Edge-Grundsatz

> Zielgruppe: Anwender und Betreuer · Stand: 06.11.2026

Der Edge ist das Eingangstor für Menschen. Oberflächen und Dashboards bekommen dort einen eigenen Hostnamen. Maschinen sprechen intern miteinander und nie über den Edge.

Regeln

- **Für Menschen über den Edge:** Web-Oberflächen (z. B. Traefik-Dashboard, Nomad-UI, Grafana, Graylog) bekommen einen Hostnamen unter der passenden Wildcard (Lab: `*.lab.bre1.dexpro.services`) und einen Router am Edge-Traefik.
- **Keine Umwege:** keine SSH-Tunnel, keine Port-Forwards, keine ungeschützten Admin-Ports.
- **Maschinen intern:** Dienste untereinander (z. B. Backup-Jobs zur Nomad-API, Consul zu Nomad) nutzen interne Namen wie `*.service.consul` und nie Edge-Hostnamen.
- **Nie über den Edge:** interne Jobs, APIs für Maschinen und OpenBao.

> Ein interner Dienst, der über den Edge erreichbar ist, ist von außen angreifbar. Im Zweifel bleibt ein Dienst intern.

Vorgehen: Oberfläche veröffentlichen

1. Hostnamen unter der Wildcard der Umgebung wählen.
2. Bei Diensten in Nomad oder Consul: Route über Tags im Consul-Katalog definieren. Der Edge übernimmt sie automatisch. Wie das geht, steht in Router per Consul-Tags definieren. Ob der Weg direkt oder über den internen Ingress läuft, erklärt Dienst veröffentlichen: Edge oder interner Ingress.
3. Prüfen, dass die Oberfläche eine Anmeldung hat. Der Edge ersetzt keine Authentifizierung.

Stolperfallen

- Admin-APIs von Traefik lauschen nur lokal (`127.0.0.1:8080`). Das Dashboard läuft über einen eigenen Router.
- Datenbank-Verbindungen über Edge-TCP-Entrypoints sind nur intern. Die Datenbank sieht dabei die IP des Edges, nicht die des Clients. Grants mit Host-Beschränkung müssen das berücksichtigen.

Weiterführend

- Dienst veröffentlichen: Edge oder interner Ingress
- Buch Traefik: Router per Consul-Tags definieren
- Firewall-Freigaben anfragen
- Buch OpenBao: Erreichbarkeit

Revision #2
Created 2026-11-06 19:01:55 UTC by Alexander Golembek
Updated 2026-11-06 20:28:25 UTC by Alexander Golembek