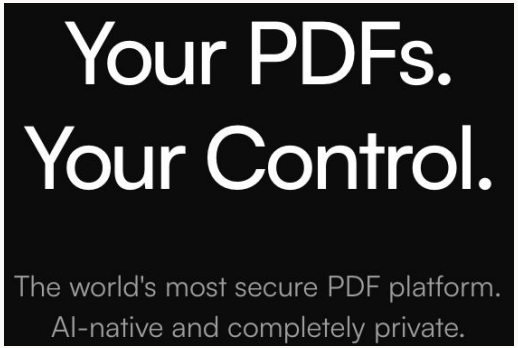
Warning: Self-hosting is addictive

June 2, 2025:
0 Containers

March 4, 2026:
33 Containers

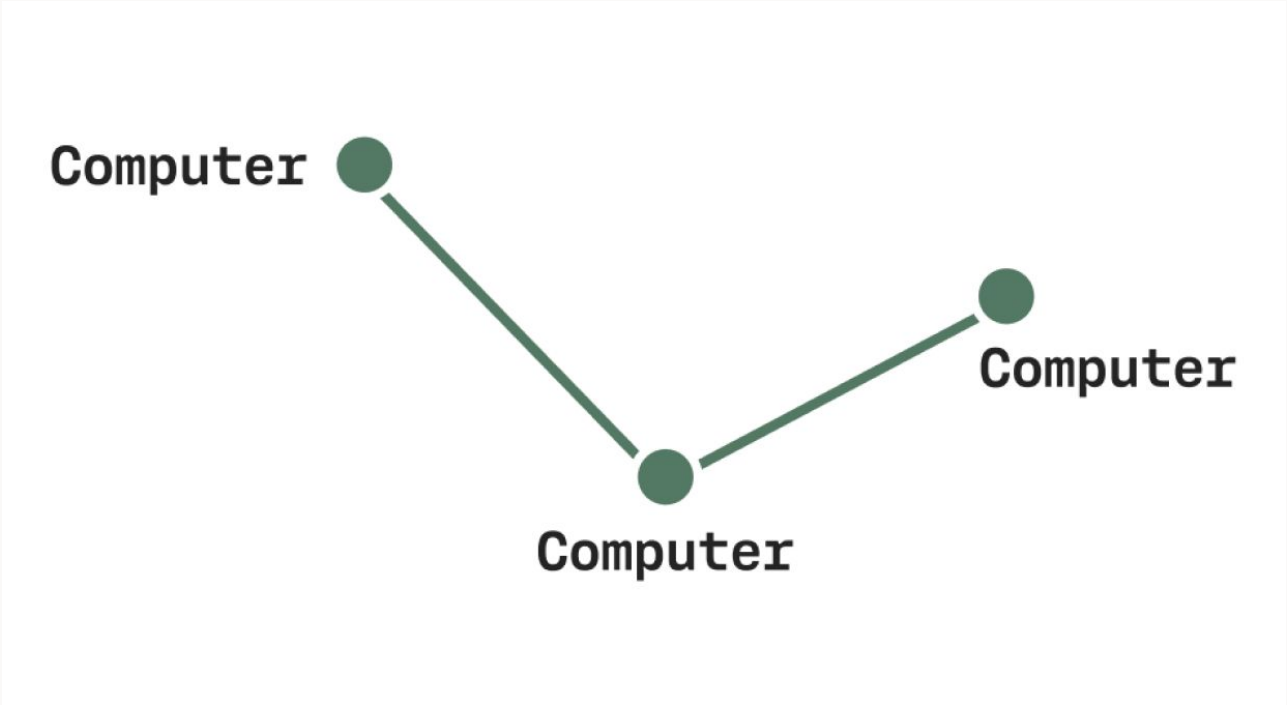


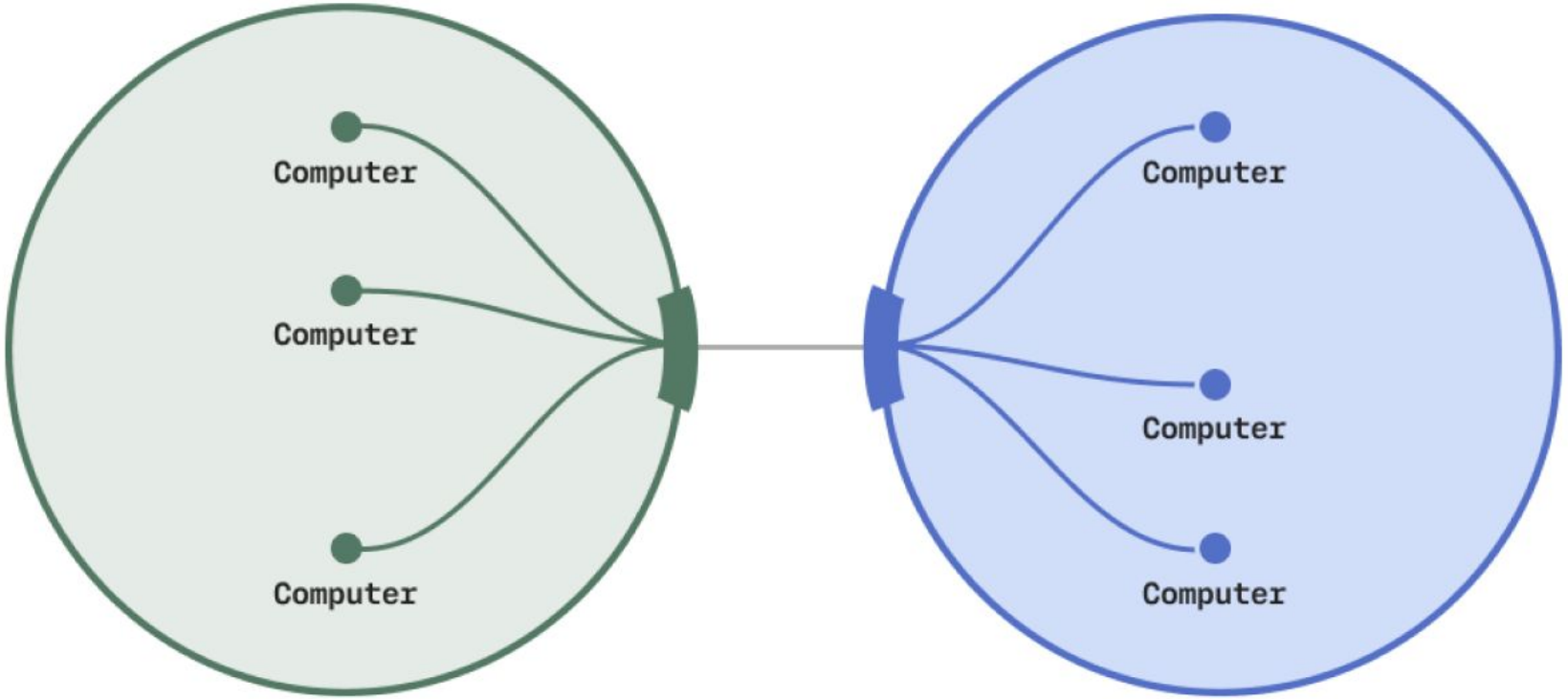


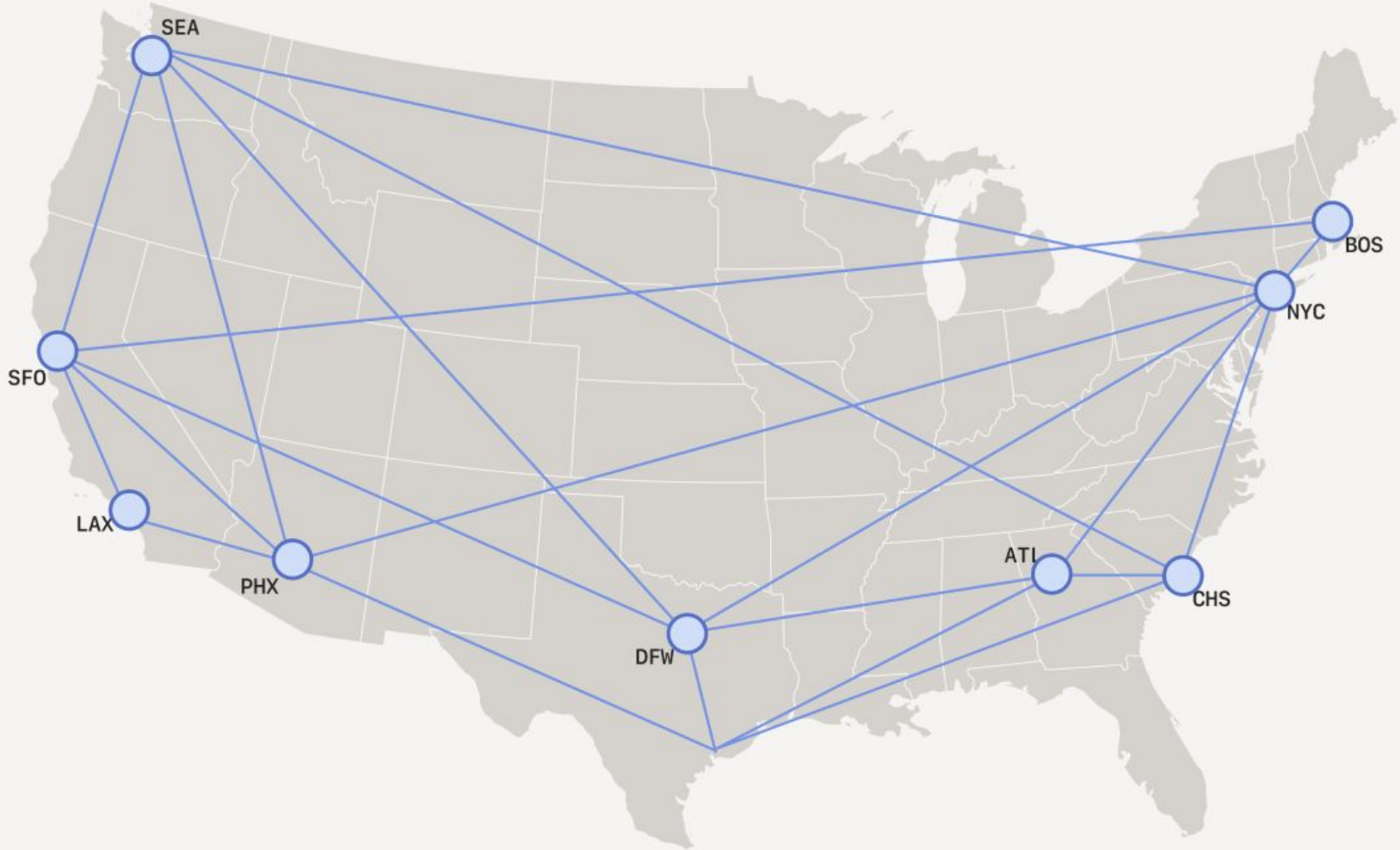


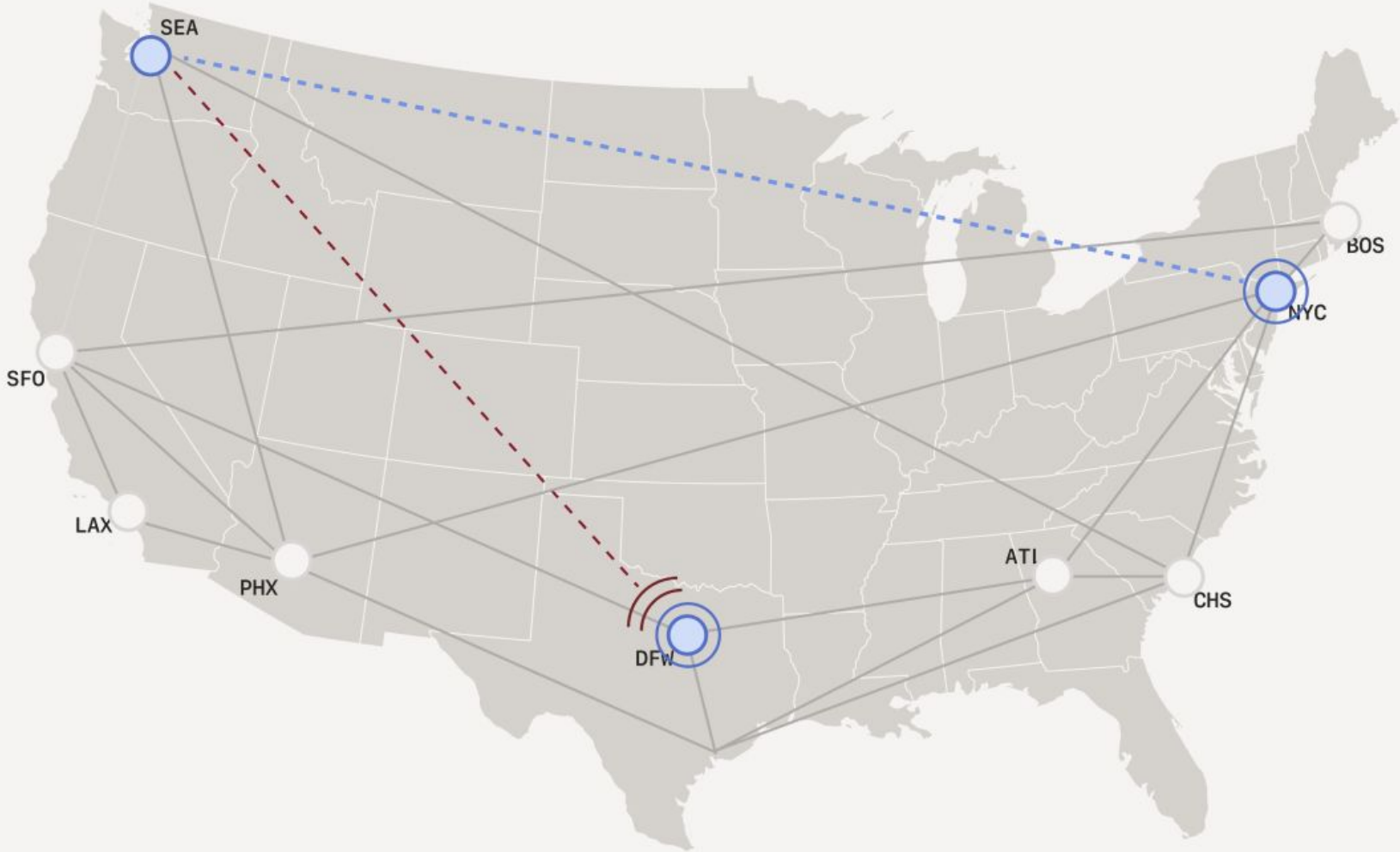
I thought this talk was about firewalls and ports?

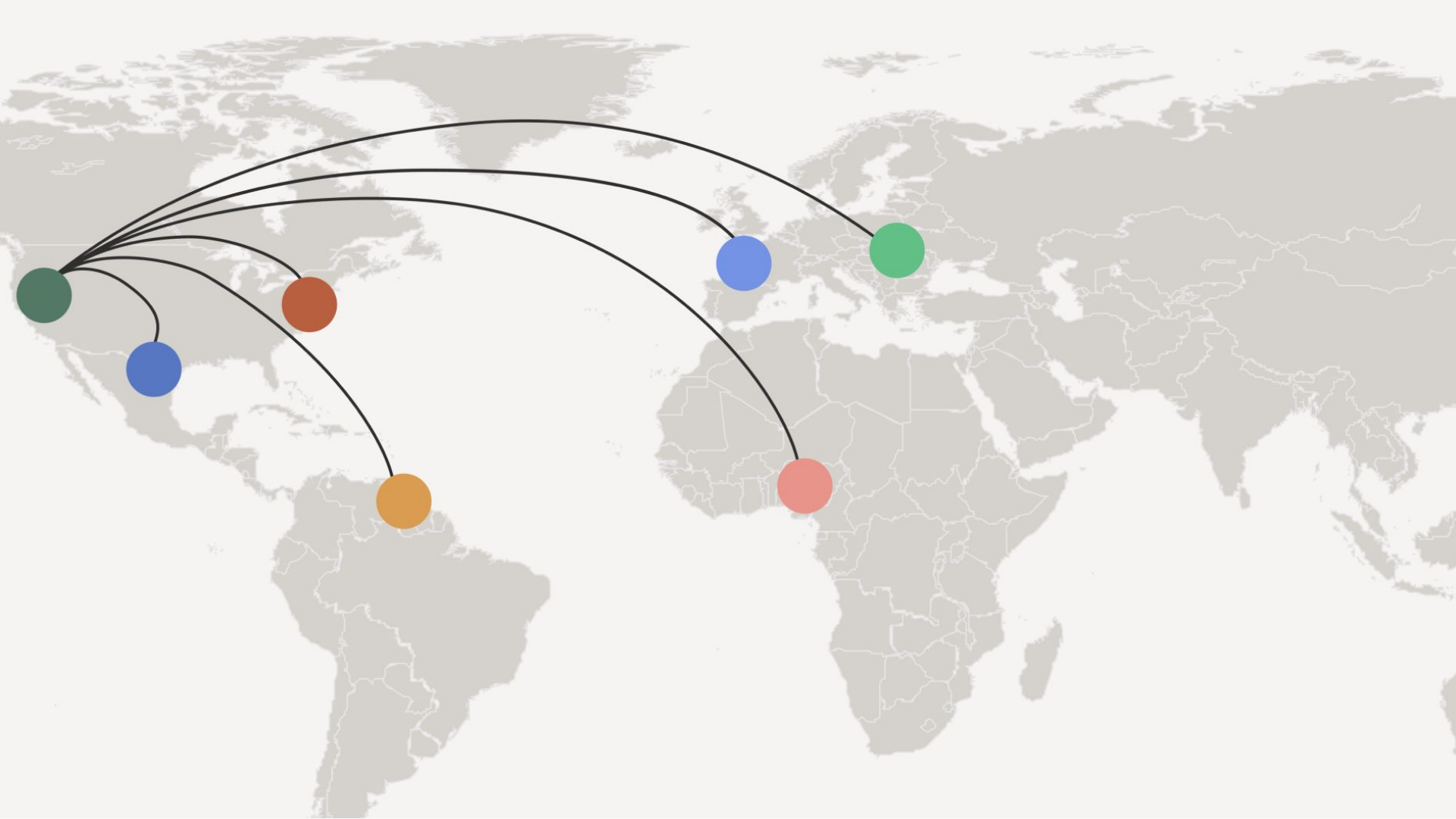
Computer

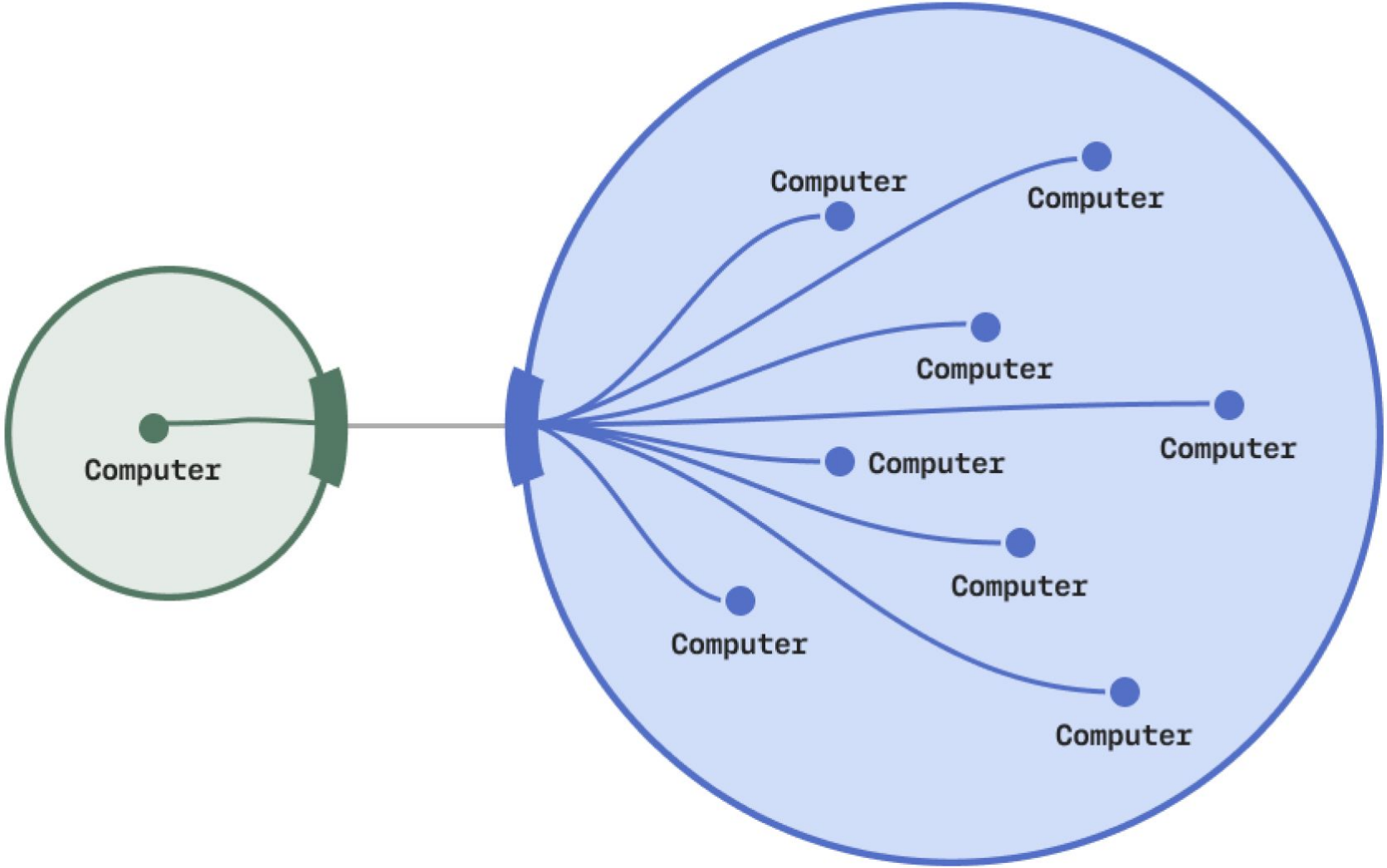





SEA
BOS
NYC
SFO
LAX
PHX
ATL
CHS
DFW

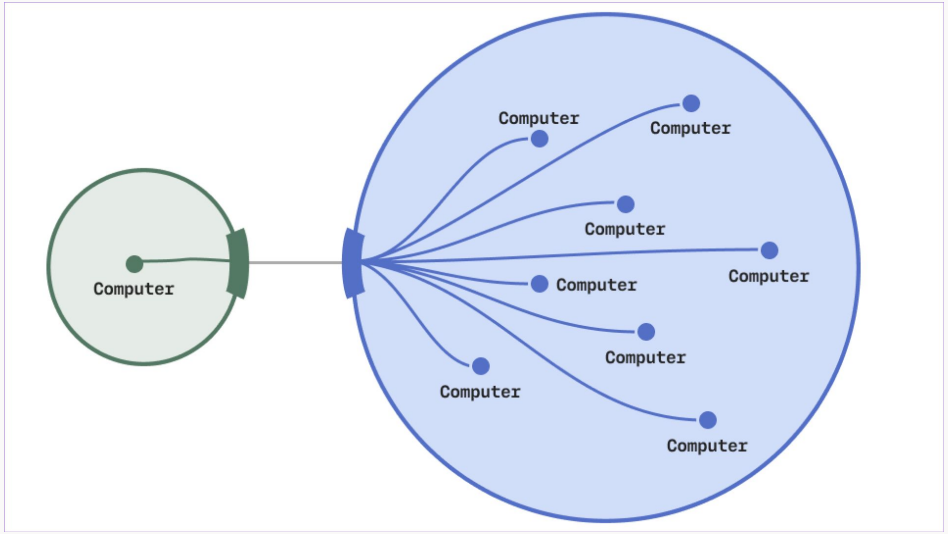

SEA
BOS
NYC
SFO
LAX
PHX
ATI
CHS
DFW

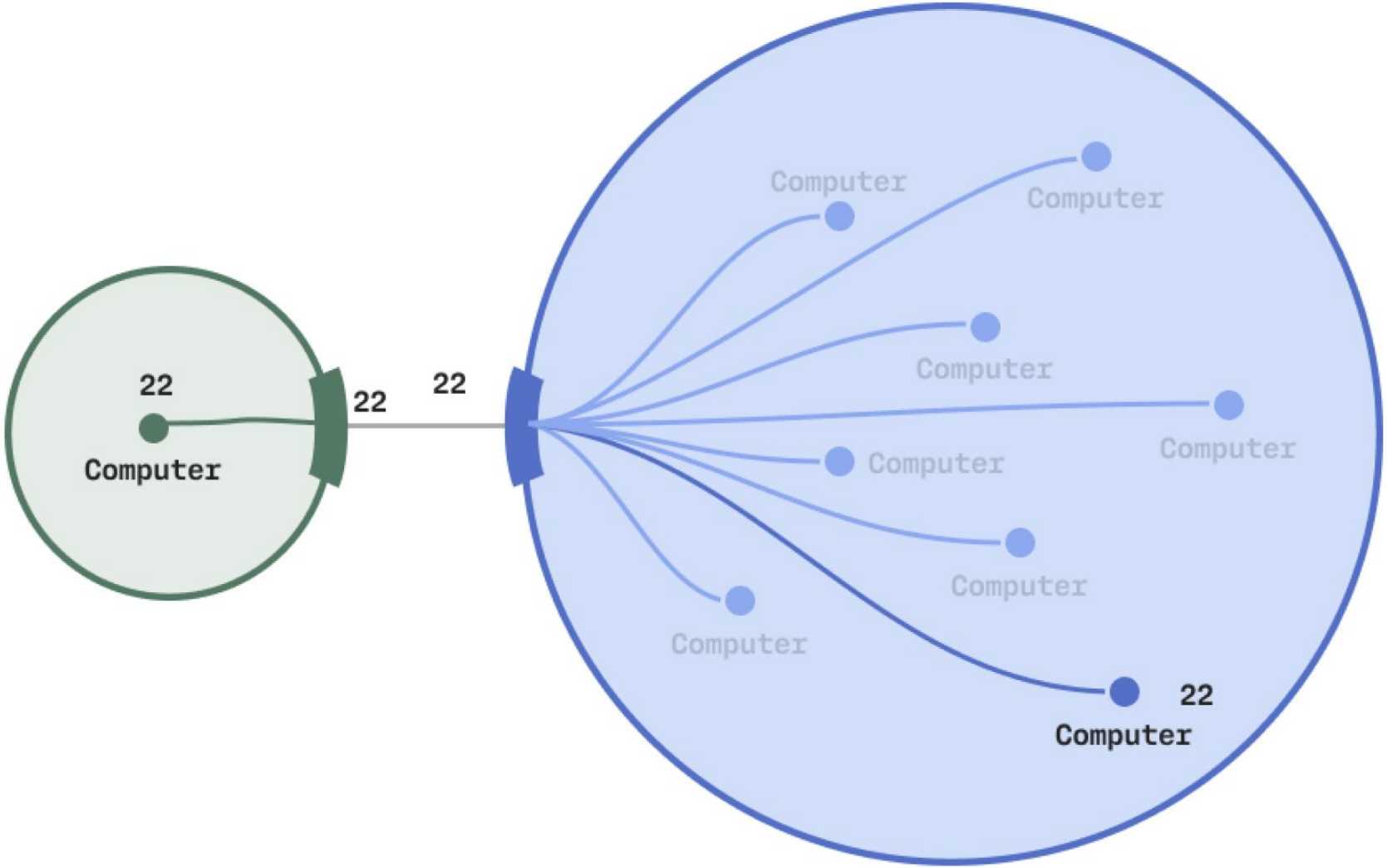



Computer
Computer
Computer
Computer
Computer
Computer
Computer
Computer
Computer

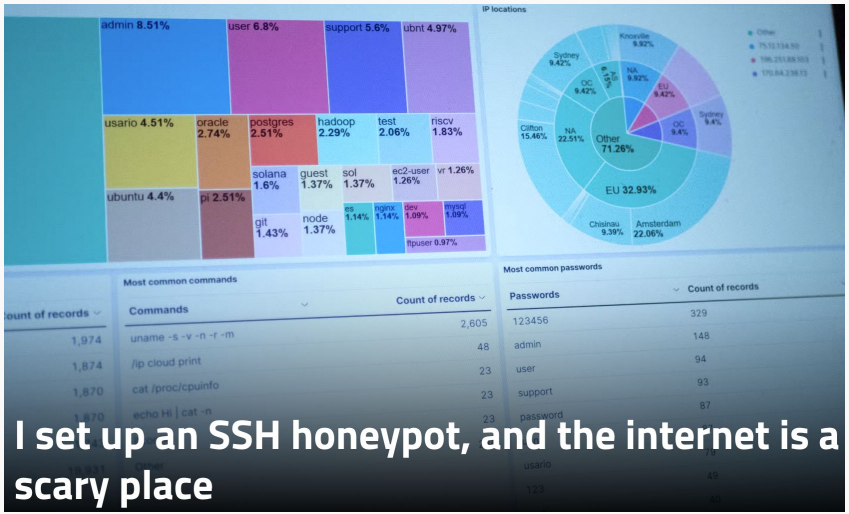
Network Address Translation (NAT)

Allows multiple devices on a private network to share a single public IP when accessing the internet.



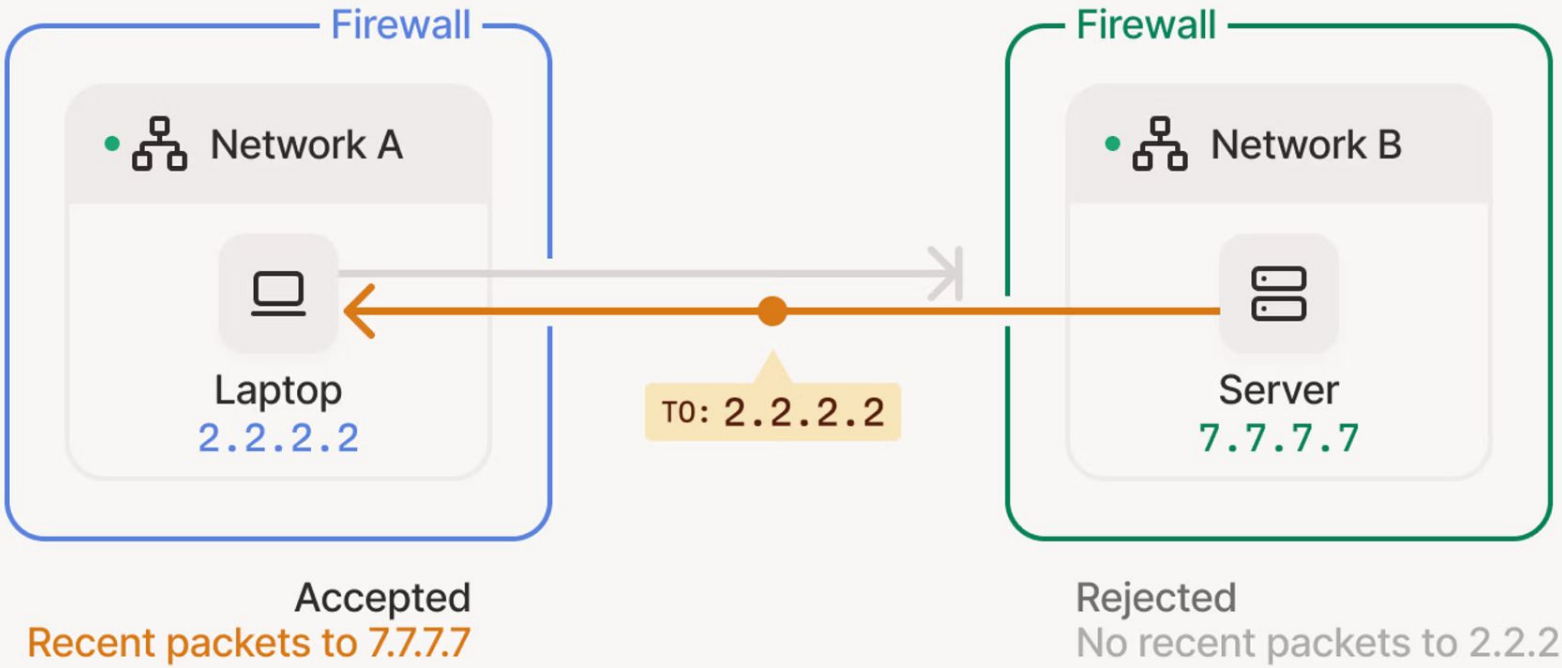

22
22
Computer
22
Computer
Computer
Computer
Computer
Computer
Computer
Computer
22
Computer

Why don’t we just forward ports?



- 29,282 unique interactions
- 447 unique IP addresses
- NoaBot, IRC worms, Telegram grabs

NATs, firewalls: Now what?



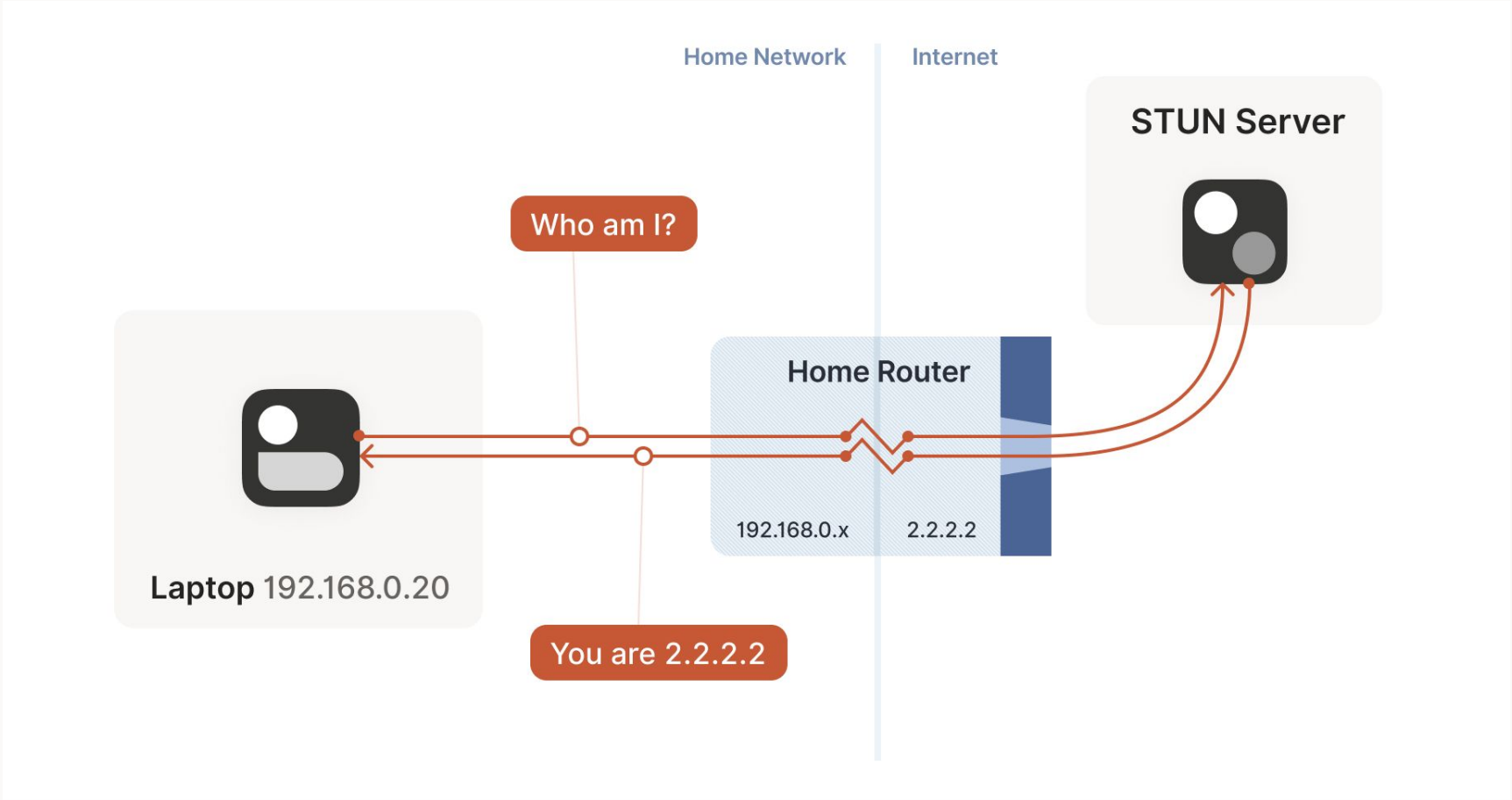
/me reaches into bag of tricks

STUN

What actual address did these packets come from?

```
192.168.1.50:12345
 >>>
203.0.113.7:45123
```

“Here’s the address your packets actually came from”



UDP hole-punching

Let’s show these firewalls we’re good friends

Coordination server has both sides send packets at the same time

Each firewall sees:

`203.0.113.7:45123` → `192.168.1.42:41641`
`192.168.1.42:41641` → `203.0.113.7:45123`

Let the packets flow!

Nothing says the packets must be related to each other!

Symmetric (“Hard”) NAT

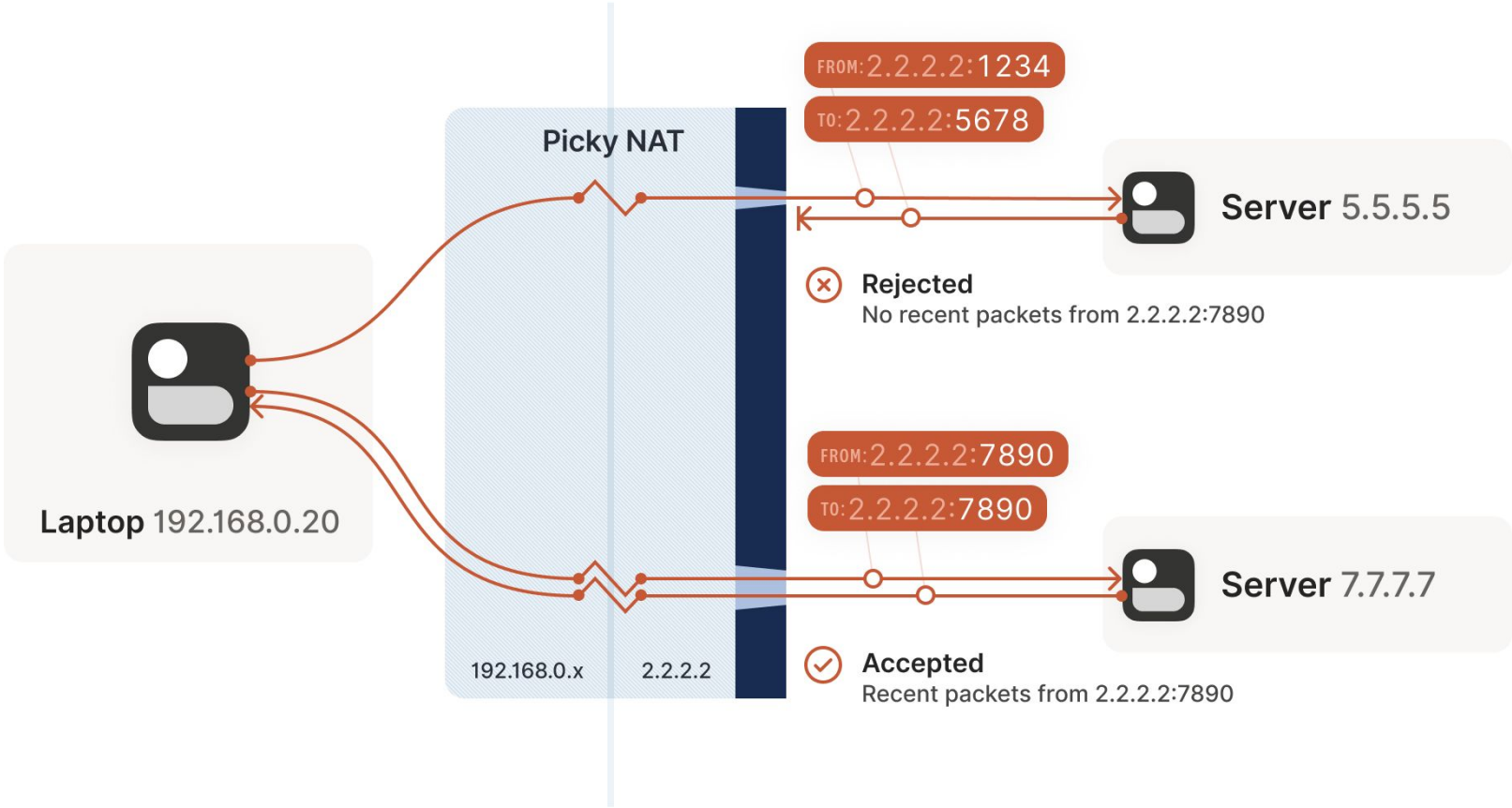
Randomize the port for every outgoing connection

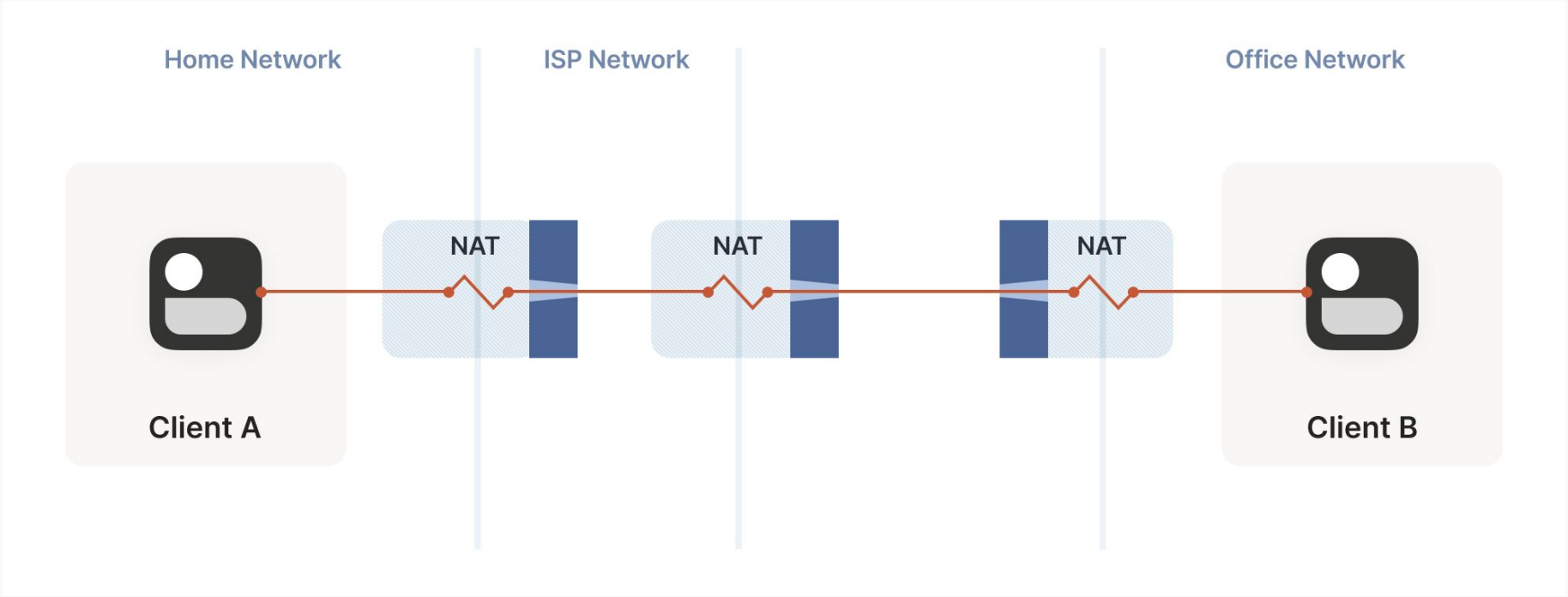
192.68.1.42 wants to go to 7.7.7.7:

“You are 2.2.2.2:1234”

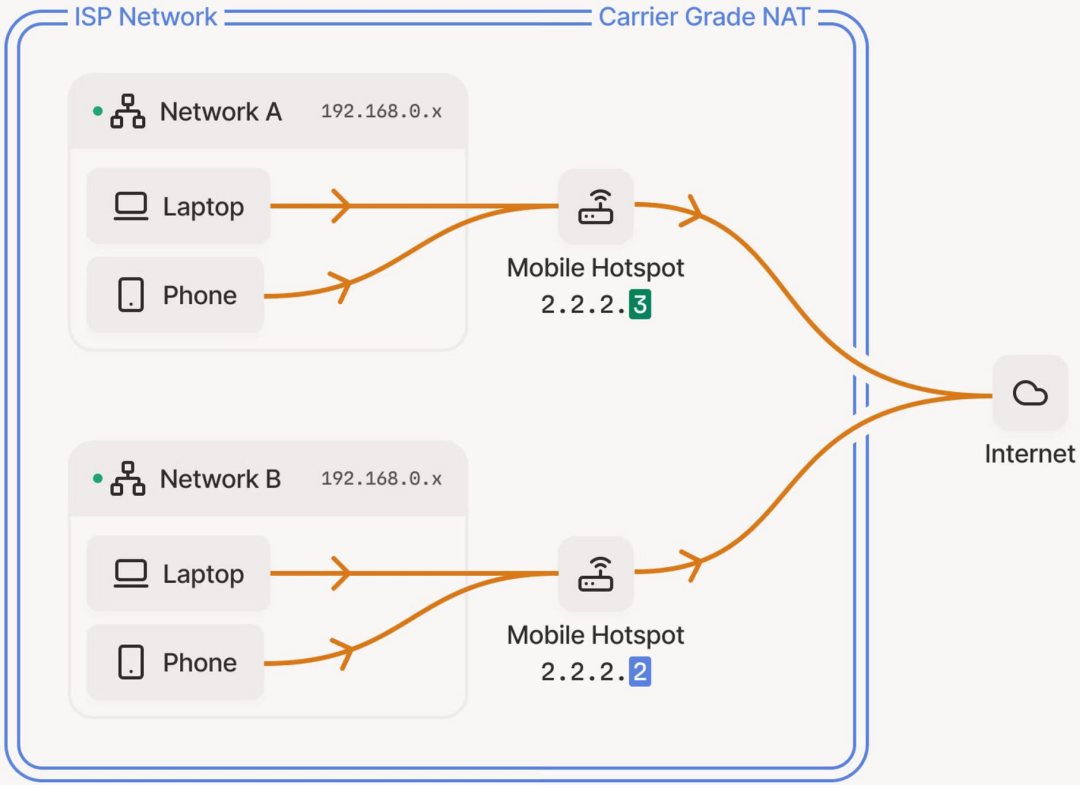
192.168.1.42 wants to go to 8.8.8.8:

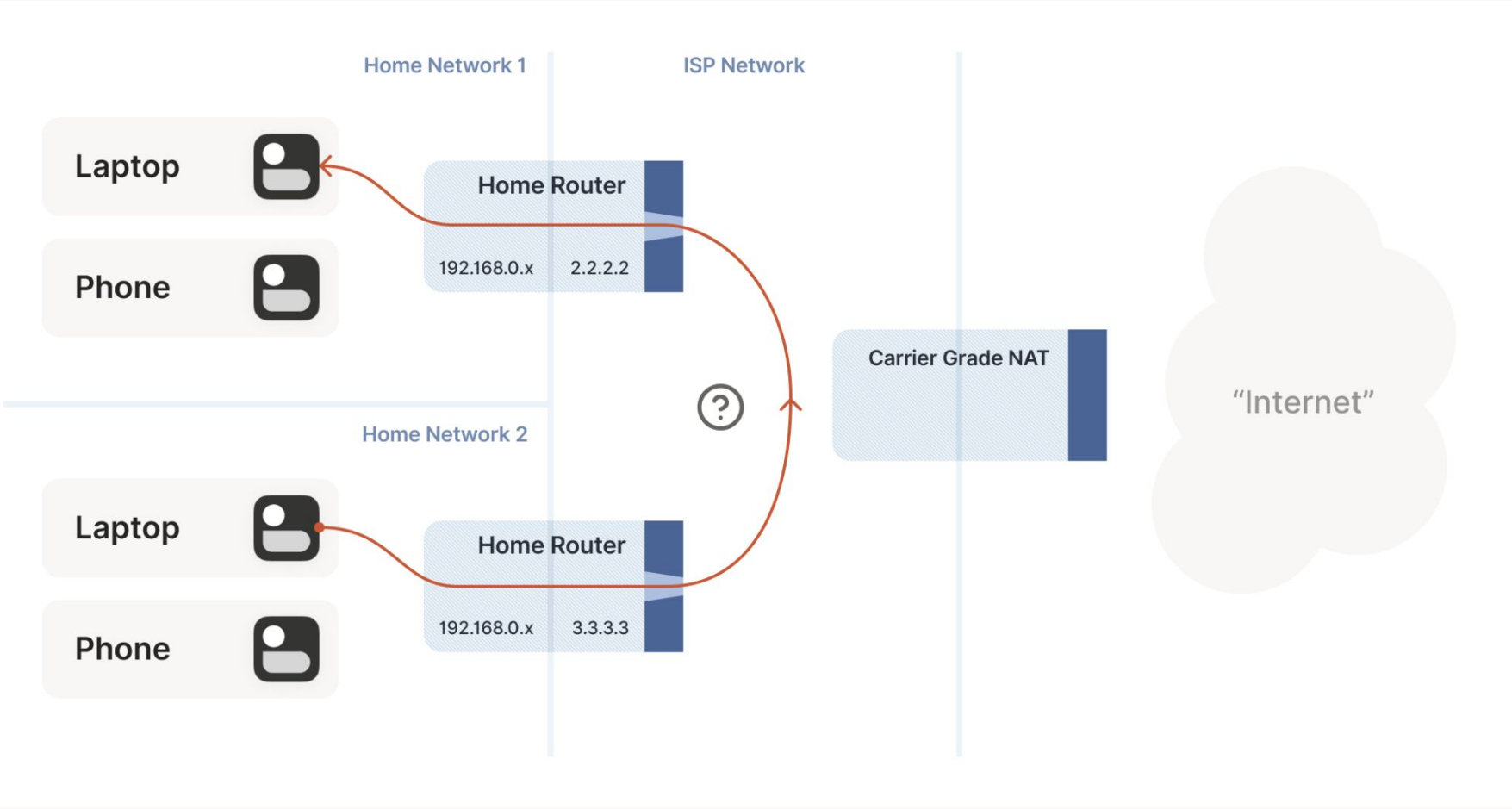
“You are 2.2.2.2:6789”





Carrier-





Deeper in the bag of tricks

The “Birthday Paradox”

Number of random probes	Chance of success
174	50%
256	64%
1024	98%
2048	99.9%

The “Halo and Zoom” Set

- UPnP
  - A whole bunch of late 90’s tech to temporarily forward ports
- NAT-PMP (v2) / PCP
  - A sane, reduced NAT traversal tool

Side channels

- “Let’s talk in private about our ports”

ICE: Let’s try everything! (responsibly)

- IPv6
- IPv4 LAN ports (local)
- IPv4 WAN (STUN)
- IPv4 WAN mapped by protocol
- Static port-forwards

Open a side channel, check both sides’ options, send some UDP, and see what works best

And then there were Relays

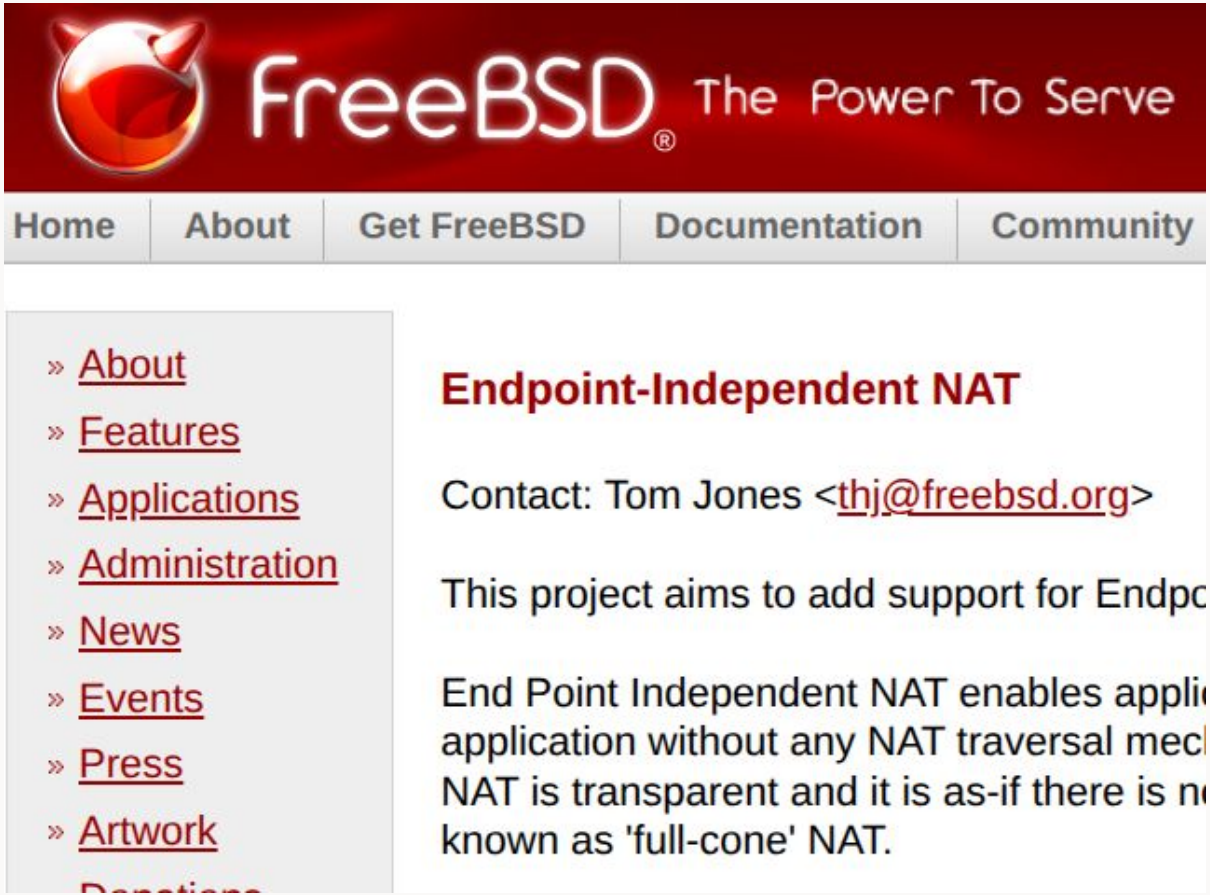
Like humans, some networks aren’t complicated, they’re just jerks

- Enterprise firewalls
- Symmetric NAT
- Carrier-grade NAT
- Carrier-grade NAT that explicitly disallows “hairpinning”
- Hotel/conference Wi-Fi
- Blocking UDP entirely
- Cloud gateways (AWS, Azure, the mean GCS)

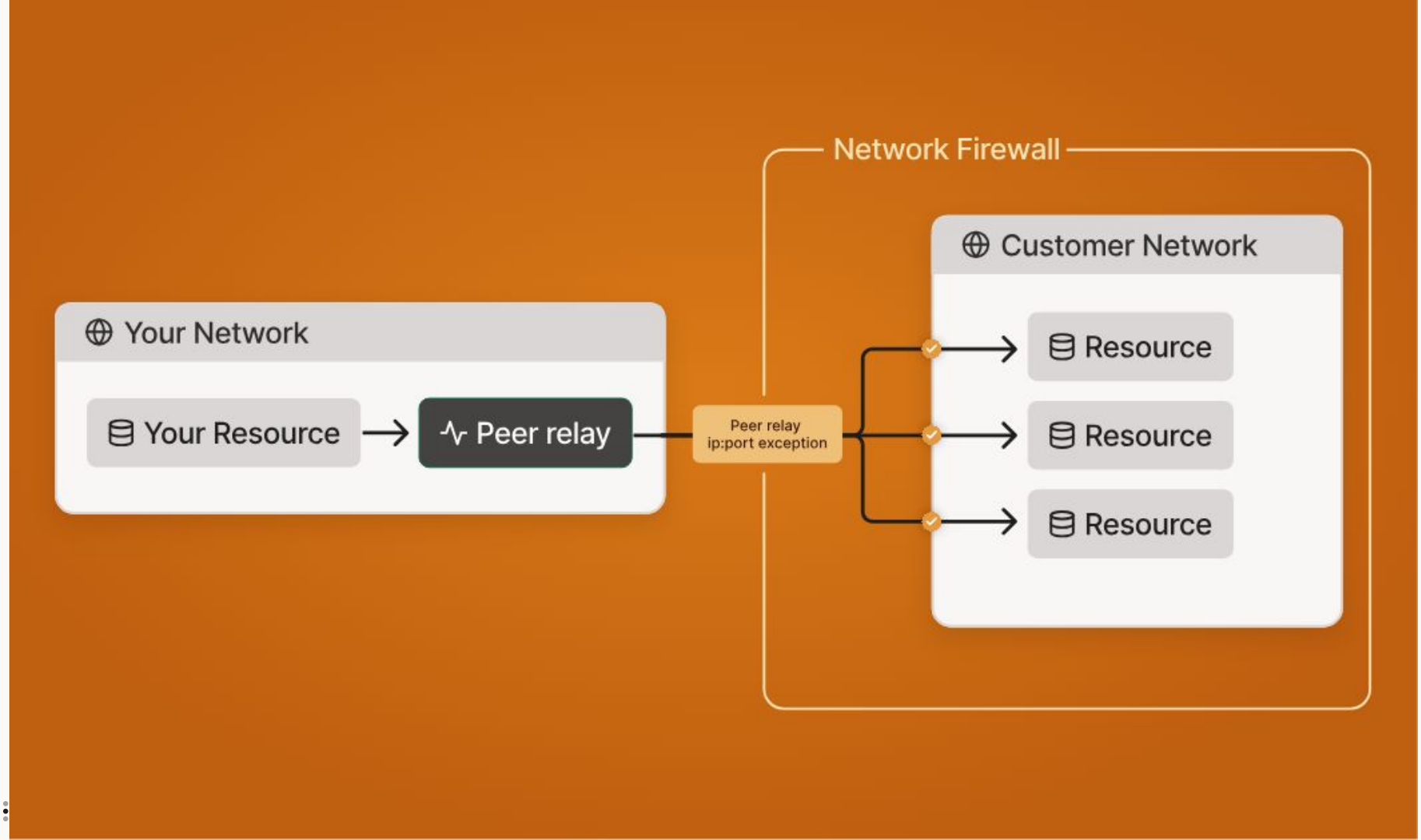
NAT traversal is basically optimistic packet spam combined with careful observation of which packets make it through.

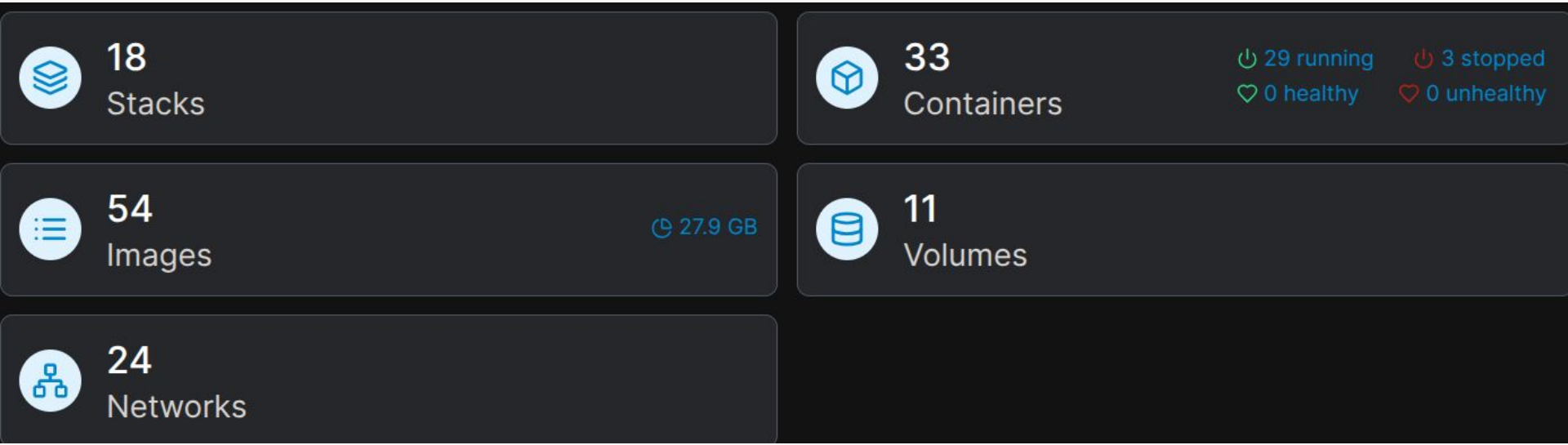
(I call it “Genially FA and Responsibly FO”)

Other “tricks”



Have a pandemic!


Network Firewall
Customer Network
Your Network
Your Resource
Peer relay
Peer relay
ip:port exception
Resource
Resource
Resource



Alright, your turn

tailscale