Historie und Gültigkeit

Gültiger Stand, offene Punkte und Verlauf der Entscheidungen.

- Gültiger Stand und Verlauf

Gültiger Stand und Verlauf

> Zielgruppe: Anwender und Betreuer · Stand: 06.11.2026

Hier steht, was für Traefik bei DEXPRO gerade gilt und wie es dazu kam. Traefik ist zum einen der Edge-Router für alles, was Menschen von außen oder aus dem Büro erreichen sollen, und zum anderen der interne Ingress im Nomad-Cluster.

Gültiger Stand

- **Konzept** (29.10.2026): Ein Edge besteht aus zwei Traefik-Knoten mit keepalived-VIPs. Gebaut wird er über das Modul `terraform-modules/proxmox/traefik-loadbalancer` (Linie `0.3`) und die Rolle `ansible/roles/traefik`. Es gibt die Entrypoints `https` (interne VIP), `https-node` (Node-Adresse, Dashboard und Metriken) sowie `public` und `public-http` (öffentliche VIP). Nur Router mit `entryPoints = ["public"]` sind öffentlich erreichbar.
- **Regel** (21.10.2026): Oberflächen für Menschen laufen über den Edge, interne Dienste und OpenBao nie. Siehe Edge-Grundsatz.
- **Regel** (20.10.2026): Routen für Dienste im Consul-Katalog entstehen über Tags am Service. Der Edge übernimmt nur Services mit `traefik.enable=true` und dem Tag seiner Stage. Siehe Router per Consul-Tags definieren.
- **Regel** (20.10.2026): Der Edge liest den Consul-Katalog mit einem eigenen Token der Policy `traefik-catalog`. Ein Default-Token gibt es nicht.
- **Entscheidung** (20.10.2026): Der Ingress-Traefik im Nomad-Cluster hat keine festen Ports 80/443. Der Edge erreicht ihn über Consul Connect (mTLS) als Dienst `edge-traefik-<stage>` (connectAware).
- **Konzept** (20.10.2026): TCP-Entrypoints des Edge (z. B. für Datenbanken) kommen aus Consul KV `traefik/<stage>/tcp/<entrypoint>`, die Router dazu aus Tags mit `HostSNI(*)`.
- **Regel** (29.10.2026): API und Dashboard lauschen nur lokal auf `127.0.0.1:8080`. Erreichbar ist das Dashboard nur über einen eigenen Router hinter `admin-allowlist@file` und optional einer Anmeldung per forwardAuth.
- **Regel** (20.10.2026): Backends mit HTTPS prüft Traefik mit einer eigenen CA über einen `serversTransport`. `insecureSkipVerify` ist verboten.
- **Fakt** (30.10.2026): Das Failover berücksichtigt die Zertifikate. Jeder Knoten prüft seine eigene Node-Adresse (nie die VIP), gibt die VIP vor jedem Restart ab und bekommt beim Neuaufbau die ACME-Daten vom Partnerknoten.

Verlauf

- **Fakt** (30.10.2026): Das Lab wurde abgerissen. Die Lab-Edges bleiben stehen.

- **Fakt** (21.10.2026): Lab-PoC: Der Weg Edge → Connect → `cpi-traefik` → Connect → Demo-Dienst ist nachgewiesen. Intentions: alles verboten, nur `edge-traefik-<stage>` → `cpi-traefik` und `cpi-traefik` → Demo-Dienst erlaubt.
- **Fakt** (21.10.2026): Lab-PoC: Der Edge nutzt connectAware. Er übernimmt nur Dienste mit dem Tag `dev`, weil das Lab (Stage `pre-development`) im DEV-Netz läuft.
- **Fakt** (20.10.2026): Abgelaufene Backend-Zertifikate fallen erst beim Neustart von Traefik auf. Vor jedem Neustart die Backend-Zertifikate prüfen.