

02.4 – Routing- und Policy-Konzept

Routing- und Policy-Konzept

Grundsatz

NetBird wird nicht als flaches VPN aufgebaut. Zugriffe werden nach Funktion, Standort und Geräteklasse getrennt.

Vorgesehene Gruppen

- site-lathen-muehlentannen-router
- site-lathen-bahnhof-router
- site-lathen-garten-router
- site-barsbuettel-router
- site-heppenheim-router
- clients-homeoffice
- clients-roadwarrior
- resources-data
- resources-voice
- optional weitere fachliche Benutzer-/Gerätegruppen

Networks und Resources

Pro Standort soll mindestens ein logisch abgegrenztes Network angelegt werden. Daten-LAN und Voice-VLAN werden als getrennte Ressourcen geführt. Damit können Policies für Telefonie unabhängig von normalen Standortzugriffen gepflegt werden.

Policy-Grundsätze

1. Default-Deny als Zielzustand.
2. Site-to-Site nur für tatsächlich benötigte Netze.
3. Voice-Verkehr ausschließlich zwischen den benötigten Voice-Ressourcen und OmniPCX-Komponenten.
4. Roadwarrior erhalten keinen pauschalen Zugriff auf komplette Standortnetze.
5. HomeOffice-Zugriffe werden nach benötigten Diensten bzw. Ressourcengruppen freigegeben.
6. Administrative Netze und Managementoberflächen erhalten eigene restriktive Regeln.
7. Änderungen an Policies müssen dokumentiert und getestet werden.

Masquerading

Für die erste Site-to-Site-Implementierung wird Masquerading auf Linux-Routing-Peers verwendet. Dadurch sehen Zielsysteme grundsätzlich die LAN-Adresse des lokalen Routing-Peers als Quelle. Für Systeme, bei denen die tatsächliche Client-/Overlay-IP benötigt wird, ist eine gesonderte technische Entscheidung erforderlich.

Revision #1

Created 2026-08-26 14:05:52 UTC by Thomas Fried

Updated 2026-08-26 14:05:52 UTC by Thomas Fried