Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DNS-фильтрация в офисе: блокируем фишинг на уровне сети

Как мы разворачиваем AdGuard Home и Pi-hole v6 в сети с AD и закрываем обходы

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Шифровальщик заходит в малый офис не через дыру в Windows, а через клик: сотрудник открывает поддельный домен, скачивает «форму» и запускает её. Антивирус успевает не всегда — фишинговый домен живёт часы. Мы решаем задачу иначе: закрываем резолв опасных доменов для всей сети сразу, включая кассы, камеры, МФУ и старые АРМ, куда агент не поставить в принципе.

Почему это важно бизнесу

- Восстановление после шифровальщика — по нашим внедрениям это 1–2 рабочих дня простоя даже при живых резервных копиях
- Фильтр на уровне сети накрывает устройства без агента: МФУ, IP-камеры, кассы, ТСД, гостевой Wi-Fi и машины на устаревших ОС
- Обрыв канала «зловред → командный сервер» тормозит уже проникшее заражение до шифрования и выгрузки данных
- Лицензий нет: расход — одна VM на 512 МБ и работа по настройке, дальше ноль рублей в месяц за узел
- Журнал DNS даёт доказательную базу инцидента: какое устройство, когда и к какому домену обращалось

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

0.107.79

Версия AdGuard Home, которую ставим в прод: ветка 0.107.x со строгой проверкой ответов DoH

релизы AdGuard Home

FTL v6.7

Стек Pi-hole v6 (Core 6.4.3, Web v6.6) — берём там, где нужен DHCP и правка pihole.toml

релизы Pi-hole

1 ч

filters_update_interval вместо суточного значения по умолчанию: фишинговый домен живёт часы

наш стандарт настройки

1232

edns-buffer-size в unbound: при этом размере ответы не фрагментируются на офисных каналах

гайд Pi-hole по unbound

20 q/s

Дефолтный dns.ratelimit в AdGuard Home: адреса DC добавляем в dns.ratelimit_whitelist

доки AdGuard Home

91 день

database.maxDBdays в Pi-hole v6 — глубина журнала запросов на разбор инцидента постфактум

доки Pi-hole v6

РЕАЛИЗАЦИЯ 1 ИЗ 3

Ядро фильтрации: AdGuard Home на выделенной VM

Что настраиваем

Debian 12, 1 vCPU / 512 МБ / 8 ГБ, статический IP в серверной подсети, служба AdGuardHome под systemd

Как мы это делаем

1. Ставим бинарь в /opt/AdGuardHome, регистрируем службу через ./AdGuardHome -s install, проходим мастер на :3000 и сразу закрываем панель паролем и ACL
2. В секции dns: upstream_dns, bootstrap_dns, cache_size: 33554432 (32 МиБ), cache_ttl_min: 0; в filtering: blocking_mode: nxdomain, blocked_response_ttl: 10
3. Списки: базовый набор плюс фиды по фишингу и malware, filters_update_interval: 1 (значение в часах); свои правила — в отдельный custom-фильтр
4. Клиентов заводим в clients.persistent по IP, CIDR, MAC или ClientID с тегами; querylog.interval и statistics.interval задаём строкой часов, например 2160h
5. Пилот на 3–5 машинах 5–7 дней: смотрим Query Log, выносим ложные срабатывания в whitelist и только потом переключаем всю сеть

РЕЗУЛЬТАТ

Резолвер поднимается за вечер и держит офис на 30–50 устройств в пределах 50 МБ памяти. По нашим внедрениям доля блокируемых запросов ложится в 10–15% — это наш ориентир нормы. Рекламные и трекерные домены отвечают из фильтра мгновенно, а не тянутся из интернета.

КЛЮЧЕВОЙ НЮАНС

cache_ttl_min: 0 принципиален. Поднимете минимальный TTL — разблокированный домен продолжит лежать в кэше до конца срока, и чинить будете совсем не ту проблему.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Интеграция с Active Directory: DC впереди, фильтр форвардером

Что настраиваем

Два контроллера домена Windows Server, офисный DHCP-scope, периметр на pfSense или Keenetic

Как мы это делаем

1. В DHCP option 006 оставляем только адреса контроллеров домена — иначе ломаются SRV-записи, вход в домен и применение групповых политик
2. На каждом DC: Set-DnsServerForwarder -IPAddress <AGH1>,<AGH2> -UseRootHint $false; условные форвардеры оставляем под партнёрские и внутренние зоны
3. На периметре: DNAT исходящего 53 на свой резолвер, наружу закрыты 853/TCP (DoT), 784 и 8853/UDP (DoQ) и известные публичные DoH-эндпоинты
4. Браузеры: ADMX-политика DnsOverHttpsMode = off в Chrome и Edge, DNSOverHTTPS Enabled=false в Firefox (эквивалент network.trr.mode=5)
5. Канареечный use-application-dns.net резолвер гасит сам; проверка — nslookup SRV-записи через DC, dig блокируемого домена отдаёт NXDOMAIN

РЕЗУЛЬТАТ

Домен продолжает жить на своих DNS, а весь внешний резолв идёт через фильтр. Агентов на машинах нет, старые АРМ и сетевые устройства закрыты тем же контуром. Уход в браузерный DoH и на сторонний публичный резолвер закрыт политикой и правилами периметра.

КЛЮЧЕВОЙ НЮАНС

После форварда с DC запросы в журнале приходят с одного IP и персональные профили по IP перестают работать. Группы разделяем VLAN, ClientID или отдельными инстансами.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Отказоустойчивость и своя рекурсия: два узла плюс unbound

Что настраиваем

Два экземпляра резолвера на разных гипервизорах, unbound на 127.0.0.1:5335, общий VRRP-адрес на keepalived

Как мы это делаем

1. unbound: в /etc/unbound/unbound.conf.d/pi-hole.conf — port: 5335, edns-buffer-size: 1232, prefetch: yes, harden-glue: yes, use-caps-for-id: no
2. Там же harden-dnssec-stripped: yes; корневые подсказки берём из пакета dns-root-data и не правим руками, upstream резолвера — 127.0.0.1:5335
3. Второй узел: конфиг и списки синхронизируем по регламенту, VIP держим на keepalived, в forwarders обоих DC прописаны оба адреса резолверов
4. Мониторинг: проба резолва контрольного домена, доля блокировок, возраст последнего обновления списков, живость службы — алерт в Telegram

РЕЗУЛЬТАТ

Падение узла или окно обновлений не оставляет офис без DNS: клиенты уходят на второй адрес за секунды. Своя рекурсия снимает зависимость от резолвера провайдера и его подмен, DNSSEC проверяется локально, а не принимается на веру.

КЛЮЧЕВОЙ НЮАНС

Резолвер по определению единая точка отказа. Пока нет второго узла и внешней пробы «резолвится ли контрольный домен», фильтрацию мы не считаем внедрённой.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Клиентам выдали DNS фильтра вместо DC**
  В домене ломаются SRV-записи, вход и GPO. Клиенты смотрят только на контроллеры домена, фильтр подключаем форвардером на самом DC.

- **Один адрес в DHCP option 006**
  Перезагрузка узла — и офис без DNS. Даём два адреса резолверов или VRRP-VIP и проверяем переключение до сдачи работ.

- **Браузерный DoH обходит фильтрацию**
  Chrome, Edge и Firefox уводят резолв в свой DoH. Гасим политикой DnsOverHttpsMode и запретом публичных DoH-эндпоинтов на периметре.

- **Все запросы в журнале с одного IP**
  После форварда с DC клиент неразличим. Профили и статистику по отделам строим через VLAN, ClientID или отдельные инстансы.

- **Сразу включили агрессивные списки**
  Под нож попадают эквайринг, телеметрия 1С и CDN. Стартуем с базового набора и добавляем строгость после недели наблюдения.

- **Высокий минимальный TTL в кэше**
  Домен добавили в whitelist, а он ещё долго не резолвится. Держим cache_ttl_min: 0 и blocked_response_ttl: 10 секунд.

- **Ratelimit душит трафик от DC**
  Весь офис идёт с одного IP и упирается в дефолт 20 q/s. Адреса DC — в dns.ratelimit_whitelist, в Pi-hole ставим rateLimit.count: 0.

- **Списки обновляются раз в сутки**
  Фишинговый домен живёт часы, суточный интервал не успевает. Ставим filters_update_interval: 1 и мониторим возраст фидов.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Один резолвер на VM 512 МБ, базовые списки, форвардер с DC, апдейт раз в час
- DHCP option 006 — только контроллеры домена, исходящий 53 порт наружу закрыт
- Whitelist ведём отдельным custom-фильтром и версионируем его

НОРМАЛЬНО

- Второй узел резолвера, оба адреса в forwarders, проверенный failover
- Своя рекурсия на unbound 127.0.0.1:5335 вместо DNS провайдера
- Профили фильтрации по группам: бухгалтерия, продажи, руководство
- Мониторинг службы и доли блокировок с алертом в Telegram

ХОРОШО

- VRRP-VIP и регламентная синхронизация конфигов и списков между узлами
- DoH/DoT с ClientID для филиалов и сотрудников на удалёнке
- Запрет публичных DoH и политика DnsOverHttpsMode на всех браузерах парка
- Журнал запросов 90 дней и выгрузка событий фишинга в разбор инцидентов

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Клиенты получают в DHCP адреса контроллеров домена, а не резолвера напрямую?
- [ ] На DC прописаны оба адреса фильтра в forwarders и выключен -UseRootHint?
- [ ] Исходящий 53 и 853 наружу закрыт, DNAT на свой резолвер настроен?
- [ ] DnsOverHttpsMode в Chrome и Edge и DNSOverHTTPS в Firefox выключены политикой?
- [ ] Есть второй узел резолвера и failover проверен реальным отключением первого?
- [ ] filters_update_interval: 1 и возраст последнего обновления списков мониторится?
- [ ] Whitelist лежит в отдельном custom-фильтре и переживает обновление списков?
- [ ] Глубины журнала (querylog.interval, maxDBdays) хватает на разбор задним числом?
- [ ] Настроен алерт на падение службы DNS и на аномальный рост доли блокировок?
- [ ] Пилот на группе машин проведён до переключения всей сети?

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 AdGuard Home или Pi-hole v6 под ключ: VM, списки, связка с AD и DHCP
- Настраиваем свою рекурсию на unbound с DNSSEC и уводим офис от DNS провайдера
- Закрываем обходы: DoH в браузерах, публичные резолверы, прямой 53 порт наружу
- Ставим второй узел, VRRP-адрес и мониторинг с алертами в Telegram
- Ведём whitelist и разбираем ложные срабатывания в первые недели после запуска

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 AdGuard Home Wiki — Configuration: секции dns, filtering, querylog (github.com — 0.107.x)

02 AdGuard Home Wiki — Getting Started: установка службой -s install (github.com — 0.107.79)

03 Pi-hole docs — Configuration: /etc/pihole/pihole.toml (docs.pi-hole.net — FTL v6.7)

04 Pi-hole guides — unbound как рекурсивный резолвер (docs.pi-hole.net — 2026)

05 unbound.conf — справочник директив NLnet Labs (unbound.docs.nlnetlabs.nl — 2026)

06 Set-DnsServerForwarder, параметр -UseRootHint (learn.microsoft.com — WS2025)

07 Chrome Enterprise policy list — DnsOverHttpsMode (chromeenterprise.google — 2026)

08 Шаблон ITfresh: AdGuardHome.yaml, unbound.conf, Zabbix-темплейт (itfresh.ru — наш)

Основано на официальной документации продуктов и нашей практике внедрения.