Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Kill-switch для 1С и банк-клиента при падении VPN

Трёхуровневая блокировка приложений без туннеля: MikroTik policy-routing, GPO Firewall, наш аг…

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Гибридная команда работает с 1С, банк-клиентом и CRM через WireGuard до офиса. Туннель падает молча — ноутбук уходит в открытый Wi-Fi, трафик банк-клиента идёт через чужого провайдера: DNS и SNI светятся, а компания об этом не узнаёт. Мы строим kill-switch: без живого туннеля критичные приложения физически не работают — блокировка на трёх независимых уровнях.

Почему это важно бизнесу

- Банк-клиент в открытом Wi-Fi — утечка платёжных данных доверителей; регламент и 152-ФЗ требуют защищённого канала для мобильных РМ
- Разрыв VPN незаметен пользователю: трафик тихо уходит мимо туннеля, инцидент никто не фиксирует
- Один инцидент с деньгами клиента дороже всего проекта: договорная ответственность по NDA и удар по репутации фирмы
- Ручной контроль 28 ноутбуков в офисе, дома и в командировках невозможен — работает только автоматика

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

180 с

Reject-After-Time протокола: handshake старше 180 с — туннель мёртв, агент гасит процессы

по докам wireguard.com

25 с

PersistentKeepalive на каждом пире: NAT-state оператора живёт ~30 с, keepalive держит канал

по докам wireguard.com

5 с

Интервал опроса wg.exe show all latest-handshakes агентом — быстрая реакция без нагрузки

наш стандарт

7.1+

RouterOS с нативным WireGuard: mangle mark-routing + таблица wg-only — слой №1 на роутере

по докам help.mikrotik.com

1380

MTU туннеля вместо 1420 + change-mss в mangle: убирает фрагментацию и тормоза 1С на 4G/LTE

наш стандарт

1.0

WireGuard for Windows на клиентах (драйвер WireGuardNT): служба автозапуска туннеля + wg.exe д...

WireGuard for Windows

РЕАЛИЗАЦИЯ 1 ИЗ 3

Слой 1: policy-routing на MikroTik — маршрут умирает вместе с туннелем

Что настраиваем

Офисный CCR2004-16G-2S+, RouterOS 7.16: трафик к серверу 1С, банк-клиенту и CRM — только через интерфейс wireguard1

Как мы это делаем

1. /routing/table add name=wg-only fib; в mangle chain=prerouting — mark-routing по dst-address сервера 1С и address-list банка
2. Default route 0.0.0.0/0 в таблице wg-only только через wireguard1: интерфейс упал → маршрут исчез → пакеты дропаются
3. Address-list банка динамический: скрипт в /system/scheduler раз в час резолвит DNS-имена CDN и дополняет список IP
4. Persistent-keepalive=25 на пирах; MTU 1420→1380 и change-mss — для командировочных на 4G
5. Резерв для сетей, режущих UDP: второй туннель на 443/TCP через udp2raw, конфиг выдаём мобильным сотрудникам

РЕЗУЛЬТАТ

Kill-switch работает даже там, где ноутбук вне нашего контроля: без живого туннеля у трафика к чувствительным сервисам физически нет маршрута. Падение канала — мгновенный дроп без таймаутов и «полудоступности», поведение детерминировано в обе стороны.

КЛЮЧЕВОЙ НЮАНС

В доках RouterOS смотрим Policy Routing: mark-routing вешается до routing decision (chain=prerouting), а таблицу создаём с флагом fib — без него метка есть, а маршрутизации нет.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Слой 2: GPO Windows Firewall — правила на exe с привязкой к туннелю

Что настраиваем

Домен клиента, GPO KillSwitch-GPO на OU ноутбуков; охват — 4 критичных exe: 1cv8c, банк-клиент, cons, Bitrix24

Как мы это делаем

1. New-NetFirewallRule -Program <exe> -Direction Outbound -Action Allow с привязкой к интерфейсу туннеля: allow работает только через WireGuard
2. Парное Block-правило на те же exe для остальных профилей и интерфейсов — default deny для всего чувствительного списка
3. Правила кладём в -PolicyStore домена (GPO): локальный админ их не снимет, слияние с локальной политикой запрещаем
4. Исключение для печати: 1cv8c.exe → принт-сервер 192.168.10.5:9100 разрешён во всех профилях, иначе печать из 1С падает

РЕЗУЛЬТАТ

Даже если роутер сбоит или сотрудник сидит в чужой сети, файрвол не выпустит трафик 1С и банк-клиента мимо туннеля. Политика доезжает автоматически на весь парк, пользователь снять её не в состоянии.

КЛЮЧЕВОЙ НЮАНС

По докам learn.microsoft.com правило с -InterfaceAlias жёстко привязано к имени интерфейса: фиксируем имя туннеля в конфиге клиента — после переустановки WireGuard alias меняется и allow-правило молча умирает.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Слой 3: PowerShell-агент — контроль handshake и стоп процессов

Что настраиваем

Служба на каждом ноутбуке: PowerShell под NT AUTHORITY\SYSTEM, обёртка nssm 2.24, лог C:\ProgramData\ITfresh\killswitch.log

Как мы это делаем

1. Каждые 5 с читаем wg.exe show all latest-handshakes; handshake старше 180 с (Reject-After-Time) — туннель мёртв
2. Гасим процессы списка: сначала мягкий Stop-Process, через 10 с — принудительный -Force; каждое действие в лог с меткой времени и PID
3. Раскатка GPO startup-script'ом: копия агента и nssm из NETLOGON + регистрация службы; обновление — перезапись в NETLOGON и рестарт
4. Задача на Power Event перезапускает туннель при выходе из сна — лечит ноутбуки, не восстанавливающие peer после 8 ч простоя

РЕЗУЛЬТАТ

Последний рубеж, независимый от GPO и роутера: даже при несработавшей политике процессы 1С и банк-клиента живут после последнего handshake не дольше ~185 с (порог 180 с + опрос 5 с). Лог даёт разбор каждого срабатывания — время, процесс, возраст handshake — и превращает споры «у меня 1С у...

КЛЮЧЕВОЙ НЮАНС

wg show отдаёт latest-handshake в epoch-секундах, а 0 означает «handshake ещё не было» — этот случай обрабатываем отдельно с grace-таймером, иначе агент неверно судит о свежеподнятом туннеле.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **AllowedIPs уже, чем реальный трафик**
  Сервер отвечает с NAT-адреса вне AllowedIPs — WireGuard молча дропает ответ. Прописываем все подсети ответа, вплоть до /16, и проверяем с обеих сторон

- ✕ **CDN банка меняет IP-адреса**
  Статичный address-list устаревает после ребаланса CDN. Держим динамический список: scheduler-скрипт резолвит имена раз в час, плюс маски по AS банка

- ✕ **Оператор режет длинные UDP-сессии**
  Мобильные сети классифицируют долгий UDP как P2P и рвут его. Резервный туннель 443/TCP через udp2raw + инструкция переключения для командировочных

- ✕ **Туннель не встаёт после сна**
  После долгого Modern Standby peer не находится, хотя интерфейс жив. Задача на Power Event перезапускает туннель при каждом пробуждении

- ✕ **Firewall блокирует локальную печать**
  Default deny для 1С режет и путь до офисного принтера. Явное allow-исключение: exe → IP принт-сервера, порт 9100, во всех профилях

- ✕ **Один уровень защиты — всегда лазейка**
  GPO может не примениться, роутер — деградировать, файрвол — быть выключен. Три автономных слоя дублируют друг друга без общих точек отказа

- ✕ **Handshake=0 у свежего туннеля**
  Сразу после подъёма интерфейса handshake нулевой — наивный парсер убьёт приложения на старте. Ноль обрабатываем как отдельное состояние с grace-тайме...

- ✕ **Keepalive не задан на пирах**
  NAT-state у провайдера истекает за ~30 с тишины — туннель «флапает» несколько раз в день. PersistentKeepalive=25 и на клиенте, и на роутере

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- WireGuard с PersistentKeepalive=25 и автозапуском службы на всех ноутбуках
- Утверждённый список критичных exe: банк-клиент, 1С, CRM, правовая система
- Правила Windows Firewall: allow только через туннель, block в остальных профилях

НОРМАЛЬНО

- Policy-routing на роутере: таблица wg-only, default route только через туннель
- Динамический address-list банковских сервисов: резолв по расписанию + AS-маски
- GPO-доставка правил файрвола с запретом локального переопределения
- MTU 1380 + mss-clamping для мобильных клиентов на 4G/LTE

ХОРОШО

- Агент-служба: контроль handshake каждые 5 с, стоп процессов при простое >180 с
- Резервный канал 443/TCP (udp2raw) для сетей, где оператор режет UDP
- Перезапуск туннеля по Power Event при выходе ноутбука из сна
- Лог срабатываний kill-switch + ежемесячный разбор причин падений VPN

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Утверждён ли письменно список приложений, которым запрещено работать без VPN?
- [ ] Исчезает ли маршрут трафика критичных приложений при падении VPN-интерфейса (policy-routing)?
- [ ] Задан ли PersistentKeepalive=25 на всех пирах — и на клиентах, и на роутере?
- [ ] Доставлены ли правила файрвола через GPO так, что локальный админ их не отключит?
- [ ] Обновляется ли address-list банковских CDN автоматически, а не разово при внедрении?
- [ ] Проверено ли восстановление туннеля после 8+ часов сна ноутбука?
- [ ] Есть ли резервный TCP-канал для сетей, где оператор режет UDP?
- [ ] Пишется ли лог каждого срабатывания kill-switch: время, процесс, возраст handshake?
- [ ] Прогнан ли пилот на 2-3 ПК с эмуляцией обрыва (disable интерфейса туннеля) и проверкой всех трёх слоёв?

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 трёхуровневый kill-switch под ключ: MikroTik + GPO Firewall + агент, за 5 рабочих дней
- Разворачиваем WireGuard на MikroTik: пир на сотрудника, keepalive, MTU-тюнинг, TCP-резерв через udp2raw
- Пишем и сопровождаем агент контроля туннеля: служба, лог срабатываний, раскатка через GPO на весь парк
- Разбираем инциденты по логам: кто, когда и почему пытался работать без VPN — отчёт руководителю

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 — RouterOS Documentation (help.mikrotik.com — 7.x)

02 Policy Routing / Mangle (mark-routing) — RouterOS (help.mikrotik.com — 7.x)

03 wg(8), wg-quick(8) — wireguard-tools man pages (wireguard.com — 2026)

04 WireGuard Protocol: таймеры rekey/reject (whitepaper) (wireguard.com — 2020)

05 New-NetFirewallRule — модуль NetSecurity (learn.microsoft.com — 2025)

06 Windows Firewall: развёртывание правил через GPO (learn.microsoft.com — 2025)

07 NSSM — the Non-Sucking Service Manager (nssm.cc — 2.24)

08 Наш шаблон KillSwitch-GPO + агент killswitch.ps1 (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.