

04 – Technischer Anhang

- [04.1 – Inventarisierungsmatrix](#)
- [04.2 – Technische Leitplanken](#)
- [04.3 – Quellen und Versionshinweise](#)

04.1 –

Inventarisierungsmatrix

Inventarisierungsmatrix

Standort	Daten-CIDR	Voice VLAN	Voice CIDR	OPNsense LAN-IP	Routing-Peer-IP	OmniPCX-Komponente	Status
Mühlentannen	192.168.110.0/23	TBD	TBD	TBD	TBD	Zentrale	offen
Bahnhofstraße	TBD	TBD	TBD	TBD	TBD	TBD	offen
Gartenstraße	TBD	TBD	TBD	TBD	TBD	TBD	offen
Barsbüttel	192.168.104.0/24	TBD	TBD	TBD	TBD	Nebenteil	offen
Heppenheim	192.168.0.0/24	TBD	TBD	TBD	TBD	Nebenteil	offen

Zusätzlich je Standort aufnehmen

- WAN-Anbieter und Anschlussart
- öffentliche bzw. CGNAT-Situation
- vorhandene WireGuard-Endpunkte
- AllowedIPs
- statische Routen
- relevante OPNsense-Firewallregeln
- VLAN-Trunks und Gateway-Zuordnung
- DHCP-Scopes und DHCP-Optionen
- DNS- und NTP-Abhängigkeiten
- Bandbreite und typische WAN-Latenz
- Virtualisierungsplattform für Routing-Peers
- Ausfall-/Redundanzkonzept

04.2 – Technische Leitplanken

Technische Leitplanken

1. Für neue Site-to-Site-Konfigurationen wird das NetBird-`Networks`-Modell verwendet; Legacy-`Routes` werden nicht als Standard für den Neuaufbau vorgesehen.
2. Site-to-Site-Routing-Peers werden als Linux-Systeme ausgeführt. Die OPNsense bleibt Firewall/Router, ist aber nicht der bevorzugte NetBird-Routing-Peer.
3. Routing-Peers müssen IP-Forwarding und die notwendigen Firewall-/Netfilter-Funktionen bereitstellen.
4. Für Site-to-Site wird initial Masquerading verwendet.
5. Bei deaktiviertem Masquerading wären explizite Rückrouten zum NetBird-Overlay erforderlich; dies ist nur nach gesonderter Bewertung zulässig.
6. Hochverfügbare Routing-Peers sind in unterschiedlichen Fehlerdomänen zu platzieren.
7. Die Control-Plane und Relay-Dienste müssen von extern zuverlässig erreichbar sein.
8. Firewallfreigaben werden minimal gehalten und aus der finalen NetBird-Version/Deployment-Dokumentation abgeleitet.
9. Overlay-, Standort- und Voice-Netze dürfen sich nicht überschneiden.
10. Der endgültige NetBird-Adressbereich ist vor Produktivbetrieb festzulegen und gegen sämtliche vorhandenen sowie geplanten RFC1918-/CGNAT-Nutzungen zu prüfen.

04.3 – Quellen und Versionshinweise

Quellen und Versionshinweise

Technische Grundlage des Entwurfs ist die NetBird-Dokumentation mit Stand August 2026.

Relevante Themen:

- How Routing Peers Work
- Networks / Network Resources
- Site-to-Site
- Masquerade
- Access Control
- Self-hosted Deployment

Wichtiger Versionshinweis: NetBird entwickelt Routing und Access Control aktiv weiter. Vor der produktiven Umsetzung sind die Anforderungen dieses Pflichtenhefts gegen die konkret eingesetzte NetBird-Version zu validieren.

Dokumentationslinks:

- <https://docs.netbird.io/manage/networks/how-routing-peers-work>
- <https://docs.netbird.io/use-cases/remote-access/site-to-site>
- <https://docs.netbird.io/manage/networks/masquerade>
- <https://docs.netbird.io/manage/network-routes/access-control>