Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

VPN и сеть офиса до 50 PM: как мы строим канал на WireGuard

WireGuard-удалёнка и site-to-site, сегментация VLAN, два провайдера с автопереключением

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сотрудники работают с 1С, файлами и банк-клиентом из дома и филиалов, а офис держится на одном роутере с пробросом RDP наружу и единственным провайдером. Это подбор паролей по открытому 3389, обрывы туннелей и полный простой при аварии канала. Мы перестраиваем периметр: WireGuard по ключам, VLAN-изоляция, два WAN с автопереключением и мониторинг каналов.

Почему это важно бизнесу

- Открытый наружу RDP — главный вектор шифровальщиков: простой бухгалтерии и 1С на дни плюс восстановление из бэкапов
- Падение единственного канала останавливает банк-клиент, телефонию и облачные сервисы — офис на 50 человек стоит целиком
- Подписочные VPN-сервисы — постоянные платежи и чужие серверы; свой WireGuard работает на вашем железе без абонентки
- Плоская сеть без сегментации: заражённый ноутбук гостя видит сервер 1С и банк-клиент напрямую

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

CE 2.8.1

Актуальный pfSense на периметре: пакет WireGuard, gateway groups и dpinger уже в комплекте

по докам Netgate pfSense

25 с

PersistentKeepalive для пиров за NAT — держит трансляцию открытой, обратный трафик не пропадает

по докам WireGuard

1420

MTU WireGuard-интерфейса (1500 минус 80 байт оверхеда) — без фрагментации поверх PPPoE и LTE

wg-quick, наш стандарт

7.23

RouterOS 7 stable на MikroTik филиалов: WireGuard встроен в систему начиная с версии 7

help.mikrotik.com

20%

Порог потерь dpinger, после которого шлюз помечается down и gateway group уводит трафик на рез…

pfSense Multi-WAN

51820/UDP

Единственный порт, который мы открываем снаружи вместо проброса RDP 3389 на сервер

наш стандарт периметра

РЕАЛИЗАЦИЯ 1 ИЗ 3

Удалённый доступ: WireGuard-концентратор на pfSense

Что настраиваем

Периметр офиса на pfSense CE 2.8.1: доступ бухгалтерии и удалённщиков к 1С и файловому серверу

Как мы это делаем

1. Ставим пакет WireGuard, поднимаем туннель tun_wg0: порт 51820/UDP, подсеть 10.6.0.0/24; ключи — парой wg genkey | wg pubkey, по отдельному peer на сотрудника
2. На клиенте прописываем узкие AllowedIPs: только серверная VLAN 10.1.10.0/24, а не 0.0.0.0/0 — личный трафик сотрудника через офис не гоняем
3. Пирам за NAT задаём PersistentKeepalive = 25 и MTU 1420; живость проверяем по latest handshake и счётчикам rx/tx в выводе wg show
4. На WG-интерфейсе правила фаервола: к серверу 1С только TCP 1541 и 1560-1591, к файловому — SMB 445; остальная LAN из VPN закрыта
5. Конфиг отдаём файлом или QR-кодом; отзыв доступа — удаление одного peer, общий секрет перевыпускать не нужно

РЕЗУЛЬТАТ

Сотрудник подключается за секунды (рукопожатие — один round-trip), туннель переживает смену Wi-Fi на LTE без переподключения. Снаружи открыт один UDP-порт вместо RDP; на пакеты без валидного ключа WireGuard не отвечает — сканеры порт просто не видят.

КЛЮЧЕВОЙ НЮАНС

AllowedIPs в WireGuard — одновременно маршрутизация и ACL (cryptokey routing): пакет из туннеля с адресом вне AllowedIPs пира отбрасывается. Поэтому каждому peer выдаём ровно один /32 и не пересекаем подсети.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Site-to-site: офис ↔ склад и филиал на MikroTik

Что настраиваем

Роутеры филиалов MikroTik на RouterOS 7.23 ↔ pfSense офиса; склад с ТСД и филиал с кассовыми РМ

Как мы это делаем

1. /interface/wireguard add name=wg-office listen-port=51820; между площадками обмениваемся только публичными ключами — приватный не покидает роутер
2. В peer офиса заносим AllowedIPs 10.1.0.0/16, на офисной стороне — подсеть филиала 10.2.0.0/24; маршруты — статикой через wg-интерфейс
3. Филиал за серым IP всегда инициатор: endpoint = белый IP офиса, persistent-keepalive=25s — белый адрес нужен только одной стороне
4. Где оператор режет UDP WireGuard — запасной профиль IPsec IKEv2 (strongSwan 6.0/swanctl: AES-256-GCM, обмен ключами curve25519)
5. Возраст last handshake и счётчики rx/tx обоих пиров заводим в мониторинг: рукопожатие старше 3 минут — алерт

РЕЗУЛЬТАТ

Склад и филиал работают в единой адресации с офисом: ТСД ходят в 1С напрямую, принтеры этикеток печатают из офисной базы. Филиалы живут за CG-NAT провайдера без доплат за белый IP — статический адрес держим только на офисном периметре.

КЛЮЧЕВОЙ НЮАНС

У WireGuard нет состояния «туннель упал» — интерфейс всегда up. Единственный честный индикатор — возраст last handshake (новое рукопожатие проходит примерно каждые 2 минуты), его и мониторим, а не статус линка.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Два провайдера: автопереключение без ручных действий

Что настраиваем

WAN-уровень pfSense: оптика основного оператора + резерв (второй провайдер или LTE-модем)

Как мы это делаем

1. Каждому WAN — свой gateway с уникальным monitor IP: внешние анкеры, не шлюз провайдера, иначе канал «жив» при мёртвой магистрали
2. dpinger: порог задержки 500 мс, потерь 20%, интервал проб 500 мс — при превышении шлюз помечается down
3. Gateway group WAN_FAILOVER: основной Tier 1, резерв Tier 2, trigger = Member down; правило LAN направляет default-трафик через группу
4. Исходящий NAT переводим в hybrid под оба WAN; для SIP-телефонии — правило со Static Port на UDP 5060, чтобы АТС не теряла регистрацию из-за подмены порта
5. Оба канала под Zabbix 7.0 LTS: icmppingloss по анкерам + SNMP-счётчики интерфейсов, алерт в Telegram при каждом переключении

РЕЗУЛЬТАТ

Обрыв оптики офис замечает по одному алерту: трафик уезжает на резерв за интервал проверки (секунды), банк-клиент и телефония продолжают работать. Возврат на основной канал — автоматический после стабилизации, без выезда инженера и перезагрузок роутера.

КЛЮЧЕВОЙ НЮАНС

Проверяем не «пинг до шлюза», а реальный выход в интернет: monitor IP должен лежать за пределами сети провайдера и быть уникальным для каждого WAN — pfSense один адрес двум шлюзам не даст.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **AllowedIPs 0.0.0.0/0 на клиентах**
  Весь личный трафик сотрудников едет через офисный канал и забивает его. Режем AllowedIPs до рабочих подсетей — VPN только для 1С и файлов.

- ✕ **Нет keepalive у пиров за NAT**
  NAT-трансляция у оператора протухает, офис не может инициировать трафик к клиенту — туннель «односторонний». PersistentKeepalive 25 с держит её.

- ✕ **MTU 1500 внутри туннеля**
  Поверх PPPoE/LTE пакеты фрагментируются: RDP подвисает, SMB рвётся на больших файлах. Считаем оверхед ~80 байт и фиксируем MTU 1420 или ниже.

- ✕ **Один конфиг VPN на всех**
  Уволенный уносит доступ, отозвать без перевыпуска всем нельзя. Только персональные peer: отзыв — удаление одной записи на сервере.

- ✕ **VPN-клиенты видят всю LAN**
  Из туннеля доступны камеры, принтеры и чужие ПК. На VPN-интерфейсе ставим явные разрешения по серверам и портам, остальное — deny по умолчанию.

- ✕ **Monitor IP = шлюз провайдера**
  Шлюз оператора отвечает даже при аварии магистрали — failover не срабатывает. Мониторим внешние анкеры, по уникальному адресу на каждый WAN.

- ✕ **Статус туннеля по интерфейсу up**
  wg-интерфейс всегда «зелёный», это ничего не значит. Мониторим возраст latest handshake и приросты rx/tx — только они показывают живой канал.

- ✕ **Периметр на заводской прошивке**
  Роутер с известными CVE и админкой в WAN — готовая точка входа. Календарь обновлений RouterOS/KeeneticOS/pfSense и запрет WebUI со стороны WAN.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Закрыть проброс RDP 3389: доступ снаружи — только через WireGuard по ключам
- Персональный peer на сотрудника, keepalive 25 с, MTU 1420
- Обновить прошивку периметра, запретить админку роутера из WAN

НОРМАЛЬНО

- pfSense/MikroTik на периметре, правила на VPN-подсеть по конкретным портам
- Site-to-site до филиалов с узкими AllowedIPs и мониторингом last handshake
- Второй канал с failover: dpinger, gateway group, уникальные monitor IP
- VLAN-сегментация: серверы, пользователи, гостевой Wi-Fi и камеры раздельно

ХОРОШО

- Zabbix 7.0 LTS: анкеры ICMP, SNMP-интерфейсы, алерты о переключениях в Telegram
- Резервный профиль IPsec IKEv2 на случай блокировки UDP-транспорта оператором
- Бэкап конфигураций периметра в git, восстановление роутера за 15 минут
- Регламент: квартальные обновления прошивок и ревизия списка peer

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Снаружи закрыты RDP, SMB и админки — из интернета доступен только UDP-порт VPN?
- [ ] У каждого сотрудника личный peer, и доступ уволенного отзывается за минуту?
- [ ] VPN-клиенты видят только нужные серверы и порты, а не всю сеть с камерами и принтерами?
- [ ] Для пиров за NAT задан PersistentKeepalive, а MTU туннеля посчитан под канал связи?
- [ ] Есть второй интернет-канал, и автопереключение проверено отключением основного, а не «на бумаге»?
- [ ] Monitor IP шлюзов — внешние адреса, а не шлюз провайдера?
- [ ] Мониторится возраст last handshake туннелей, а не «зелёный» статус интерфейса?
- [ ] Прошивки роутеров, свитчей и pfSense обновлялись за последние три месяца?
- [ ] Конфигурация периметра лежит в бэкапе, и восстановление отрепетировано?

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).

- Проектируем периметр офиса до 50 РМ: pfSense/MikroTik/Keenetic, адресный план, VLAN-сегментация
- Разворачиваем WireGuard для удалёнки и site-to-site с филиалами, с правилами доступа по ролям
- Настраиваем двух провайдеров с автопереключением и алертами о падении канала
- Подключаем сеть к мониторингу Zabbix 7.0 LTS: каналы, туннели, свитчи, UPS
- Сопровождаем периметр: обновления прошивок, ревизия peer-листа, бэкапы конфигураций

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 и man wg-quick (AllowedIPs, PersistentKeepalive) (wireguard.com — 2026)

02 pfSense Docs: пакет WireGuard, Gateway Groups и Multi-WAN (docs.netgate.com — CE 2.8.1)

03 MikroTik RouterOS Documentation: WireGuard (help.mikrotik.com — 7.23)

04 strongSwan Documentation: IKEv2 и swanctl.conf (docs.strongswan.org — 6.0)

05 Zabbix Manual: ICMP- и SNMP-мониторинг сети (zabbix.com — 7.0 LTS)

06 Наш шаблон адресного плана и правил периметра для офиса до 50 PM (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.