Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Site-to-site IPsec на Linux: три города в одну

Full-mesh IKEv2 на strongSwan 6.0 (swanctl/vici): PKI, филиал за CGNAT, failover и мониторинг

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Филиалы работают с 1С и файлами головного офиса по RDP через открытый интернет: медленно, соединения рвутся, порт 3389 открыт всему миру. Мы объединяем три площадки в единую защищённую сеть site-to-site IPsec на strongSwan: AES-256-GCM, аутентификация по X.509, автоматический failover. Бездействие — это перехват учёток, брутфорс RDP и простой филиалов при каждом сбое канала.

Почему это важно бизнесу

- Открытый RDP наружу — прямой вектор брутфорса и шифровальщиков; одна украденная учётка кладёт 1С всей компании
- Тормоза 1С у филиалов — часы простоя проектировщиков и бухгалтерии каждый день, оплаченные из ФОТ
- Свой шлюз на Linux — без ежегодных лицензий коммерческих VPN-железок; хватает мини-ПК или виртуалки
- Full-mesh убирает единую точку отказа: обмен между филиалами не зависит от шлюза головного офиса

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

6.0.x

strongSwan: новые внедрения только на swanctl.conf/vici — стек ipsec.conf (stroke) устарел

docs.strongswan.org

4 ч / 1 ч

rekey_time IKE_SA и CHILD_SA — дефолты swanctl, укорачиваем только child на слабых каналах

swanctl.conf, defaults

30 с

dpd_delay на всех шлюзах: проверка живости пира; с start_action=trap туннель встаёт сам

наш стандарт

UDP 4500

encap = yes на филиале за CGNAT: ESP заворачивается в NAT-T, проброс протокола 50 не нужен

docs.strongswan.org

20 с

charon.keep_alive — NAT-keepalive, чтобы трансляция провайдера не выбрасывала «тихий» туннель

strongswan.conf, default

<2

порог Zabbix-триггера: на узле full-mesh из трёх городов два IKE_SA; меньше двух — алерт

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Оффлайн-PKI и сертификаты X.509 вместо PSK

Что настраиваем

Корневой CA — на отдельной машине вне контура; ключи и серты — на трёх шлюзах (Москва, СПб, Казань)

Как мы это делаем

1. pki --gen --type rsa --size 4096 и pki --self --ca --lifetime 3652: корневой CA живёт только офлайн, на шлюзы уезжает лишь ca-cert
2. Шлюзам выпускаем серты pki --issue --lifetime 1825 с SAN вида gw-msk.corp.local и флагом serverAuth; identity в конфиге = FQDN из SAN
3. Раскладка: ключ в /etc/swanctl/private, серт в x509, CA в x509ca; права 600, владелец root; загрузка swanctl --load-creds
4. В connections: local.auth = pubkey, local.certs = gw-msk.pem; CA подхватывается из x509ca автоматически, PSK-секции удаляем совсем
5. До включения PKI сверяем время: chrony на каждом шлюзе, иначе IKE отвергнет серт как «ещё не действительный»

РЕЗУЛЬТАТ

Компрометация одного филиала не раскрывает общий секрет: у каждого шлюза свой приватный ключ, отзыв — перевыпуском серта без остановки остальных туннелей. Замена сертификатов — плановая, по календарю lifetime, а не по инциденту.

КЛЮЧЕВОЙ НЮАНС

PSK допускаем только как экспресс-тест связности на один день. По доке swanctl.conf приватные ключи подхватываются из каталога private/ сами — отдельной строки «: RSA» из ipsec.secrets больше нет.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Full-mesh IKEv2 в swanctl.conf на три узла

Что настраиваем

Три туннеля МСК—СПб, МСК—Казань, СПб—Казань; шлюзы — виртуалка в HQ и мини-ПК на Debian в филиалах

Как мы это делаем

1. connections: version = 2, mobike = no, proposals = aes256gcm16-prfsha384-ecp384 — для AEAD-шифра в IKE обязательно указываем PRF
2. children: local_ts/remote_ts списками подсетей (10.10.0.0/24,10.11.0.0/24 ↔ 10.20.0.0/24), esp_proposals = aes256gcm16-ecp384 — PFS на каждом rekey
3. start_action = trap + dpd_delay = 30s: политика ставится в ядро сразу, туннель поднимается первым же пакетом и сам после обрывов
4. Правки применяем swanctl --load-all без рестарта демона; статус — swanctl --list-sas, счётчик ESTABLISHED уходит в Zabbix
5. Маршруты рабочим местам раздаём DHCP-опцией 121 (classless static routes) — новая подсеть не требует обхода компьютеров

РЕЗУЛЬТАТ

Трафик между филиалами идёт напрямую, канал головного офиса — не узкое место и не единая точка отказа. Четвёртый город добавляется тремя секциями connections по нашему шаблону, без перепроектирования сети.

КЛЮЧЕВОЙ НЮАНС

mobike = no для статичных шлюзов и непересекающиеся пары local_ts/remote_ts — иначе трафик утекает не в тот child. Синтаксис proposals сверяем по таблице в доке swanctl.conf, а не по памяти.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Филиал за CGNAT, failover и мониторинг

Что настраиваем

Казанский шлюз без белого IP + резервный провайдер в HQ; Zabbix-агент на всех трёх шлюзах

Как мы это делаем

1. Филиал — всегда инициатор: remote_addrs = белый IP HQ, encap = yes — ESP сразу в UDP 4500, CGNAT провайдера не мешает
2. На стороне HQ remote_addrs = %any, пира узнаём по identity из сертификата — серый IP филиала может меняться хоть ежедневно
3. charon.keep_alive = 20s держит трансляцию NAT; обрыв в IKEv2 фиксируют retransmit-таймауты charon (dpd_timeout — только IKEv1)
4. Failover в HQ: systemd-timer раз в 60 с пингует удалённый LAN, при молчании — swanctl --terminate и --initiate резервного connection
5. Zabbix UserParameter: swanctl --list-sas | grep -c ESTABLISHED; на узле mesh их два, триггер <2 — алерт в Telegram нам и админу клиента

РЕЗУЛЬТАТ

Филиал за серым IP работает полноценным узлом сети без покупки статики. Обрыв основного канала HQ превращается в паузу до минуты вместо простоя до приезда инженера; о падении любого SA мы узнаём раньше пользователей.

КЛЮЧЕВОЙ НЮАНС

dpd_timeout в IKEv2 не действует — живость определяют retransmit_tries/retransmit_timeout из strongswan.conf. Это прямое указание документации: не тратим время на настройку мёртвого параметра.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

× **Часы шлюзов разошлись**
Сдвиг в минуты — и IKE отвергает сертификат как «ещё не действительный». Ставим chrony на каждый шлюз и проверяем офсет до внедрения PKI.

× **MASQUERADE поверх VPN-подсетей**
Старое NAT-правило маскирует трафик в туннель под внешний IP: SA есть, пакеты в никуда. Исключение для удалённых подсетей — выше MASQUERADE.

× **MTU и фрагментация внутри ESP**
Провайдер режет пакеты больше ~1400: SSH живёт, а 1С и SMB виснут. Лечим TCPMSS --clamp-mss-to-pmtu в FORWARD и проверяем ping -M do -s.

× **PSK оставили в продакшене**
Общий секрет на все узлы: утечка с одного шлюза — компрометация всей сети. Только X.509 со своим ключом на узел; PSK — лишь для стартового теста.

× **dpd_timeout в IKEv2**
Параметр действует только в IKEv1 — в IKEv2 обрыв фиксируют retransmit-таймауты charon. Настраиваем dpd_delay и не ждём эффекта от мёртвой опции.

× **Пересечение адресных планов**
Одинаковые 192.168.0.0/24 в двух офисах ломают маршрутизацию до всякого IPsec. Перед стартом перенумеровываем LAN в непересекающиеся подсети.

× **Остатки ipsec.conf рядом со swanctl**
Два стека грузят дублирующиеся conn — случайные конфликты SA. Мигрируем целиком на swanctl.conf, пакеты со stroke-интерфейсом убираем.

× **DNS не знает соседний офис**
Туннель есть, но 1С «не видит сервер»: имена чужого домена не резолвятся. Настраиваем условный форвардинг зон на DNS каждого филиала.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- IKEv2 + AES-256-GCM, туннели хотя бы hub-and-spoke через головной офис
- X.509 вместо PSK, корневой CA отдельно от шлюзов, chrony на всех узлах
- MSS clamping и закрытие RDP из интернета сразу после запуска туннелей

НОРМАЛЬНО

- Full-mesh между всеми площадками, start_action = trap, dpd_delay = 30s
- Филиалы за NAT — encap = yes и аутентификация по identity, а не по IP
- Маршруты клиентам — DHCP Option 121, счётчик SA — в мониторинг

ХОРОШО

- Второй провайдер в HQ и автоматический failover по systemd-timer
- Алерты по каждому SA в Telegram, журнал charon — в центральный syslog
- Регламент ротации сертификатов по lifetime и тест восстановления раз в квартал
- Документация схемы и обучение штатного админа процедурам диагностики

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Прямой RDP/SMB между офисами через интернет закрыт, доступ только внутри туннелей?
- [ ] Аутентификация шлюзов — сертификаты X.509, а не общий PSK?
- [ ] Корневой CA хранится вне шлюзов, приватные ключи — с правами 600?
- [ ] Туннель сам поднимается после обрыва (проверяли выдёргиванием канала)?
- [ ] Адресные планы всех офисов не пересекаются?
- [ ] MSS clamping включён — большие пакеты 1С и SMB ходят без зависаний?
- [ ] Число ESTABLISHED SA снимается мониторингом и алертит при падении?
- [ ] Время на шлюзах синхронизировано NTP и офсет контролируется?
- [ ] Новый филиал добавляется без ручной правки маршрутов на рабочих местах?
- [ ] Даты истечения сертификатов известны и есть напоминание о ротации?

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 каналов и адресных планов, схема full-mesh или hub-and-spoke под ваши офисы
- Разворачиваем PKI и шлюзы strongSwan под ключ: swanctl-конфиги, NAT-T, failover
- Подключаем мониторинг туннелей в Zabbix с алертами в Telegram 24/7
- Переносим 1С и файлообмен внутрь VPN, закрываем RDP из интернета
- Обучаем вашего админа: логи charon, процедуры восстановления, документация

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, children, secrets (docs.strongswan.org — 6.0)

02 Migration from ipsec.conf (stroke) to swanctl (vici) (docs.strongswan.org — 6.0)

03 NAT Traversal — encap, charon.keep_alive (docs.strongswan.org — 6.0)

04 pki — выпуск CA и сертификатов шлюзов (docs.strongswan.org — 6.0)

05 Retransmission — retransmit_tries/timeout (IKEv2) (docs.strongswan.org — 6.0)

06 RFC 3442 — Classless Static Route Option (код 121) (rfc-editor.org — 2002)

07 Наш шаблон site-to-site + Zabbix vpn.established (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.