

01 – Ist-Dokumentation

- [01.1 – Ziel und Geltungsbereich](#)
- [01.2 – Bestehende Netzarchitektur](#)
- [01.3 – Schaubild Ist-Zustand](#)
- [01.4 – Telefonie und Voice-VLANs](#)

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 Mühlintannen angebunden ist, erfolgt die Standortkopplung derzeit über direkte WireGuard-Verbindungen zum Hauptrouter in Lathen-Mühlintannen. Damit bildet Mühlintannen 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 – Mühlintannen	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
Barsbüttel	192.168.104.0/24	Niederlassung Nord

Standort	Netz	Bemerkung
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.