Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IP-камеры в офисе: изолируем от рабочей сети

VLAN 802.1Q для камер, локальный NVR и WireGuard — без китайских облаков и открытых портов

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Камеры, воткнутые в общую офисную сеть, — это десяток неуправляемых Linux-устройств с дефолтными паролями рядом с 1С и клиентскими документами. Боты находят их за 24–48 часов: камера продолжает писать видео и параллельно участвует в DDoS, а поток через P2P-облако уходит на чужие серверы. Мы решаем это сегментацией: VLAN, локальный NVR и VPN-доступ — без замены самих камер.

Почему это важно бизнесу

- Видеопоток с переговорной и столов с документами уходит через облачные серверы вендора — утечка, которую никто не контролирует
- Заражённая камера — плацдарм внутри сети: с неё сканируют и атакуют 1С, файловый сервер и бухгалтерию
- Участие в DDoS с IP компании — блокировки от провайдера и попадание адреса в чёрные списки
- Без архива 30 суток и уведомления сотрудников запись бесполезна для страховой и как доказательство

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

VLAN 30

Выделенный сегмент камер 192.168.30.0/24 — без маршрута в интернет и в рабочие VLAN 10/20

наш стандарт

7.x

RouterOS с bridge vlan-filtering=yes: один бридж, VLAN-таблица, hw-offload на свитч-чип

по докам help.mikrotik.com

0.17.x

Стабильная ветка Frigate — open-source NVR: запись по движению, роли admin/viewer

по докам docs.frigate.video

16+

Минимальная длина пароля камеры; учёт в KeePass: IP, MAC, серийник, дата проверки прошивки

наш стандарт

30 сут

Минимальная глубина видеоархива, которую закладываем при расчёте дисков NVR

наш стандарт

10–18 ГБ

Сутки записи одной 4 Мп камеры при H.265+ — 8 камер на 30 дней укладываются в 3–4 ТБ

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Сегментация камер: bridge VLAN filtering на MikroTik

Что настраиваем

Периметр офиса до 50 РМ: роутер MikroTik (RouterOS 7.x), управляемый PoE-коммутатор 802.1Q, 4–16 камер

Как мы это делаем

1. Один bridge с vlan-filtering=yes; камерные порты — untagged pvid=30, аплинк к PoE-свитчу — tagged; членство фиксируем в /interface/bridge/vlan
2. Интерфейс vlan30 (192.168.30.1/24), DHCP-пул только для камер со static lease по MAC — чужое устройство адрес не получит
3. Firewall: drop всего forward из VLAN30 в WAN и офисные сегменты; accept только камера→NVR (RTSP 554/tcp) и admin-станция→камеры (HTTPS)
4. Изоляция камер друг от друга: bridge horizon на камерных портах либо switch port-isolation с forwarding-override на порт NVR — камеры видят только NVR
5. Неделя контроля после запуска: счётчики drop-правил и torch по vlan30 — исходящих соединений из сегмента должен быть ноль

РЕЗУЛЬТАТ

Камеры физически не могут выйти в интернет и достать до 1С и файловых серверов: даже прописанный руками DNS 8.8.8.8 умирает на drop-правиле. Участие в ботнете и уход видеопотока в чужие облака исключены на уровне сети, а не настроек самой камеры

КЛЮЧЕВОЙ НЮАНС

С RouterOS 7 правильная схема — единый bridge + VLAN-таблица (hw-offload на поддерживаемых чипах); отдельный bridge на каждый VLAN — устаревший антипаттерн, ломающий offload и производительность

РЕАЛИЗАЦИЯ 2 ИЗ 3

Локальная запись: Frigate NVR в Docker

Что настраиваем

Мини-ПК (Intel NUC или аналог) с Ubuntu 22.04+ и Docker внутри VLAN камер; альтернатива — железный Hikvision NVR с PoE

Как мы это делаем

1. Docker Compose с образом ghcr.io/blakeblackshear/frigate:stable; каталог записей — отдельный диск WD Purple, проброшенный в контейнер
2. Камеры в config.yml по RTSP через go2rtc restream — один поток с камеры на детекцию и запись; detect на суб-потоке 720p
3. Детекция объектов на Coral TPU или OpenVINO (iGPU) — CPU разгружен; ретеншен: record → motion → days: 30, непрерывную запись (continuous) держим 1–2 дня
4. Просмотр для сотрудников — учётки с ролью viewer (без доступа к настройкам); события движения в нерабочее время Frigate публикует в MQTT, наш бот доставляет их в Te…

РЕЗУЛЬТАТ

Запись по движению вместо 24/7 сокращает объём архива примерно втрое; видео хранится только локально, без облака производителя и подписок; глубина 30+ суток помещается в 3–4 ТБ для 8 камер

КЛЮЧЕВОЙ НЮАНС

Пишем всегда основной поток камеры (record), а детектируем по суб-потоку — так рекомендует документация Frigate; иначе либо мыло в архиве, либо лишняя нагрузка на декодирование

РЕАЛИЗАЦИЯ 3 ИЗ 3

Удалённый просмотр: WireGuard вместо проброса портов

Что настраиваем

Роутер MikroTik RouterOS 7.x (WireGuard встроен в систему), телефоны руководителя и ответственных — 2–5 пиров

Как мы это делаем

1. /interface/wireguard: интерфейс wg-remote, listen-port 51820/udp; на каждый телефон — свой peer со своим ключом и allowed-address /32
2. Firewall input: accept udp/51820 из WAN, остальное к роутеру — drop; из WG-подсети открыт доступ только к web-интерфейсу NVR, не ко всему LAN
3. Клиенту отдаём конфиг QR-кодом в официальное приложение WireGuard; просмотр — веб Frigate или iVMS через туннель, как из офиса
4. Проверяем снаружи: 554/8000/8443 закрыты, UPnP на роутере выключен — сканеру виден только 51820/udp, который без ключа молчит

РЕЗУЛЬТАТ

Наружу не торчит ни один сервис камер или NVR — брутфорсить нечего; доступ отзывается удалением peer за минуту при увольнении сотрудника или потере телефона

КЛЮЧЕВОЙ НЮАНС

WireGuard не отвечает на пакеты без валидного ключа — порт не виден при сканировании; это принципиально лучше reverse-proxy с Basic Auth, который остаётся публичной поверхностью атаки

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Камеры в общей подсети с 1С**
  Скомпрометированная камера сканирует рабочую сеть изнутри. Выносим в отдельный VLAN и режем forward на роутере — переезд без замены камер, 2–4 часа

- ✕ **P2P-облако и UPnP включены с завода**
  Камера сама строит исходящий туннель к серверам вендора. Гасим P2P/UPnP/Telnet/FTP на каждой камере и дублируем запретом исходящего на роутере

- ✕ **Дефолтный пароль после монтажа**
  Боты находят камеру с admin/12345 за 24–48 часов. Ставим уникальные пароли 16+ символов, ведём в KeePass: IP, MAC, серийник, дата проверки прошивки

- ✕ **Проброс 554/8000 наружу «для телефона»**
  Открытый RTSP/SDK-порт брутфорсят с первых минут. Убираем все dst-nat на камеры и NVR, удалённый просмотр — только через WireGuard

- ✕ **Неуправляемый свитч в цепочке камер**
  Свитч без 802.1Q не тегирует трафик — изоляция рушится. Минимум для VLAN: DGS-1100-08 / TL-SG108E; PoE-порты камер закрепляем за VLAN на уровне порта

- ✕ **Камеры видят друг друга внутри VLAN**
  Взломанная камера атакует соседей и NVR в своём сегменте. Включаем bridge horizon на камерных портах либо switch port-isolation с forwarding-override…

- ✕ **Прошивки со сторонних сайтов**
  Под видом прошивки встречаются трояны под ARM. Берём только с официального портала вендора; no-name камеры без обновлений в проекты не ставим

- ✕ **Диски не рассчитаны под глубину архива**
  Архив затирается раньше требуемых 30 суток. Считаем заранее: 10–18 ГБ/сутки на камеру при H.265+, ставим WD Purple, контролируем retention в NVR

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Отдельный VLAN для камер, полный запрет исходящего в интернет из сегмента
- Уникальные пароли 16+ символов на каждой камере, учёт в менеджере паролей
- Отключены UPnP, P2P, Telnet, FTP и облачный доступ на всех камерах
- Запись на локальный NVR, а не в облако производителя

НОРМАЛЬНО

- Изоляция портов камер (bridge horizon / port-isolation): камеры общаются только с NVR
- Удалённый просмотр только через WireGuard, ни одного проброса наружу
- Архив 30 суток на H.265+, диски видеонаблюдательной серии (WD Purple)
- Static lease по MAC в DHCP камерного VLAN

ХОРОШО

- Frigate с детекцией на Coral TPU/OpenVINO: запись по движению, алерты в Telegram чер...
- Ежеквартальная проверка и обновление прошивок с официальных порталов
- Мониторинг drop-счётчиков и доступности камер (ICMP + RTSP-проба в Zabbix)
- Резервирование NVR: RAID 1 и контроль S.M.A.R.T. дисков

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Камеры вынесены в отдельный VLAN, а не живут в одной подсети с 1С и файловым сервером?
- [ ] Исходящий трафик из VLAN камер в интернет полностью запрещён на роутере?
- [ ] На всех камерах сменены заводские пароли и отключены P2P, UPnP, Telnet?
- [ ] Наружу не проброшен ни один порт камер или NVR (554, 8000, 8443)?
- [ ] Видео пишется на локальный NVR, глубина архива не меньше 30 суток?
- [ ] Удалённый просмотр организован через VPN (WireGuard), а не через облако вендора?
- [ ] Камеры изолированы друг от друга внутри VLAN (bridge horizon или port isolation)?
- [ ] Прошивки камер проверялись за последние 3 месяца и ставились с официального сайта?
- [ ] Сотрудники уведомлены о видеонаблюдении: таблички и соглашения оформлены?

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 текущей схемы: куда реально ходит трафик камер и что открыто наружу — отчёт за 1 день
- Сегментация без замены камер: VLAN, firewall, изоляция портов на MikroTik/Cisco за 1–2 дня
- Разворачиваем локальный NVR (Frigate или Hikvision) с расчётом дисков под 30+ суток архива
- Настраиваем WireGuard-доступ с телефонов руководителя и закрываем все пробросы портов
- Берём видеонаблюдение на обслуживание: прошивки, мониторинг, контроль глубины архива

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 Bridging and Switching: Bridge VLAN Table, VLAN (help.mikrotik.com — ROS 7)

02 WireGuard — RouterOS documentation (help.mikrotik.com — ROS 7)

03 Frigate Docs: Recording, Camera setup, go2rtc (docs.frigate.video — 0.17)

04 Hikvision Network Security Hardening Guide (hikvision.com — 2025)

05 Наш шаблон firewall-правил сегмента видеонаблюдения (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.