HOLGER REIBOLD

INKLUSIVE E-BOOK

AdminMission

Das NetBird-Handbuch

Zero-Trust-Netzwerke mit WireGuard aufbauen, betreiben und prüfsicher dokumentieren

40 interaktive Missionen
mit dem Online-Lernspiel AdminMission



BRAIN-MEDIA.DE

Holger Reibold

Das NetBird-Handbuch

Zero-Trust-Netzwerke mit WireGuard aufbauen, betreiben und prüfsicher dokumentieren

BRAIN-MEDIA.DE

27 Anhang D – Glossar

Access Control Policy: Zugriffsrichtlinie in NetBird, die eine Quellgruppe mit einer Zielgruppe oder Ressource verbindet und Protokoll, Ports und Richtung festlegt.

Activity Log: Aktivitätsprotokoll aller Verwaltungsvorgänge in NetBird.

AGPLv3: GNU Affero General Public License, Lizenz der Serverkomponenten von NetBird seit Version 0.53.

AllowedIPs: Parameter in WireGuard, der festlegt, welche Adressen einem Peer zugeordnet sind. Wirkt beim Senden als Routing, beim Empfangen als Filter.

App-Rolle: in einer App-Registrierung von Entra ID definierte Rolle, die im Token mit lesbarem Wert erscheint.

BeyondCorp: Zero-Trust-Modell von Google, beschrieben in einer Artikelreihe von 2014 bis 2018.

Carrier-Grade-NAT (CGNAT): Adressübersetzung durch den Provider, bei der sich viele Kunden eine öffentliche IPv4-Adresse teilen.

Community Edition: frei nutzbare, quelloffene Fassung von NetBird für den Eigenbetrieb.

Control Center: grafische Übersicht im Dashboard über Peers, Gruppen, Netze und Richtlinien, mit Entwurfsmodus.

Cryptokey Routing: Bindung von Adressen an öffentliche Schlüssel in WireGuard.

Custom Zone: von NetBird selbst verteilte DNS-Zone mit A-, AAAA- und CNAME-Einträgen.

Dashboard: Weboberfläche von NetBird, arbeitet über die REST-API.

Datenebene (Data Plane): der Weg der Nutzdaten, bei NetBird die WireGuard-Tunnel zwischen den Peers.

Debug-Bundle: Archiv mit Protokollen und Konfiguration eines Clients für die Fehlersuche.

Draft Mode: Entwurfsmodus des Control Centers für die Planung von Änderungen.

Exit Node: Routing Peer, über den der gesamte Internetverkehr eines Clients geleitet wird.

Hole Punching: Verfahren, bei dem zwei Peers gleichzeitig Pakete senden, um durch NAT-Router eine direkte Verbindung aufzubauen.

ICE (Interactive Connectivity Establishment): Standard für den Aufbau von Verbindungen durch NAT, RFC 8445.

Identity Provider (IdP): Dienst, der Benutzer authentifiziert und Tokens ausstellt, etwa Entra ID oder Keycloak.

JWT Group Sync: Übernahme von Gruppen aus dem Token des Identity Providers in NetBird.

Lazy Connection: Verbindung zwischen Peers, die erst bei Bedarf aufgebaut und nach Leerlauf abgebaut wird.

Management: Dienst der Steuerungsebene, der Peers registriert, Richtlinien auswertet und Netzwerkkarten verteilt.

Masquerading: Ersetzen der Absenderadresse durch die des Routing Peers.

Match-Domain: Domain, für die eine Nameserver-Gruppe zuständig ist.

Mesh-Overlay: virtuelles Netz, in dem sich Geräte direkt miteinander verbinden.

Mikrosegmentierung: Beschränkung von Zugriffen auf einzelne Geräte und Dienste statt auf ganze Netze.

NetBird-Only-Dienst: über den Reverse Proxy nur im Overlay angebotener Dienst mit der Identität als Zugangsnachweis.

Network: Zusammenfassung von Routing Peers und Ressourcen einer Umgebung in NetBird.

Netzwerkkarte (Network Map): vom Management je Peer berechnete Liste der erlaubten Gegenstellen mit Schlüsseln und Regeln.

OIDC (OpenID Connect): Standard für die Anmeldung über einen Identity Provider.

OSCAL: Open Security Controls Assessment Language des NIST für maschinenlesbare Controls und Nachweise.

Overlay: virtuelles Netz über einem bestehenden Netz, dem Underlay.

PCP (Port Control Protocol): Protokoll, mit dem ein Gerät beim Router eine Portzuordnung anfordert.

Peer: Gerät im Overlay.

Policy Decision Point, Policy Enforcement Point: Entscheidungs- und Durchsetzungspunkt im Zero-Trust-Modell des NIST.

Posture Check: Prüfung des Gerätezustands als Bedingung für eine Richtlinie.

Relay: Dienst, der verschlüsselte Pakete weiterleitet, wenn keine direkte Verbindung möglich ist.

Rosenpass: Protokoll für einen Post-Quanten-Schlüsselaustausch, dessen Ergebnis als Preshared Key in WireGuard einfließt.

Routing Peer: Peer, der Verkehr aus dem Overlay in ein lokales Netz weiterleitet.

Setup-Key: Geheimnis für die Registrierung von Geräten ohne Benutzeranmeldung.

Signal: Dienst, der den Austausch von Verbindungsinformationen zwischen Peers vermittelt.

Split DNS: Aufteilung der Namensauflösung nach Domains auf verschiedene Nameserver.

Steuerungsebene (Control Plane): Management, Signal und Relay.

STUN: Protokoll zur Ermittlung der eigenen öffentlichen Adresse, RFC 8489.

Traffic-Events: Verbindungsprotokolle der Clients.

ULA (Unique Local Address): privater IPv6-Adressbereich fd00::/8.

Underlay: das Netz, über das die verschlüsselten Pakete transportiert werden.

WireGuard: VPN-Protokoll, auf dem NetBird aufbaut.

Zero Trust: Sicherheitsmodell, in dem kein Zugriff allein aufgrund des Standorts im Netz gewährt wird.

28 Anhang E – Versionsübersicht der wichtigsten Funktionen

Version	Zeitpunkt	Neuerung
Umbenennung	44621	Wiretrustee wird NetBird
0.25.4	2023	Rosenpass eingebettet
0.26	2024	Posture Check für das Betriebssystem
0.27	2024	Exit Nodes
0.29	2024	eigener Relay-Dienst statt Coturn
0.39	2025	Traffic-Events auf Clientseite
0.48	2025	Portbereiche in Richtlinien
0.53.0	45870	Serverkomponenten unter AGPLv3
0.55	2025	Auto Apply für Exit Nodes
Dashboard	45931	Control Center
0.60	Ende 2025	identitätsbasiertes NetBird SSH
0.61	46023	SSH mit Zuordnung lokaler Konten, automatische Client-Updates (Beta)
0.62	Anfang 2026	eingebauter Identity Provider mit lokalen Benutzern
0.63	Anfang 2026	Custom Zones
0.65	46054	Reverse Proxy, zusammengefasster Server-Container, Traefik als Standard
0.69	46113	PCP, CrowdSec für den Reverse Proxy

0.71	46143	Dual-Stack-Overlay mit IPv6
0.72	46174	NetBird-Only-Dienste, Bring Your Own Proxy
Dashboard 2.39	46174	neue Navigation
Agent Network	46174	schlüsselloser Zugriff auf Sprachmodelle
0.74	2026	Lazy Connections Standard in neuen Konten, Posture Checks während der Sitzung
0.75	46204	neue Desktop-App, verwaltete Einstellungen per MDM
0.76	46204	Absicherung der lokalen Daemon-Schnittstelle (GHSA-qcpp-8vwj-hhwr)
Dashboard 2.92	46266	Entwurfsmodus im Control Center
0.78	2026	Rollen im Agent Network, Kennzahlen am Client, Fernabruf von Debug-Bundles nur mit Freigabe

Tabelle E.1: Versionsübersicht (Zeitangaben nach Veröffentlichungen des Herstellers, teils gerundet).

AUSZUG AUS DEM BUCH

Das NetBird-Handbuch

Zero-Trust-Netzwerke mit WireGuard aufbauen,
betreiben und prüfsicher dokumentieren

- 22 Kapitel, 500 Seiten, Hardcover
- Fallbeispiel Saarmetall GmbH durch alle Kapitel
- In jedem Kapitel: Kasten „Evidenz“ mit den Nachweisen für ISO 27001, NIS-2 und IT-Grundschutz
- E-Book als PDF inklusive
- NetBird-Missionen im Praxislabor AdminMission

39,00 EUR · ISBN 978-3-95444-379-6

Bestellen bei Amazon:
amazon.de/dp/3954443791

Mehr zum Buch, Leseprobe und Begleitmaterial:
brain-media.de/Buecher/buch-netbird.html

© 2026 Brain-Media.de · Dr. Holger Reibold · Alle Rechte vorbehalten.