Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративный VPN под регуляторными ограничениями

Как мы строим site-to-site IKEv2/IPsec и ZTNA, которые не рассыпаются под фильтрацией

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Связка «филиал — офис — облачная 1С» у большинства клиентов держится на одном туннеле через одного провайдера. Когда на транзите включается фильтрация, IKE-инициация уходит без ответа: SA не поднимается, ERP и файлы филиала недоступны, а мониторинг молчит — он смотрит на WAN-интерфейс, а не на туннель. Мы делаем связность функцией протокола, топологии и резерва, а не удачи.

Почему это важно бизнесу

- Простой филиала останавливает отгрузки и приём заказов: 40 рабочих мест без 1С стоят дороже годовой аренды второго канала.
- Диагностика «просто пропала связь» без телеметрии туннеля растягивается на дни: ищут у провайдера, а обрыв на транзите.
- Зарубежный VPS в роли VPN-хаба — единая точка отказа: его недоступность одномоментно гасит все площадки сразу.
- Перестройка топологии в режиме аварии всегда дороже плановой: миграция хаба и второй uplink в спешке идут по тройной цене.
- Нет описи подсетей, пиров и протоколов — нечего предъявить при проверке и не с чем идти к оператору связи.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

ike2

exchange-mode в /ip ipsec peer: заводское значение main — это IKEv1, IKEv2 включаем явно

RouterOS 7.24, /ip ipsec peer

8s

заводской dpd-interval живёт в /ip ipsec profile, а не в peer; dpd-maximum-failures при IKEv2…

RouterOS 7.24, /ip ipsec profile

1360

new-mss в mangle change-mss с protocol=tcp, tcp-flags=syn и ipsec-policy=out,ipsec — снимает з…

наш стандарт периметра

0s

заводской dpd_delay в connections.<conn> swanctl.conf: liveness выключен, ставим 30s

strongSwan 6.0, swanctl.conf

30 с

интервал icmpping и icmppingloss до хоста ЗА туннелем в мониторинге каждой площадки

Zabbix 7.0 LTS, simple checks

85 %

заводской thr-loss-percent в netwatch: до него хост считается живым; мы опускаем до 20 %

RouterOS 7.24, /tool netwatch

РЕАЛИЗАЦИЯ 1 ИЗ 3

Базовый туннель: IKEv2/IPsec на RouterOS 7 между площадками

Что настраиваем

Два периметровых роутера RouterOS 7.21.5 (long-term), сети 10.10.0.0/24 (офис) и 10.20.0.0/24 (филиал), статические WAN на обеих...

Как мы это делаем

1. /ip ipsec profile: hash-algorithm=sha256, enc-algorithm=aes-256, dh-group=modp2048, dpd-interval=8s — заводские sha1 и aes-128 меняем всегда, DPD настраивается имен...
2. /ip ipsec peer: exchange-mode=ike2 (заводское main — это IKEv1), address, local-address, порт остаётся штатный UDP 500 с NAT-T на 4500.
3. /ip ipsec proposal: auth-algorithms=sha256, enc-algorithms=aes-256-cbc, pfs-group=modp2048 вместо заводского modp1024, lifetime=30m; при переходе на aes-256-gcm обя...
4. /ip ipsec policy: tunnel=yes — заводское no даёт transport-режим; level=require заводской, но сверяем его печатью policy и installed-sa.
5. /ip ipsec identity: my-id и remote-id типа fqdn вместо auto, а на сертификатах auth-method=digital-signature с certificate и remote-certificate — значения rsa-signa...

РЕЗУЛЬТАТ

Туннель живёт на UDP 500/4500 — тех же портах, что использует любой корпоративный маршрутизатор. Реконнект после смены адреса проходит без ручного вмешательства, а факт падения фиксируется мониторингом за полминуты, а не по звонку бухгалтера из филиала.

КЛЮЧЕВОЙ НЮАНС

Заводские значения /ip ipsec — это IKEv1, sha1, aes-128 и pfs modp1024, и остаются они чаще, чем кажется. Перед сдачей построчно сверяем profile, peer, proposal, policy и identity с таблицами дефолтов в докуме...

РЕАЛИЗАЦИЯ 2 ИЗ 3

Резерв канала: netwatch, рекурсивные маршруты, второй uplink

Что настраиваем

Периметр каждой критичной площадки: два независимых uplink и одинаковый набор политик IPsec, привязанных к обоим адресам

Как мы это делаем

1. /tool netwatch type=icmp на адрес за шлюзом провайдера: interval=10s и packet-count=10 заводские, а thr-loss-percent опускаем с 85 до 20 при thr-avg=100ms.
2. up-script и down-script меняют distance в /ip route, а также local-address в /ip ipsec peer и sa-src-address в /ip ipsec policy, чтобы SA пересобралась с адреса жив…
3. Встречная сторона держит нас по DNS-имени в address пира и переустанавливает SA после смены нашего адреса без правки конфигурации.
4. Маршрут до пира делаем рекурсивным с check-gateway=ping и явным target-scope: падение канала снимает маршрут, а не оставляет чёрную дыру.
5. NAT: в chain=srcnat перед masquerade ставим action=accept на подсеть дальней площадки (или ipsec-policy=out,none в самом masquerade), иначе трафик натируется и не п…

РЕЗУЛЬТАТ

Переключение на резервный канал укладывается в 30-60 секунд и не требует участия инженера. Плановые работы основного провайдера перестают быть инцидентом: туннель поднимается на втором uplink, а в мониторинге остаётся только всплеск RTT.

КЛЮЧЕВОЙ НЮАНС

Netwatch с заводским thr-loss-percent=85 считает хост живым почти при полной потере пакетов: канал формально «работает», а IPsec уже развалился. Пороги по потерям и средней задержке задаём явно и сверяем с раз…

РЕАЛИЗАЦИЯ 3 ИЗ 3

ZTNA для людей: NetBird self-hosted на площадке в РФ

Что настраиваем

Management, Signal, Relay, Dashboard и Coturn на одном VPS в России; доступ сотрудников и подрядчиков поверх контура site-to-site

Как мы это делаем

1. Ставим NetBird 0.75+ за reverse proxy: наружу открыты только TCP 80 и 443 плюс UDP 3478 на Coturn; прямые порты 33073, 10000 и 33080 из варианта без прокси не публи…
2. В setup.env задаём NETBIRD_DOMAIN, NETBIRD_AUTH_OIDC_CONFIGURATION_ENDPOINT, NETBIRD_AUTH_CLIENT_ID и NETBIRD_AUTH_AUDIENCE — вход только через корпоративный IdP, M…
3. Setup-key выдаём на группу с ограниченным сроком и лимитом хостов; подрядчику — отдельная группа и политика ровно до одного порта одного сервера.
4. Где нужен минимальный стек без IdP, разворачиваем Headscale 0.29.3: policy.mode=file и policy.path на HuJSON с Grants (ACL помечены как legacy), DERP-сервер встроен…

РЕЗУЛЬТАТ

Удалённый доступ перестаёт быть ещё одним концентратором на периметре: подрядчик видит маршрут ровно до нужного порта, а отзыв доступа — это удаление ключа в панели, а не правка правил фаервола на роутере ночью.

КЛЮЧЕВОЙ НЮАНС

Coturn нужен именно как relay для площадок со сложным NAT: без доступного UDP 3478 часть клиентов молча деградирует. Долю relay-сессий держим в дашборде как отдельный показатель здоровья.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **exchange-mode оставлен заводским**
  В /ip ipsec peer дефолт main — это IKEv1. Ставим exchange-mode=ike2 явно и подтверждаем версию печатью /ip ipsec active-peers print.

- ✕ **DPD ищут в /ip ipsec peer**
  dpd-interval и dpd-maximum-failures — свойства /ip ipsec profile. Правим профиль, помня, что при IKEv2 dpd-maximum-failures игнорируется, работает то…

- ✕ **Политика без tunnel=yes**
  Заводское tunnel=no даёт transport-режим: политика вроде есть, трафик между сетями не инкапсулируется. Проверяем /ip ipsec policy print и installed-s…

- ✕ **dpd_delay=0s на strongSwan**
  В swanctl.conf liveness по умолчанию выключен. Ставим dpd_delay=30s в секции connections, а dpd_action=restart — в children, где его дефолт clear.

- ✕ **Общий PSK на все пиры**
  Ключ не отзывается точечно и живёт годами. На узлах с несколькими пирами переходим на auth-method=digital-signature с сертификатами своего CA.

- ✕ **Мониторится WAN, а не туннель**
  Интерфейс up, SA нет, алерта нет. Заводим icmpping до адреса на дальней стороне туннеля и контроль числа installed-sa.

- ✕ **VPN-хаб на зарубежной площадке**
  Одна точка терминации становится общим отказом для всех филиалов. Хаб переносим в РФ, а прямые туннели филиал-филиал держим резервом.

- ✕ **MTU и MSS не подогнаны**
  Оверхед ESP плюс отфильтрованный ICMP type 3 code 4 дают зависание сессий 1С и SMB. Клампим MSS по tcp-flags=syn и проверяем ping с флагом DF.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- IKEv2/IPsec на UDP 500/4500, sha256 и aes-256, dh-group не ниже modp2048
- В каждой политике tunnel=yes, level=require сверен по installed-sa
- Проверка icmpping до хоста за туннелем с интервалом 30 секунд
- Схема адресации и выгрузка конфигурации периметра в одном месте

НОРМАЛЬНО

- dpd-interval задан явно и симметрично в /ip ipsec profile на обеих сторонах
- Второй uplink с netwatch и рекурсивным маршрутом, сходимость до 60 секунд
- Аутентификация пиров через digital-signature с сертификатами своего CA
- Алерты по потере SA и росту RTT в Telegram дежурному инженеру

ХОРОШО

- ZTNA-слой на NetBird или Headscale для сотрудников и подрядчиков
- VPN-хаб на площадке в РФ, прямые туннели филиал-филиал как резерв
- Ежеквартальные учения: гашение primary uplink с замером сходимости
- Опись подсетей, пиров и протоколов в NetBox, ревизия при каждом изменении

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Все site-to-site туннели подняты по IKEv2 на UDP 500/4500, а не на нестандартных портах?
- [ ] В /ip ipsec policy у каждой политики выставлен tunnel=yes, а level=require подтверждён по installed-sa?
- [ ] Профиль и proposal отличаются от заводских: sha256 и aes-256 вместо sha1 и aes-128, pfs-group выше modp1024?
- [ ] DPD задан явно в профиле с обеих сторон, а не оставлен в дефолте (8s у MikroTik, 0s у strongSwan)?
- [ ] У каждой критичной площадки есть второй uplink и хотя бы раз проверенный сценарий переключения?
- [ ] Мониторинг проверяет ping до хоста ЗА туннелем, а не только состояние WAN-интерфейса?
- [ ] Точки терминации VPN размещены на площадках в РФ и имеют статические адреса или DNS-имя?
- [ ] Есть ли актуальная опись: подсети, адреса пиров, протоколы, ответственный за сеть?
- [ ] MSS-клампинг настроен по protocol=tcp и tcp-flags=syn, большие пакеты 1С и SMB проходят туннель?
- [ ] Доступ подрядчика выдаётся до конкретного сервиса и отзывается одним действием?

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 действующих туннелей: profile, peer, proposal, policy, DPD, MSS и сверка с дефолтами вендора
- Проектирование и настройка site-to-site IKEv2/IPsec на MikroTik, pfSense, strongSwan
- Второй uplink и автоматический failover с протоколом замера времени сходимости
- Развёртывание ZTNA на NetBird или Headscale с подключением к корпоративному IdP
- Мониторинг туннелей в Zabbix 7.0 LTS и алерты в Telegram по потере SA

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 RouterOS: IPsec — profile, peer, proposal, policy, identity (manual.mikrotik.com — 7.24)

02 RouterOS: Netwatch — типы проб, пороги, up/down-script (manual.mikrotik.com — 7.24)

03 RouterOS: IP Routing — check-gateway, target-scope, рекурсия (manual.mikrotik.com — 7.24)

04 strongSwan: swanctl.conf — dpd_delay, dpd_action, rekey_time, mobike (docs.strongswan.org — 6.0)

05 Zabbix: Simple checks — icmpping, icmppingloss, icmppingsec (zabbix.com — 7.0 LTS)

06 Zabbix: шаблон Mikrotik by SNMP, templates/net/mikrotik/mikrotik_snmp (git.zabbix.com — 7.0)

07 NetBird: Self-hosted guide — компоненты, порты, setup.env и OIDC (docs.netbird.io — 0.75+)

08 Headscale: Policy (Grants), policy.mode и встроенный DERP (headscale.net — 0.29.3)

09 ITfresh: шаблон описи подсетей, пиров и протоколов в NetBox (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.