Headscale + Tailscale に移行中

Kazuhiro NISHIYAMA

LILO&東海道らぐオフラインミーティング

2026-02-01

経緯

- ほぼ使わなくなっていた OpenVPN のルート証明書の10年の期限が近付いた
  - 古くなって使わなくなった VPN 設定を全体的に見直すチャンス
- WireGuard に移行していたが、LAN 内でも動的 IP 同士だと VPN 経由になってしまう
  - Tailscale は自動で良い感じにしてくれる
  - 固定 IP 同士でもすべてのペアで個別設定追加が大変

Tailscale

- https://tailscale.com/
  - The best secure connectivity platform for devs, IT, and security
- WireGuard ベースでメッシュネットワーク
- 個人なら 3 users, 100 devices まで無料
  - tailscale.com のサーバーを使う場合

Headscale

- https://headscale.net/stable/
  - An open source, self-hosted implementation of the Tailscale control server
  - Design goal
    Headscale aims to implement a self-hosted, open source alternative to the Tailscale control server. Headscale's goal is to provide self-hosters and hobbyists with an open-source server they can use for their projects and labs. It implements a narrow scope, a single Tailscale network (tailnet), suitable for a personal use, or a small open-source organisation.

概念

- Control Server: Tailscale.com のサーバー or Headscale で自前
- Tailnet: キャリアグレード(CG)NAT用の `100.64.0.0/10` と `[fd7a:115c:a1e0::]/48` を使った VPN 網
- Tailscale ノード: Tailnet に接続する端末
- ユーザー: ノードが所属するユーザー
- タグ: ノードにつけられるタグ、ACL 設定に使っている

Headscale or Tailscale.com

- `100.64.0.0/10` と `[fd7a:115c:a1e0::]/48` の変更に未対応で共存できない
- 大規模なら Tailscale.com 一択
- 小規模でサーバーを用意できるなら Headscale も選択肢に
- 困ったら消しやすそうなので Tailscale.com ではなく Headscale を選択

Headscale 用サーバー準備

- 料金タイプ 512MB CPU 1Core, SSD 30GB
  - 時間課金 512MB 750円/月
  - 36ヶ月 325 円/月 → 296 円/月 60%オフ
    - キャンペーン期間 2026年2月17日(火) 16:00まで https://vps.conoha.jp/campaign/yearafteryear2025/
  - Ubuntu だと 1GB 以上になって高い
  - 512MB にするために Debian を選択
    - 12.05 (x86_64) まで (13 はない)
  - 申込料金 10,637 円/3年

Headscale インストール

- https://headscale.net/stable/setup/install/official/
- Official releases の Using packages for Debian/Ubuntu (recommended)
- v0.27.1 amd64 を deb でインストール

サーバー設定

- hs.example.jp (自分のドメインのサブドメインの hs に設定)
- Headscale が Let’s encrypt で HTTPS の証明書を自動設定

ユーザー作成

- 特にポリシーが決まっていなかった
  - 後でノードを別ユーザーに移動できるので、適当でも良い
  - 端末のグループごとに作成してみた
    - サーバーの場所: sakura, conoha, home
    - 手元の端末: kazu

ノード追加

- `headscale preauthkey create -u $user_id`
- tailscale インストール https://tailscale.com/download/linux
  - Debian 13 は未対応、Ubuntu は 25.04 まで対応
- `sudo tailscale up --login-server=https://hs.example.jp --authkey $preauthkey`
  - 必要に応じてオプション追加
    - `--advertise-routes=192.168.11.0/24`
    - `--advertise-tags tag:home,tag:zabbix-agent`

ノード追加の注意点

- preauthkey はノードごとに作成
- macOS や Windows は `https://hs.exmaple.jp` を指定して追加
  - ブラウザーが開くのでその指示に従って headscale で許可
- `--advertise-tags` は ACLs が影響
- `--advertise-routes` も headscale 側で許可が必要
  - `headscale nodes approve-routes --identifier $node_id --routes 192.168.11.0/24`

routes

- 家のラズパイ2台で同じ routes を設定
- 一度に1台だけ使われる
- 再起動などで Primary が自動で切り替わる

```
# headscale nodes list-routes
ID | Hostname   | Approved         | Available        | Serving (Primary)
9  | raspi4b2   | 192.168.11.0/24 | 192.168.11.0/24 |
10 | raspi4b3   | 192.168.11.0/24 | 192.168.11.0/24 | 192.168.11.0/24
```

exit node

- インターネットへの出口を変更
  - 出先で家の回線からインターネット接続など
- `tailscale set --advertise-exit-node`
  - `tailscale up` のときに指定し忘れても、後から `tailscale set` で設定可能
- `0.0.0.0/0` (と `::/0`) 宛の routes として headscale 側で許可が必要
  - `headscale nodes approve-routes --identifier $node_id --routes 0.0.0.0/0`

ACLs

- Tailscale の無料プランでは使えなさそう
- Tailscale では Grants の方が新しいが Headscale は未対応
- huJSON (コメントなどに対応した JSON) で記述

ACLs で困った点

- ACLs で許可すると ufw で許可しなくても通る
  - ノード間では通る
  - routes で LAN の他機器への通信は ufw も影響
- ACLs で許可していないノードは `tailscale status` で出てこない?
  - 見えない条件がいまいち把握できていない
  - 最近家のネット回線が不安定になることがあるのでその影響かも?

まとめ

- 個人用途なら Headscale で問題なさそう
  - 無料で ACL を使いたいなら Headscale
- Headscale でも使える機能か悩みたくないなら Tailscale.com
  - `tailscale ssh` などまだ試していない機能がある
  - `tailscale serve` などは使えないのでは? と思っている(未確認)