Dynamisches WireGuard

Warum haben VPNs ihren eigenen Client?

WireGuard

- Integriert im Linux-Kernel
- Kryptografisch sicher
- Nur IP-Pakete über UDP
- Öffentliche Schlüssel

IPsec

- Vertrauenswürdige Quelle
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange

IPsec Aufbau

Internet Key Exchange

- Verhandlung
- Diffie-Hellman Key Exchange
- Authentifizierung

IPsec Tunnel

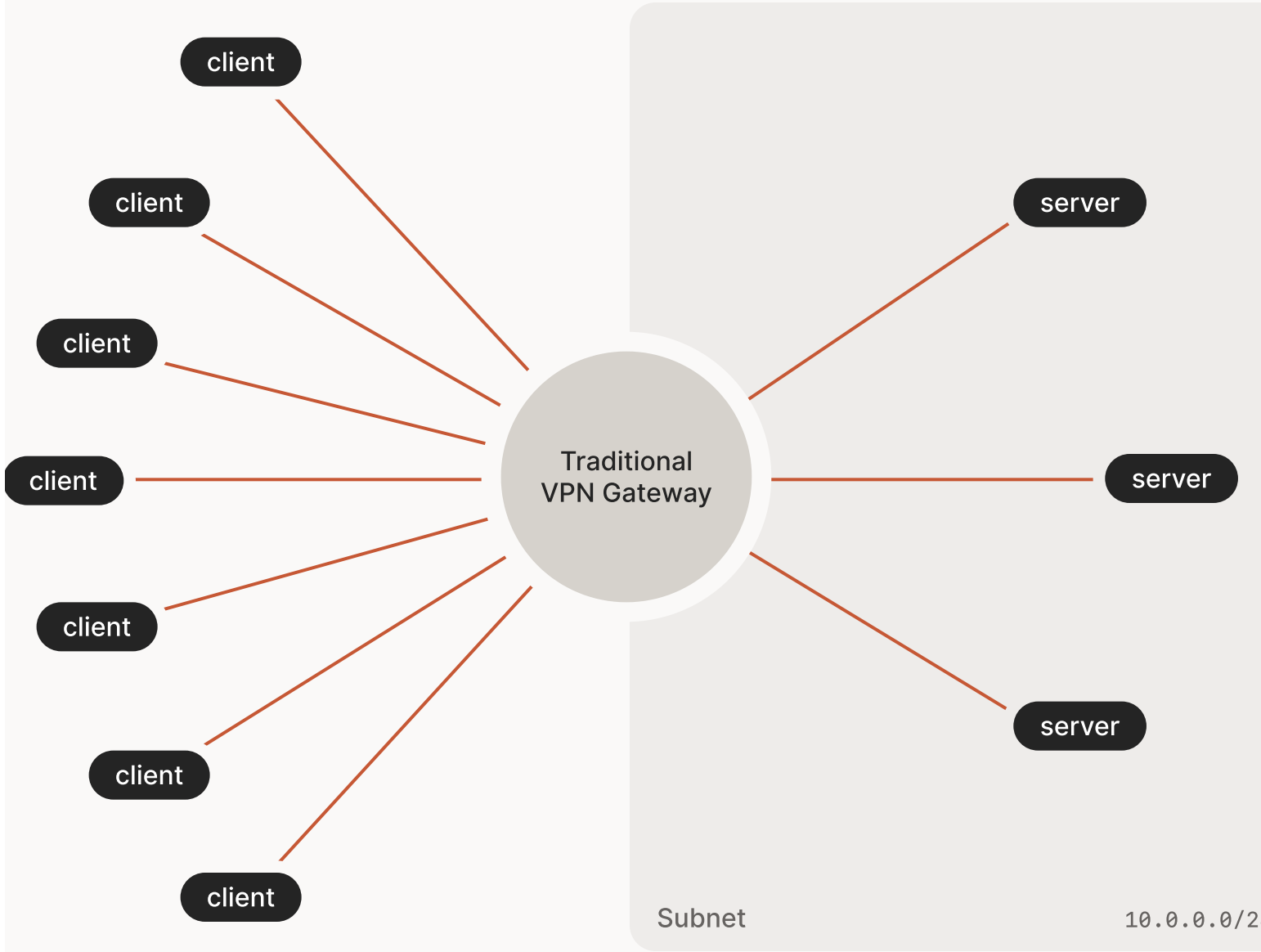
- Quick Mode
- IPsec Security Association

IPsec übertragung

- Daten verschlüsselung
- AH oder ESP
- IP Header
- Abschicken

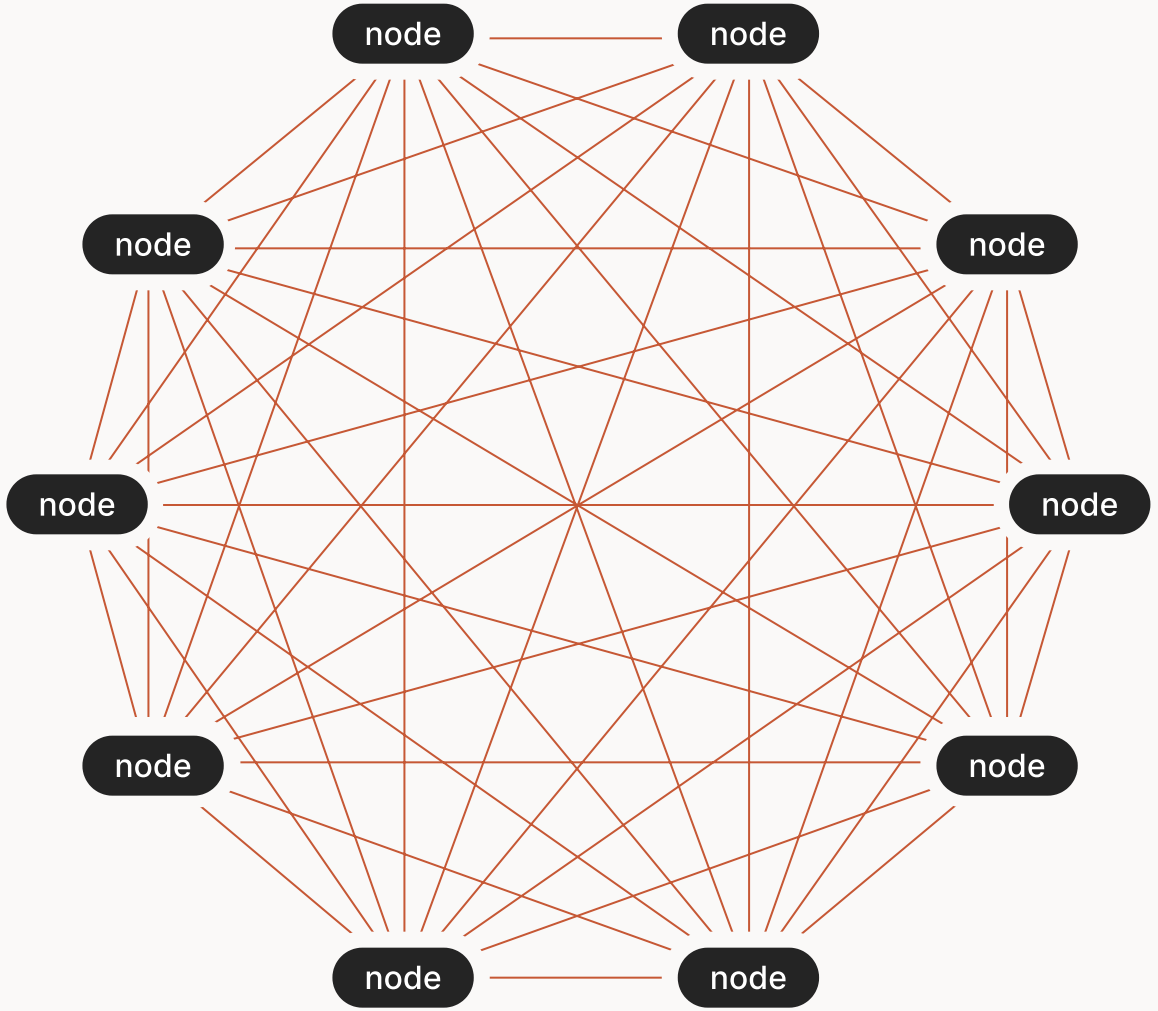
Netzwerk Architektur

- Hub-and-spoke



Netwerk Architektur

- Mesh
- Coordination Server



`n(n-1) = 90 WireGuard endpoints (for 45 connections)`

Authentifizierung

- LDAP
- RADIUS
- OpenID
  ↓
- Öffentliche Schlüssel akzeptieren

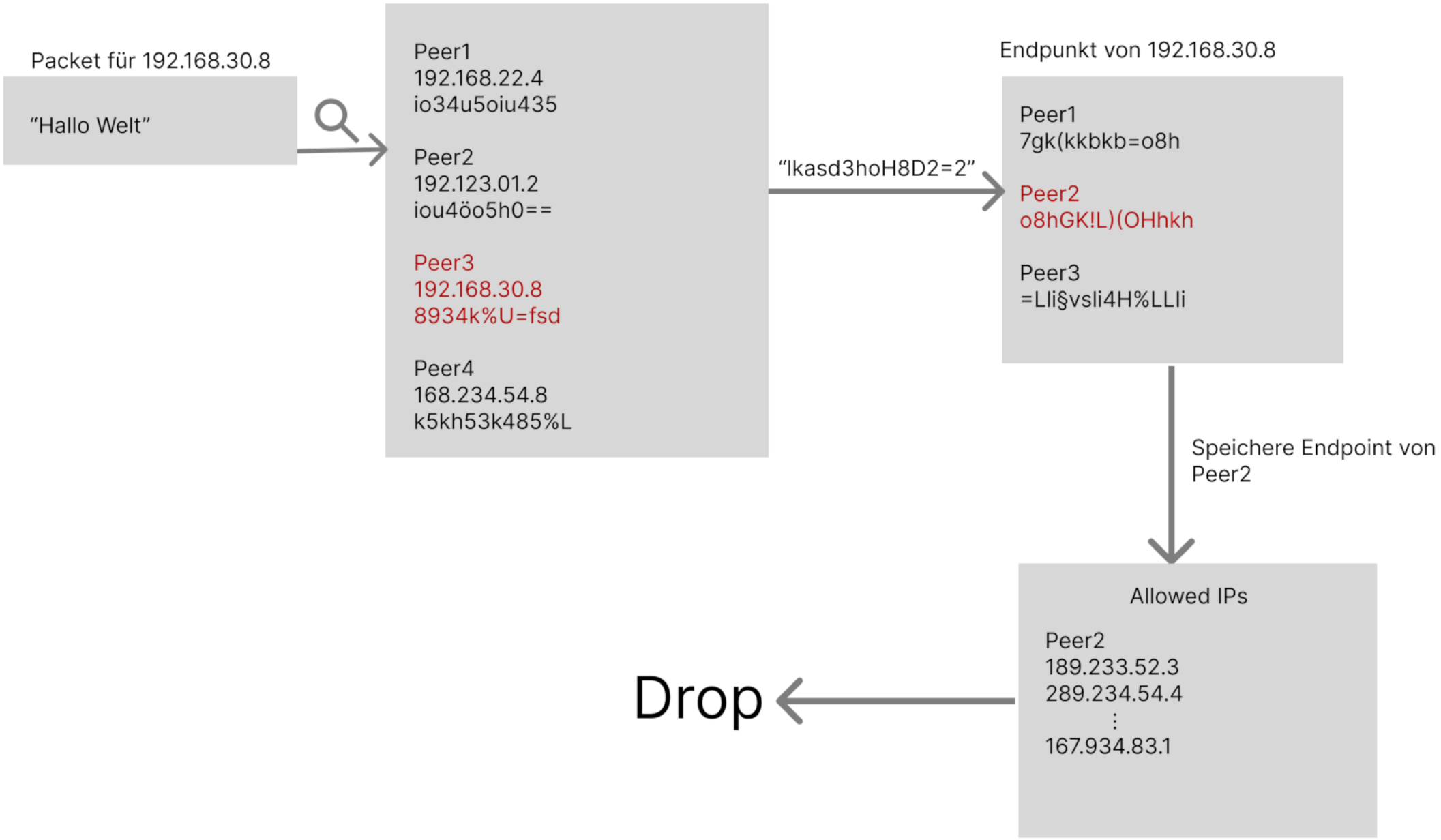
Manuelle Konfiguration eines WireGuard-Tunnels (Server)

```
[Interface]
**Address = 10.192.122.1/24**
**Address = 10.10.0.1/16**
**SaveConfig = true**
PrivateKey = yAnz5TF+lXXJte14tji3zlMNq+hd2rYUIgJBgB3fBmk=
istenPort = 51820

[Peer]
PublicKey = xTIBA5rboUvnH4htodjb6e697QjLERt1NAB4mZqp8Dg=
AllowedIPs = 10.192.122.3/32, 10.192.124.1/24
```

Manuelle Konfiguration eines WireGuard-Tunnels (Client)

```
[Interface]
**Address = 10.200.100.8/24**
**DNS = 10.200.100.1**
PrivateKey = oK56DE9Ue9zK76rAc8pBl6opph+1v36lm7cXXsQKrQM=

[Peer]
PublicKey = GtL7fZc/bLnqZldpVofMCD6hDjrK28SsdLxevJ+qtKU=
PresharedKey = /UwcSPg38hW/D9Y3tcS1FOV0K1wuURMbS0sesJEP5ak=
AllowedIPs = 0.0.0.0/0
Endpoint = vpn.hu-berlin.de:51820
```

Ablauf WireGuard & Cryptokey Routing


Packet für 192.168.30.8
“Hallo Welt”
Peer1
192.168.22.4
io34u5oiu435
Peer2
192.123.01.2
iou4öo5h0==
Peer3
192.168.30.8
8934k%U=fsd
Peer4
168.234.54.8
k5kh53k485%L
“lkasd3hoH8D2=2”
Endpunkt von 192.168.30.8
Peer1
7gk(kkbkb=o8h
Peer2
o8hGK!L)(OHhkh
Peer3
=Lli§vsli4H%LLli
Speichere Endpoint von Peer2
Allowed IPs
Peer2
189.233.52.3
289.234.54.4
⋮
167.934.83.1
Drop

Perfect Forward Secrecy (PFS)

- Schlüssel (Curve25519)
- Client
  - Eigener Private Key
  - Öffentliche Schlüssel
  - Ephemeral Key
- Shared Secrets

Handshake

- Key Derivation Function (HKDF)
- Symmetrischer Preshared Key (optional)
- 2 Minuten

Risiken?

- Privater Schlüssel Authentifizierung
- Altes Sicher (kein Ephemeral Key)
- DOS resistent
- PQC

Wie dynamisch ist WireGuard

- Full-Roaming (nach erstem Handshake)
- Wildcard Client
- Begrenzter lokaler statischer Adressraum

Dynamsche Möglichkeiten

- In-band
  - Layer 3
  - IPv6 link-local
  - leased IPs added to Adresses
- Overlay-Netz
  - Client
  - erzeugt .conf Dateien
  - wg set
  - IP Manager

Tailscale/ Headscale

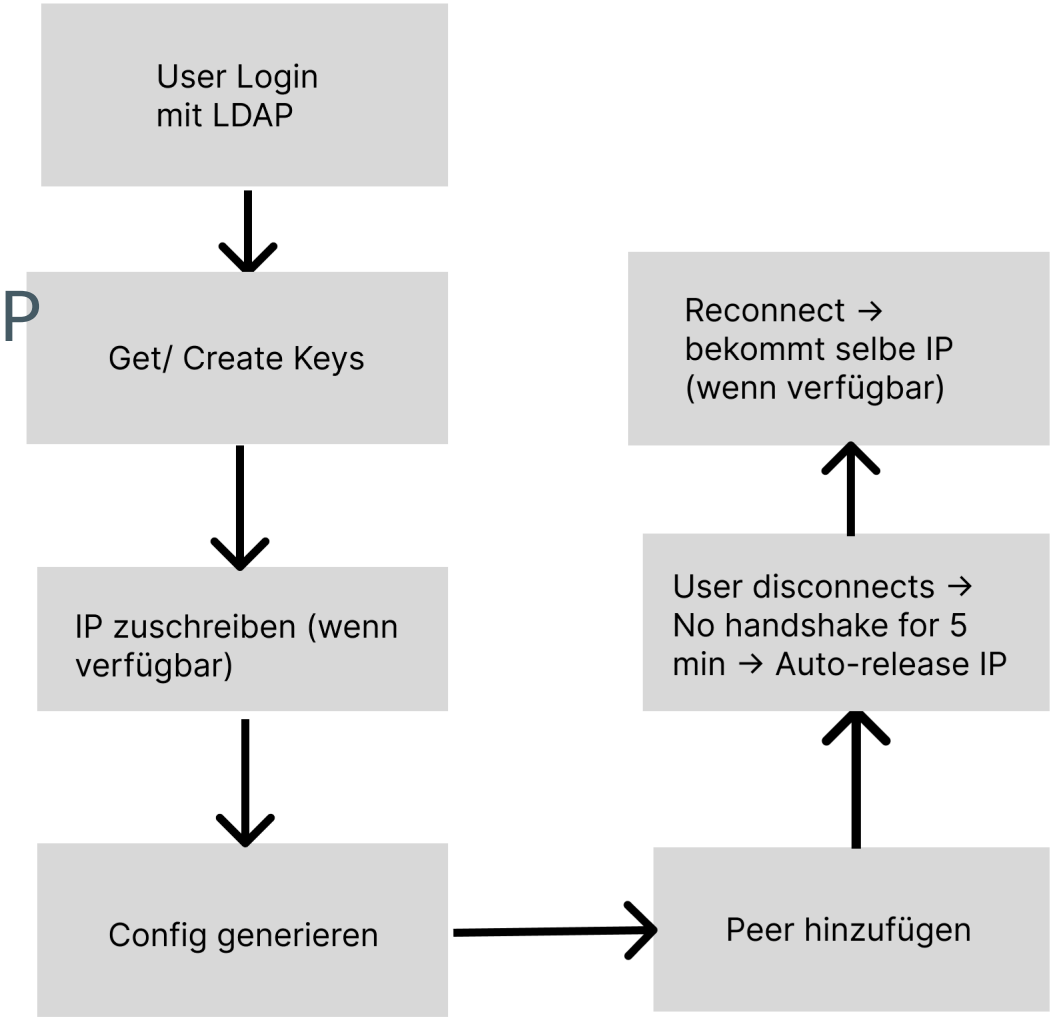
- OpenSource (fast)
- Mesh-Netzwerk
- 1000 statische Enpunkte oder 80 dynamische
- OpenID (Basic Registration)
- NAT traversal

NAT traversal

- Stateful Firewall
  - Für Ausgehend, Eingehend
  - Coordination Server
  - Senden ohne Antwort
- NAT devices
  - STUN

Unsere Demo

- Webauthentifizierung mit OpenLDAP
- IP-Pool Datenbank
- Cleanup Background-Worker



Danke fürs Zuhören