Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Защита удалённого доступа к серверам офиса: наш контур 2026

WireGuard-периметр, SSH-hardening по OpenSSH 10.x, MFA на RDP и Wazuh-мониторинг — как мы это...

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сотрудникам нужен доступ к 1С, файлам и терминалу из дома — и в типовом офисе это решено пробросом порта наружу. Такой узел сканеры находят за часы, дальше — подбор пароля из утечек, шифрование баз и простой на недели. Мы закрываем периметр наглухо: единственная точка входа — VPN, поверх него — ключи, второй фактор и централизованный контроль событий входа.

Почему это важно бизнесу

- Шифрование базы 1С — это остановка продаж, зарплаты и отчётности; восстановление без бэкапа занимает недели
- Открытый RDP/SSH — вопрос не «если», а «когда»: автоматический перебор идёт по всем адресам провайдеров непрерывно
- Утечка клиентской базы — претензии по 152-ФЗ и потеря доверия заказчиков
- Правильный контур не мешает людям: подключение к VPN занимает 2-3 секунды, скорость — как по проводу

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

10.4

OpenSSH: целевая версия sshd; с 9.8 механизм PerSourcePenalties штрафует брутфорс на уровне де...

по докам openssh.com

51820/UDP

Единственный открытый порт наружу — WireGuard; RDP, SSH и порты 1С доступны только внутри тунн...

наш стандарт

25 с

PersistentKeepalive для пиров за NAT/LTE — туннель не «засыпает» у мобильных сотрудников

по докам wireguard.com

3/600/86400

fail2ban jail [sshd]: maxretry/findtime/bantime — бан на сутки после 3 неудач за 10 минут

наш шаблон jail.local

4.14.x

Wazuh: агенты на Windows/Linux + syslog с MikroTik; наш набор правил на брутфорс и шифровальщи...

по докам wazuh.com

3-2-1

Схема бэкапа: 3 копии, 2 носителя, 1 вне офиса — облачная копия с Object Lock, без права удале...

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Периметр: WireGuard на MikroTik RouterOS 7

Что настраиваем

Граница офиса — роутер MikroTik (RouterOS 7.x); наружу остаётся один UDP-порт, админка и сервисы — только из LAN и VPN

Как мы это делаем

1. /ip firewall filter, chain=input: accept established,related → accept udp/51820 → accept из interface-list LAN → drop всё остальное
2. /interface wireguard add name=wg-office mtu=1420 listen-port=51820; ключевая пара Curve25519 генерируется на роутере, приватный ключ его не покидает
3. Каждому сотруднику — свой peer с allowed-address=/32: увольнение закрывается удалением одной записи, а не перевыпуском общего конфига
4. /ip service: telnet, ftp, www, api отключаем; winbox и ssh — только с address-list управления; UPnP выключен
5. Для мобильных клиентов в конфиге пира persistent-keepalive=25 — туннель живёт за NAT сотового оператора

РЕЗУЛЬТАТ

Внешний сканер видит устройство без единого открытого TCP-порта: WireGuard не отвечает на пакеты без валидного ключа. Удалённка работает на скорости канала, подключение из приложения — 2-3 секунды, батарею телефона туннель не сажает.

КЛЮЧЕВОЙ НЮАНС

Порядок правил input критичен: accept established,related — первым, иначе каждый пакет сессии проходит весь фильтр и CPU роутера ложится; drop — строго последним, после accept для LAN.

РЕАЛИЗАЦИЯ 2 ИЗ 3

SSH-hardening: ключи, sshd_config, fail2ban

Что настраиваем

Linux-узлы офиса: сервер бэкапов, IP-АТС Asterisk, файловый сервер Samba; целевой стек OpenSSH 10.x

Как мы это делаем

1. Drop-in /etc/ssh/sshd_config.d/00-hardening.conf: PasswordAuthentication no, PermitRootLogin no, AllowGroups ssh-users, MaxAuthTries 3, ClientAliveInterval 300
2. Ключи только ed25519 (ssh-keygen -t ed25519), раздача через ssh-copy-id; пароли глушим лишь после проверенного входа по ключу из второй сессии
3. PerSourcePenalties (включён по умолчанию с OpenSSH 9.8): штрафы authfail/invaliduser гасят перебор ещё до срабатывания fail2ban
4. fail2ban jail [sshd]: maxretry=3, findtime=600, bantime=86400, ignoreip = LAN + VPN-подсеть
5. Перед рестартом — sshd -t (валидация конфига); systemctl restart ssh выполняем при открытой запасной сессии

РЕЗУЛЬТАТ

Подбор пароля к SSH невозможен в принципе — парольная аутентификация выключена, а сам порт виден только из VPN-подсети. fail2ban за месяц банит 0 адресов: снаружи стучаться просто некому, и это — критерий правильной архитектуры.

КЛЮЧЕВОЙ НЮАНС

sshd_config работает по first-match: выигрывает первое совпадение, а drop-in из sshd_config.d читаются раньше основного файла — override именуем 00-*, иначе его перебьёт дефолт дистрибутива.

РЕАЛИЗАЦИЯ 3 ИЗ 3

RDP: RD Gateway, MFA и мониторинг Wazuh

Что настраиваем

Терминальный сервер 1С и RDSH на Windows Server 2019/2022; вход бухгалтерии из дома

Как мы это делаем

1. RDP наружу не публикуем вовсе; для бухгалтерии — роль Remote Desktop Gateway: RDP заворачивается в HTTPS/443, доступ по политикам CAP/RAP на группы AD
2. NLA обязательна на всех RDSH: через GPO фиксируем уровень безопасности SSL/TLS (реестр SecurityLayer=2) и UserAuthentication=1
3. Второй фактор: TOTP-провайдер (RFC 6238) на входе в терминал; секреты — в приложении-аутентификаторе, аварийные коды — в сейфе клиента
4. Учётку Administrator переименовываем через GPO; заводим ловушку с именем Administrator без прав — любая попытка входа в неё даёт мгновенный алерт
5. Wazuh 4.14 agent на RDSH и DC: серии событий 4625, создание учёток 4720/4732, сессии TerminalServices 21/25 — алерты в Telegram дежурному

РЕЗУЛЬТАТ

Бухгалтерия работает из дома через HTTPS-шлюз со вторым фактором, ни один RDP-порт не опубликован. Каждая сессия фиксируется: кто, когда, с какого IP и к какой машине — вопрос «кто заходил в 1С ночью» решается за минуту по журналу.

КЛЮЧЕВОЙ НЮАНС

RDG сам по себе не отменяет пароль как единственный фактор — без TOTP шлюз лишь переносит точку перебора на порт 443. Поэтому MFA включаем до открытия внешнего доступа, а не «потом донастроим».

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Порт 3389 наружу «на один день»**
  Временный проброс забывают закрыть. У нас NAT-правило живёт только с комментарием-датой, а еженедельный внешний скан периметра ловит забытое

- ✕ **Нестандартный порт как защита**
  Сканеры проверяют весь диапазон 1-65535. Перенос порта лишь убирает шум в логах — доступ всё равно даём только из VPN-подсети

- ✕ **Один VPN-конфиг на весь офис**
  Общий ключ нельзя отозвать точечно. Делаем peer на человека с allowed-address /32 — увольнение закрывается удалением одной записи

- ✕ **MTU по умолчанию в туннеле**
  За PPPoE/LTE пакеты фрагментируются: туннель «висит», RDP рвётся. На WireGuard-интерфейсе фиксируем mtu=1420

- ✕ **fail2ban без ignoreip**
  Три опечатки бухгалтера — и офисный IP в бане на сутки. В jail.local вносим LAN и VPN-подсеть, бан работает только по внешним адресам

- ✕ **AllowTcpForwarding для всех**
  Скомпрометированный ключ превращает сервер в прокси внутрь сети. Где проброс не нужен — ставим AllowTcpForwarding no в sshd_config

- ✕ **Бэкап виден с сервера по SMB**
  Шифровальщик обходит сетевые пути наравне с дисками. Третья копия — в S3 с Object Lock (compliance), сервисная учётка без права delete

- ✕ **Anydesk, поставленный «самому себе»**
  Облачные агенты пробивают периметр исходящим каналом. Блокируем их домены на роутере, установку — через SRP/AppLocker; взамен даём VPN + RDG

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Ни одного RDP/SSH/веб-админки наружу: снаружи открыт только UDP-порт WireGuard
- SSH только по ключам ed25519: PasswordAuthentication no, PermitRootLogin no
- Персональный VPN-peer каждому сотруднику, отзыв при увольнении в тот же день
- Бэкап 1С по схеме 3-2-1, третья копия недоступна на запись с серверов

НОРМАЛЬНО

- fail2ban + PerSourcePenalties на Linux; учётка-ловушка Administrator на Windows
- RD Gateway с NLA и вторым фактором (TOTP) для терминального доступа
- Запрет Anydesk/TeamViewer: AppLocker/SRP плюс блок доменов на роутере
- Ежеквартальный тестовый restore базы 1С на стенде

ХОРОШО

- Wazuh 4.14: агенты на серверах, syslog с роутера, алерты в Telegram дежурному
- Регулярный внешний скан периметра со сверкой против эталонного списка портов
- Object Lock (immutable) на облачной копии бэкапа, ретенция от 30 дней
- Отдельная VPN-подсеть и отдельные учётки для административного доступа

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Снаружи открыт только порт VPN — и это подтверждает свежий внешний скан, а не «мы так помним»?
- [ ] Вход по SSH возможен только по ключу, а PermitRootLogin выключен на всех Linux-узлах?
- [ ] У каждого сотрудника персональный VPN-peer и есть процедура отзыва при увольнении?
- [ ] RDP к серверу 1С недоступен из интернета даже по нестандартному порту?
- [ ] На терминальном входе есть второй фактор (TOTP), а не только пароль?
- [ ] Попытка входа в учётку-ловушку Administrator поднимает алерт дежурному?
- [ ] Логи VPN-подключений и RDP-сессий собираются централизованно и хранятся не меньше 90 дней?
- [ ] Третья копия бэкапа физически недоступна для удаления с офисных серверов?
- [ ] Восстановление базы 1С из бэкапа реально проверялось за последний квартал?
- [ ] Сотрудники не могут сами поставить Anydesk/TeamViewer на рабочие станции?

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 периметра: внешний скан, инвентаризация пробросов, письменный отчёт с планом закрытия
- WireGuard на MikroTik/pfSense под ключ: конфиги сотрудникам, инструктаж, регламент отзыва доступа
- SSH/RDP-hardening серверов и MFA на терминальный доступ (RD Gateway + TOTP)
- Wazuh-мониторинг с нашим набором правил и алертами в Telegram, реагирует дежурный инженер
- Бэкап 3-2-1 с immutable-копией в облаке и квартальными тестами восстановления

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 OpenSSH 10.4 Release Notes; man sshd_config (PerSourcePenalties) (openssh.com — 10.4)

02 WireGuard: Quick Start, Cryptokey Routing, известные ограничения MTU (wireguard.com — 2026)

03 RouterOS Documentation — WireGuard, IP/Firewall/Filter, Services (help.mikrotik.com — 7.x)

04 Wazuh Documentation — Ruleset, Agent enrollment, Integrations (documentation.wazuh.com — 4.14)

05 Remote Desktop Services — Remote Desktop Gateway, CAP/RAP (learn.microsoft.com — 2025)

06 fail2ban — jail.conf/jail.local reference (github.com/fail2ban/fail2ban — 1.1)

07 Наш шаблон: чек-лист закрытия периметра офиса до 50 PM (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.