Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

OpenVPN или WireGuard для офиса: как мы выбираем и внедряем

Критерии выбора, эталонные конфигурации WireGuard/OpenVPN и процедуры отзыва доступа

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сотрудникам нужен защищённый доступ к 1С, файловым шарам и CRM из дома и командировок, а филиалам — единая сеть с офисом. Неверно выбранный VPN-протокол оборачивается медленной 1С через туннель, разрывами при смене Wi-Fi/LTE и невозможностью мгновенно отозвать доступ уволенному. Мы выбираем между WireGuard и OpenVPN по формальным критериям и разворачиваем по своим эталонным конфигурациям.

Почему это важно бизнесу

- Тормозящая через VPN 1С — оплаченные часы простоя каждого удалённого сотрудника ежедневно
- Не отозванный в день увольнения доступ — открытый канал к бухгалтерии и клиентской базе
- Разрывы туннеля при переключении Wi-Fi/LTE срывают работу руководителей в дороге
- Неверный протокол = переделка через год: повторная раздача конфигов всем сотрудникам

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2.7

актуальная ветка OpenVPN: multi-socket сервер и работа с kernel-модулем ovpn (Linux 6.16+)

по докам OpenVPN; релиз 2.7.0 — 11.02.2026

5.6+

ядро Linux со встроенным WireGuard — на актуальных дистрибутивах модуль уже в ядре

wireguard.com

25 с

PersistentKeepalive для клиентов за NAT — иначе входящий трафик до пира обрывается

по докам WireGuard

x2

рост пропускной способности OpenVPN с DCO: шифрование уходит из user space в ядро

по докам OpenVPN DCO

51820/udp

порт WireGuard: без валидного ключа сервер не отвечает — сканеры порт не видят

наш стандарт + доки WireGuard

7.21.5

RouterOS long-term с нативным WireGuard — VPN на офисном MikroTik без отдельного VDS

по докам MikroTik, 07.2026

РЕАЛИЗАЦИЯ 1 ИЗ 3

Удалённый доступ на WireGuard: эталонный контур

Что настраиваем

VDS Ubuntu 24.04 LTS, wg0 10.66.66.0/24, до 50 удалёнников

Как мы это делаем

1. Интерфейс wg0: ListenPort 51820, ключи wg genkey | wg pubkey под umask 077; модуль WireGuard в ядре с Linux 5.6, доставить нужно только пакет wireguard-tools
2. Клиентам в AllowedIPs — только офисные подсети (например 10.10.0.0/16), не 0.0.0.0/0: личный интернет-трафик через сервер не гоняем
3. PersistentKeepalive = 25 каждому клиенту за NAT; DNS = внутренний сервер, чтобы резолвились имена 1С и файловых серверов
4. Выпуск пользователя скриптом: ключи, .conf и QR (qrencode); на сервере wg set wg0 peer <pub> allowed-ips <ip>/32 + wg-quick save wg0
5. net.ipv4.ip_forward=1 в sysctl.d и правила FORWARD/MASQUERADE в PostUp/PostDown — без них трафик в локалку не пойдёт

РЕЗУЛЬТАТ

Подключение быстрее секунды, бесшовный roaming Wi-Fi↔LTE без разрыва 1С и RDP, экономия батареи. Новый сотрудник получает доступ за минуты: QR телефоном или импорт .conf на ноутбуке.

КЛЮЧЕВОЙ НЮАНС

AllowedIPs — одновременно маршрутизация и криптографический ACL: пересечение адресов двух peer'ов молча ломает маршруты, поэтому ведём реестр выданных IP по каждому серверу.

РЕАЛИЗАЦИЯ 2 ИЗ 3

OpenVPN 2.6/2.7 там, где нужны TCP/443, AD и 2FA

Что настраиваем

Шлюз на периметре или VDS; PKI на easy-rsa 3.2.6, парк до 200 пользователей

Как мы это делаем

1. PKI с офлайн-CA: easyrsa build-ca, серверный и клиентские сертификаты; вместо общего tls-auth — tls-crypt-v2 с отдельным ключом на клиента
2. data-ciphers AES-256-GCM:CHACHA20-POLY1305; основной инстанс на udp/1194 и резервный на tcp/443 для сетей, где UDP зарезан
3. Доменная авторизация: plugin auth-pam + sssd к Active Directory, второй фактор — TOTP через pam_google_authenticator
4. Отзыв доступа: easyrsa revoke <имя> && easyrsa gen-crl, в конфиге сервера crl-verify crl.pem — сертификат гаснет без рестарта службы
5. На ядрах 6.16+ включаем DCO (модуль ovpn, OpenVPN 2.7): шифрование данных в ядре, примерно вдвое выше пропускная способность

РЕЗУЛЬТАТ

Работает из сетей, где открыты только 80/443; вход по доменному паролю с одноразовым кодом; блокировка уволенного — одна команда, действует на все копии конфига.

КЛЮЧЕВОЙ НЮАНС

CRL имеет собственный срок действия: просроченный crl.pem валит авторизацию всем сразу. Обновляем gen-crl по systemd-таймеру и мониторим дату Next Update.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Site-to-site и малый офис на MikroTik

Что настраиваем

RouterOS 7.x (long-term 7.21.5), связка офис — склад — филиал без отдельного сервера

Как мы это делаем

1. /interface wireguard add listen-port=51820, peer'ы с allowed-address подсетей второй площадки, статические маршруты в обе стороны
2. Firewall: forward из wg-интерфейса в LAN — accept по нужным подсетям; input udp/51820 — только с внешних IP площадок
3. Контроль связи: /interface wireguard peers print — last-handshake живого туннеля не старше 2-3 минут
4. На 50+ одновременных пиров следим за CPU (/system resource): при упоре в шифрование выносим hub на отдельный VDS

РЕЗУЛЬТАТ

Филиалы объединяются в одну сеть силами уже стоящих роутеров: 1С, шары и принтеры работают между площадками без лишнего сервера и абонплаты за VDS.

КЛЮЧЕВОЙ НЮАНС

У WireGuard нет статуса «подключён»: диагностика только по last-handshake и счётчикам rx/tx — сразу закладываем эти метрики в мониторинг Zabbix.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Забытый ip_forward**
  Туннель поднят, а в локалку трафик не идёт: нужны net.ipv4.ip_forward=1 (sysctl.d) и правило FORWARD. Проверяем прохождение до 1С сразу после деплоя.

- ✕ **AllowedIPs = 0.0.0.0/0 всем подряд**
  Весь интернет пользователя летит через офисный сервер: канал забит, всё «тормозит». Отдаём в туннель только рабочие подсети.

- ✕ **Нет PersistentKeepalive за NAT**
  NAT провайдера закрывает мапинг за минуты простоя — входящие пакеты теряются. 25 с — интервал, рекомендованный документацией WireGuard.

- ✕ **Общий tls-auth вместо tls-crypt-v2**
  Один статический ключ на всех: утечка у одного клиента раскрывает защиту канала управления всем. Выдаём per-client ключи tls-crypt-v2.

- ✕ **CRL не выпущен после увольнения**
  Сертификат OpenVPN действует до конца срока: без easyrsa revoke + gen-crl и crl-verify в конфиге уволенный сохраняет доступ месяцами.

- ✕ **Конфиги с ключами в мессенджере**
  .conf с приватным ключом в чате — вечная копия у неизвестного круга лиц. Храним в Vault, отдаём одноразовой ссылкой с TTL 24 часа.

- ✕ **VPN-подсеть совпадает с домашней**
  192.168.0.0/24 и 192.168.1.0/24 заняты домашними роутерами — маршруты клиента ломаются. Берём нетиповой диапазон вроде 10.66.66.0/24.

- ✕ **MTU по умолчанию на PPPoE/LTE**
  Фрагментация: пинг ходит, а 1С и RDP виснут на больших пакетах. Для WireGuard фиксируем MTU 1420, для OpenVPN подбираем mssfix/tun-mtu.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- WireGuard на VDS: в AllowedIPs только офисные подсети, keepalive 25 с
- ip_forward + firewall: из VPN доступны только нужные серверы
- Реестр выданных ключей и отзыв доступа в день увольнения

НОРМАЛЬНО

- Выпуск клиентов скриптом: ключи, .conf, QR; ротация при увольнениях
- Мониторинг last-handshake и rx/tx пиров в Zabbix, алерт на молчание
- Резервный OpenVPN-инстанс на tcp/443 для сетей с зарезанным UDP
- Ключи и конфиги в Vault, выдача одноразовыми ссылками

ХОРОШО

- OpenVPN 2.7 + DCO (ядро 6.16+); AD-авторизация с TOTP через PAM
- Site-to-site на MikroTik RouterOS 7 long-term между площадками
- Веб-панель (Firezone/NetBird) при 50+ пользователях и текучке
- Плейбук Ansible: пересборка VPN-сервера с нуля за минуты

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Уволенный теряет VPN-доступ в тот же день (peer remove / revoke + CRL)?
- [ ] В AllowedIPs клиентов только рабочие подсети, а не 0.0.0.0/0?
- [ ] У всех клиентов за NAT задан PersistentKeepalive = 25?
- [ ] Есть резервный вход по tcp/443 для сетей, где режут UDP?
- [ ] Приватные ключи и .conf лежат в защищённом хранилище, а не в чатах?
- [ ] CRL OpenVPN обновляется автоматически и не просрочен?
- [ ] Мониторинг видит last-handshake каждого пира и CPU шлюза?
- [ ] VPN-подсеть не пересекается с домашними 192.168.0.0/24 и 192.168.1.0/24?
- [ ] Версии актуальны: OpenVPN 2.6/2.7 с закрытыми CVE, RouterOS long-term?

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).

- Подбираем протокол под задачи: замеры канала, требования AD/2FA, география сотрудников
- Разворачиваем под ключ: WireGuard, OpenVPN с PKI или site-to-site на MikroTik
- Каждому сотруднику — пакет: конфиг, QR, инструкция; ключи храним в Vault
- Настраиваем мониторинг туннелей в Zabbix и отзыв доступа за минуты
- Сопровождаем: ротация ключей, обновления версий, дежурный инженер

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 WireGuard Quick Start, man wg(8) / wg-quick(8) (wireguard.com — 2025)

02 OpenVPN Reference Manual и Changes.rst ветки 2.7 (openvpn.net — 2.7.0, 02.2026)

03 OpenVPN README.dco — модуль ovpn в Linux 6.16+ (github.com/OpenVPN — 2026)

04 Easy-RSA 3: build-ca, revoke, gen-crl (github.com/OpenVPN/easy-rsa — 3.2.6)

05 MikroTik RouterOS Documentation — WireGuard (help.mikrotik.com — 7.x)

06 Наш шаблон add_client.sh и плейбук Ansible OpenVPN+2FA (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.