Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

WireGuard mesh-сети: Tailscale и Netmaker в наших внедрениях

Строим P2P-сеть офисов, серверов и удалёнки без единого VPN-концентратора

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Классический VPN-концентратор (OpenVPN/IPsec) — звезда: весь трафик филиалов и удалёнки идёт через один сервер. Падает он — у всех сразу встают 1С, RDP и файловые шары; latency между площадками растёт в разы. Мы переводим клиентов на WireGuard mesh (Tailscale/Headscale или Netmaker): трафик идёт напрямую между узлами, ключи раздаёт координатор, единой точки отказа нет.

Почему это важно бизнесу

- Отказ VPN-концентратора останавливает всех удалённых сотрудников и филиалы одновременно — простой считается в человеко-часах
- P2P-туннели убирают лишний хоп: RDP и 1С между площадками работают с latency канала, а не «через Москву»
- Подключение нового сотрудника — минуты через SSO, а не ручной выпуск сертификата админом
- ACL по группам вместо «VPN = вся сеть»: подрядчик видит один сервер, а не всю инфраструктуру
- WireGuard в ядре Linux даёт гигабит на недорогом VPS — мощный выделенный VPN-сервер не нужен

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

1.98.x

клиент Tailscale: пиним одну версию на весь парк, обновляем волной после проверки на стенде

Tailscale changelog, 06.2026

v1.6.x

сервер Netmaker для self-hosted инсталляций: kernel WireGuard, egress/gateway-relay, enrollmen...

docs.netmaker.io, v1.6

5.6+

минимальное ядро Linux со встроенным модулем WireGuard — на более старых ставим dkms-пакет

wireguard.com, докум. протокола

25 с

PersistentKeepalive для узлов за NAT — держит пробитый UDP-маппинг живым

наш стандарт

180 дн

дефолтный key expiry Tailscale; серверам и шлюзам отключаем истечение ключа явно

tailscale.com/kb, key expiry

41641/udp

порт прямых соединений Tailscale — открываем исходящий UDP, иначе трафик уйдёт в DERP-relay

tailscale.com/kb, firewall

РЕАЛИЗАЦИЯ 1 ИЗ 3

Tailscale/Headscale: mesh для офиса и удалёнки

Что настраиваем

Охват: офисная LAN через subnet router, 20–50 сотрудников со входом по SSO, серверы с тегами tag:srv

Как мы это делаем

1. Разворачиваем координатор: SaaS Tailscale или self-hosted Headscale на VPS клиента; клиентов ставим закреплённой версией из apt-репозитория (apt pin)
2. Серверы вводим pre-authorized auth-ключами с тегами (tailscale up --advertise-tags=tag:srv), людям — вход через SSO
3. Офисный шлюз: tailscale up --advertise-routes=192.168.10.0/24 + net.ipv4.ip_forward=1, маршрут approve в админ-консоли
4. ACL deny-by-default: группы group:buh, group:admin; доступ только к нужным тегам и портам (3389, 1540–1541, 1560–1591)
5. MagicDNS + split-DNS: зону AD-домена отдаём офисному DC, остальные имена резолвит tailnet

РЕЗУЛЬТАТ

Удалёнка ходит в RDP и 1С напрямую в офис без проброса портов наружу; отказ координатора не рвёт уже установленные туннели — WireGuard-сессии живут на обменянных ключах до следующей ротации

КЛЮЧЕВОЙ НЮАНС

На серверах и шлюзах сразу отключаем key expiry (по умолчанию 180 дней) — иначе через полгода шлюз молча выпадает из сети, обычно в выходной

РЕАЛИЗАЦИЯ 2 ИЗ 3

Netmaker: self-hosted mesh между площадками

Что настраиваем

Охват: 2–4 площадки плюс ДЦ; netmaker-server в Docker на VPS клиента, netclient на шлюзах

Как мы это делаем

1. Поднимаем сервер по официальному docker-compose: NM_DOMAIN, MASTER_KEY (openssl rand -hex 32), брокер Mosquitto за reverse-proxy на 443/wss
2. Создаём сеть 10.10.0.0/16; узлы вводим enrollment-ключами с привязкой к сети и тегам: netclient join -t <key>
3. Шлюзы площадок делаем egress gateway на локальные подсети — mesh заменяет site-to-site IPsec
4. Для узлов за строгим NAT назначаем gateway-узел (relay) на VPS с белым IP; имена внутри сети — встроенный CoreDNS
5. Бэкапим БД сервера и .env с MASTER_KEY в offsite — без них парк не переконфигурировать

РЕЗУЛЬТАТ

Все ключи и метаданные соединений остаются на серверах клиента (частое требование СБ); kernel WireGuard даёт скорость канала между площадками без выделенного железа под VPN

КЛЮЧЕВОЙ НЮАНС

Netmaker управляет узлами через MQTT-брокер: если Mosquitto лёг, туннели живут, но изменения конфигурации не доезжают — брокер мониторим как критичный сервис

РЕАЛИЗАЦИЯ 3 ИЗ 3

Эксплуатация: мониторинг mesh и регламент обновлений

Что настраиваем

Охват: все узлы mesh; Zabbix на нашей стороне, регламент версий клиентов и бэкапов координатора

Как мы это делаем

1. tailscale status и tailscale netcheck по cron: ловим узлы, съехавшие с direct на relay, и деградацию DERP
2. В Zabbix — возраст последнего handshake (wg show <if> latest-handshakes): порог 3 мин при keepalive 25 с
3. Обновления клиентов волнами: стенд → серверы → пользователи; авто-апдейт на серверах выключен
4. Бэкап координатора ежедневно offsite: Headscale — SQLite и ключи из /var/lib/headscale, Netmaker — БД и .env
5. Ежеквартальная ревизия ACL и удаление мёртвых узлов (offline дольше 30 дней)

РЕЗУЛЬТАТ

Проблемы NAT и уход трафика в relay видим раньше пользователей; обновление клиента, ломающее совместимость с Headscale, останавливается на стенде и не доезжает до прода

КЛЮЧЕВОЙ НЮАНС

Handshake старше пары минут при включённом keepalive — ранний признак умершего UDP-маппинга или блокировки UDP у провайдера; алертим до жалоб пользователей

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Relay вместо direct-соединения**
  Закрытый исходящий UDP загоняет трафик в DERP-relay — latency растёт в разы. Открываем UDP 41641 и проверяем tailscale netcheck
- ✕ **Key expiry на серверах**
  Через 180 дней узел молча теряет сеть. Серверам и шлюзам отключаем истечение ключа, людям оставляем re-auth через SSO
- ✕ **Маршрут объявлен, но не approved**
  Шлюз анонсировал подсеть, а в консоли её не подтвердили, плюс забыт ip_forward=1 — офис недоступен. Проверяем оба пункта чек-листом
- ✕ **ACL «allow all» по умолчанию**
  Стартовая политика пускает всех ко всем. Переписываем на deny-by-default: группы → теги → порты; подрядчикам — отдельная группа
- ✕ **MagicDNS против AD**
  Резолвер 100.100.100.100 перехватывает DNS и ломает домен AD. Настраиваем split-DNS: корпоративную зону отдаём на DC клиента
- ✕ **Обновление клиента ломает Headscale**
  Свежий клиент Tailscale может не завестись со старым Headscale. Пиним версии в apt и обновляем связку парой после стенда
- ✕ **MASTER_KEY без бэкапа**
  Потеря .env и БД Netmaker означает пересборку всей сети вручную. Конфиг и БД координатора бэкапим offsite ежедневно
- ✕ **Userspace там, где нужен kernel**
  wireguard-go упирается в CPU уже на гигабите. На Linux-шлюзах используем kernel-модуль: ядро 5.6+ либо wireguard-dkms

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Tailscale SaaS: вход по SSO, теги на серверы, ACL deny-by-default
- Subnet router в офис вместо проброса RDP наружу
- Отключён key expiry на серверах, keepalive 25 с за NAT

НОРМАЛЬНО

- Self-hosted координатор (Headscale или Netmaker) на VPS клиента
- Split-DNS с AD-доменом, MagicDNS для остальных имён
- Мониторинг handshake и direct/relay в Zabbix
- Пин версий клиентов, обновление волнами через стенд

ХОРОШО

- Два mesh-шлюза на площадку с резервированием маршрутов
- Свой relay/DERP на VPS с белым IP ближе к пользователям
- Ежедневный offsite-бэкап БД и ключей координатора
- Ежеквартальная ревизия ACL и зачистка мёртвых узлов

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Переживёт ли компания отказ VPN-сервера — есть ли P2P-связность между площадками?
- [ ] Идёт ли трафик между узлами direct, а не через relay (видно в tailscale status)?
- [ ] Отключено ли истечение ключей на серверах и шлюзах?
- [ ] Политика ACL построена как deny-by-default, подрядчики отделены от основной сети?
- [ ] Настроен ли split-DNS — mesh не ломает резолв AD-домена?
- [ ] Есть ли бэкап координатора (БД, ключи, .env) вне самого сервера координатора?
- [ ] Зафиксированы ли версии клиентов и порядок их обновления через стенд?
- [ ] Мониторится ли возраст WireGuard-handshake и доступность MQTT/DERP?

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 текущего VPN и проект перехода на WireGuard mesh без остановки работы
- Развёртывание Tailscale/Headscale или Netmaker: ACL, SSO, subnet-шлюзы, split-DNS
- Раскатка клиентов на весь парк через Ansible/GPO и плановый вывод старого OpenVPN
- Мониторинг mesh в Zabbix с алертами в Telegram и регламентом обновлений
- Поддержка по SLA: ревизия ACL, бэкапы координатора, разбор сетевых инцидентов

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 Tailscale Docs — ACLs/grants, key expiry, subnet routers (tailscale.com — 2026)

02 Tailscale changelog — клиент 1.98.x (tailscale.com — 06.2026)

03 Netmaker Docs — Install (Docker), Egress, Gateways/Relay, Enrollment keys (docs.netmaker.io — v1.6)

04 Headscale Docs — self-hosted координатор tailnet (headscale.net — 2026)

05 WireGuard — протокол, kernel-модуль, PersistentKeepalive (wireguard.com — 2026)

06 Наш Ansible-шаблон раскатки mesh-клиентов ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.