Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Zero Trust для офиса до 50 РМ: сеть без доверенного периметра

Наша методология: identity-слой Keycloak, оверлей NetBird с ACL и ZTNA-публикация вместо VPN

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У клиентов до 50 РМ сеть обычно «периметральная»: наружу проброшен RDP, VPN даёт доступ ко всей подсети, внутри — плоский сегмент, где РС бухгалтера видит все серверы. Один фишинг или утёкший пароль VPN — и атакующий свободно идёт до 1С и файлов (lateral movement). Мы перестраиваем такие сети на Zero Trust: доступ по identity к конкретным портам, а не «в сеть целиком».

Почему это важно бизнесу

- Шифровальщик, дошедший до 1С и файлового сервера, — простой бухгалтерии и продаж на дни плюс восстановление из бэкапа
- Проброшенный наружу RDP брутфорсят круглосуточно: одна слабая учётка = полный захват сервера
- Подрядчики с VPN «во всю сеть» — неконтролируемый канал утечки баз и ПДн (риски по 152-ФЗ)
- Уволенный сотрудник с не закрытыми вовремя доступами — типовой инцидент; без единого IdP отключение растягивается на дни
- Стек собирается на open-source и штатных средствах: платим за работу инженера, а не за лицензии

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

0.74.x

NetBird self-hosted: WireGuard-оверлей с SSO, группами пиров и ACL вместо классического VPN

по докам docs.netbird.io

26.6

Keycloak — единый IdP: OIDC для всех сервисов, федерация с AD по LDAPS, обязательный TOTP

по докам keycloak.org

30 мин

SSO Session Idle в Keycloak: неактивная сессия гаснет, Access Token живёт 5 минут

наш стандарт (дефолты Keycloak)

до 50

пользователей в Cloudflare Zero Trust бесплатно — Access + Tunnel закрывают типовой офис

по докам developers.cloudflare.com

25 с

PersistentKeepalive для WireGuard-пиров за NAT — туннель не «засыпает» за офисными роутерами

по докам WireGuard

v0.32

Pomerium — self-hosted ZTNA-прокси, когда данные нельзя выносить за контур: политики per-route

по докам pomerium.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Этап 1. Слой идентичности: IdP, MFA, ревизия доступов

Что настраиваем

Все сотрудники и сервисы клиента; узел — VM Keycloak 26.6 (Docker) в серверном VLAN за reverse-proxy nginx

Как мы это делаем

1. Разворачиваем Keycloak 26.6 (quay.io/keycloak/keycloak, start --optimized) за nginx с LE-сертификатом; realm клиента, федерация с AD по LDAPS 636 (edit mode READ_ON…
2. Включаем обязательный OTP: required action «Configure OTP», TOTP 6 цифр / 30 с; Brute Force Detection — Max Login Failures = 5
3. Режем сессии: SSO Session Idle 30 мин, SSO Session Max 10 ч, Access Token Lifespan 5 мин — украденный токен быстро протухает
4. Каждому сервису — свой OIDC-клиент с client secret и точным redirect_uri; общие учётки и «вечные» пароли ликвидируем

РЕЗУЛЬТАТ

Появляется единая точка решений о доступе (Policy Decision Point по NIST SP 800-207): один логин + MFA на все сервисы. Блокировка учётки в IdP отключает всё сразу — увольнение сотрудника становится одной операцией вместо обхода десятка систем.

КЛЮЧЕВОЙ НЮАНС

Федерация с AD — только по LDAPS и сервисной УЗ с правами read-only: Keycloak не должен уметь писать в домен. Обязательно сверяем NTP на PC и сервере — при дрейфе часов TOTP-коды перестают приниматься.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Этап 2. Оверлей-сеть NetBird вместо VPN «во всю сеть»

Что настраиваем

Удалёнка и межофисные связи; management/signal/relay NetBird 0.74 self-hosted на VPS клиента, пиры — PC и серверы

Как мы это делаем

1. Ставим self-hosted NetBird 0.74 по advanced-гайду (Docker Compose), SSO через Keycloak по OIDC; клиенты подключаются командой netbird up с SSO-логином
2. Делим пиров на группы: srv-1c, srv-files, ws-buh, ws-admin; дефолтную политику all-to-all удаляем до подключения первого пира
3. Пишем ACL: ws-buh → srv-1c только tcp/1541,1560-1591,443; ws-admin → серверы tcp/3389,5985; всё остальное — deny by default
4. Включаем posture checks: минимальные версии клиента и ОС, гео только RU — несоответствие = пир не получает доступов по политике
5. Закрываем наружные RDP/WinRM на роутере: администрирование — только через оверлей, снаружи остаётся whitelist мониторинга

РЕЗУЛЬТАТ

Компрометация одного ноутбука не даёт lateral movement: пир видит только разрешённые порты своих групп, а не подсеть целиком. Подрядчик 1С получает ровно tcp/1541+443 к одному серверу. Пробросы RDP наружу исчезают — вместе с брутфорс-шумом в журналах безопасности.

КЛЮЧЕВОЙ НЮАНС

За симметричным NAT проверяем, поднялся ли прямой p2p или трафик ушёл через relay (netbird status -d): relay на слабом VPS — узкое место. На серверах нужен kernel-модуль WireGuard, userspace-режим ест CPU.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Этап 3. ZTNA-публикация веб-сервисов и контроль

Что настраиваем

Веб-контуры: 1С (http-публикация), Grafana/Zabbix, файлы; PEP — Cloudflare Access (до 50 юзеров) или Pomerium v0.32 on-prem

Как мы это делаем

1. Прячем сервисы за cloudflared-туннель: снаружи нет открытых портов; Access-политика — email-домен + группа из IdP, MFA наследуется от Keycloak
2. Для контуров с ПДн — Pomerium v0.32 on-prem: routes from/to, PPL-политика allow: and: [claim groups из токена IdP, client_certificate по SPKI-hash]
3. Session lifetime ZTNA: 8–12 ч сотрудникам, 1 ч подрядчикам; каждое access-решение (allow/deny) пишется в лог
4. Логи Access/Pomerium шлём в SIEM (Wazuh); алерты на серию deny, вход с нового устройства и гео вне RU — в Telegram дежурному

РЕЗУЛЬТАТ

Публикация без открытых портов: сканеры не видят сервис вообще, а каждый запрос авторизуется по identity, а не по IP-адресу. Появляется полный audit trail «кто-куда-когда» по каждому ресурсу — то, чего логи firewall не дают в принципе.

КЛЮЧЕВОЙ НЮАНС

Legacy-клиенты (толстый 1С, SMB-шары) через HTTP-ZTNA не ходят — оставляем их в оверлее NetBird с ACL. Гибрид «ZTNA для веба + оверлей для legacy» — рабочая норма, а не компромисс.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **«Zero Trust купим как продукт»**
  Это архитектура по NIST SP 800-207, а не коробка. Начинаем с PDP (IdP + MFA), затем PEP — оверлей и ZTNA-прокси; каждый этап ценен сам по себе.

- ✕ **Отключить VPN в один день**
  Толстый клиент 1С и SMB-шары через HTTP-ZTNA не работают. Ведём гибрид: legacy — в оверлее с ACL, веб — через ZTNA; старый VPN гасим последним.

- ✕ **Default-политика all-to-all в оверлее**
  NetBird из коробки создаёт правило «все ко всем» — это тот же плоский VPN. Удаляем его до подключения пиров и строим ACL по группам deny-by-default.

- ✕ **MFA сломал сервисные учётки**
  Интеграции падают на интерактивном OTP. Для них — отдельные OIDC-клиенты client credentials с коротким Access Token Lifespan и без прав пользователя.

- ✕ **МФУ и сканеры вне модели**
  Устройства без агента (принтеры, СКУД, кассы) в оверлей не встанут. Выносим в отдельный VLAN и режем ACL на роутере по IP/портам (tcp/445 к шаре).

- ✕ **Самоблокировка админов**
  Ошибка в политике или падение IdP отрезает всех. Держим break-glass: локальную учётку вне MFA-политик и консольный/IPMI-доступ к гипервизору.

- ✕ **Логи есть — алертов нет**
  Access-решения без корреляции бесполезны. Настраиваем алерты на серии deny, новые устройства и гео вне RU — в Telegram дежурному в течение минут.

- ✕ **Relay вместо p2p незаметно**
  За симметричным NAT NetBird уходит на relay — весь трафик через слабый VPS. Диагностируем netbird status -d, чиним UDP/STUN или переносим relay ближе.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Убрать пробросы RDP/SSH наружу; админ-доступ — только по whitelist IP
- MFA на почту, VPN и все внешние панели; отключить мёртвые учётки
- Гостевой Wi-Fi и МФУ — в отдельный VLAN без маршрута в серверный сегмент

НОРМАЛЬНО

- Единый IdP (Keycloak 26.6 / Entra ID) с федерацией AD и SSO на ключевые сервисы
- Оверлей NetBird с группами и ACL по портам вместо L2TP/OpenVPN «во всю сеть»
- Posture-проверки: версии ОС и клиента, гео; несоответствие = нет доступа
- Централизованные логи входов и доступов (SIEM) с базовыми алертами

ХОРОШО

- ZTNA-публикация всех веб-сервисов без открытых портов (Access / Pomerium)
- Client-cert/mTLS для админ-панелей; сессии 8 ч сотрудникам, 1 ч подрядчикам
- Микросегментация серверного VLAN: ACL между серверами, а не только к ним
- Ежеквартальный рецерт доступов: сверка групп IdP с фактическими ролями

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Закрыты ли на роутере пробросы RDP/WinRM/SSH наружу (или сведены к whitelist из 2–3 IP)?
- [ ] Есть ли единый IdP и включён ли MFA для всех внешних входов, включая почту и панели управления?
- [ ] Даёт ли ваш VPN доступ ко всей подсети — или только к нужным портам конкретных серверов?
- [ ] Отделены ли гостевой Wi-Fi, МФУ и IoT в свой VLAN без маршрута в серверный сегмент?
- [ ] Отключается ли весь доступ уволенного одной операцией в IdP, а не обходом десяти сервисов?
- [ ] Проверяется ли состояние устройства (версия ОС, клиента) перед выдачей маршрутов и доступа?
- [ ] Видит ли подрядчик один сервис и порт — или всю сеть после подключения?
- [ ] Пишутся ли access-решения (allow/deny) в централизованный лог и есть ли алерты на аномалии?
- [ ] Есть ли break-glass доступ (локальная учётка, консоль/IPMI) на случай отказа IdP или ZTNA?

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).

- Аудит периметра: открытые порты, пробросы, плоские сегменты — карта рисков за 2–3 дня
- Разворачиваем identity-слой: Keycloak / Entra ID, MFA, федерация с AD, ревизия учёток
- Мигрируем с L2TP/OpenVPN на оверлей NetBird с ACL и posture-проверками без простоя
- Публикуем 1С и внутренние веб-сервисы через ZTNA (Cloudflare Access / Pomerium) без открытых портов
- Подключаем контроль: логи access-решений в SIEM, алерты в Telegram, сопровождение по SLA

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 NIST SP 800-207 — Zero Trust Architecture (PE / PA / PEP)
(nvlpubs.nist.gov — 2020)

02 Keycloak Server Administration Guide — sessions, OTP, LDAP
(keycloak.org — 26.6 (20…)

03 NetBird Docs — Self-hosted, Access Control, Posture Checks
(docs.netbird.io — 0.74 (20…)

04 Pomerium Docs — Routes & Pomerium Policy Language
(pomerium.com — v0.32 (2…)

05 Cloudflare One Docs — Access, Tunnel, Device Posture
(developers.cloudflare.com — 2026)

06 Microsoft Entra — Conditional Access (compliant device)
(learn.microsoft.com — 2026)

07 Наш шаблон сегментации pfSense/Keenetic (VLAN, whitelist)
(itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.