itdog
14 окт в 11:39

Точечный обход блокировок по доменам на роутере с OpenWrt

Средний 13 мин 12K

Настройка Linux*, Системное администрирование*, Сетевые технологии*

Туториал

Статья о том, как настроить точечный обход блокировок по нужным доменам на роутере с OpenWrt. На мой взгляд, это самый удобный способ, который можно реализовать сейчас.

Я предоставляю уже готовый конфиг с самыми востребованными доменами, который можно дополнять.

Настроить роутер можно с помощью скрипта. Если вдруг не заведётся сразу, то другим скриптом можно найти, что не работает. Настройка с помощью Ansible никуда не делась, только модифицировалась и стала лучше.

Помимо инструкций по настройке туннелей Wireguard и OpenVPN, написал инструкцию по использованию технологий, которые помогут в обходе блокировок по протоколу: Shadowsocks, VLESS и прочими.

Эта инструкция написана под свежую OpenWrt 23.05 и скрипт работает только с ней. Но на предыдущих версиях можно также настроить всё вручную, либо с помощью Ansible. На них всё работает, но есть свои особенности, которые описаны в первой статье.

Видеоверсия

Зачем обходить блокировки точечно

Думаю, в 2023 году большинство людей сами могут ответить на этот вопрос. Но список лишним не будет:

- Есть российские сайты, которые блокируют доступ с нероссийских IP-адресов. Уверен, вы с этим сталкивались
- Высокий Latency, время ожидания открытия ресурса. Если вы, например, находитесь в Москве, а сервер с сайтом в Подмосковье, то у вас короткий маршрут. Через VPN делается петля через другую страну. Это влияет на скорость загрузки ресурса
- Сайты определяют вашу локацию по стране, где расположен VPN-сервер. Например, гугл вас будет приветствовать по-немецки. Нужно будет переключать локацию вручную, чтоб делать поиск по российским ресурсам
- Если у вас не быстрый VPN-сервер, то все ваши гигабиты по оптике превращаются в тыкву. VPN создаёт бутылочное горлышко

- Юрисдикция другой страны. Например, у некоторых правообладателей поставлены на поток обнаружение раздач нелегальных копий их контента. Система обнаружения отработает, и владелец VPN-сервера получит автоматическую абузу на сервер и вытекающие из неё проблемы
- Нагрузка на сам VPN-сервер. Об этом мало задумываются. Точечный обход блокировок - жирный плюс для VPN-сервера

Проблемы готовых списков IP-адресов

Главная проблема - это отсутствие необходимого вам ресурса в подготовленных списках. Как это решать? Можно резолвить домены, получать IP-адреса ресурса и заносить их в свой ещё один список. Со временем эти IP-адреса меняются и придётся делать по новой.

Antifilter постарались решить эту проблемы с помощью community списка. Чтоб каждый мог добавить нужный ему сайт. Есть список доменов и список IP-адресов, которые автоматически добавляются через резолвинг доменов. Крутая идея, но многих доменов нет, а их добавление не факт, что будет одобрено. Как я понимаю, резолвинг доменов в списки работает не из одной локации, но всё равно бывает так, что адрес, который резолвится у вас, будет отсутствовать в списках.

Вторая проблема касается непосредственно OpenWrt. В 22ой версии совершился переход от iptables к nftables. Nftables sets потребляет больше памяти, чем ipset. Большие списки IP-адресов на роутерах с небольшим количеством оперативной памяти стали выдавать ошибку:

```
netlink: Error: Could not process rule: No buffer space available
The rendered ruleset contains errors, not doing firewall restart.
```

Это означает переполнение памяти. Если эта ошибка появляется только при перезагрузке фаервола (тут срабатывает атомарность nftables, существующие списки не удаляются сразу, а ждут полного добавления новых из файла), то помогает "обнуление" списков перед загрузкой новых `nft flush ruleset`.

Моя реализация списка доменов

Каждому по отдельности вытаскивать самостоятельно домены заблокированных сервисов довольно непродуктивно для сообщества. Поэтому я сформировал свои списки доменов. Да, именно спискИ.

На данный момент есть три списка:

- Россия, для людей внутри страны. Тут всё понятно думаю
- Россия, для людей извне. Список из сайтов, которые пускают к себе только с российских IP-адресов
- Украина. Тут просто берётся список с ресурса https://uablacklist.net/

Раньше приходилось конвертировать списки в конфиг dnsmasq прямо на роутере. Я сделал уже готовый конфиг для dnsmasq и получились такие форматы:

- RAW - это просто списки доменов
- Dnsmasq ipset - готовый конфиг для ipset+iptables (Для OpenWrt 21ой версии и более ранних)
- Dnsmasq nfset - готовый конфиг для nfset+nftables (Для OpenWrt начиная с 22ой версии)

Сейчас они лежат просто в репозитории на GitHub:
https://github.com/itdoginfo/allow-domains

Более подробно почитать о том, как можно добавить свои домены, как формируются списки и т.д. можно в README репозитория.

Ну а если вы думаете, что ваш домен точно нужен только вам или вы не хотите показывать его другим 😉, то в конце статьи показывается как его добавить только для вашего роутера.

Плюсы и минусы использования списков доменов

Плюсы:

- Вы оперируете доменами, не опускаетесь до резолвинга
- Универсальность: подходит для обхода блокировок в любой стране

- В sets не будет IP-адреса вашего VPN-сервера
- Помимо готового списка доменов, можно добавлять свои прям на роутере
- В маршрутизации участвуют только необходимые IP-адреса, полученные из доменов. Меньше IP-адресов в списках - меньше потребление памяти

Минусы:

- Механизм резолвинга не идеален. При первом обращении к сайту вам придётся немного подождать, чтоб dnsmasq добавил IP-адрес в sets. Но после добавления всё происходит моментально
- Существуют приложения, которые не используют DNS-сервер роутера, а используют свою встроенную реализацию резолвинга прям в приложении. Здесь просто требуется отключение этой функции, подробнее в конце статьи.

Как это работает?

Тут нет никакой магии, всё реализуется довольно распространёнными open source инструментами. Два главных участника этой затеи - это dnsmasq и nftables.

Рассмотрим всё на примере сайта graylog.org. WAF Cloudflare настроен у него на блокировку по стране, это означает, что с российского IP доступ запрещён.

Для соединения с сайтом прежде всего компьютер отправляет роутеру DNS запрос, в котором просит зарезолвить домен. Начиная с этого момента включается механизм обхода. За DNS в OpenWrt отвечает dnsmasq. У него есть крутая фича: можно задать домен в конфигурации и все зарезолвенные IP-адреса этого домена он будет складывать в nftables sets.

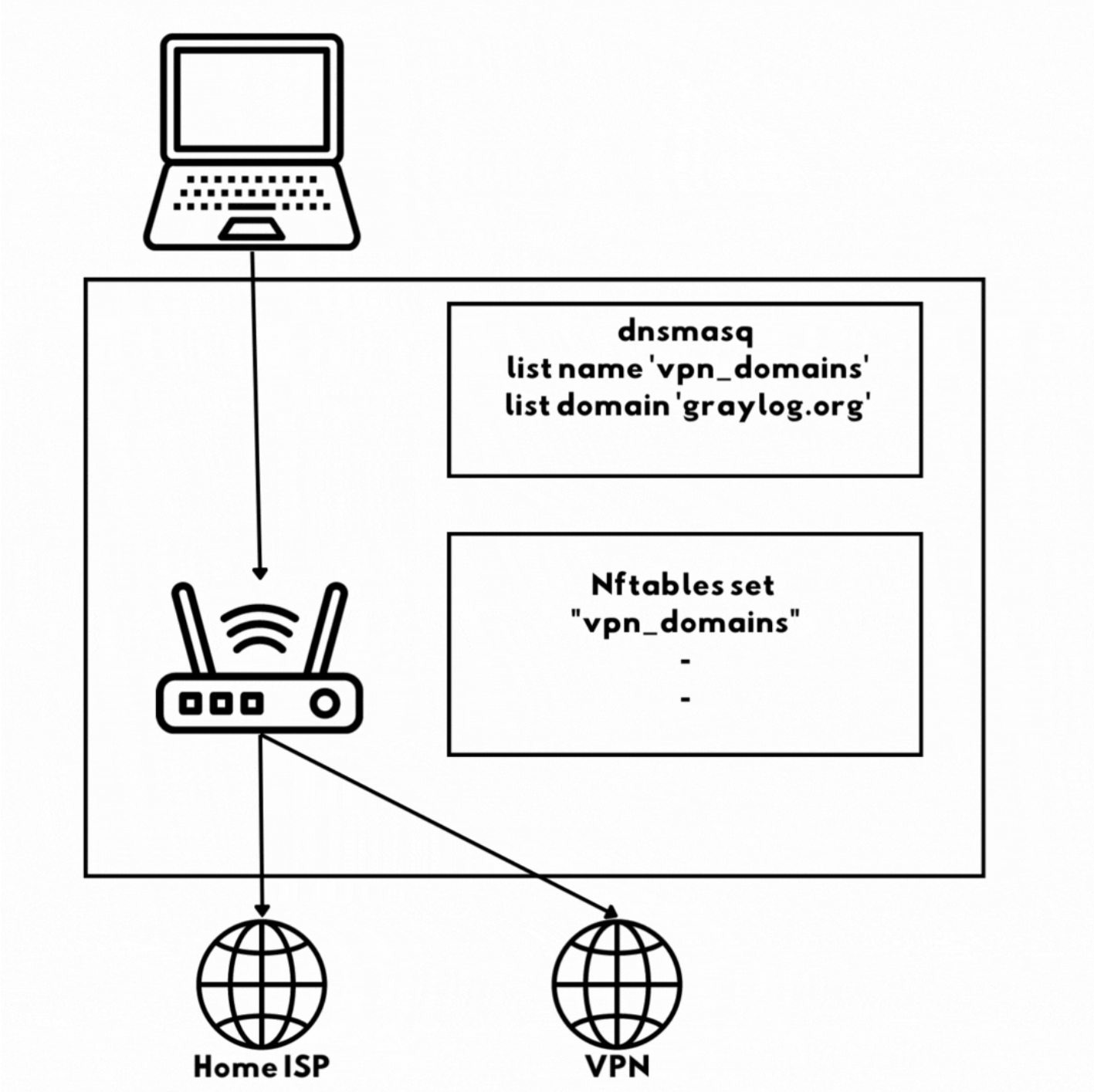
Выглядит конфигурация таким образом:

```
config ipset
        list name 'vpn_domains'
        list domain 'graylog.org'
```

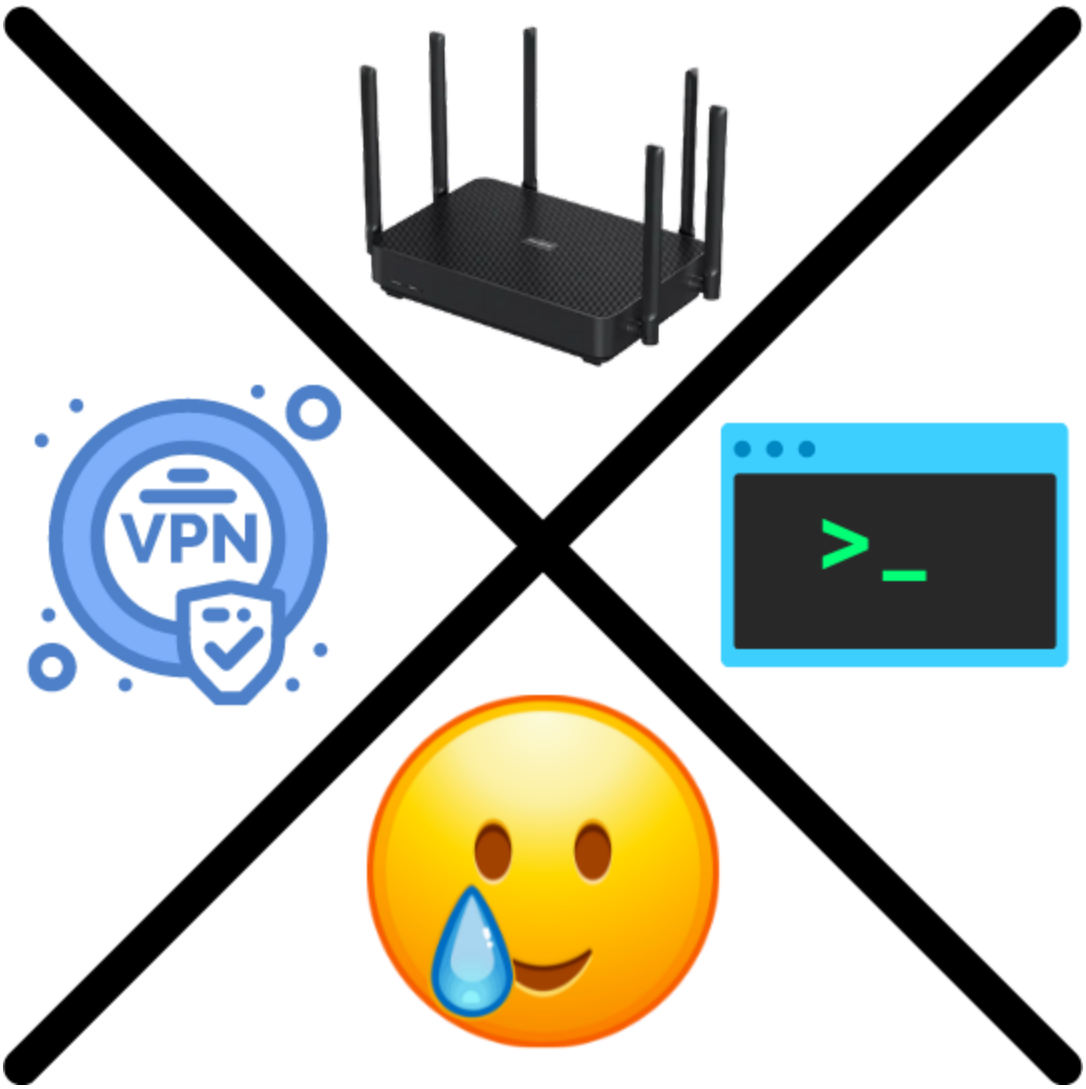
`list name` - это тот самый set, в который требуется складывать IP-адреса.

Dnsmasq получает запрос на резолвинг домена graylog.org, спрашивает адрес у вышестоящего DNS сервера, получает их. После этого отдаёт IP-адрес клиенту и складывает их в set vpn_domains.

Далее, когда роутеру приходит пакет, направленный к IP-адресу из списка, маршрутизация отправляет его в заранее поднятый туннель. А весь остальной трафик идёт, как раньше - через провайдера. Более подробно о маршрутизации и туннелях будет чуть дальше, а пока посмотрите схему работы, которую я нарисовал в одном заблокированном сервисе благодаря этому методу:



Что потребуется



1. В первую очередь, роутер, поддерживающий OpenWrt. Если у вас нет роутера, поддерживающего OpenWrt, то я составил список подходящих роутеров, которые можно купить в России и в соседних странах. С выходом 23.05 список поддерживаемых роутеров расширился, смотрите рекомендации по поиску в конце той статьи.
2. Какой-нибудь VPN. Точно работают с OpenWrt: Wireguard, OpenVPN, Shadowsocks. Если давно хотели свой сервер с VPN, то вот моя подборка VPS провайдеров, у которых есть российский эквайринг и сервера вне России (в России у них тоже есть). Wireguard наиболее прост в настройке, но есть вероятность его блокировки в ближайшем будущем. Но пока что можно начать с него, чтоб не забуксовать на этом этапе. Статья с обзором решений для простого разворачивания и управления WG-сервером.
3. Умение работать в консоли Linux или желание научиться этому.

4. Осознание, что это не простая установка VPN на винду, а решение состоящее из нескольких связаных программ, которое может не заработать с первого раза. Существует вероятность, что придётся страдать и разбираться.

Настройка

Автоматическая установка и настройка через shell-скрипт

Я написал скрипт, который автоматизирует всё, что написано ниже.
Предполагается, что у вас свежая установка OpenWrt или не особо навороченная. В случаях, когда у вас уже есть туннели, и какая-то другая логика обхода, скрипт может отработать неверно.

Вам нужно зайти на роутер по ssh и запустить:

```
sh <(wget -O - https://raw.githubusercontent.com/itdoginfo/ansible-openwrt-hirkn/m
```

Habr не поддерживает встраивание asciinema. Визуально ход настройки через скрипт можно посмотреть на сайте asciinema:
https://asciinema.org/a/614149

В первую очередь вам нужно выбрать какой туннель будет использовать роутер. Для WG можно сразу предоставить данные, и скрипт вам сам настроит WG.

OpenVPN, sing-box, tun2socks конфигурируется чуть сложнее. Поэтому для них создаются необходимые зона, правило маршрутизации и переадресации. А саму конфигурацию клиента нужно будет настроить самостоятельно по инструкциям ниже. Для sing-box скрипт создаст файл с уже подготовленным темплейтом.

Если ваш провайдер подменяет DNS запросы, то согласитесь на установку DNSCrypt-proxy2 или stubby. Второй занимает намного меньше места, давая тот же результат. Если не знаете, нужно ли оно вам, можете пропустить. Потом можно будет установить заново запустя скрипт.

Далее нужно будет выбрать необходимый список доменов.

С помощью скрипта можно поменять один туннель на другой. Он исправит правила в firewall. Но остановить другой туннель нужно будет самостоятельно. Например, у вас был OpenVPN с интерфейсом tun0, и вы поставили sing-box. Здесь будет конфликт интерфейсов. Нужно будет стопнуть openvpn службу и убрать её из автозапуска. Или можно вручную поменять один из них с tun0 на tun1.

Если возникли вопросы по определенным пунктам или хотите настроить вручную, читайте дальше.

Настраиваем туннель

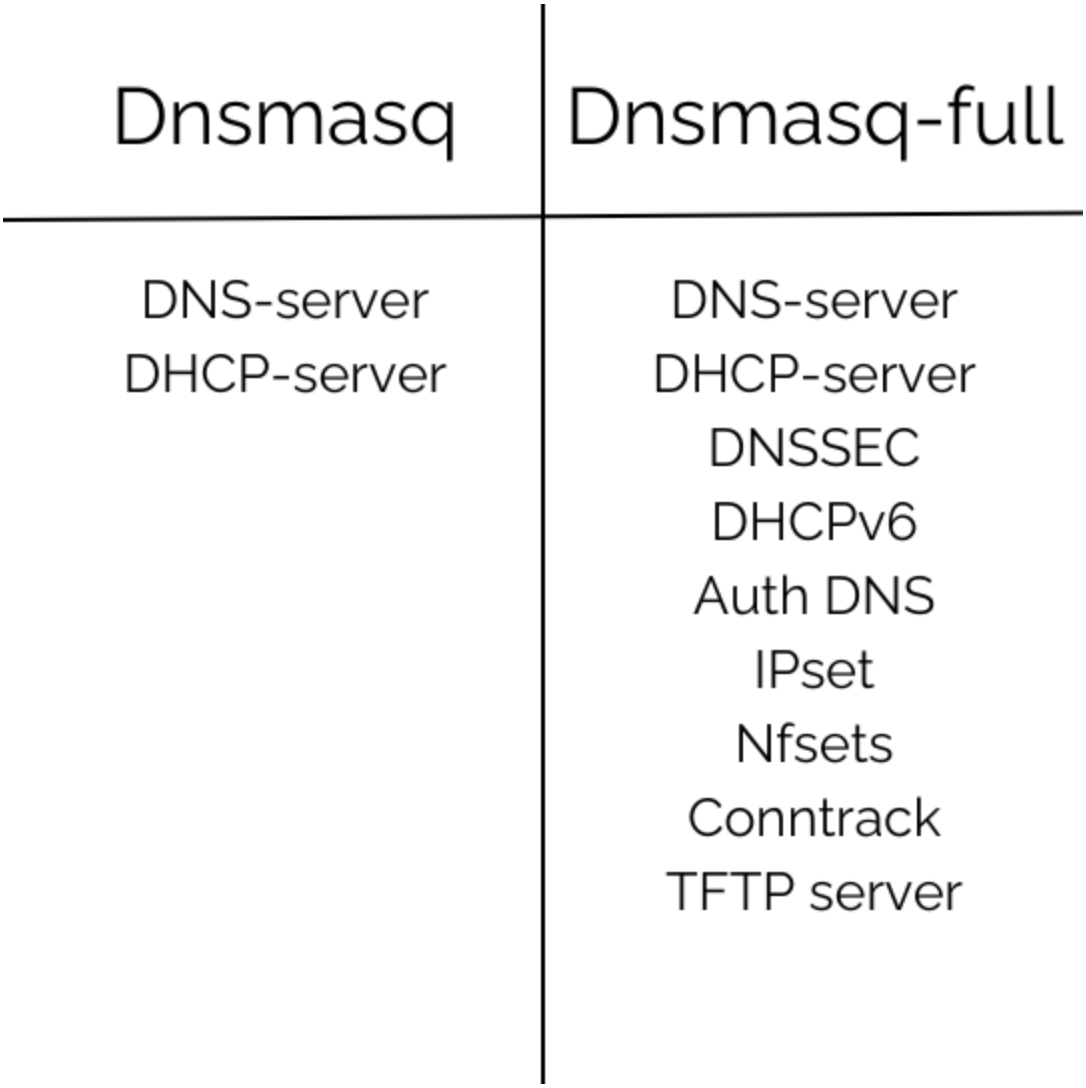
OpenWrt поддерживает несколько туннелей. Чтобы не перегружать эту статью, для каждого протокола есть свой мануал:

- Wireguard на OpenWrt
- OpenVPN на OpenWrt
- Sing-box и tun2socks на OpenWrt. Они поддерживают Shadowsocks, SOCKS5, Trojan, VMess, VLESS итд

Если вы покупаете VPN как продукт, он, скорее всего, поддерживает OpenVPN.

Установка пакетов

В первую очередь нужен пакет dnsmasq-full. По дефолту в OpenWrt идёт урезанный dnsmasq для экономии места.



Dnsmasq ключевой пакет в системе и его удаление ломает DNS на роутере. Поэтому для установки сначала нужно выгрузить его пакет в /tmp.
Если у вас что-то важное настроено в `/etc/config/dhcp`, не выполняйте последнюю строку, перенесите конфигурацию вручную.

```
opkg update && cd /tmp/ && opkg download dnsmasq-full
opkg remove dnsmasq && opkg install dnsmasq-full --cache /tmp/
mv /etc/config/dhcp-opkg /etc/config/dhcp
```

Также для скрипта обновления списков и скрипта проверки потребуется curl

```
opkg install curl
```

Настройка маршрутизации

Чтобы управлять трафиком, его нужно маркировать правилами фаервола и весь маркированный направлять в отдельную таблицу маршрутизации. А весь трафик, который проходит через эту таблицу, будет направляться в туннель.

Начнём с создания специальной таблицы маршрутизации. Можно командой

```
echo '99 vpn' >> /etc/iproute2/rt_tables
```

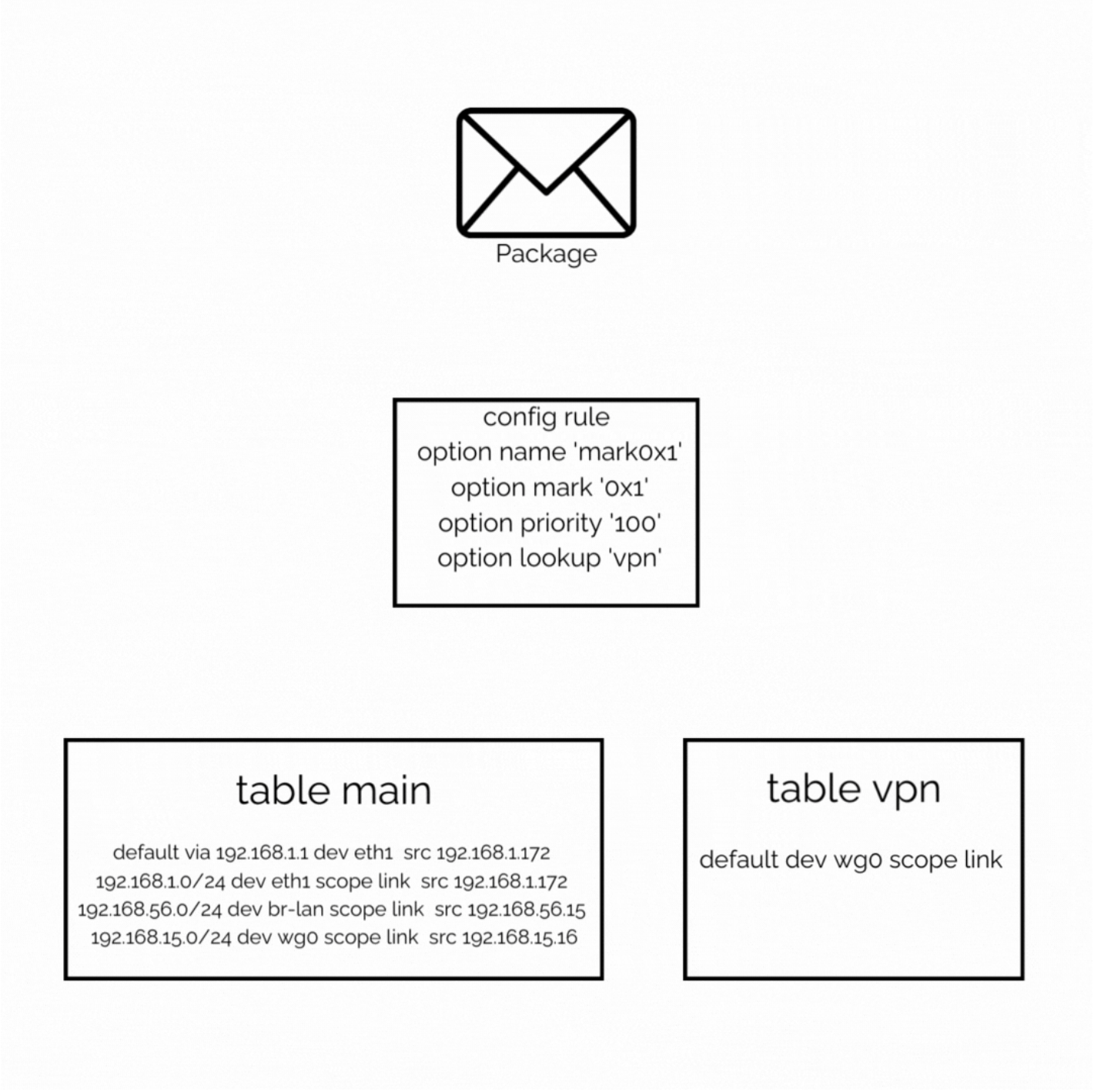
Можно добавить вручную строку `99 vpn` последней строкой в файл /etc/iproute2/rt_tables.

Добавим правило, чтоб весь маркированный трафик уходил в созданную таблицу. Через UCI:

```
uci add network rule
uci set network.@rule[-1].name='mark0x1'
uci set network.@rule[-1].mark='0x1'
uci set network.@rule[-1].priority='100'
uci set network.@rule[-1].lookup='vpn'
uci commit network
```

Либо добавляем это правило в файл `/etc/config/network`

```
config rule
    option name 'mark0x1'
    option mark '0x1'
    option priority '100'
    option lookup 'vpn'
```



Добавляем правило для таблицы маршрутизации, чтоб весь трафик, направленный в эту таблицу, уходил в туннель.

В случае с WG используем interface wg0. Раньше через UCI нельзя было сделать такое правило и приходилось костылять через hotplug. Теперь можно через UCI:

```
uci set network.vpn_route=route
uci set network.vpn_route.interface='wg0'
uci set network.vpn_route.table='vpn'
```

```
uci set network.vpn_route.target='0.0.0.0/0'
uci commit network
```

Либо добавляем это правило в `/etc/config/network`

```
config route 'vpn_route'
    option name 'vpn'
    option interface 'wg0'
    option table 'vpn'
    option target '0.0.0.0/0'
```

Если вам нужно временно выключить обход блокировок, просто закомментируйте строку `option interface`.

В случае с OpenVPN, Sing-box, tun2socks всё так же костыляем через hotplug. Потому что они сами создают интерфейс, который обозначается в OpenWrt как `device`, а тип `device` в route записать нельзя.

Создаём файл `/etc/hotplug.d/iface/30-rknroute` со скриптом внутри:

```
#!/bin/sh

sleep 5
ip route add table vpn default dev tun0
```

Задержка нужна для sing-box. Вероятно, для других можно обойтись без неё.

Можно сделать конфигурацию с прослойкой в `/etc/config/network`, что бы в route закидывать interface. Но на sing-box интерфейс tun0 не поднимается при рестарте сети. Вероятно, для OpenVPN может быть другое поведение. Поэтому вот пример с конфигурацией прослойки:

```
config interface 'vpn0'
    option name 'vpn0'
    option proto 'none'
```

```
    option auto '1'
    option device 'tun0'

config route 'vpn_route'
    option name 'vpn_route'
    option interface 'vpn0'
    option table 'vpn'
    option target '0.0.0.0/0'
```

Настройка firewall

Необходимо создать зону для туннеля, чтобы разрешить хождение трафика через туннель. Эта настройка описана в каждом мануале по туннелям.

Добавляем nftables set с именем vpn_domains, это список, куда будут складываться заблокированные IP-адреса. И правило, которое будет маркировать весь трафик, который идёт к IP-адресам из этого списка.

```
uci add firewall ipset
uci set firewall.@ipset[-1].name='vpn_domains'
uci set firewall.@ipset[-1].match='dst_net'

uci add firewall rule
uci set firewall.@rule[-1]=rule
uci set firewall.@rule[-1].name='mark_domains'
uci set firewall.@rule[-1].src='lan'
uci set firewall.@rule[-1].dest='*'
uci set firewall.@rule[-1].proto='all'
uci set firewall.@rule[-1].ipset='vpn_domains'
uci set firewall.@rule[-1].set_mark='0x1'
uci set firewall.@rule[-1].target='MARK'
uci set firewall.@rule[-1].family='ipv4'
uci commit firewall
```

Файлы, откуда будем брать IP-адреса, больше не нужны. Ваш роутер сам будет формировать список IP-адресов под ваши потребности.

Подтягиваем список доменов скриптом

Изначальный скрипт hirkn со временем разросся новыми списками, проверкой доступности интернета и конвертацией для доменов. А загрузка списков IP-адресов в sets занимала прилично времени.

При использовании доменов нужен только один список, а точнее, конфигурация для dnsmasq, которую нужно закинуть в `/tmp/dnsmasq.d/`. Там хранятся "временные" конфигурации dnsmasq.

Конфиг выглядит так:

```
nftset=/graylog.org/4#inet#fw4#vpn_domains
nftset=/terraform.io/4#inet#fw4#vpn_domains
```

Это означает, что когда приходит запрос на резолвинг домена graylog.org и всех его субдоменов, все зарезолвенные IP-адреса будут добавляться в список vpn_domains.

Когда я использовал community список от antifilter.download, приходилось конвертировать список доменов в dnsmasq конфиг скриптом на роутере. Но теперь есть готовые конфиги, которые просто надо скачать.

Таким образом, теперь всё, что требуется делать скриптом:

- Проверять есть ли доступ к интернету. Тут поясню: после перезагрузки роутера доступ к интернету может появиться не сразу (поиск сети в 4G, отсутствие электричества у коммутатора в доме) и скрипт просто не выполнится. Это значит обход блокировок работать не будет. Без такой проверки нужно будет заходить на роутер и запускать скрипт вручную
- Выкачка готового конфига сразу в `/tmp/dnsmasq.d/`
- Проверка конфига. У меня настроен CI, который проверяет валидность конфигов после их генерации, но перепроверка лишней не будет
- Если конфиг валидный, то рестарт Dnsmasq

Скрипт для примера с конфигом для inside-dnsmasq-nfset.lst. Ссылки на другие списки в репозитории.

```
#!/bin/sh /etc/rc.common

START=99

start () {
    DOMAINS=https://raw.githubusercontent.com/itdoginfo/allow-domains/main/Russia/

    count=0
    while true; do
        if curl -m 3 github.com; then
            curl -f $DOMAINS --output /tmp/dnsmasq.d/domains.lst
            break
        else
            echo "GitHub is not available. Check the internet availability [$count
            count=$((count+1))
        fi
    done

    if dnsmasq --conf-file=/tmp/dnsmasq.d/domains.lst --test 2>&1 | grep -q "synta
        /etc/init.d/dnsmasq restart
    fi
```

Складываем его в `/etc/init.d/getdomains`.

Делаем исполняемым и добавляем в автозагрузку

```
chmod +x /etc/init.d/getdomains
ln -sf ../init.d/getdomains /etc/rc.d/S99getdomains
```

Добавим автоматическое обновление доменов. Открываем редактирование crontab
`crontab -e`
И вставляем строку

```
0 */8 * * * /etc/init.d/getdomains
```

Рестартуем сеть и первый раз запускаем скрипт вручную

```
service network restart
service getdomains start
```

Теперь у вас работает обход блокировок на роутере 🎉

Свои домены

Открываем конфиг `/etc/config/dhcp` и добавляем в конец:

```
config ipset
        list name 'vpn_domains'
        list domain 'graylog.org'
        list domain 'terraform.io'
```

Каждый необходимый домен добавляем новой строкой. Dnsmasq работает по wildcard, поэтому субдомены добавлять не нужно.

Провайдер нарушает работу DNS

У вас может работать обход блокировок, но провайдер будет подменять IP-адреса у заблокированных доменов. Из-за этого обход блокировок не будет работать.

Какие бывают ситуации?
Опишу, что я видел лично. Пойдём по возрастанию в степени упоротости.

1. DNS-серверы провайдера просто подменяют IP-адреса, если использовать их. В этом случае можно просто поменять DNS сервер на роутере с провайдерского на 8.8.8.8, 8.8.4.4 и т.д.
2. DNS-серверы подменяют запросы на своих серверах. Помимо этого, если обращаться к другим DNS-серверам (например 8.8.8.8), то оборудование провайдера перехватывает эти запросы и подменяет их.
3. Провайдер тупо блокирует весь трафик по 53 порту, кроме запросов к своим DNS-серверам. Тут в принципе не получится использовать другие DNS-серверы.

Если у вас первый вариант, то просто поменяйте DNS-сервер в настройках. А вот если 2 или 3, то вам нужно настроить резолвер, который использует DNS over TLS или DNS over HTTPS.

Для OpenWrt есть два варианта:

- DNSCrypt-proxy2 - много чего умеет, но занимает 10.7M
- Stubby - не такой навороченный и поэтому занимает 36K + библиотеки

Оба приложения решают проблемы 2 и 3. Выбирать вам. Если у вас на роутере 16M флешка, то выбор очевиден.

DNSCrypt-proxy2

```
opkg update && opkg install dnscrypt-proxy2
```

Его конфигурационный файл находится в `/etc/dnscrypt-proxy2/dnscrypt-proxy.toml`
Можно поменять используемые серверы в `server_names`.

После этого нужен рестарт

```
service dnscrypt-proxy restart
```

Получили резолвер, который шифрует свои запросы. Он висит по дефолту на `127.0.0.53:53`.

Можно послать ему DNS-запрос прямо на роутере

```
nslookup itdog.info 127.0.0.53:53
```

Настраиваем dnsmasq, чтоб он использовал dnscrypt как DNS-сервер.

Необходимо в конфиге `/etc/config/dhcp` в блоке `config dnsmasq`

- Убрать или заккомментировать параметры `list server`
- Добавить `option noresolv '1'`
- Добавить dnscrypt как сервер `list server '127.0.0.53#53'`

Можно это сделать через команды UCI:

```
uci set dhcp.@dnsmasq[0].noresolv="1"
uci -q delete dhcp.@dnsmasq[0].server
uci add_list dhcp.@dnsmasq[0].server="127.0.0.53#53"
uci commit dhcp
```

Перезагрузить dnsmasq

```
service dnsmasq restart
```

Stubby

```
opkg update && opkg install stubby
```

Stubby использует по дефолту DNS-серверы Cloudflare. Если нужно поменять, настраивается в `/etc/config/stubby`.
По дефолту висит на `127.0.0.1:5453`.

Настройка dnsmasq идентичная, только вместо `127.0.0.53#53`, нужно указать `127.0.0.1#5453`.

Настройка через Ansible

Плейбук проапгреджен:

- Теперь через него можно настроить OpenVPN и sing-box, пока что тоже в полуручном режиме
- Можно настроить помимо доменов ещё списки IP-адресов
- Появился выбор между DNSCrypt-proxy2 и Stubby, либо вообще их отсутствие.
- Для доменов можно выбрать необходимый список
- И через него можно настраивать все последние (21, 22, 23) версии OpenWrt

Подробности в репозитории.

Поиск ошибок и возможные проблемы

Есть скрипт для автоматического поиска ошибок. Как его использовать описано тут

```
root@OpenWrt:~# ./check.sh
Model: Xiaomi Mi Router 3G
Version: OpenWrt 23.05.0-rc3 r23389-5deed175a5
[✓] Curl package
[✓] Dnsmasq-full package
[✓] Dnsmasq service
[✓] Check Internet
[x] Wireguard-tools package
If you don't use WG it's OK
[x] OpenVPN package
If you don't use OpenVPN it's OK
[✓] Sing-box package
[✓] Sing-box. VPN IP: [redacted]
[x] tun2socks package
If you don't use tun2socks it's OK
[✓] vpn_domains set
[✓] IPs in vpn_domains
[x] vpn_ip set
If you don't use vpn_ip set, it's OK
But if you want use, check config: https://cli.co/AwUGeM6
[x] vpn_subnet set
If you don't use vpn_subnet set, it's OK
But if you want use, check config: https://cli.co/AwUGeM6
[x] vpn_community set
If you don't use vpn_community set, it's OK
But if you want use, check config: https://cli.co/AwUGeM6
[x] Script hirkn
Script don't exists in /etc/init.d/hirkn. If you don't use old hirkn script, it's OK
[✓] Script getdomains
[✓] Script getdomains in crontab
[x] Dnscrypt-proxy2 package
If you don't use Dnscrypt, it's OK
[✓] Stubby package
[✓] Stubby service
[✓] Dnsmasq config for Stubby
```

Также есть отдельная статья, с подробным разбором каждого пункта.

В плане туннелей там описан поиск ошибок только для WG. OpenVPN проверяется примерно так же, а как проверять sing-box и tun2socks описано в их статье.

Если не получилось разобраться самостоятельно, есть чат для взаимопомощи.

Не работает на определённой программе или устройстве

Такое может встречаться, когда DNS запросы не доходят до роутера. И причина в том, что сейчас некоторые программы и даже целые операционные системы стали по дефолту шифровать DNS.

Если у вас возникает такая проблема на устройстве или программе, слова для гугла: "$PROGRAM + DNS encrypt/DNS over https/DNS over tls".

Firefox

Firefox какое-то время назад начал это делать по умолчанию. Цитата с support.mozilla.org:

> В 2019 году мы завершили развёртывание DoH по умолчанию для всех пользователей Firefox для компьютера в Соединённых Штатах и в 2021 году — для всех пользователей Firefox для компьютера в Канаде. Мы начали развёртывание по умолчанию для пользователей Firefox на ПК в России и Украине в марте 2022 года. Сейчас мы работаем над развёртыванием DoH в большем числе стран.

Отключается в **Settings** - **Privacy & Security** - в самом низу **DNS over HTTPS** - **Off**.

Android

Начиная с 9ой версии это включено по умолчанию. Здесь идёт шифрование всех запросов в системе.

В обычном Android отключается в **Settings** - **Network & Internet** - **Advanced** - **Private DNS** - **Off**

В MIUI: **Settings** - в поиске "dns" - **Private DNS** - **Off**.

Пишите в комментарии, где ещё сталкивались с этим.

DNS-сервер роутера не является основным в локальной сети

Например, у вас на домашнем сервере развёрнут DNS-сервер и он раздаётся клиентам через DHCP. Все DNS запросы идут к нему, а не к dnsmasq на роутере. В этой ситуации создание списков IP-адресов не работает.

Клиенты должны использовать DNS-сервер OpenWrt роутера, а он уже будет обращаться к вашему отдельному DNS-серверу. Это настраивается в `/etc/config/dhcp`

```
list server '192.168.1.2#53'
```

Благодарности

Благодарю @viloncool за направление в сторону доменов.

Также спасибо за помощь в исправлении ошибок и советы, как сделать лучше, следующим людям:
@sigo73, @Grayver, @SantaClaus16, @dborzov, hotsezus.

Материалы про VPN и точечный обход блокировок, которые не дотягивают до полноценной статьи, публикую в моём телеграм-канале.

Теги: точечный обход блокировок, обход блокировок, dnsmasq, nftables, openwrt

Хабы: Настройка Linux, Системное администрирование, Сетевые технологии

78 Карма 38 Рейтинг

@itdog

Пользователь

Комментарии 21

Публикации

ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ

BabayMazay
22 часа назад

Электролизер для домашней мастерской

Сложный 9 мин 5.7K

+60 37 67

Tzimie
23 часа назад

Гипотеза континуума, современное состояние

Средний 8 мин 9.3K

+58 34 68

ifap
7 часов назад

Яндекс.Спам

Простой 6 мин 8.2K

Кейс

+53 14 16

alizar
7 часов назад

Наручные атомные часы стали ближе. Определение координат без GPS

Простой 6 мин 6.9K

Обзор

+40 20 58

OlegSivchenko
20 часов назад

Гикеаны, потомки нептунов

8 мин 3.1K

+27 11 17

webzuweb
21 час назад

Ломаем Android. Русификация китайских авто

Средний 8 мин 11K

Кейс

+24 69 37

CyberexTech
8 часов назад

Детектор Судного дня или как я разработал датчик радиации для Home Assistant

Простой 6 мин 2.1K

Кейс

+21 22 16

DRoman0v
15 часов назад

Больше ОЗУ для одноплатников: Orange Pi 5, 5B и 5 Plus получили сразу 32 ГБ оперативки. Что это за девайсы?

5 мин 5.7K

+18 19 21

ru_vds
3 часа назад

Возможные векторы кибератак на новые французские цифровые удостоверения личности

Сложный 12 мин 1.6K

Кейс Перевод

+17 7 1

PatientZero
5 часов назад

Полосы прокрутки становятся проблемой

Простой 7 мин 2.3K

Мнение Перевод

+16 14 10

Как устроен электронный документооборот в ЕВРАЗе

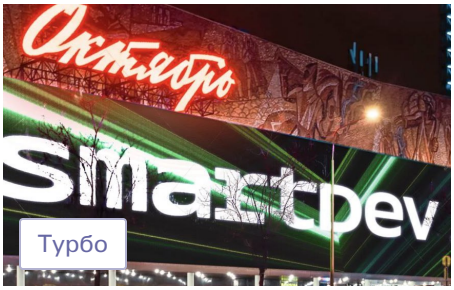
Турбо

Показать еще

МИНУТОЧКУ ВНИМАНИЯ

Глупым вопросам и ошибкам — быть! IT-менторство на ХК

Который час? Время проверить новые события в Календаре



Выясняем со Сбером, на что будет опираться будущее IT

ВОПРОСЫ И ОТВЕТЫ

Можно ли установить OpenWrt на модем?

OpenWrt · Средний · 0 ответов

OpenWRT:какую прошивку ставить на ZyXEL?

ZyXEL · Простой · 1 ответ

Как скрыть трафик не подключаясь к удаленному серверу?

Mikrotik · Простой · 3 ответа

Как использовать pam_cracklib в OpenWrt?

Linux · Средний · 0 ответов

Рандомизированный mac адрес?

Компьютерные сети · Сложный · 2 ответа

Больше вопросов на Хабр Q&A

ЧИТАЮТ СЕЙЧАС

«Если продукт не нужен, как его ни упаковывай, толку не будет»: как технологические компании работают над интерфейсами

9K 0

Эксперты обнаружили муху под видеочипом Nvidia GeForce RTX 4090 Founders Edition из-за которой видеокарта не работала

66K 86

Яндекс.Спам

8.2K 16

Наручные атомные часы стали ближе. Определение координат без GPS

6.9K 58

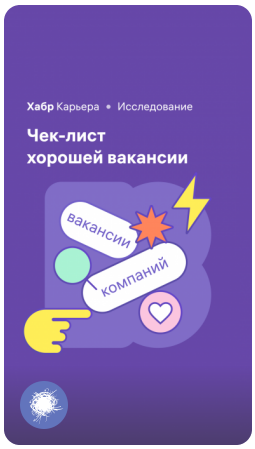
До какого возраста можно эффективно растить мышцы?

8.3K 17

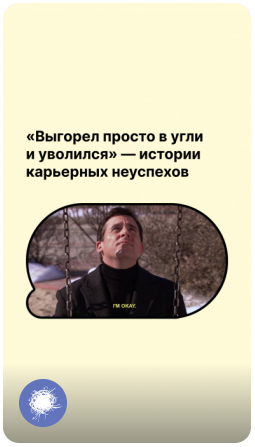
Как устроен электронный документооборот в ЕВРАЗе

Турбо

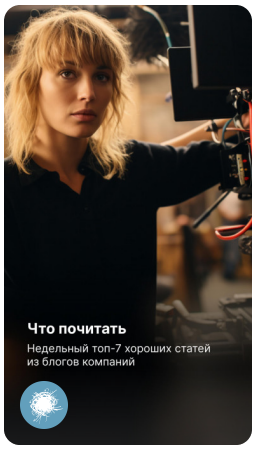
ИСТОРИИ



Чек-лист хорошей вакансии



Истории карьерных неуспехов



Годнота из блогов компаний

А теперь скажите: «Я принимаю оффер»

Перевернуть календарь и добавить событие

РАБОТА

Системный администратор
116 вакансий

DevOps инженер
46 вакансий

Все вакансии