Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративный DNS-фильтр на Pi-hole и WireGuard

Pi-hole v6 + Unbound + WireGuard: фильтрация, свой резолвер и VPN для офиса и школы без лицензий

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Офису и школе нужна контентная фильтрация и защита от фишинговых доменов, но бюджета на коммерческие DNS-сервисы нет. Мы закрываем задачу связкой Pi-hole v6 + Unbound + WireGuard: единый DNS-фильтр с журналом запросов, собственный рекурсивный резолвер и VPN для удалёнки. Без фильтра клик по фишинговой ссылке заканчивается заражением, а школа не проходит проверку по 436-ФЗ.

Почему это важно бизнесу

- Фишинговый домен блокируется на уровне DNS до открытия страницы — дешевле любого разбора инцидента с шифровальщиком
- Для школ фильтрация и журнал DNS-запросов — требование 436-ФЗ; предписание прокуратуры означает жёсткие сроки
- 0 ₽ за лицензии: Pi-hole, Unbound и WireGuard — open source, платим только за внедрение и сопровождение
- Блокировка рекламы и трекеров разгружает канал и заметно ускоряет браузеры на сотнях устройств

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

6.4.3/6.7

Pi-hole ветки 6 (Core/FTL): встроенный веб-сервер, весь конфиг — в /etc/pihole/pihole.toml

релиз Pi-hole 06.07.2026

5335

порт Unbound 1.25.1 на 127.0.0.1 — свой рекурсивный резолвер вместо Google/Cloudflare

по докам Pi-hole

1232

edns-buffer-size в unbound.conf — UDP-ответы без IP-фрагментации (DNS Flag Day 2020)

unbound.conf, 1.25.1

51820/udp

порт WireGuard; PersistentKeepalive=25 держит туннель сотрудника за домашним NAT

по докам WireGuard

dst-nat :53

правило dstnat на MikroTik заворачивает весь сторонний DNS на Pi-hole; DoT 853 режем

RouterOS 7, наш стандарт

~78 000

доменов в базовом unified-списке StevenBlack; расширения gambling/porn — по группам

StevenBlack hosts, 07.2026

РЕАЛИЗАЦИЯ 1 ИЗ 3

Ядро фильтра: Pi-hole v6 + Unbound на мини-VM

Что настраиваем

VM 2 vCPU / 2 ГБ RAM / 50 ГБ, Debian 12 + Docker; до 500 устройств во всех VLAN

Как мы это делаем

1. Разворачиваем pihole/pihole (Core 6.4.3 / FTL 6.7) в Docker; параметры задаём переменными FTLCONF_* — они ложатся в /etc/pihole/pihole.toml
2. Ставим Unbound 1.25.1 на 127.0.0.1#5335: root hints, prefetch: yes, edns-buffer-size: 1232 — резолвер ходит к корневым серверам напрямую
3. В Pi-hole единственный upstream — 127.0.0.1#5335; DNSSEC проверяем: dig dnssec-failed.org даёт SERVFAIL, валидные ответы несут флаг ad
4. Подключаем StevenBlack unified (~78 тыс. доменов) и тематические расширения; раздаём их по ролям через Group Management
5. До запуска собираем белый список учебных сервисов (uchi.ru, resh.edu.ru, sferum.ru) — иначе первая неделя утонет в жалобах

РЕЗУЛЬТАТ

Один узел фильтрует и журналирует DNS всех VLAN; ответы из кэша — единицы миллисекунд, запросы организации не уходят внешним DNS-провайдерам.

КЛЮЧЕВОЙ НЮАНС

В ветке 6 нет lighttpd и php — веб-интерфейс отдаёт сам FTL на 80/443. При апгрейде с v5 проверяем занятость портов и переносим кастомные dnsmasq-строки в misc.dnsmasq_lines.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Принудительный DNS: MikroTik против обхода фильтра

Что настраиваем

RB4011, RouterOS 7; VLAN учеников, учителей и администрации плюс гостевой Wi-Fi

Как мы это делаем

1. Заворот DNS: chain=dstnat protocol=udp dst-port=53 action=dst-nat to-addresses=<Pi-hole>; дублируем правило для tcp/53
2. Из правила исключаем src-address самого Pi-hole: Unbound обязан ходить к корневым серверам по 53/udp, иначе резолвер зациклится сам на себя
3. Режем DoT (drop tcp/853 наружу); известные DoH-хосты — dns.google, cloudflare-dns.com, NextDNS — собираем в address-list и блокируем по 443
4. Оставляем dns.specialDomains.mozillaCanary=true в pihole.toml: на use-application-dns.net уходит NXDOMAIN, и Firefox штатно отключает DoH
5. В DHCP каждого VLAN единственный DNS — Pi-hole; подсети привязываем к группам фильтрации (ученикам — жёстче, администрации — мягче)

РЕЗУЛЬТАТ

Смена DNS на устройстве и браузерный DoH фильтр не обходят: любой запрос на 53-й порт возвращается в Pi-hole, известные DoH-endpoints недоступны из LAN.

КЛЮЧЕВОЙ НЮАНС

Canary-домен закрывает только Firefox; для Chrome и смартфонов работает лишь блок DoH-адресов на роутере — этот address-list живой, его нужно сопровождать.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Удалёнка через WireGuard: домашние сотрудники под тем же фильтром

Что настраиваем

Интерфейс wg0 на том же узле; 30 peer-конфигов, служебная подсеть 10.6.0.0/24

Как мы это делаем

1. Интерфейс wg0: ListenPort=51820/udp; на каждого сотрудника — свой peer с уникальной парой ключей и AllowedIPs=10.6.0.x/32
2. В клиентском конфиге DNS = 10.6.0.1 (Pi-hole) и PersistentKeepalive = 25 — туннель не рвётся за домашним NAT
3. Split-tunnel: в AllowedIPs клиента только корпоративные подсети и 10.6.0.1/32 — домашний трафик через организацию не гоняем
4. Ключи генерируем скриптом (wg genkey | tee privatekey | wg pubkey), для смартфонов выдаём конфиг QR-кодом через qrencode
5. Подсеть 10.6.0.0/24 назначаем в отдельную группу Pi-hole — удалённые получают тот же профиль фильтрации, что и в здании

РЕЗУЛЬТАТ

Удалённые сотрудники ходят через корпоративный фильтр и попадают в общий журнал; подключение нового человека — один файл конфига или QR-код за минуту.

КЛЮЧЕВОЙ НЮАНС

PersistentKeepalive нужен только клиентам за NAT, на сервере он лишний. WireGuard не отвечает на непрошеные пакеты — порт 51820 при сканировании снаружи выглядит закрытым.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Единственный DNS — точка отказа**
  Падение узла кладёт весь интернет. Ставим второй Pi-hole (синхронизация конфигов + Teleporter-бэкап) и выдаём оба адреса в DHCP каждого VLAN.

- **DoH обходит фильтр за 30 секунд**
  Браузер шлёт DNS внутри HTTPS мимо 53-го порта. Блокируем известные DoH-хосты на роутере и оставляем включённым dns.specialDomains.mozillaCanary в pihole.toml.

- **Заворот DNS ловит сам Pi-hole**
  Правило dstnat без исключения src-address узла режет исходящие запросы Unbound к корневым серверам — резолвер зацикливается и вся сеть без DNS.

- **Rate-limit FTL при NAT-завороте**
  Если после NAT запросы приходят с одного IP роутера, они бьются о лимит 1000 запросов/60 с на клиента (dns.rateLimit.count/interval). Сохраняем src-адреса или правим лимит.

- **Ложные срабатывания списков**
  Агрессивные списки ломают CDN и платёжные виджеты. Первые две недели дежурим по Query Log и правим whitelist, а не выключаем фильтр целиком.

- **Журнал DNS — персональные данные**
  История запросов привязана к устройству. Ограничиваем доступ к веб-интерфейсу, задаём срок хранения database.maxDBdays (по умолчанию 91 день) и фиксируем политику по 152-ФЗ.

- **Апгрейд v5 → v6 сносит кастом**
  lighttpd и php удалены, конфиги переехали в pihole.toml. Перед апгрейдом снимаем Teleporter-бэкап и переносим правки из setupVars.conf и dnsmasq.d.

- **Pi-hole — не файрвол**
  Зловред, стучащийся на C2 по прямому IP, DNS-фильтр не остановит. Это один слой защиты: дополняем антивирусом и правилами межсетевого экрана.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Один Pi-hole v6 со списком StevenBlack; в DHCP всех сетей DNS — только он
- Заворот 53/udp+tcp на роутере (dst-nat), исключение для самого Pi-hole
- Белый список рабочих и учебных сервисов собран до включения фильтра
- Еженедельный Teleporter-бэкап конфигурации и списков

НОРМАЛЬНО

- Unbound 1.25.1 на 127.0.0.1#5335 как единственный upstream, DNSSEC включён
- Группы Pi-hole по VLAN: свои списки ученикам, учителям, администрации
- Блок DoT (853/tcp) и address-list известных DoH-серверов на MikroTik
- WireGuard для удалёнки: DNS клиентов — Pi-hole, keepalive 25 с

ХОРОШО

- Второй Pi-hole с синхронизацией конфигурации, оба адреса в DHCP
- Срок хранения журнала (database.maxDBdays) и доступ оформлены по 152-ФЗ
- Еженедельный отчёт руководителю: топ блокировок, всплески, жалобы
- Мониторинг узла: доступность 53/udp, время ответа, место под базу FTL

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Запрос с «чужим» DNS в настройках устройства всё равно попадает в Pi-hole (dst-nat отрабатывает)?
- [ ] DoT (853/tcp) и известные DoH-серверы заблокированы на уровне роутера?
- [ ] Есть второй DNS-узел или план действий на случай падения единственного Pi-hole?
- [ ] Белый список рабочих и учебных сервисов собран до включения жёстких списков?
- [ ] Группы фильтрации соответствуют VLAN и ролям, а не «один профиль на всех»?
- [ ] Срок хранения журнала запросов задан, доступ к нему ограничен (152-ФЗ)?
- [ ] DNSSEC работает: dnssec-failed.org даёт SERVFAIL, валидные домены — флаг ad?
- [ ] Удалённые сотрудники ходят через WireGuard и тот же фильтр, а не напрямую?
- [ ] Обновление gravity-списков выполняется по расписанию и не завершается ошибкой?
- [ ] Есть регламент разбора жалоб «сайт не открывается» со сроком правки whitelist?

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 Pi-hole v6 + Unbound под ключ: от аудита сети до групп фильтрации по VLAN
- Настраиваем MikroTik/pfSense: принудительный DNS, блокировка DoH/DoT, изоляция гостевых сетей
- Поднимаем WireGuard для удалёнки: персональные конфиги и QR-коды каждому сотруднику
- Готовим школу к проверке: журнал по 436-ФЗ, политика хранения по 152-ФЗ, отчёты руководству
- Берём на сопровождение: обновление списков, разбор ложных блокировок, мониторинг узла

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 Pi-hole docs — unbound (recursive DNS resolver) (docs.pi-hole.net — v6, 2026)

02 Pi-hole release: FTL v6.7, Web v6.6, Core v6.4.3 (pi-hole.net — 06.07.2026)

03 Pi-hole docs — pihole.toml (dns, database, misc) (docs.pi-hole.net — v6, 2026)

04 Unbound documentation — unbound.conf(5) (unbound.docs.nlnetlabs.nl — 1.25.1)

05 WireGuard Quick Start / persistent keepalive (wireguard.com — 2026)

06 RouterOS — IP/Firewall/NAT (chain dstnat) (help.mikrotik.com — ROS 7)

07 StevenBlack unified hosts (blocklist) (github.com — 07.2026)

08 Наш шаблон групп фильтрации «школа/офис» (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.