

NetBird für das Unternehmensnetz

Für die neue Cyberversicherung muss binnen 90 Tagen nach Abschluss der Versicherung der Netzzugang mit TOTP ausgestattet werden. Zur Umsetzung dient dieses Pflichtenheft.

- [01 – Ist-Dokumentation](#)
 - [01.1 – Ziel und Geltungsbereich](#)
 - [01.2 – Bestehende Netzarchitektur](#)
 - [01.3 – Schaubild Ist-Zustand](#)
 - [01.4 – Telefonie und Voice-VLANs](#)
- [02 – Pflichtenheft NetBird](#)
 - [02.1 – Zielarchitektur](#)
 - [02.2 – Schaubild Zielarchitektur](#)
 - [02.3 – Funktionale Anforderungen](#)
 - [02.4 – Routing- und Policy-Konzept](#)
 - [02.5 – Telefonie-Konzept](#)
 - [02.6 – Remote Access](#)
 - [02.7 – Migration und Abnahme](#)
 - [02.8 – Betriebs- und Dokumentationsanforderungen](#)
- [03 – Anhang Standortneubau](#)
 - [03.1 – Änderung nach Fertigstellung des neuen Hauptstandorts](#)
 - [03.2 – Abnahmecheckliste Neubau](#)
- [04 – Technischer Anhang](#)
 - [04.1 – Inventarisierungsmatrix](#)
 - [04.2 – Technische Leitplanken](#)

- [04.3 – Quellen und Versionshinweise](#)

01 – Ist-Dokumentation

01.1 – Ziel und Geltungsbereich

Ziel und Geltungsbereich

Diese Dokumentation beschreibt die derzeitige Standort- und Remote-Access-Vernetzung des Unternehmens als Ausgangsbasis für die Ablösung der bestehenden WireGuard-Einzelverbindungen durch eine zentral verwaltete, selbstgehostete NetBird-Infrastruktur.

Berücksichtigt werden:

- Lathen – Mühlentannen als heutiger Hauptstandort und zentraler Routerstandort
- Lathen – Bahnhofstraße
- Lathen – Gartenstraße
- Niederlassung Nord – Barsbüttel
- Niederlassung Süd – Heppenheim
- HomeOffice-Arbeitsplätze
- mobile Roadwarrior-Geräte, insbesondere Tablets
- Daten-LANs und Voice-VLANs
- die zentrale OmniPCX am Hauptstandort und deren abgesetzte Komponenten an den Niederlassungen

Die Dokumentation trennt bekannte Fakten von noch zu erhebenden Parametern. Nicht bekannte VLAN-IDs, Subnetze oder Portbereiche werden ausdrücklich als TBD geführt und nicht geschätzt.

01.2 – Bestehende Netzarchitektur

Bestehende Netzarchitektur

Grundprinzip

An allen festen Standorten befindet sich eine OPNsense-Firewall. Bis auf den Standort Bahnhofstraße, der per LeasedLine mit 1GB/s direkt an das Netz Mühlentannen angebunden ist, erfolgt die Standortkopplung derzeit über direkte WireGuard-Verbindungen zum Hauptrouter in Lathen-Mühlentannen. Damit bildet Mühlentannen logisch den Hub der Standortvernetzung.

HomeOffice-Arbeitsplätze und mobile Geräte werden über einen separaten WireGuard-Server im Unternehmensnetz angebunden.

Neben den normalen Datennetzen müssen die Telefonie-Netze berücksichtigt werden. Am Hauptstandort befindet sich eine OmniPCX. An den Niederlassungen existieren abgesetzte Komponenten, deren Kommunikation mit der zentralen Anlage über die Standortverbindungen gewährleistet sein muss. Zurzeit befindet sich die Telefonie noch auf separaten Switchen in einem separaten Netz mit eigener Internetanbindung und Vernetzung über das IPsec-Protokoll. Da die eingesetzten bintec-Router EOL sind, sollen sie in naher Zukunft per VLAN in die "normale" Infratraktur integriert werden. Dieser Schritt wird in einer separaten Planung berücksichtigt.

Bekannte Datennetze

Standort	Netz	Bemerkung
Lathen – Mühlentannen	192.168.110.0/23	Hauptstandort
Lathen – Bahnhofstraße	192.168.110.0/23	entfällt nach Standortneubau
Lathen – Gartenstraße	192.168.144.0/24	entfällt nach Standortneubau

Standort	Netz	Bemerkung
Barsbüttel	192.168.104.0/24	Niederlassung Nord
Heppenheim	192.168.0.0/24	Niederlassung Süd

Voice-Netze

Die Voice-VLANs und zugehörigen Subnetze sind vor der Migration vollständig zu inventarisieren. Für jedes Voice-Netz sind mindestens VLAN-ID, IPv4-Netz, Gateway, DHCP-Optionen, DNS/NTP-Abhängigkeiten, OmniPCX-Zielsysteme sowie benötigte Signalisierungs- und RTP-Verbindungen zu dokumentieren.

01.3 – Schaubild Ist-Zustand

Schaubild – Ist-Zustand

flowchart TB

```
MT["Lathen – Mühlentannen<br/>OPNsense / Hauptrouter<br/>LAN 192.168.110.0/23<br/>OmniPCX + Voice-VLAN"]
BF["Lathen – Bahnhofstraße<br/>OPNsense<br/>LAN TBD + Voice-VLAN TBD"]
GS["Lathen – Gartenstraße<br/>OPNsense<br/>LAN TBD + Voice-VLAN TBD"]
NO["Niederlassung Nord – Barsbüttel<br/>OPNsense<br/>LAN 192.168.104.0/24<br/>Voice-VLAN + OmniPCX-Nebenteil"]
SU["Niederlassung Süd – Heppenheim<br/>OPNsense<br/>LAN 192.168.0.0/24<br/>Voice-VLAN + OmniPCX-Nebenteil"]
WG["WireGuard-Server<br/>Remote Access"]
HO["HomeOffice"]
RW["Roadwarrior / Tablets"]

BF <-->|"WireGuard Site-to-Site"| MT
GS <-->|"WireGuard Site-to-Site"| MT
NO <-->|"WireGuard Site-to-Site"| MT
SU <-->|"WireGuard Site-to-Site"| MT
HO <-->|"WireGuard"| WG
RW <-->|"WireGuard"| WG
WG --- MT
```

Bewertung

Die bestehende Architektur ist technisch überschaubar, führt aber zu einer zunehmenden Zahl statischer Tunnel-, Routing- und Firewall-Konfigurationen. Änderungen an Standorten, Netzen oder Remote-Access-Zugriffen müssen an mehreren Stellen konsistent gepflegt werden. Eine zentrale Identitäts-, Gruppen- und Policy-Steuerung für Standort- und Clientzugriffe ist in diesem Modell nur eingeschränkt vorhanden.

01.4 – Telefonie und Voice-VLANs

Telefonie und Voice-VLANs

Die Telefonie ist ein migrationskritischer Bestandteil. Die NetBird-Umstellung darf nicht ausschließlich anhand der Daten-LANs geplant werden.

Zu erfassende Kommunikationsbeziehungen

1. OmniPCX-Zentrale in Lathen-Mühlentannen zu den abgesetzten Komponenten.
2. Abgesetzte Komponenten zurück zur OmniPCX-Zentrale.
3. IP-Telefone zu lokalen bzw. zentralen Telefonie-Komponenten.
4. Managementzugriffe auf Telefoniekomponenten.
5. Signalisierung, Medien-/RTP-Verkehr, Provisionierung, DNS, NTP und gegebenenfalls weitere Herstellerdienste.

Anforderungen

- Voice-VLANs müssen als eigenständige Netzressourcen behandelt werden.
- Zwischen Voice-Netzen darf nur der für die Telefonie erforderliche Verkehr freigegeben werden.
- NAT zwischen OmniPCX-Komponenten ist nach Möglichkeit zu vermeiden, sofern die konkrete NetBird-Architektur und die OmniPCX dies zulassen.
- MTU, Fragmentierung, UDP-Verhalten, Jitter, Paketverlust und Latenz sind explizit zu testen.
- Bestehende QoS-Markierungen sollen im lokalen Netz erhalten bleiben. Eine garantierte Ende-zu-Ende-QoS über öffentliche Internetzugänge kann NetBird nicht herstellen.

- Vor Produktivumschaltung ist ein realer Last- und Sprachtest zwischen allen Standorten durchzuführen.

02 – Pflichtenheft NetBird

02.1 – Zielarchitektur

Zielarchitektur NetBird

Ziel

Die bestehenden einzeln administrierten WireGuard-Verbindungen werden durch eine zentral verwaltete, selbstgehostete NetBird-Infrastruktur ersetzt. NetBird übernimmt Overlay-Vernetzung, Peer-Verwaltung, Gruppen, Policies und die kontrollierte Veröffentlichung der Standortnetze.

Für neue Site-to-Site-Konfigurationen ist das aktuelle NetBird-Modell **Networks / Network Resources / Routing Peers** zu verwenden. Die älteren `Routes` gelten für neue Site-to-Site-Implementierungen nicht als bevorzugtes Modell.

Architekturprinzip

Die OPNsense bleibt an jedem Standort Internet-Gateway, lokale Firewall, VLAN-Router und gegebenenfalls DHCP-/Routinginstanz. NetBird ersetzt nicht die Standortfirewall.

Pro Standort wird mindestens ein dedizierter Linux-Routing-Peer vorgesehen. Dieser besitzt Zugriff auf die lokalen Netze, die über NetBird veröffentlicht werden sollen. Für produktionskritische Standorte soll geprüft werden, zwei Routing-Peers auf unterschiedlichen Virtualisierungs-/Hardware-Fehlerdomänen einzusetzen.

Die NetBird-Control-Plane wird selbst gehostet und über einen öffentlichen DNS-Namen mit TLS erreichbar gemacht. Relay-Funktionalität ist insbesondere für Roadwarrior und HomeOffice vorzusehen, wenn keine direkte Peer-to-Peer-Verbindung möglich ist.

Wesentliche Designentscheidung

Für normales Site-to-Site-Routing wird zunächst Masquerading auf den Linux-Routing-Peers vorgesehen. Dies entspricht dem aktuellen NetBird-Site-to-Site-Modell und vermeidet zusätzliche

Rückrouten in allen Standortnetzen. Wo Quell-IP-Transparenz zwingend erforderlich ist, muss dies separat bewertet werden, da die Deaktivierung von Masquerading zusätzliche Rückrouten benötigt und Auswirkungen auf Hochverfügbarkeit hat.

02.2 – Schaubild

Zielarchitektur

Schaubild – Zielarchitektur

flowchart TB

CP["Self-hosted NetBird
Management / Signal / Relay
öffentlicher DNS + TLS"]

subgraph MT["Lathen – Mühlentannen"]

FWMT["OPNsense"]

RPMT["Linux NetBird Routing Peer"]

LANMT["Daten-LAN
192.168.110.0/23"]

VOMT["Voice-VLAN
TBD / OmniPCX"]

FWMT --- RPMT

RPMT --- LANMT

RPMT --- VOMT

end

subgraph BF["Bahnhofstraße – Übergangsphase"]

FWBF["OPNsense"]

RPBF["Linux NetBird Routing Peer"]

NETBF["LAN + Voice
TBD"]

FWBF --- RPBF --- NETBF

end

subgraph GS["Gartenstraße – Übergangsphase"]

FWGS["OPNsense"]

RPGS["Linux NetBird Routing Peer"]

NETGS["LAN + Voice
TBD"]

FWGS --- RPGS --- NETGS

end

```

subgraph NO["Barsbüttel"]
    FWN0["OPNsense"]
    RPN0["Linux NetBird Routing Peer"]
    NETN0["LAN 192.168.104.0/24<br/>+ Voice-VLAN"]
    FWN0 --- RPN0 --- NETN0
end

```

```

subgraph SU["Heppenheim"]
    FWSU["OPNsense"]
    RPSU["Linux NetBird Routing Peer"]
    NETSU["LAN 192.168.0.0/24<br/>+ Voice-VLAN"]
    FWSU --- RPSU --- NETSU
end

```

```

H0["HomeOffice-PCs<br/>NetBird Client"]
RW["Tablets / Roadwarrior<br/>NetBird Client"]

```

```

CP -. "Steuerung / Vermittlung" .- RPMT
CP -.-> RPBF
CP -.-> RPGS
CP -.-> RPN0
CP -.-> RPSU
CP -.-> H0
CP -.-> RW

```

```

RPMT <-->|"verschlüsseltes NetBird Overlay"| RPBF
RPMT <-->|"verschlüsseltes NetBird Overlay"| RPGS
RPMT <-->|"verschlüsseltes NetBird Overlay"| RPN0
RPMT <-->|"verschlüsseltes NetBird Overlay"| RPSU
H0 <-->|"NetBird Overlay"| RPMT
RW <-->|"NetBird Overlay"| RPMT

```

Die Control-Plane liegt nicht im Nutzdatenpfad einer erfolgreichen direkten Peer-Verbindung. Wo direkte Verbindungen nicht möglich sind, muss Relay-Verkehr berücksichtigt werden.

02.3 – Funktionale Anforderungen

Funktionale Anforderungen

Muss-Anforderungen

ID	Anforderung	Abnahmekriterium
F-001	NetBird muss vollständig selbst gehostet betrieben werden.	Management und erforderliche Vermittlungs-/Relay-Dienste laufen unter eigener administrativer Kontrolle.
F-002	Alle fünf derzeit relevanten Standorte müssen während der Übergangsphase gekoppelt werden können.	Gegenseitige Erreichbarkeit der freigegebenen Testressourcen.
F-003	Standort-LANs müssen ohne NetBird-Agent auf jedem Endgerät erreichbar sein.	Routing über lokale Linux-Routing-Peers funktioniert.
F-004	Voice-VLANs müssen standortübergreifend transportiert werden können.	Erfolgreiche OmniPCX- und Sprachtests.
F-005	Roadwarrior-Tablets müssen gezielt auf freigegebene Ressourcen zugreifen können.	Zugriff entsprechend Policy; nicht freigegebene Ressourcen bleiben gesperrt.
F-006	HomeOffice-Arbeitsplätze müssen über NetBird angebunden werden.	Client verbindet sich und erhält ausschließlich definierte Zugriffe.
F-007	Gruppenbasierte Zugriffspolitik muss möglich sein.	Testnutzer verschiedener Gruppen erhalten unterschiedliche Berechtigungen.
F-008	Standortnetze und Voice-Netze müssen logisch getrennt administrierbar sein.	Separate Network Resources/Resource Groups und Policies vorhanden.

ID	Anforderung	Abnahmekriterium
F-009	Der Ausfall eines Remote-Clients darf keine Standortverbindung beeinflussen.	Standort-Routing bleibt unabhängig von Client-Peers verfügbar.
F-010	Bestehendes WireGuard muss während der Migration parallel betreibbar bleiben.	Pilotbetrieb ohne sofortige Abschaltung der Alt-Tunnel.
F-011	Die Lösung muss den späteren Wegfall Bahnhofstraße und Gartenstraße ohne Neuaufbau der Gesamtarchitektur ermöglichen.	Standorte können durch Entfernen ihrer Ressourcen/Peers sauber stillgelegt werden.
F-012	Änderungen müssen nachvollziehbar dokumentiert werden.	Konfigurations- und Änderungsdocumentation vorhanden.

Soll-Anforderungen

- Zwei Routing-Peers für besonders kritische Standortnetze, soweit technisch und wirtschaftlich sinnvoll.
- Zentrale Anmeldung über den vorhandenen Unternehmens-Identity-Provider, sofern mit der gewählten Self-hosted-Konfiguration vorgesehen.
- Automatisierte Sicherung der NetBird-Konfiguration und der zugrunde liegenden persistenten Daten.
- Monitoring von Control-Plane, Relay und Routing-Peers.
- Benennungskonventionen für Peers, Gruppen, Networks und Resources.
- Zeitlich begrenzte Setup Keys für automatisierte bzw. unbeaufsichtigte Routing-Peer-Registrierung.

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.

02.5 – Telefonie-Konzept

Telefonie-Konzept

Ziel

Die bestehende OmniPCX-Topologie muss über NetBird mindestens dieselbe funktionale Konnektivität erhalten wie über die heutigen WireGuard-Tunnel.

Umsetzung

Jedes Voice-VLAN wird als eigene NetBird-Netzressource dokumentiert und veröffentlicht. Der lokale Linux-Routing-Peer muss das Voice-VLAN über die lokale Routing-Infrastruktur erreichen können. Die OPNsense bleibt für die lokale Segmentierung verantwortlich.

Vor Freigabe werden die tatsächlich benötigten Verbindungen anhand der OmniPCX-Konfiguration und Paketmitschnitten der bestehenden WireGuard-Verbindungen ermittelt. Es werden keine pauschalen `ANY-ANY`-Freigaben als Dauerlösung vorgesehen.

Abnahmetests Telefonie

- Registrierung bzw. Status aller abgesetzten OmniPCX-Komponenten
- interne Telefonate Standort ↔ Hauptstandort
- Telefonate zwischen Niederlassungen
- eingehende und ausgehende Gespräche entsprechend der bestehenden Telefoniearchitektur
- Rufaufbauzeit
- bidirektionales Audio
- Halten, Rückfrage und Vermitteln
- längere Gespräche
- mehrere parallele Gespräche
- Neustart einer Außenstelle

- Ausfall und Wiederherstellung des NetBird-Pfades
- Messung von Latenz, Jitter und Paketverlust
- Prüfung auf MTU-/Fragmentierungsprobleme

02.6 – Remote Access

HomeOffice und Roadwarrior

HomeOffice

Auf verwalteten HomeOffice-Arbeitsplätzen wird der NetBird-Client installiert. Die Geräte werden einer eigenen Gruppe zugeordnet. Der Zugriff erfolgt nicht über eine pauschale Standort-Vollroute, sondern über definierte Ressourcen und Policies.

Roadwarrior / Tablets

Tablets und andere mobile Geräte werden als eigene Geräteklasse behandelt. Aufgrund wechselnder Netze, Carrier-NAT und restriktiver WLANs ist die Relay-Funktion für diese Geräte betriebsrelevant.

Sicherheitsanforderungen

- eindeutige Gerätezuordnung
- Entzug eines Gerätes muss zentral möglich sein
- Gruppenmitgliedschaften nach dem Least-Privilege-Prinzip
- keine pauschale Erreichbarkeit der Voice-VLANs durch Roadwarrior
- administrative Zugriffe nur für explizit berechtigte Geräte/Benutzer
- Prüfung von Posture Checks für verwaltete Endgeräte, soweit für die eingesetzten Plattformen sinnvoll

02.7 – Migration und Abnahme

Migration und Abnahme

Phase 1 – Inventarisierung

Alle LANs, VLANs, Gateways, WireGuard-Tunnel, AllowedIPs, Firewallregeln und Telefonie-Kommunikationsbeziehungen werden aufgenommen. Fehlende TBD-Werte dieses Dokuments werden ersetzt.

Phase 2 – NetBird-Control-Plane

Self-hosted NetBird wird produktionsnah aufgebaut, mit öffentlichem DNS, TLS, Relay-Funktion, Backup und Monitoring.

Phase 3 – Pilot

Ein nicht kritischer Standort bzw. ein abgegrenztes Testnetz wird parallel zum bestehenden WireGuard angebunden. Datenverkehr und Policies werden validiert.

Phase 4 – Standortmigration

Die Standorte werden einzeln migriert. Der bestehende WireGuard-Tunnel bleibt je Standort zunächst als Rückfallweg vorhanden, darf aber nicht gleichzeitig konkurrierende aktive Routen erzeugen.

Phase 5 – Telefonie

Voice-Ressourcen werden zunächst parallel getestet. Die Altverbindung wird erst entfernt, wenn Signalisierung und Sprachpfade nachweislich stabil funktionieren.

Phase 6 – HomeOffice und Roadwarrior

Clients werden gruppenweise migriert. Bestehender WireGuard-Remote-Access bleibt bis zum erfolgreichen Abschluss als Rückfalloption erhalten.

Phase 7 – Abschaltung Altbestand

Direkte WireGuard-Tunnel und der bisherige Remote-Access-WireGuard-Server werden erst nach dokumentierter Abnahme und definierter Beobachtungsphase außer Betrieb genommen.

Abbruchkriterien

Die Migration eines Standortes wird zurückgerollt bei:

- instabiler OmniPCX-Kommunikation
- reproduzierbaren Audiofehlern
- nicht erklärbaren Routing-Loops
- unzulässigem Zugriff zwischen Sicherheitszonen
- erheblichem Paketverlust oder nicht akzeptabler zusätzlicher Latenz
- fehlender Rückfallmöglichkeit

02.8 – Betriebs- und Dokumentationsanforderungen

Betrieb und Dokumentation

Für alle Komponenten sind Soll-Konfiguration und Abweichungen vom Standard zu dokumentieren. Bei jeder Abweichung ist nicht nur die technische Änderung, sondern ausdrücklich auch der Grund für die Abweichung festzuhalten.

Zu dokumentieren sind mindestens:

- NetBird-Versionen
- Hostsysteme der Control-Plane
- öffentliche DNS-Namen und Zertifikatsverfahren
- verwendete Ports
- Relay-Konfiguration
- Backup- und Restore-Verfahren
- Routing-Peers inklusive Standort, IP und Fehlerdomäne
- Networks, Resources und Resource Groups
- Peer-/Benutzergruppen
- Policies
- Setup Keys und deren Verwendungszweck, jedoch keine geheimen Schlüsselwerte
- lokale OPNsense-Routen und Firewallregeln
- Voice-VLANs und OmniPCX-Kommunikationsmatrix
- Monitoring und Alarmierung
- Notfall-/Rollback-Verfahren
- Änderungsprotokoll

03 – Anhang Standortneubau

03.1 – Änderung nach Fertigstellung des neuen Hauptstandorts

Änderungsanhang – neuer Hauptstandort Lathen- Mühlentannen

Ausgangslage

Nach Fertigstellung des neuen Hauptstandorts in Lathen-Mühlentannen entfallen die Standorte Bahnhofstraße und Gartenstraße. Die NetBird-Architektur muss deshalb so aufgebaut werden, dass diese Änderung keine grundlegende Neuplanung des Overlays erfordert.

Zielbild

flowchart TB

CP["Self-hosted NetBird
Control Plane + Relay"]

MT["NEUER Hauptstandort
Lathen – Mühlentannen
OPNsense + NetBird Routing
Peers
Daten-LAN(s) + Voice-VLAN(s)
OmniPCX"]

N0["Barsbüttel
OPNsense + Routing Peer
192.168.104.0/24 + Voice"]

```
SU["Heppenheim<br/>OPNsense + Routing Peer<br/>192.168.0.0/24 + Voice"]
H0["HomeOffice"]
RW["Roadwarrior / Tablets"]

CP -. -> MT
CP -. -> N0
CP -. -> SU
CP -. -> H0
CP -. -> RW

MT <- ->|"NetBird Site-to-Site"| N0
MT <- ->|"NetBird Site-to-Site"| SU
H0 <- ->|"NetBird"| MT
RW <- ->|"NetBird"| MT
```

Erforderliche Änderungen

1. Neue LAN-/VLAN-Struktur des Hauptstandorts vollständig aufnehmen.
2. Neue Routing-Peers am Hauptstandort bereitstellen und testen.
3. Neue Daten- und Voice-Ressourcen in NetBird anlegen.
4. Policies auf die neuen Ressourcen umstellen.
5. OmniPCX-Kommunikation aus allen Niederlassungen zum neuen Netz testen.
6. DNS-, DHCP-, AD-, NTP- und sonstige Infrastrukturabhängigkeiten auf neue Adressen anpassen.
7. Bahnhofstraße und Gartenstraße erst nach vollständiger Dienstmigration aus NetBird entfernen.
8. Alte Routing-Peers deaktivieren und anschließend löschen.
9. Nicht mehr benötigte Network Resources und Policies entfernen.
10. Alte OPNsense-/WireGuard-Konfigurationen dokumentiert stilllegen.
11. Dokumentation und Netzpläne auf den neuen Sollzustand aktualisieren.

Wichtiger Grundsatz

IP-Netze des Neubaus dürfen nicht allein aus Bequemlichkeit aus der Altstruktur übernommen werden. Vor Festlegung ist zu prüfen, ob der Neubau für eine saubere Segmentierung genutzt werden soll. NetBird darf dabei nicht als Ersatz für VLAN-Trennung und lokale Firewallsegmentierung missverstanden werden.

03.2 – Abnahmecheckliste

Neubau

Abnahmecheckliste Neubau

- ☐ Daten-LANs und VLAN-IDs dokumentiert
- ☐ Voice-VLANs dokumentiert
- ☐ OPNsense-Routing und Firewallregeln dokumentiert
- ☐ mindestens ein produktiver Linux-NetBird-Routing-Peer vorhanden
- ☐ Hochverfügbarkeitskonzept entschieden
- ☐ alle NetBird Network Resources angelegt
- ☐ Gruppen und Policies geprüft
- ☐ Barsbüttel erreicht freigegebene Ressourcen
- ☐ Heppenheim erreicht freigegebene Ressourcen
- ☐ HomeOffice-Zugriffe funktionieren
- ☐ Roadwarrior-Zugriffe funktionieren
- ☐ OmniPCX-Nebenteile vollständig verbunden
- ☐ Sprachtests erfolgreich
- ☐ DNS/AD/NTP und interne Dienste geprüft
- ☐ Monitoring aktiv
- ☐ Backup und Restore der NetBird-Infrastruktur getestet
- ☐ Rollback-Verfahren dokumentiert
- ☐ Bahnhofstraße stillgelegt
- ☐ Gartenstraße stillgelegt
- ☐ veraltete Routen und Policies entfernt
- ☐ finale Netz- und Betriebsdokumentation aktualisiert

04 – Technischer Anhang

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>