Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Шифрование корпсети на 50 РМ: наша рабочая конфигурация

PKI на AD CS, TLS 1.3, IPsec IKEv2 на pfSense, SMB Encryption и BitLocker

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Мы приходим на площадку 50 РМ, где шифрование сложилось стихийно: TLS 1.0 на старом сервисе, самоподписанные сертификаты, шары без SMB Encryption, ноутбуки без BitLocker, туннель в облако рвётся по нескольку раз в день. Нестандартный handshake на транзитном оборудовании даёт плавающие обрывы, а в логах приложения причина не видна. Итог — простой 1С и данные в открытом виде.

Почему это важно бизнесу

- Рвущийся туннель в облако — это остановка 1С и отдела продаж, причём в логах приложения причина не видна вообще.
- Утечка чертежей или платёжных реквизитов с незашифрованной шары стоит дороже всей инфраструктуры и всплывает месяцами позже.
- Ноутбук без BitLocker — готовый инцидент с персданными: диск снимается и читается без пароля за считанные минуты.
- Самоподписанные сертификаты приучают сотрудников жать «Продолжить», и настоящий MITM пройдёт незамеченным.
- Плавающие обрывы у удалённых сотрудников съедают часы поддержки каждый месяц и списываются на «интернет плохой».

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

6.0.7

Ветка strongSwan на облачной стороне туннеля: конфигурация целиком в swanctl.conf

docs.strongswan.org, swanctl.conf 6.0

4h / 1h

Дефолтные rekey_time для IKE_SA и CHILD_SA; задаём явно, чтобы срок не плавал

*docs.strongswan.org, connections.**

1400

Maximum MSS для TCP через IPsec на pfSense — дефолт, от которого начинаем подбор

docs.netgate.com, Firewall & NAT

AES-256-GCM

Набор шифрования SMB 3.1.1 на шарах с базами 1С и конструкторскими файлами

learn.microsoft.com, Server 2022+

XTS-AES 256

Метод BitLocker на ноутбуках: по умолчанию система берёт XTS-AES 128, задаём GPO

learn.microsoft.com, BitLocker GPO

5.0.13003

Сертифицированная сборка КриптоПро CSP 5.0 R3 на местах под ГОСТ TLS и госпорталы

cryptopro.ru, КриптоПро CSP 5.0 R3

РЕАЛИЗАЦИЯ 1 ИЗ 3

PKI: офлайн Root CA и Enterprise Issuing CA в домене

Что настраиваем

Два Windows Server 2022 в домене AD DS: изолированная ВМ под корневой CA и рядовой сервер AD CS под выдачу

Как мы это делаем

1. Root CA поднимаем на изолированной ВМ без сети: StandaloneRootCA, RSA 4096, SHA-384, срок 10 лет; включаем раз в год под переподпись Issuing CA.
2. Issuing CA ставим командой Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA; CDP и AIA публикуем на внутреннем HTTP, а не только в LDAP.
3. Шаблоны: Computer, User с S/MIME, Web Server, отдельный шаблон под IKEv2 с Client и Server Authentication в EKU, Code Signing для внутренних ps1.
4. Автовыдачу включаем GPO «Certificate Services Client — Auto-Enrollment»; окно перевыпуска берётся из Renewal period шаблона, а не из желания админа.
5. CRL: период публикации и delta-CRL делаем короче окна ротации, результат проверяем на клиенте через certutil -verify -urlfetch, а не на самом CA.

РЕЗУЛЬТАТ

Сертификаты появляются на станциях сами, без заявок в поддержку. Отзыв доступа уволенному — одна запись в CRL вместо обхода 50 машин. Все последующие слои (TLS, IPsec, S/MIME) опираются на один корень доверия, и браузеры перестают ругаться на внутренние сервисы.

КЛЮЧЕВОЙ НЮАНС

В AD CS решают не алгоритмы, а публикация CDP/AIA и срок CRL: почти все инциденты «сертификат недействителен» — это недоступная точка распространения списка отзыва, а не слабый шифр.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Транспорт наружу: TLS 1.3 на парке, легаси за reverse-proxy

Что настраиваем

50 станций Windows 11 и серверы 2022 плюс nginx на периметре под внутренние сервисы без современного TLS

Как мы это делаем

1. GPO пишет ветку SCHANNEL\Protocols: TLS 1.0 и 1.1 — Enabled=0 и DisabledByDefault=1 в Client и Server, TLS 1.2 и 1.3 — наоборот.
2. Порядок наборов задаём в Cryptography\Configuration\SSL\00010002, параметр Functions: оставляем AEAD с ECDHE, убираем CBC, 3DES и RC4.
3. ECH (RFC 9849) в корпоративных браузерах выключаем политикой EncryptedClientHelloEnabled=0: он ломает фильтрацию по SNI и разбор обрывов по логам.
4. Легаси не переписываем: TLS 1.3 по RFC 8446 терминирует nginx на периметре, дальше локальный сегмент с доступом по firewall-правилу.
5. Госпорталы — отдельным маршрутом: КриптоПро CSP 5.0 R3 и Chromium-Gost на трёх-четырёх местах бухгалтерии, остальному парку ГОСТ не ставим.

РЕЗУЛЬТАТ

Одинаковый TLS-профиль на всём парке: нет машины, которая тихо договорилась на 1.0 с CBC. Старые внутренние панели живут за прокси и больше не блокируют отключение слабых протоколов. ФНС и госпорталы открываются с выделенных мест, без ГОСТ-провайдера на каждой станции.

КЛЮЧЕВОЙ НЮАНС

Наборы TLS 1.3 зафиксированы стандартом: политика порядка cipher suites управляет только TLS 1.2. И SCHANNEL правим всегда парой Client+Server, иначе сервис ломается односторонне.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Туннели: site-to-site офис↔облако и IKEv2 для удалённых

Что настраиваем

pfSense 2.8.1 на периметре офиса, strongSwan 6.0.7 на облачной ВМ, 12 удалённых сотрудников по IKEv2

Как мы это делаем

1. Phase 1 на pfSense: IKEv2, AES256-GCM, DH group 20 (ECP-384), Lifetime 28800; на второй стороне срок ставим примерно на 10% больше.
2. Аутентификация — сертификаты нашего Issuing CA вместо общего PSK: Peer identifier сверяем с SAN, CRL подключаем в Cert. Manager.
3. MOBIKE в Phase 1 включаем руками: по умолчанию он выключен, и туннель к мобильному клиенту не переживает смену адреса.
4. DPD оставляем 10 секунд и 5 промахов; на стороне strongSwan это dpd_delay, у которого дефолт 0s — то есть проверок живости нет вообще.
5. PMTU лечим Maximum MSS 1400 и IKE-фрагментацией по RFC 7383: длинный IKE_AUTH с сертификатами перестаёт зависать на LTE-канале.

РЕЗУЛЬТАТ

Туннель переживает переключение WAN и смену адреса у мобильных клиентов: MOBIKE переносит SA без переустановки соединения. Удалённые конструкторы работают по сертификату, без общих паролей. Падение CHILD_SA видно в Zabbix раньше, чем о нём напишет пользователь.

КЛЮЧЕВОЙ НЮАНС

Сначала сверяем таблицы допустимых значений на обеих сторонах, потом ищем «несовместимость». Половина проблем — это разъехавшиеся DH-группа, lifetime и признак фрагментации, а не сам стек.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **MOBIKE на pfSense выключен по умолчанию**
  Phase 1 поднимается, но при смене адреса клиента SA не переносится и туннель уходит в реконнект. Включаем явно в Advanced Options фазы 1.

- ✕ **DPD не настроен — обрыв видят только люди**
  У strongSwan dpd_delay по умолчанию 0s: проверок живости нет, мёртвая SA висит до таймаута. Ставим 10 секунд и 5 промахов с обеих сторон.

- ✕ **RejectUnencryptedAccess переводят в $false**
  По умолчанию он $true и клиент без SMB 3 просто не пускается. Ради NAS и МФУ параметр снимают — и шифрование шары становится необязательным.

- ✕ **Мандат шифрования SMB валит NAS и МФУ**
  В Windows 11 24H2 и Server 2025 клиент можно обязать шифровать всё исходящее. Устройства без SMB 3 отваливаются: сначала инвентаризация, потом мандат.

- ✕ **BitLocker шифрует XTS-AES 128**
  Без политики метод по умолчанию — XTS-AES 128. Меняем GPO до первого шифрования: на зашифрованном диске смена метода требует полной расшифровки.

- ✕ **IKE-фрагментация не согласована**
  Сертификаты на 4096 бит раздувают IKE_AUTH. Ищем в логе charon FRAGMENTATION_SUPPORTED; нет его — правим сторону, где фрагментация отключена.

- ✕ **Ноутбук пропустил окно перевыпуска**
  Автообновление идёт внутри Renewal period шаблона. Машина, месяц не видевшая домен, приезжает с просроченным сертификатом — перевыпускаем руками.

- ✕ **ГОСТ-провайдер раскатывают на весь парк**
  КриптоПро нужен трём-четырём местам с госпорталами. Массовая установка мешает обычному TLS-стеку и добавляет поддержке работы на ровном месте.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Отключить TLS 1.0 и 1.1 политикой SCHANNEL на станциях и серверах
- Включить SMB Encryption на шарах с базами 1С и документами
- BitLocker XTS-AES 256 на ноутбуках, ключи восстановления — в AD
- Убрать самоподписанные сертификаты с внутренних веб-сервисов

НОРМАЛЬНО

- Двухуровневая PKI: офлайн Root CA плюс Enterprise Issuing CA
- Автовыдача шаблонов Computer, Web Server и IKEv2 через GPO
- Site-to-site IKEv2 на сертификатах вместо общего PSK
- Легаси-сервисы вынести за reverse-proxy с TLS 1.3

ХОРОШО

- S/MIME для договорной и конструкторской переписки
- Мониторинг CHILD_SA, доступности CRL и сроков сертификатов
- Запрет нешифрованного SMB после инвентаризации устройств
- Выделенные места с КриптоПро CSP 5.0 R3 и Chromium-Gost

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли у вас внутренний CA или сертификаты выпускаются вручную и живут до первой жалобы?
- [ ] Отключены ли TLS 1.0 и 1.1 в ветках Client и Server, а не только на веб-сервере?
- [ ] Знаете ли вы прямо сейчас, какие сетевые шары отдают документы без шифрования?
- [ ] Каким методом зашифрованы ноутбуки — XTS-AES 256 или дефолтным XTS-AES 128?
- [ ] Лежат ли ключи восстановления BitLocker в AD и читаются ли они оттуда на практике?
- [ ] Site-to-site туннель поднят на сертификатах или на PSK, который знают уволившиеся?
- [ ] Видит ли мониторинг падение CHILD_SA раньше, чем о нём сообщит бухгалтерия?
- [ ] Попадёт ли сертификат сотрудника в CRL в день увольнения, а не через квартал?
- [ ] Проверяли ли вы доступность CDP и AIA с рабочей станции, а не только с сервера CA?
- [ ] Включены ли MOBIKE и DPD на обеих сторонах туннеля или только на одной?

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).

- Разворачиваем двухуровневую PKI на Windows Server 2022 и настраиваем автовыдачу шаблонов
- Приводим TLS-профиль парка к единому виду по GPO и выносим легаси за reverse-proxy
- Строим site-to-site IKEv2 офис-облако на сертификатах и удалённый доступ сотрудникам
- Включаем SMB Encryption и BitLocker XTS-AES 256 с депонированием ключей в Active Directory
- Ставим мониторинг туннелей, CRL и сроков сертификатов, ведём ежемесячное сопровождение

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, rekey_time, dpd_delay, fragmentation (docs.strongswan.org — 6.0.7)

02 IPsec Phase 1: Key Exchange, DH Group, MOBIKE, DPD; Maximum MSS (docs.netgate.com — 2.8)

03 TLS registry settings и Cipher Suites in TLS/SSL (Schannel SSP) (learn.microsoft.com — 2026)

04 SMB security: шифрование SMB 3.1.1 и RejectUnencryptedAccess (learn.microsoft.com — 2026)

05 Configure BitLocker: метод шифрования и депонирование ключей в AD (learn.microsoft.com — 2026)

06 RFC 8446 (TLS 1.3) и RFC 9849 (Encrypted Client Hello) (datatracker.ietf.org — 2026)

07 КриптоПро CSP 5.0 R3: ГОСТ TLS и браузер Chromium-Gost (cryptopro.ru — 5.0 R3)

08 Наш шаблон: карта шифрования площадки и матрица шаблонов CA (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.