Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Аудит периметра при DPI: какие протоколы выживают в 2026

Замер живучести VPN, RDP, 1С-облака и почты юрлица, перевод на устойчивый транспорт

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Каналы до 1С-облака, RDP-шлюза, банк-клиента и почты юрлица идут через транзитные сети с глубокой инспекцией трафика. Деградация приходит незаметно: туннель пересобирается каждые полчаса, крупные пакеты гибнут на ретрансмите, браузер ждёт таймаута QUIC и откатывается в TCP. Мы замеряем периметр инструментально и переводим рабочие сервисы на транспорт, который стабильно доходит.

Почему это важно бизнесу

- Простой удалённого доступа к 1С и складу останавливает отгрузки и приём документов у всего отдела, а не у одного рабочего места
- Разрывы туннеля каждые 20-40 минут рвут сеансы RDP и клиент-банка: платежи и отчётность уезжают на следующий день
- Недоставленная почта юрлица по SMTP — это пропущенные счета, требования ФНС и претензии контрагентов
- Без замеров вина перекладывается между провайдером, подрядчиком и оборудованием, а простой оплачивает бизнес
- Нестабильный транспорт маскируется под «1С тормозит»: деньги уходят на апгрейд серверов, который не помогает

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

6.0.1

strongSwan в Debian 13 stable: fragmentation и mobike там по умолчанию = yes

по докам strongSwan 6.0

500/4500

UDP-порты IKE и NAT-T: держим открытыми и мониторим отдельными проверками

RFC 7296 / RFC 3948

1360

MSS на клампинге: замеренный MTU пути 1400 минус 20 байт IP и 20 байт TCP

наш стандарт

30 с

dpd_delay в swanctl.conf: по умолчанию 0s, то есть DPD выключен — включаем явно

по докам strongSwan 6.0

20%

{$ICMP_LOSS_WARN}: штатный порог шаблона, с него канал считаем деградировавшим

Zabbix 7.0 LTS, шаблон ICMP Ping

443/3391

TCP/UDP шлюза удалённых рабочих столов: RDP в HTTPS, UDP держим управляемым

по докам Microsoft RDS

Дни 1-2: инструментальный замер периметра

Что настраиваем

Пограничный роутер, оба WAN (оптика и LTE-резерв), станции офиса до 50 PM и все внешние сервисы компании

Как мы это делаем

1. Снимаем топологию: модель и версию прошивки роутера, таблицу маршрутов, NAT, состав VLAN, список внешних сервисов — 1С-облако, RDP-шлюз, банк-клиенты, SMTP/IMAP
2. Проверяем рабочие домены: openssl s_client -connect host:443 -servername host -tls1_3, фиксируем время рукопожатия, цепочку сертификатов и стабильность повторов
3. Ищем реальный MTU пути: ping -M do -s <размер> и tracepath до каждого сервиса, отдельно с оптики и с LTE-резерва
4. Строим профиль потерь и задержек: mtr --tcp --port 443 -c 300 по каждому каналу, параллельно icmppingloss и icmppingsec в Zabbix
5. Сводим замеры с журналом инцидентов клиента за две недели по часам: видно окно деградации, а не размытое «иногда тормозит»

РЕЗУЛЬТАТ

На выходе таблица «сервис — канал — час — успешность». По ней видно, что именно проседает: транспорт, оборудование или сам сервис. Разговор с провайдером идёт цифрами, а решения по перестройке периметра принимаются по замеру, а не по ощущениям сисадмина.

КЛЮЧЕВОЙ НЮАНС

Замер обязателен на обоих каналах и в разное время суток: деградация транспорта почти всегда привязана к часам пик, а разовая проверка вечером рисует идеальную картину.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Корпоративный VPN: IKEv2/IPsec как основной транспорт

Что настраиваем

Концентратор strongSwan 6.0.1 на Debian 13 в DMZ либо роль RRAS на Windows Server 2022; клиенты — ноутбуки и смартфоны

Как мы это делаем

1. В swanctl.conf держим fragmentation = yes и mobike = yes: в ветке 6.x это значения по умолчанию, проверяем явно, чтобы их не выключили при миграции
2. Задаём dpd_delay = 30s и rekey_time = 4h; dpd_timeout на IKEv2 не действует — обрыв ловят штатные таймауты повторной передачи IKEv2
3. Профили: proposals = aes256gcm16-prfsha384-ecp384, esp_proposals = aes256gcm16-ecp384, сертификаты своего CA, EAP — только вторым фактором
4. На RRAS ставим EnableServerFragmentation=1 (REG_DWORD) в HKLM\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\Ikev2, перезапускаем RemoteAccess и RasMan
5. Заводим 500/UDP и 4500/UDP в мониторинг отдельными проверками и следим за числом пересборок туннеля на каждого клиента

РЕЗУЛЬТАТ

Удалённый доступ к 1С, файловым шарам и терминальным сессиям живёт на одном предсказуемом протоколе с внятной диагностикой. Переход сотрудника с Wi-Fi на LTE не рвёт сеанс, а крупные пакеты аутентификации не теряются на узком участке маршрута.

КЛЮЧЕВОЙ НЮАНС

IKE-фрагментация (RFC 7383) и MOBIKE (RFC 4555) нужны с обеих сторон: односторонняя настройка даёт режим «подключается, но иногда» — самый дорогой в диагностике.

РЕАЛИЗАЦИЯ 3 ИЗ 3

MTU, MSS и прикладной транспорт рабочих сервисов

Что настраиваем

Пограничный MikroTik RouterOS 7.x, доменные GPO станций, шлюз удалённых рабочих столов и почтовый шлюз юрлица

Как мы это делаем

1. Клампим MSS: /ip firewall mangle add chain=forward out-interface-list=WAN protocol=tcp tcp-flags=syn action=change-mss new-mss=1360 tcp-mss=1361-65535
2. Приводим MTU внешнего интерфейса к замеренному значению пути и проверяем, что ICMP type 3 code 4 не режется на периметре
3. Отключаем QUIC на станциях: QuicAllowed=0 (REG_DWORD) в HKLM\Software\Policies\Google\Chrome и в HKLM\Software\Policies\Microsoft\Edge
4. RDP наружу публикуем только через шлюз: 443/TCP обязателен, 3391/UDP — управляемая опция, которую отключаем при потерях
5. Почту держим на 465/TCP (implicit TLS) и 587/TCP (STARTTLS) по RFC 8314, MTA-STS кладём в TXT _mta-sts и в /.well-known/mta-sts.txt

РЕЗУЛЬТАТ

Уходят плавающие симптомы: обрыв больших выгрузок из 1С, зависание печати через RDP, письма с вложениями, которые «отправляются вечно». Прикладной трафик укладывается в реальный MTU пути и не зависит от того, доходят ли ICMP-сообщения PMTUD.

КЛЮЧЕВОЙ НЮАНС

MSS-клампинг лечит только TCP. Для UDP-сервисов уменьшаем полезную нагрузку на стороне приложения либо переводим их на TCP-транспорт, иначе симптом вернётся на первом крупном пакете.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Диагностика одним ping до 8.8.8.8**
  ICMP проходит там, где рвётся TCP-сессия с полезной нагрузкой. Проверяем сам сервис: mtr --tcp --port 443 и openssl s_client до рабочего домена.

- **MTU оставлен по умолчанию 1500**
  На PPPoE (1492) и внутри туннелей реальный MTU пути ниже. Крупные пакеты гибнут на ретрансмите и выглядят как «1С тормозит», а не как обрыв связи.

- **Ставка на автоопределение PMTUD**
  ICMP type 3 code 4 часто фильтруется в транзите, и окно не подстраивается. Клампим MSS явно на пограничном роутере, а не надеемся на PMTUD.

- **IKE-фрагментация только на сервере**
  При односторонней настройке крупный IKE_AUTH с сертификатом теряется. Держим fragmentation = yes на концентраторе и проверяем поддержку у клиентов.

- **dpd_timeout как страховка на IKEv2**
  В swanctl.conf эта опция на IKEv2 не действует, работают штатные таймауты повторной передачи. Живость peer задаём через dpd_delay, по умолчанию он 0s.

- **QUIC включён по умолчанию**
  Браузер тратит время на попытку HTTP/3 и откатывается в TCP уже после таймаута. На корпоративных станциях выключаем QuicAllowed через GPO.

- **RDP опубликован напрямую в интернет**
  Это и подбор пароля, и нестабильный транспорт без диагностики. Ставим шлюз удалённых рабочих столов на 443/TCP с сертификатом и NLA.

- **Замер сделан один раз вечером**
  Деградация транспорта привязана к часам пик. Оставляем постоянные проверки в Zabbix и смотрим историю за две недели, а не единичный снимок.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Актуальный список внешних сервисов: адреса, порты, владельцы, часы работы
- MSS-клампинг на WAN и MTU интерфейса по реально замеренному значению
- Мониторинг каждого сервиса, а не только шлюза: net.tcp.service и web.page.get
- Резервный канал связи, проверенный переключением под рабочей нагрузкой

НОРМАЛЬНО

- IKEv2/IPsec с fragmentation и MOBIKE вместо самодельных туннелей
- RDP только через шлюз на 443/TCP с сертификатом и обязательным NLA
- QuicAllowed=0 политикой на станциях, рабочий трафик идёт по TCP
- Почта юрлица на 465/587 с TLS, настроены SPF, DKIM и DMARC

ХОРОШО

- Плановый замер периметра раз в полгода с отчётом по каждому сервису
- Дашборд icmppingsec и icmppingloss по критичным сервисам в Zabbix
- Отдельный канал управления для админа, независимый от основного VPN
- Автопереключение на резервный WAN по check-gateway с замером сходимости

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли актуальный список внешних сервисов компании с портами и ответственными?
- [ ] Замерен ли реальный MTU пути до 1С-облака и до VPN-концентратора с каждого WAN?
- [ ] Настроен ли MSS-клампинг на пограничном роутере для трафика в сторону WAN?
- [ ] Включены ли IKE-фрагментация и MOBIKE на VPN-концентраторе и на всех клиентах?
- [ ] Публикуется ли RDP только через шлюз на 443/TCP с сертификатом и проверкой NLA?
- [ ] Отключён ли QuicAllowed на станциях, откуда ходят в рабочие веб-сервисы?
- [ ] Мониторится ли доступность каждого критичного сервиса, а не только интернет-канала?
- [ ] Проверялось ли переключение на резервный канал под реальной рабочей нагрузкой?
- [ ] Сохраняется ли история замеров по часам, чтобы видеть деградацию в пиковое время?
- [ ] Посчитана ли стоимость часа простоя удалённого доступа и почты юрлица?

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).

- Замеряем периметр за 3 рабочих дня: топология, MTU, потери, доступность сервисов по часам
- Разворачиваем IKEv2/IPsec-концентратор с сертификатами и профилями для Windows, iOS и Android
- Настраиваем MTU и MSS на роутере и политики станций, убираем плавающие обрывы в 1С и RDP
- Публикуем RDP через шлюз на 443/TCP и приводим почту юрлица к TLS с SPF, DKIM и DMARC
- Ставим мониторинг каналов и сервисов в Zabbix с оповещением раньше жалоб пользователей

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 swanctl.conf: connections.<conn> — fragmentation, mobike, dpd_delay (docs.strongswan.org — 6.0)

02 Firewall Mangle: действие change-mss и матчер tcp-mss (help.mikrotik.com — 7.x)

03 Ports that are used by Remote Desktop Services (learn.microsoft.com — WS2022)

04 [MS-IKEE] IKEv2 Fragmentation; [MS-RRASM] реестр RemoteAccess (learn.microsoft.com — 2024)

05 Chrome Enterprise Policy List: QuicAllowed (chromeenterprise.google — 2026)

06 RFC 7383 (фрагментация IKEv2), RFC 4555 (MOBIKE) (rfc-editor.org — 2006-2014)

07 RFC 8314 (Implicit TLS), RFC 8461 (MTA-STS) (rfc-editor.org — 2018)

08 Шаблон ICMP Ping: icmppingloss, {$ICMP_LOSS_WARN} (zabbix.com — 7.0 LTS)

Основано на официальной документации продуктов и нашей практике внедрения.