Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IPsec IKEv2 на strongSwan: рабочая схема

Site-to-site туннели hub-and-spoke на swanctl.conf с PKI: как мы связываем филиалы 20–50 РМ

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Филиалы гоняют 1С, файловый обмен и кассовое ПО через открытый интернет: RDP наружу, тормоза межофисного трафика, риск перехвата. Мы решаем это site-to-site IPsec IKEv2 на strongSwan: шифрованные туннели между офисами с аутентификацией по сертификатам. Без этого — утечки данных, простой филиала при каждом обрыве и невозможность централизовать сервисы в HQ.

Почему это важно бизнесу

- RDP и файловый обмен через открытый интернет — прямой риск утечки баз и остановки работы шифровальщиком
- Без стабильного шифрованного канала нельзя централизовать 1С и кассовое ПО — филиалы живут на разрозненных копиях
- Обрыв туннеля без автовосстановления — остановка продаж в точке; watchdog сжимает простой с часов до минут
- strongSwan бесплатен: ни лицензий на VPN, ни дорогих железок — шлюз филиала это компактный x86-мини-ПК

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

6.0.x

актуальная ветка strongSwan: только swanctl.conf/VICI, legacy ipsec.conf не используем

по докам strongswan.org

AES-256-GCM

esp_proposals = aes256gcm16: AEAD-шифр для ESP, разгружается AES-NI, без отдельного HMAC

IKEv2 Cipher Suites, strongSwan

30 с

dpd_delay: пустые INFORMATIONAL для контроля живости пира, dpd_action = restart на CHILD SA

swanctl.conf + наш стандарт

24 ч

rekey_time IKE SA в нашем шаблоне; у CHILD SA дефолтный 1 ч — смена ключей без разрыва

swanctl.conf, дефолты strongSwan

1360

MSS clamping: ESP добавляет ~60–80 байт overhead, без клампа большие TCP-пакеты молча зависают

наш стандарт

4096/2048

RSA: 4096 бит у корневого CA (ключ офлайн), 2048 бит у шлюзов со сроком 730 дней и SAN

pki, docs.strongswan.org

РЕАЛИЗАЦИЯ 1 ИЗ 3

Шлюзы филиалов и корпоративный PKI

Что настраиваем

Debian-шлюз в каждом офисе (HQ + филиалы), офлайн-CA на управляющей машине ITfresh

Как мы это делаем

1. Ставим strongswan, strongswan-pki и charon-плагины; включаем net.ipv4.ip_forward, гасим ICMP-redirects через /etc/sysctl.d/90-vpn.conf
2. Открываем UDP/500, UDP/4500 и протокол ESP на периметре; проверяем, что MASQUERADE не накрывает IPsec-префиксы
3. pki --gen/--self: корневой CA RSA-4096 на 3650 дней; ключ CA сразу уходит в холодный бэкап, на шлюзах его нет
4. pki --issue: сертификаты шлюзов RSA-2048 на 730 дней с SAN (FQDN + IP) и флагом serverAuth
5. Раскладка по swanctl: CA в /etc/swanctl/x509ca, сертификат в x509, приватный ключ в private с правами 600

РЕЗУЛЬТАТ

Каждый шлюз аутентифицируется сертификатом, PSK нигде не живёт; добавление нового филиала — выпуск пары ключей и один блок в swanctl.conf, без пересмотра секретов на всём парке.

КЛЮЧЕВОЙ НЮАНС

Компрометация одного филиала не роняет доверие сети: отзываем один сертификат и публикуем CRL. Ключ CA держим офлайн — это единственный артефакт, который нельзя восстановить процедурой.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Hub-and-spoke в swanctl.conf

Что настраиваем

HQ — хаб со статическим IP, 2–4 филиала — spoke; меж-филиальный трафик идёт транзитом через HQ

Как мы это делаем

1. connections: version = 2, proposals = aes256-sha256-modp2048 для IKE, esp_proposals = aes256gcm16 — списки идентичны на обеих сторонах
2. auth = pubkey, id — FQDN шлюза; у филиала с динамическим IP local_addrs = %any, на HQ соответственно remote_addrs = %any
3. За NAT провайдера ставим encap = yes (форс UDP-инкапсуляции на 4500); mobike включён по умолчанию — смена IP без разрыва
4. start_action = start, close_action = start, dpd_action = restart — туннель поднимается и переустанавливается сам
5. В remote_ts филиала включаем и сеть HQ, и сети других филиалов — транзит между филиалами без full-mesh

РЕЗУЛЬТАТ

Одна точка конфигурации и мониторинга; новый филиал добавляется блоком в swanctl.conf на HQ. После обрывов провайдера туннели переустанавливаются автоматически, без заявок в поддержку.

КЛЮЧЕВОЙ НЮАНС

Секреты выносим в отдельный файл swanctl-каталога с ограниченными правами; дефолты сверяем с докой — rekey_time IKE SA 4 ч, CHILD SA 1 ч — и меняем осознанно, а не копипастой.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг, watchdog и бэкап конфигурации

Что настраиваем

Все шлюзы; метрики — в наш Zabbix, копии конфигурации — в хранилище клиента и наш ДЦ

Как мы это делаем

1. swanctl --list-sas / --list-conns в скрипте-обвязке: число активных CHILD SA отдаём в Zabbix как item, триггер на ноль
2. vpn-watchdog.sh по systemd-таймеру раз в 5 минут: ping адреса в удалённой LAN, при потере — swanctl --terminate и --initiate по child
3. MSS clamping в iptables -t mangle/FORWARD: TCPMSS --set-mss 1360 для пакетов с политикой ipsec (-m policy --pol ipsec)
4. Ночной tar /etc/swanctl + /etc/strongswan.d с ротацией 30 дней и rsync в два независимых хранилища

РЕЗУЛЬТАТ

Обрывы каналов провайдера отрабатываются без инженера; падение туннеля видно в Zabbix раньше звонка клиента, восстановление шлюза с нуля из бэкапа — 20–30 минут.

КЛЮЧЕВОЙ НЮАНС

Пинговать надо адрес в удалённой LAN, а не внешний IP пира: внешний отвечает и при мёртвом CHILD SA. Глубокую диагностику ведём по journalctl, поднимая loglevel charon до 2–3.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Несовпадение крипто-предложений**
  «no proposal chosen» в логе: списки proposals/esp_proposals различаются на сторонах. Держим единый список в шаблоне и копируем на оба конца.

- ✕ **Разные форматы ID сторон**
  id «vpn-hq.x.ru» и «@vpn-hq.x.ru» — разные идентификаторы. Пишем FQDN одинаково на обеих сторонах и сверяем с SAN сертификата.

- ✕ **Забытый NAT-T на филиале**
  Филиал за NAT провайдера без encap = yes: ESP фильтруется, туннель живёт секунды. Форсим UDP-инкапсуляцию на порту 4500.

- ✕ **MASQUERADE поверх IPsec-префиксов**
  NAT на шлюзе переписывает адреса до применения IPsec-политики — трафик не попадает в туннель. Исключаем защищённые префиксы из MASQUERADE.

- ✕ **MTU и зависшие TCP-сессии**
  ESP-overhead ~60–80 байт: мелкие пакеты ходят, большие молча теряются. Ставим MSS clamping 1360 в mangle/FORWARD по политике ipsec.

- ✕ **Неотозванный сертификат филиала**
  Закрытый офис с живым сертификатом — легальный вход в сеть. При выводе узла отзываем сертификат, публикуем CRL и проверяем её на шлюзах.

- ✕ **Legacy ipsec.conf вместо swanctl**
  Старый stroke-интерфейс устарел и в 6.x не является основным. Новые внедрения делаем только на swanctl.conf + VICI, конфиги переносимы.

- ✕ **Права на ключи в /etc/swanctl/private**
  Приватный ключ с правами шире 600 — компрометация без взлома strongSwan. Проверяем права при раскладке и в бэкап-скрипте.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- IKEv2 + сертификаты вместо PSK уже с двух площадок
- AES-256-GCM в ESP и единый список proposals на всех узлах
- DPD 30 с и dpd_action = restart на каждом соединении
- UDP/500, UDP/4500 и ESP открыты; MASQUERADE не трогает IPsec-префиксы

НОРМАЛЬНО

- Hub-and-spoke с транзитом меж-филиального трафика через HQ
- MSS clamping 1360 и encap = yes для филиалов за NAT
- Watchdog по systemd-таймеру + туннели как items в Zabbix
- Ночной бэкап /etc/swanctl с ротацией и выгрузкой во внешнее хранилище

ХОРОШО

- Офлайн-CA, CRL и регламент отзыва сертификатов при выводе узла
- Route-based VTI + OSPF при 5+ филиалах вместо разрастания политик
- Резервный канал и MOBIKE — переключение провайдера без разрыва SA
- Квартальный тест восстановления шлюза из бэкапа с фиксацией времени

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Туннели подняты по IKEv2 с аутентификацией сертификатами, а не PSK?
- [ ] Списки proposals/esp_proposals идентичны на обеих сторонах каждого туннеля?
- [ ] Ключ корневого CA хранится офлайн и отсутствует на шлюзах?
- [ ] Для филиалов за NAT включён encap = yes и проходит UDP/4500?
- [ ] MASQUERADE исключает защищённые IPsec-префиксы?
- [ ] MSS clamping настроен — большие TCP-пакеты ходят через туннель?
- [ ] Падение туннеля видно в мониторинге раньше звонка пользователей?
- [ ] Watchdog сам переустанавливает CHILD SA при потере связности?
- [ ] Есть свежий бэкап /etc/swanctl и проверенная процедура восстановления шлюза?
- [ ] Прописан регламент отзыва сертификата и публикации CRL при закрытии площадки?

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 разворачиваем site-to-site IPsec на strongSwan под ключ: от адресации до сдачи документации
- Поднимаем корпоративный PKI: офлайн-CA, выпуск и отзыв сертификатов шлюзов, публикация CRL
- Подключаем туннели в наш Zabbix: DPD, watchdog, алерты дежурному инженеру
- Мигрируем legacy ipsec.conf/IKEv1 на swanctl + IKEv2 без остановки работы филиалов
- Сопровождаем: обновления strongSwan, перевыпуск сертификатов, разбор обрывов с провайдерами

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 IKEv2 Cipher Suites (proposals) (docs.strongswan.org — 6.0)

03 pki — выпуск ключей и сертификатов (docs.strongswan.org — 6.0)

04 NAT Traversal и MOBIKE (RFC 4555) (docs.strongswan.org — 6.0)

05 strongswan.conf и уровни логирования charon (docs.strongswan.org — 6.0)

06 Наш шаблон шлюза филиала (Debian + swanctl) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.