NetBird: La rete mesh privata che manda in pensione le vecchie VPN (ed è integrata con Authentik)

NetBird: La rete mesh privata che manda in pensione le vecchie VPN (ed è integrata con Authentik)

Diciamoci la verità: le VPN tradizionali (OpenVPN, IPsec o anche WireGuard in configurazione classica hub-and-spoke) fanno onco. Sono lente, centralizzate e creano un *single point of failure* gigantesco. Se il server VPN principale va giù, l'intera baracca aziendale smette di comunicare. E se il server è su, tutto il traffico deve transitare da lì prima di raggiungere la destinazione, creando un collo di bottiglia assurdo.

Poi è arrivata l'era delle **Mesh VPN** e in particolare di **NetBird**.

Oggi vediamo cos'è NetBird, perché è mille volte meglio di una VPN di vecchia concezione e come installarlo self-hosted sfruttando il nostro mastro di chiavi di fiducia: **Authentik** (di cui abbiamo già ampiamente configurato l'infrastruttura qui).

E la notizia migliore è che, seguendo la guida ufficiale aggiornata, l'installazione è diventata semplicissima. L'installatore automatico di NetBird si occupa di configurare tutto (dal reverse proxy Nginx al Docker Compose, compreso l'Identity Provider integrato di default), lasciandoci solo il compito di agganciare Authentik direttamente dal pannello web, senza toccare una riga di file `.env`.

Perché NetBird ci cambia la vita (senza pippe commerciali)

NetBird prende il protocollo di cifratura ultra-veloce di *WireGuard* e lo trasforma in una rete sovrapposta (*overlay mesh*) intelligente.

1. **Comunicazione diretta (Peer-to-Peer)**: Se la macchina A deve parlare con la macchina B, NetBird usa un server di controllo solo per farle incontrare. Una volta stabilita la rotta, il traffico

scorre direttamente tra A e B in modo cifrato. Il server non vede passare un solo byte del nostro traffico. Niente colli di bottiglia, latenza ridotta a zero.
2. **Superamento dei NAT (NAT Traversal)**: NetBird integra STUN e TURN. Significa che i nostri nodi si connettono direttamente anche se sono dietro doppi NAT, router blindati degli ISP o reti mobili 4G/5G. Zero porte da aprire sul firewall di casa.
3. **Access Control (Zero Trust)**: Invece di far accedere l'utente a tutta la rete (come con le VPN classiche), su NetBird possiamo definire policy granulari: "*Il gruppo di utenti Sviluppatori può accedere solo alla porta 22 del Server X*".
4. **Integrazione SSO con Authentik**: Non dobbiamo gestire password o chiavi per ogni client. Chi vuole accedere alla rete si autentica su Authentik (magari con MFA obbligatoria). Se revochi l'utente su Authentik, questo viene buttato fuori dalla rete mesh all'istante.

Passo 1: La preparazione su Authentik

Per prima cosa dobbiamo dire ad Authentik che NetBird è un suo applicativo fidato. Accedi all'interfaccia amministrativa di Authentik.

Crea il Provider

1. Vai su **Applicazioni** -> **Providers** e clicca su **Crea**.
2. Seleziona **Fornitore OAuth2/OpenID** e premi Next.
3. Compila i campi:
   - **Nome**: `NetBird`
   - **Flusso di autorizzazione**: `default-provider-authorization-explicit-consent` (Authorize Application)
   - **Tipologia client**: `Confidenziale`
   - **Redirect URI/Origini**: Lascialo vuoto per ora (lo aggiungeremo nel Passo 4).
   - **Chiave di firma**: Seleziona il certificato autofirmato di Authentik.
4. Clicchiamo su **Finish**.
5. Appuntiamoci il **Client ID** e il **Client Secret** che appaiono nella schermata.

Crea l'Applicazione

1. Andiamo su **Applicazioni** -> **Applicazioni** e clicchiamo su **Crea**.
2. Compiliamo i campi:
    - **Nome**: `NetBird`
    - **Slug**: `netbird`
    - **Provider**: Selezioniamo il provider `NetBird` creato al punto precedente.
3. Clicchiamo su **Crea**.

L'indirizzo dell'Issuer OIDC di Authentik sarà: `https://<IL_TUO_DOMINIO_AUTHENTIK>/application/o/netbird/`

Passo 2: L'installazione di NetBird Self-Hosted

NetBird mette a disposizione uno script di installazione automatica che configura l'intero ambiente Docker Compose, comprensivo di Nginx e certificati SSL. Non dobbiamo inventarci configurazioni strane.

Entriamo nel nostro server di destinazione via SSH ed eseguiamo:

```
# Scarica ed esegui lo script di configurazione automatica
curl -fsSL https://github.com/netbirdio/netbird/releases/latest/download/getting-started-with-self-hosted-netbird.sh | sh
```

Lo script farà tutto il lavoro pesante e avvierà i container Docker. Una volta completato il processo, avremo la dashboard di NetBird funzionante ed accessibile sul dominio che abbiamo configurato durante lo script. In questa fase verrà chiesto anche di creare il dominio da utilizzare e che tipo di reverse proxy si intende avere (fornirà quindi il file di configurazione).

Passo 3: Configurare il Provider OIDC in NetBird

Adesso colleghiamo Authentik direttamente dall'interfaccia web di NetBird, senza modificare i file di configurazione sul server.

1. Accediamo alla dashboard web del nostro NetBird self-hosted.
2. Andiamo su **Settings** -> **Identity Providers**.
3. Clicchiamo su **Add Identity Provider**.

4. Selezioniamo **Generic OIDC** e compiliamo i campi:
    - **Name**: `Authentik` (o il nome che si preferisce visualizzare sul pulsante di login)
    - **Client ID**: Incolliamo il Client ID copiato da Authentik.
    - **Client Secret**: Incolliamo il Client Secret copiato da Authentik.
    - **Issuer**: Inseriamo l'URL dell'issuer di Authentik (es. `https://auth.example.org/application/o/netbird/`).
5. NetBird ci mostrerà un URL di reindirizzamento (**Redirect URL**). **Copiamolo** prima di proseguire, senza fare clic su Add Provider.

Passo 4: Configurare il Redirect URI in Authentik

Torniamo su Authentik per blindare la sicurezza del flusso di autenticazione.

1. Andiamo sull'amministrazione di Authentik -> **Applicazioni** -> **Providers** e selezioniamo il provider di NetBird.
2. Clicchiamo su **Edit**.
3. Sotto la voce **Redirect URIs/Origins**, incolliamo il Redirect URL copiato dalla dashboard di NetBird.
4. **Opzione fondamentale per il Logout**: Aggiungiamo come secondo indirizzo (in una nuova riga) il callback di logout di NetBird: `https://<NETBIRD_DOMAIN>/oauth2/logout/callback` (sostituendo `<NETBIRD_DOMAIN>` con il dominio del nostro NetBird). Questo farà sì che quando ci disconnettiamo da NetBird, verremo reindirizzati indietro in modo pulito.
5. Assicuriamoci che l'opzione sia impostata su **Strict** (e non Regex) per far corrispondere esattamente gli indirizzi.
6. Salviamo cliccando su **Update**.

Passo 5: Completare il setup su NetBird e testare

1. Torniamo sulla scheda della dashboard di NetBird.
2. Facciamo clic su **Add Provider**.
3. Disconnettiamoci dalla dashboard di NetBird.
4. Nella pagina di accesso, vedremo ora il pulsante **Authentik** (o il nome che abbiamo scelto).
5. Clicchiamo sul pulsante ed effettuiamo il login tramite Authentik: verremo reindirizzati indietro ed autenticati all'istante.

Passo 6: Sincronizzazione dei Gruppi Utente (JWT claims)

Se vogliamo che i gruppi configurati su Authentik si riflettano su NetBird per creare regole di rete automatiche, procediamo così:

In Authentik:

1. Andiamo su **Applicazioni** -> **Providers** ed editiamo il provider di NetBird.
2. Sotto **Advanced protocol settings**, spuntiamo la casella **Include claims in id_token**.
3. Assicuriamoci che gli scope `profile` e `groups` siano attivi per quel provider (in Authentik, lo scope `profile` include di default le informazioni sui gruppi).
4. Clicchiamo su **Update**.

In NetBird:

1. Andiamo su **Settings** -> **Groups**.
2. Abilitiamo la voce **JWT group sync**.
3. Impostiamo il campo **JWT claim** su `groups`.
4. Salviamo le impostazioni.

Da questo momento in poi, NetBird leggerà l'appartenenza ai gruppi direttamente dal token OIDC firmato da Authentik e sincronizzerà le macchine degli utenti nei rispettivi gruppi di rete.

Benvenuti nel networking moderno, pulito e senza sbattimenti di file di configurazione.

Bonus track

Ci sono casi in cui richiedere l'apertura della porta 51820/udp in ingresso/uscita per permettere il traffico peer to peer mesh può far drizzare le orecchie a qualche attempato sistemista che potrebbe intuire un tunnel.

Netbird ci permette di cambiare la porta per il p2p direttamente dal client:

```
netbird up --wireguard-port 443
```

almeno possiamo far credere che chiediamo l'apertura in/out per normale traffico HTTP/3.

[Che il talpone sia con voi]

[EOF]

Fluxer Icon

Canale di discussione e supporto

Canale di discussione e supporto. Per confrontarti su configurazioni o altro entra su fluxer.dreadful.work (https://fluxer.dreadful.work/invite/dreadful).