

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](#)

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 berechnigte 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