Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

VPN офис–склад на MikroTik: site-to-site без простоев

Наша схема на RouterOS 7: WireGuard/IPsec, VLAN-сегментация, LTE-резерв и мониторинг туннеля

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Оператор склада работает в 1С через проброшенный в интернет RDP, офис и склад живут в разорванных сетях: печать накладных и камеры недоступны, а падение провайдера останавливает отгрузки. Мы связываем площадки шифрованным site-to-site туннелем на MikroTik с сегментацией, автоматическим резервным каналом и мониторингом — без подписочных облачных сервисов.

Почему это важно бизнесу

- Открытый RDP с паролем в интернете — прямой путь к шифровальщику и остановке всей 1С
- Час простоя канала на складе в пик отгрузок — десятки тысяч рублей упущенных отправлений
- Разовое внедрение на своём железе дешевле бессрочной подписки на облачные VPN-сервисы
- Единая сеть — сквозная работа 1С, печати и видеонаблюдения без переключения учёток
- Схема hub-and-spoke масштабируется на новые точки без перестройки архитектуры

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.21.5

Ветка long-term RouterOS для боевых роутеров; stable 7.23.2 сначала обкатываем на стенде

по докам MikroTik / наш стандарт

1420

MTU интерфейса WireGuard по умолчанию; MSS в mangle зажимаем до 1360, иначе 1С «подвисает»

WireGuard, help.mikrotik.com

25 с

persistent-keepalive на spoke за NAT/LTE: держит маппинг и даёт реконнект туннеля за 1–2 с

WireGuard, help.mikrotik.com

10 с × 3

Интервал netwatch (type=icmp) и порог thr-loss-count до переключения default route на LTE-резе…

Netwatch, help.mikrotik.com

32+

Минимальная длина PSK для IPsec IKEv2; для WireGuard — только пары ключей Curve25519

наш стандарт

modp2048

DH-группа в IPsec-профиле и pfs-group в proposal; шифрование aes-256-gcm с аппаратным ускорени…

IPsec, help.mikrotik.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Туннель WireGuard офис–склад на RouterOS 7

Что настраиваем

Пара RB5009UG+S+IN (офис, hub) + hAP ax3 (склад, spoke); подсети 10.10.10.0/24 и 10.10.20.0/24, транзитная 10.10.99.0/30

Как мы это делаем

1. Разводим адресные планы: офис 10.10.10.0/24, склад 10.10.20.0/24 — уходим с дефолтной 192.168.88.0/24 до подъёма туннеля
2. /interface wireguard add listen-port=13231; между площадками передаются только публичные ключи, приватный не покидает роутер
3. allowed-address у пира = /32 туннельного адреса + LAN удалённой стороны; маршрут /ip route dst-address=10.10.20.0/24 gateway на туннель
4. В mangle — change-mss 1360 на SYN через туннель, чтобы тяжёлые выборки 1С не зависали на MTU 1420
5. Firewall: accept udp/13231 только с IP второй площадки; forward между сайтами — allowlist по портам 1С, печати и RTSP, в конце drop

РЕЗУЛЬТАТ

Через туннель ходят 1С (веб-публикация и RDP), печать накладных на складские принтеры и RTSP-потоки камер в офисный регистратор. Реконнект при смене IP — 1–2 секунды, конфигурация из десятка строк читается любым нашим инженером за пять минут.

КЛЮЧЕВОЙ НЮАНС

allowed-address — это одновременно фильтр и cryptokey-маршрутизация: забытая в нём подсеть молча дропает трафик. Проверяем поле last-handshake у пира, а не только ping.

РЕАЛИЗАЦИЯ 2 ИЗ 3

IPsec IKEv2 — вариант для зоопарка железа и серых IP

Что настраиваем

Резервная схема: когда одна из сторон не MikroTik (pfSense, Keenetic, Cisco) или склад сидит за CGNAT провайдера

Как мы это делаем

1. Фаза 1: /ip ipsec profile — hash-algorithm=sha256, enc-algorithm=aes-256, dh-group=modp2048; фаза 2: proposal aes-256-gcm, pfs-group=modp2048
2. Peer с exchange-mode=ike2; при сером IP склада офис работает в passive=yes, склад — инициатор, NAT-T через udp/4500 поднимается автоматически
3. Identity с PSK от 32 символов, отдельный secret на каждый туннель; policy строго 10.10.10.0/24↔10.10.20.0/24, tunnel=yes
4. NAT bypass: правило srcnat accept по подсетям площадок ставим place-before=0 — выше masquerade, иначе policy не увидит трафик

РЕЗУЛЬТАТ

Туннель совместим с любым корпоративным железом и переживает CGNAT; расширение в hub-and-spoke — это добавление peer + policy на хабе без перестройки схемы. Мониторится штатно: счётчики policy и список installed-sa.

КЛЮЧЕВОЙ НЮАНС

Порядок NAT-правил решает всё: accept для межсайтового трафика обязан стоять выше masquerade. Диагностируем по счётчикам /ip ipsec policy, а не по «пинг не идёт».

РЕАЛИЗАЦИЯ 3 ИЗ 3

LTE-резерв и автопереключение канала на складе

Что настраиваем

hAP ax3 + USB LTE-модем: основной канал ether1, резерв lte1; контроль netwatch, алерты в Telegram

Как мы это делаем

1. Два default route: основной distance=1 с check-gateway=ping, резервный через lte1 с distance=10 — трафик уходит на LTE только при аварии
2. netwatch: host=1.1.1.1, type=icmp, interval=10s, thr-loss-count=3; проверочный пинг прибит маршрутом /32 к основному каналу, чтобы не «лечился» через LTE
3. down-script активирует резервный маршрут, передёргивает WireGuard-пира (disable/enable), чтобы туннель ушёл на LTE, и шлёт алерт через /tool fetch в Telegram; up-sc…
4. Раз в квартал — плановый тест: гасим ether1 руками и замеряем пересборку туннеля (норматив — до 60 секунд)

РЕЗУЛЬТАТ

Падение провайдера больше не останавливает отгрузки: туннель пересобирается на LTE меньше чем за минуту, дежурный получает алерт и видит момент возврата на основной канал. Резерв не живёт «молча» неделями.

КЛЮЧЕВОЙ НЮАНС

Failover без алертов опаснее его отсутствия: склад месяц работает через LTE, а основной канал лежит. Уведомление обязательно на оба события — и down, и up.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Одинаковые подсети с обеих сторон**
  Оба роутера из коробки раздают 192.168.88.0/24 — маршрутизация рушится. Разводим адресные планы (10.10.x.0/24) до подъёма туннеля.

- ✕ **Нет MSS-clamping — 1С «подвисает»**
  Пинг ходит, мелкие формы открываются, большие выборки виснут: MTU туннеля 1420. Ставим change-mss 1360 в mangle на SYN-пакеты.

- ✕ **Allow-all между площадками**
  Заражённая машина склада дотягивается до сервера 1С. В forward — allowlist по конкретным портам сервисов, финальное правило drop.

- ✕ **Masquerade съедает межсайтовый трафик**
  srcnat NAT-ит пакеты раньше IPsec-policy — туннель «пустой». Правило accept по подсетям площадок ставим place-before=0, выше masquerade.

- ✕ **Один PSK на все туннели**
  Компрометация одной точки открывает все. Отдельный secret на каждый peer и ротация ключей при смене подрядчика или инженера.

- ✕ **Управление роутером открыто с WAN**
  winbox/www/api из интернета — главный вектор атак на RouterOS. В /ip service ограничиваем address= LAN и нашим управляющим IP.

- ✕ **Прошивка не обновляется годами**
  Под RouterOS регулярно выходят CVE. Обновляем по ветке long-term раз в квартал и не забываем firmware RouterBOARD после апдейта ОС.

- ✕ **Туннель за NAT без keepalive**
  Маппинг NAT/LTE протухает — трафик идёт только в одну сторону. На spoke-пирах ставим persistent-keepalive=25s обязательно.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Site-to-site WireGuard/IPsec вместо RDP по белому IP, PSK от 32 символов
- Непересекающиеся подсети и firewall-allowlist между площадками
- Управление роутерами только из LAN/VPN: winbox, www и api закрыты с WAN

НОРМАЛЬНО

- VLAN-сегментация: гости, телефония и камеры отдельно от сети с 1С
- MSS-clamping 1360 и мониторинг туннеля с алертами в Telegram
- Плановое обновление RouterOS long-term + firmware раз в квартал

ХОРОШО

- LTE-резерв на складе: netwatch + recursive routing, failover до 60 секунд
- Hub-and-spoke под рост: подключение новой точки по шаблону за один день
- Мини-UPS на роутер и модем склада, runbook и схема сети в документации

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Складской оператор ходит в 1С через туннель, а не через RDP на белом IP?
- [ ] Подсети офиса и склада не пересекаются и зафиксированы в адресном плане?
- [ ] В firewall между площадками allowlist по сервисам, а не allow-all?
- [ ] Winbox, www и api недоступны из интернета на обоих роутерах?
- [ ] PSK длиннее 32 символов и уникален для каждого туннеля?
- [ ] MSS зажат в mangle — большие выборки 1С через туннель не подвисают?
- [ ] Приходит алерт при падении туннеля и при переходе на резервный канал?
- [ ] Резервный канал реально тестировался в последний квартал?
- [ ] RouterOS обновлён до актуальной long-term на обоих роутерах?
- [ ] Есть runbook: схема сети, адресный план, ключи в парольном менеджере?

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 и внедряем site-to-site VPN офис–склад под ключ: адресный план, VLAN, туннель, firewall
- Подбираем и поставляем железо MikroTik под нагрузку (hAP ax3 / RB5009) с запасом по шифрованию
- Настраиваем LTE-резерв с автопереключением и Telegram-алертами, проводим тест failover
- Переводим существующие связки с проброса RDP и облачных сервисов на собственный туннель
- Берём сеть на сопровождение: обновления RouterOS, мониторинг туннелей, актуальный runbook

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 — site-to-site конфигурация и параметры пиров (help.mikrotik.com — 7.x)

02 IPsec — profiles, proposals, policies, IKEv2 (help.mikrotik.com — 7.x)

03 Netwatch и failover через recursive routing (help.mikrotik.com — 7.x)

04 Firewall и NAT: srcnat, mangle change-mss (help.mikrotik.com — 7.x)

05 Bridge VLAN Filtering (help.mikrotik.com — 7.x)

06 Changelog RouterOS: stable 7.23.2 / long-term 7.21.5 (mikrotik.com — 2026)

07 Наш шаблон адресного плана и runbook филиальной сети (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.