Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

NetBird на WireGuard: mesh-VPN для удалёнки без боли с маршрутами

Self-hosted NetBird v0.74: Management, Signal, Relay, Zero-Trust ACL и маршруты

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Удалёнка упирается в один OpenVPN-процесс: весь трафик идёт через центральный узел, шифрование не масштабируется, при смене Wi-Fi туннель рвётся, а доступ у всех плоский — ко всей сети. Мы переводим команду на mesh WireGuard с прямыми P2P-туннелями, единым кабинетом и правилами доступа по группам, чтобы скорость, отказоустойчивость и контроль доступа перестали зависеть от одной точки.

Почему это важно бизнесу

- Трафик через один сервер = узкое горло: регионы получают единицы Мбит/с и обходят VPN, гоняя рабочие файлы через личную почту и мессенджеры.
- Плоский доступ: уволенный с невыключенным ключом технически доходит до 1С и файлового сервера — прямой риск утечки и претензий по 152-ФЗ.
- Ручное заведение конфигов = полчаса на человека и очередь заявок «не подключается» каждое утро вместо работы.
- Одна VPS-точка отказа: падение сервера обрывает доступ всей удалённой команде, если нет плана переключения.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

v0.74.2

Актуальная ветка агента, которую ставим; дашборд версионируется отдельно (v2.90.3)

по докам NetBird, 2026

wt0 · 1280

Имя WG-интерфейса и MTU по умолчанию: 1280 закрывает ~140 байт служебных заголовков туннеля

по докам NetBird

100.64/10

Адресное пространство оверлея (CGNAT-диапазон) — Management раздаёт из него внутренние IP пиров

по докам NetBird

51820/udp

Порт WireGuard по умолчанию; Management и Signal сведены на один HTTP/2-порт начиная с v0.29

по докам NetBird

2 мин

Rosenpass пересогласует post-quantum PSK каждые 2 минуты и накладывает его на WG-интерфейс

по докам NetBird

~90%

Доля прямых P2P-туннелей через ICE/STUN в наших внедрениях; TURN(relay) включается лишь при жёстком NAT

наша практика

РЕАЛИЗАЦИЯ 1 ИЗ 3

Разворачиваем control-plane на российской VPS

Что настраиваем

Одна VPS 4 vCPU/8 GB/80 GB SSD, статический IP: combined-контейнер netbird-server + IdP

Как мы это делаем

1. curl getting-started.sh → docker compose поднимает Management, Signal и Relay одним контейнером netbird-server (с v0.65.0)
2. IdP по умолчанию встроенный — local users на Dex внутри netbird-server (getting-started.sh, с v0.62); внешние Zitadel/OIDC/Keycloak подключаем лишь при необходимости
3. Встроенный reverse-proxy (v0.65) сам терминирует TLS на 443/80 — отдельный Caddy/nginx для базовой схемы не нужен
4. Для 30–80 пиров переносим БД с SQLite на PostgreSQL через env-переменные, чтобы Management держал нагрузку

РЕЗУЛЬТАТ

За ~40 минут с нуля до рабочего веб-кабинета. Один узел несёт весь control-plane, а data-plane идёт мимо него прямыми WG-туннелями, поэтому VPS не становится узким горлом по трафику.

КЛЮЧЕВОЙ НЮАНС

С v0.65.0 management, signal и relay слиты в netbird-server — это сильно упрощает proxy. Проверяем, что ставим combined-схему, а не устаревшую multi-container с management.json.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Строим Zero-Trust ACL и маршруты в офис

Что настраиваем

Группы по ролям; NetBird-клиент как routing-peer на 1С, DC, файловом сервере и NVR

Как мы это делаем

1. Первым делом удаляем авто-созданную политику Default (allow-all) — иначе Zero-Trust фикция и сеть остаётся плоской
2. Заводим группы и политики source→destination: редакторы видят только 1С и файловый, бухгалтерия +клиент-банк, админы — всё
3. На Windows Server с 1С ставим клиент как routing-peer и в Networks публикуем подсеть офиса как Resource, а не только сам хост
4. Enrollment через setup keys с auto-assign группами (с v0.9.2); для массовой заливки — one-off/ephemeral ключи, удаляем после
5. Включаем posture checks: версия ОС, версия клиента, гео — несоответствующие устройства уходят в карантин

РЕЗУЛЬТАТ

Доступ выдаётся точечно per-group и деактивируется вместе с учёткой в IdP. Уволенный теряет доступ мгновенно, а аудит «кто куда ходил» смотрится в кабинете, а не в разборе логов OpenVPN.

КЛЮЧЕВОЙ НЮАНС

Ключевой нюанс — маршрут к подсети: если опубликовать только хост 1С, соседний файловый через тот же routing-peer будет недоступен. Публикуем подсеть как Resource и вешаем на неё политику.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Закладываем отказоустойчивость и бэкап control-plane

Что настраиваем

Резервная VPS в другом ЦОД: спящая копия Management + суточный бэкап БД в S3-хранилище

Как мы это делаем

1. Суточный бэкап: для SQLite — docker compose stop management + copy /var/lib/netbird/; для PostgreSQL-бэкенда — pg_dump в S3
2. Держим спящую копию Management во втором ЦОД; ручное переключение по DNS — ~15 минут
3. На клиентах при PPPoE/жёстком NAT фиксируем MTU 1280 (дефолт NetBird), чтобы не терять пакеты в туннеле
4. Для антивируса добавляем исключение на сетевой драйвер и процесс клиента (напр. KES по папке установки NetBird)

РЕЗУЛЬТАТ

Потеря БД Management инвалидирует WG-ключи и требует переподключения всей команды. Суточный бэкап и спящая реплика сводят восстановление к ~15–30 минутам вместо переустройства всей сети.

КЛЮЧЕВОЙ НЮАНС

База Management — единственная критичная точка данных. Бэкапим её по расписанию и проверяем restore; спящая реплика без свежего дампа бесполезна.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Оставили политику Default (allow-all)**
  Аккаунт создаётся с политикой, разрешающей всем всё. Пока её не удалить, Zero-Trust — фикция: сеть остаётся плоской, как старый OpenVPN.

- ✕ **Опубликовали хост вместо подсети**
  Routing-peer раздаёт только указанный IP. Публикуем подсеть офиса как Resource, иначе соседние серверы за тем же шлюзом недоступны.

- ✕ **MTU 1500 на PPPoE-провайдере**
  Инкапсуляция WireGuard режет полезный размер пакета. На проблемных провайдерах фиксируем MTU 1280 (дефолт NetBird) — потери пакетов уходят.

- ✕ **Не бэкапили базу Management**
  Потеря БД инвалидирует все WG-ключи и требует переподключить всех. Делаем суточный дамп SQLite/PostgreSQL во внешнее хранилище и тестируем restore.

- ✕ **Антивирус блокирует драйвер клиента**
  EDR/KES иногда режет сетевой драйвер NetBird. Добавляем исключение на папку установки и процесс клиента в политику антивируса.

- ✕ **Устаревшая multi-container схема**
  До v0.65 это отдельные management/signal/relay/coturn с management.json. Берём combined netbird-server — проще reverse-proxy и обновления.

- ✕ **Одна VPS без резерва**
  Падение единственного узла обрывает control-plane. Держим спящую копию Management во втором ЦОД и план ручного DNS-переключения.

- ✕ **Reusable-ключ раздали всем**
  Долгоживущий общий setup key — риск неконтролируемого enrollment. Для массовой заливки берём one-off/ephemeral ключи и удаляем после.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Self-hosted NetBird на одной VPS в РФ, combined netbird-server в Docker
- Удалить политику Default, завести хотя бы группы «Пользователи» и «Серверы»
- Суточный бэкап БД Management во внешнее хранилище

НОРМАЛЬНО

- Внешний IdP (Zitadel/OIDC) + SSO при необходимости, enrollment через setup keys с auto-assign группами
- ACL source→destination по ролям; подсети офиса опубликованы как Resource
- PostgreSQL-бэкенд, MTU 1280 на проблемных провайдерах, исключения в антивирусе

ХОРОШО

- Posture checks (версия ОС/клиента, гео) с карантином несоответствующих устройств
- Rosenpass (post-quantum PSK) на критичных пирах
- Спящая реплика Management во втором ЦОД + отработанный restore ~15 мин

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Удалена ли авто-политика Default (allow-all) и работает ли deny-by-default?
- [ ] Опубликованы ли подсети офиса как Resource, а не только отдельные хосты?
- [ ] Настроен ли суточный бэкап БД Management и проверяли ли восстановление?
- [ ] Заведён ли IdP/SSO, а enrollment идёт через setup keys с auto-assign группами?
- [ ] Разделён ли доступ по группам (редакторы/бухгалтерия/админы), а не плоско?
- [ ] Зафиксирован ли MTU 1280 на PPPoE и других проблемных провайдерах?
- [ ] Добавлены ли исключения для драйвера и процесса клиента в антивирус?
- [ ] Есть ли резервная копия Management во втором ЦОД и план переключения?
- [ ] Включены ли posture checks и деактивируется ли доступ вместе с учёткой в IdP?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Поднимаем self-hosted NetBird на вашей VPS в РФ под ключ: combined netbird-server, TLS, IdP/SSO
- Проектируем Zero-Trust ACL: группы, политики source→destination, публикация подсетей офиса
- Ставим клиенты на серверы (1С, DC, файловый, NVR) и ноутбуки, настраиваем сетевые маршруты
- Настраиваем бэкап БД, спящую реплику Management и posture checks с карантином
- Мигрируем с OpenVPN параллельным контуром без простоя и обучаем администратора

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 How NetBird Works — компоненты Management/Signal/Relay, ICE/STUN/TURN (docs.netbird.io — 2026)

02 Self-hosted quickstart и advanced guide (getting-started.sh, combined container) (docs.netbird.io — v0.74)

03 Understanding Groups and Access Policies (deny-by-default) (docs.netbird.io — 2026)

04 Register machines using Setup Keys (auto-assign, one-off/ephemeral) (docs.netbird.io — 2026)

05 Understanding NetBird Posture Checks (docs.netbird.io — 2026)

06 Enable Quantum-Resistance — Rosenpass (PSK каждые 2 мин) (docs.netbird.io — 2026)

07 CLI reference — интерфейс wt0, MTU, порт 51820 (docs.netbird.io — 2026)

08 Releases netbirdio/netbird (v0.74.x, dashboard v2.90.x) (github.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.