

[КАК СТАТЬ АВТОРОМ](#)[Тестировщики, вам сюда](#)[Инженеры, мы в ваших руках](#)

Deleted-user

29 окт 2023 в 12:12

FAQ по Shadowsocks/XRay/XTLS/Reality/Nekobox/etc. для обхода блокировок

Простой

21 мин

90K

Информационная безопасность*, Системное администрирование*, Сетевые технологии*

FAQ

Эта статья - сборник разных вопросов и ответов на них, которые звучали в комментариях к моим предыдущим статьям ([Современные технологии обхода блокировок: V2Ray, XRay, XTLS, Hysteria, Cloak и все-все-все](#), [Bleeding-edge обход блокировок с полной маскировкой: настраиваем сервер и клиент XRay с XTLS-Reality быстро и просто](#) и других из той же серии) и в личных сообщениях.

Разное

Пользуюсь прокси, и некоторые сервисы/приложения каким-то образом определяют, что я сижу через прокси, как они это делают?

Классических способов выявить прокси/VPN не так много, самые известные:

- 1) разница между часовыми поясами у клиента в браузере и в локации IP-адреса с которого он подключается (например, в браузере московский часовой пояс, а сервер в Лондоне и там пояс другой) - обойти элементарно;
- 2) выявление по MTU - ненадежно, актуально для OpenVPN/L2TP/Wireguard/SSTP, для XRay и подобных прокси не актуально, т.к. они работают на другом уровне;
- 3) сканирование IP клиента на предмет открытых стандартных портов (например, 443) - можно обойти цепочкой из двух серверов с туннелем между ними;

Если вы используете мобильное устройство, то банковское (или любое другое приложение) может смотреть, активен ли в системе VPN-интерфейс, либо сравнивать геолокацию устройства и локацию по IP-адресу. Некоторые особо тупые российские сервисы по умолчанию считают что "любой доступ из-за рубежа - значит включен VPN". И еще некоторые сервисы (типа Open AI) по умолчанию запрещают доступ с non-residential IP-адресов (то есть 99.9% VPS-хостеров).

Я настраиваю сервер с XTLS-Reality, как это сделать максимально правильно?

Суть Reality в маскировке под какой-либо популярный сайт, поэтому когда вы решаете это делать, вам нужно добиться того, чтобы ваш IP (IP вашего VPS) вел себя полностью идентично настоящему серверу, которым вы прикидываетесь. Если тот "настоящий" сервер слушает на 80-м порту (plain HTTP), то вам тоже нужно настроить nginx или правило фаервола, чтобы переадресовывать HTTP-запросы на оригинальный сервер. Если "настоящий" сервер не слушает SSH-подключения на стандартном 22-м порту, то ваш тоже не должен. Если ваш хостер предоставляет reverse-DNS записи для IP-адреса, убедитесь, что там не осталось значение по умолчанию (обычно с доменом хостера), а лучше задайте такой reverse-DNS, какой виден у IP-адреса ресурса, под который вы маскируетесь.

А почему рекомендуют избегать посещения через прокси зоны RU?

По закону Яровой у нас давно уже пишутся все метаданные интернет-активности (куда, когда, откуда были подключения, какие объемы данных передавались, и т.д.). В теории (но судя по тому, насколько часто встречается этот совет на китайских сайтах, у них это уже не в теории) возможно следующее: вы случайно (даже просто зайдя на какой-нибудь обычный сайт, который подгрузит скрипту или контент с другого сервера) через свой прокси делаете запрос на условный Яндекс/Мейл/ВК/Госуслуги. В логах метаданных видно: подключение от вас на какой-то внешний IP, и точно в тот же самый момент подключение с этого IP к сервису внутри страны (который, понятное дело, тоже подконтрольный), объемы переданных данных одинаковы (с учётом оверхеда протокола) - и после ряда таких совпадений можно однозначно сказать что на этом адресе работает прокси.

Либо ещё вариант: вы подключаетесь к сервису, сервис в ответ сканирует популярные порты IP-адреса с которого вы пришли, и видит там открытый 443 порт - тоже очень подозрительно, весьма вероятно что прокси, можно банить. Поэтому варианта два: или делать цепочку из двух прокси-серверов или один сервер с двумя разными адресами (сопоставить будет многократно сложнее), или создавать правила чтобы трафик от клиента до местных сайтов шел напрямую, а на прокси-сервере для надёжности резался.

Ну или мобильное приложение у вас на телефоне (имеющее доступ к геолокации или имени активной сотовой сети) видит что вы вроде внутри страны, но при этом подключение к их серверу происходит с какого-то иностранного адреса - тоже опачки :)

Что новенького появилось с момента обзора прокси-клиентов?

У Nekobox появилась русская локализация, а также в качестве ядра, помимо sing-box, там теперь можно использовать xray вместо безнадежно устаревшего v2ray.

Под Windows, macOS, Linux и Android появился многообещающий клиент **Hiddify-Next**, написанный на Flutter и основанный на Sing-box - у него очень простой интерфейс, работает хорошо, умеет автоматически пропускать напрямую трафик до ресурсов выбранной страны (Россия в списке тоже есть), не требуя дополнительной настройки маршрутов, поддерживает и прокси- и TUN-режимы, а ещё при получении списка серверов под подписке может пинговать их всех и автоматически использовать тот, который отвечает лучше всего. Название у него совпадает с названием известной панели, но по факту он может работать с любыми совместимыми серверами.

Под iOS появился новый клиент **Streisand** - я не пробовал, кто уже пользовался, расскажите, как оно.

А ещё новости из мира протоколов - вышла новая версия протокола Hysteria - **Hysteria2**. В Sing-box уже поддерживается.

Как цензоры умудряются заблокировать Shadowsocks даже версии 2022?

Согласно последнему **GFW Report**, детектировать Shadowsocks-2022 не умеют до сих пор даже китайцы, в итоге они просто в период обострений банят все протоколы, которые (*не опознаны на DPI*) *AND* (*не похожи на простые текстовые*).

В итоге получается прибить SS-соединения, пусть и ценой огромного collateral damage (побочных эффектов) - блокируются все неопознанные протоколы, то есть по сути дела мы имеем дело с белыми списками.

Кроме того, как заметили пользователи ntc.party *"У SS есть одна особенность, запросы к серверу не мультиплексируются. Можно считать число подключений к паре адрес:порт и блокировать при превышении лимитов. Синтетические тесты такую блокировку не выявят. Например, при открытии браузером youtube, число установленных подключений к SS достигает 18, сам браузер открывает максимум 12 (числа взяты из эксперимента и могут отличаться)." Вывод - при работе через SS включайте мультиплексирование в клиенте. Клиент и сервер для этого должны быть одинаковые, потому что у XRay и Sing-box разные, не совместимые между собой механизмы мультиплексирования.*

У меня на сервере был OpenVPN/Wireguard, после начала протокольных блокировок я установил XRay, и все равно ничего не работает

Есть свидетельства о том, что РКН в некоторых случаях банит сервера целиком по IP, если до этого на них были зафиксированы подключения по детектируемым VPN-протоколам. Решение только одно - пересоздавать сервер, чтобы был новый IP-адрес.

Про VLESS и XTLS-Reality

Правда ли что VLESS не использует шифрование, и поэтому использовать его небезопасно для конфиденциальных данных.

Нет. То, что VLESS не предусматривает шифрования на уровне протокола, не значит, что данные передаются в нешифрованном виде. VLESS всегда работает поверх TLS, трафик шифруется именно механизмами TLS, а не самого VLESS. Никакой проблемы с безопасностью тут нет, все секьюрно :)

То же самое с XTLS. XTLS отключает свой слой шифрования только в случае, если определяет, что обмен между пользователем и конечным сервером уже зашифрован TLS v1.3.

Что лучше XTLS-Reality, или просто VLESS + XTLS-Vision?

Преимущества XTLS-Reality два. Во-первых это простота настройки, не надо никаких доменов, сертификатов, и т.д. Во-вторых, из-за возможности маскировки под любой популярный сайт, с его помощью можно пролезать через белые списки цензоров - например, в Иране долгое время банили/резали все по малейшему подозрению, но yahoo.com у них был в белых списках, и прокси, маскирующиеся под него работали. В России, кстати, таким "белым" сайтом является vk.com - например, на ТСПУ запрещен протокол QUIC почти для всего, а вот до vk.com он бежит без проблем. Правда, возможно еще что у них белые списки не по домену, а по диапазонам IP или AS'кам, ну и толку от vk.com, который находится внутри страны, тоже мало.

Из недостатков: может что-нибудь сломаться на сервере, под который вы маскируетесь (как например было с microsoft.com, когда они временно отключили TLSv1.3), плюс если вы маскируетесь не очень хорошо (например, оригинальный сервер отвечает не только на 443/TCP, но и на 80/TCP и 443/UDP порту, а ваш нет, зато ваш отвечает на 22/TCP aka SSH, а оригинальный нет), то это может вызвать подозрения. И еще подозрения может вызвать то, что вы стучитесь на условный microsoft.com, но при этом не резолвили его до этого (в Иране одно время за такое банили).

Обычный VLESS (с XTLS-Vision) сложнее в настройке, не будет работать в случае белых списков доменов (т.к. вы подключаетесь к своему не сильно популярному домену, который врядли будет в белом списке), но при этом лишен описанных выше недостатков, главное не забыть поднять на нем как fallback какой-нибудь безобидный веб-сайт. Зато у него есть свой недостаток - TLS fingerprint сервера явно пахнет TLS-библиотекой языка Go, а не каким-нибудь обычным Nginx или Apache.

Мое личное мнение, как сделал бы я, если есть желание покопаться и разобраться: я бы на одном сервере поднял XTLS-Reality с каким-нибудь популярным доменом (про запас, на

всякий случай), а на другом сервере для каждодневного использования, поднял бы XTLS-Reality в режиме "steal from yourself" - когда вы настраиваете на сервере Nginx или Apache с TLS-сертификатом и своим фейковым сайтом, а XRay настраиваете как XTLS-Reality, но в "dest" = "127.0.0.1", то есть маскируясь своим же собственным сайтом. В итоге вы получаете лучшее из обоих вариантов.

И бонусом еще я бы настроил проксирование через бесплатную CDN с gRPC на тот же сайт. Так, на всякий случай, мало ли что.

Нет ли какого-нибудь решения с VLESS, что бы завести к примеру 3х пользователей, но не пускать их в интернет, а раздать им доступы в разные внутренние сетки на контурах? Кажется 3X-UI и подобные панели не умеют в разные приватные сети пользователей направлять.

3X-UI такое вроде не умеет, а голый XRay кажется настроить можно.

Сделать настройки Routing в конфиге, и в зависимости от ID пользователя, если destination IP совпадает с адресом разрешенной ему сети, то отправлять на соответствующий outbound'ы для этой сети, а все остальные запросы отправлять в block.

и в outbound'ах можно задать опцию sendthrough

(<https://xtls.github.io/en/config/outbound.html#outboundobject>), чтобы трафик шел через правильный интерфейс.

См. также: XRay (с VLESS/XTLS): проброс портов, реверс-прокси, и псевдо-VPN

Как сделать хорошую, правильную маскировку для XTLS-Reality?

Внимание к мелочам.

1. Выбирайте домен для маскировки от сайта, который хостится у того же хостера, что и вы (см. следующий вопрос)
2. Перевесьте SSH с 22 порта на какой-нибудь другой сильно повыше, а то слишком палевно
3. Если вы используете панель типа X-UI или 3X-UI - то перевесьте ее тоже со стандартного порта на какой-нибудь нестандартный сильно повыше. В идеале стоит вообще заставить ее слушать на 127.0.0.1 (localhost), а подключаться к ней через SSH: например, если панель у вас на 127.0.0.1 и порту 48888, то сделав
``ssh -L 8080:127.0.0.1:48888 user@serveradd -p <ssh_port>``
вы сможете попасть на панель пройдя браузером по адресу `http://127.0.0.1:8080`
4. Сделайте проброс порта не только на 443/TCP-порт (его делает XTLS-Reality), а еще на 443/UDP и 80/TCP до сервера, под который вы маскируетесь. Например, если вы

маскируетесь под `www.microsoft.com`, то отрезолвите его IP-адрес (с помощью `nslookup`, `ping` или какого-нибудь онлайн-сервиса), а потом добавьте правила `iptables` (можно засунуть в `/etc/rc.local`, если он у вас есть - см. инструкции для вашего Linux-дистрибутива):

```
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 443 -j DNAT --to-destination fake_site_ip:443
```

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination fake_site_ip:80
```

(вместо `eth0` должен быть ваш сетевой интерфейс, иногда бывает `ens3`, например).

5. Если ваш хостер позволяет менять PTR-записи для IP-адресов (так называемые "обратные DNS"), то поменяйте ее на такую, какая есть у IP-адреса сайта, под который вы маскируетесь, или хотя бы просто на сам этот домен.

Как выбрать сайт, под который стоит маскироваться с XTLS-Reality?

Лучше всего выбирать что-нибудь из сети того же хостера, каким пользуетесь вы. Для этого есть специальный инструмент: <https://github.com/XTLS/RealiTLSscanner>

Скачиваете его под Windows/Linux со страницы [Releases](#), или собираете сами (`go build`).

Далее, запускаете как-то так:

```
/RealiTLSscanner -addr IP_вашего_VPS -showFail
```

и ждете.

Сканер будет перебирать IP-адреса из той же подсети, что и ваш сервер, и пытаться к ним подключиться по TLS. Если он что-то найдет - вы это увидите. Пример (я сканирую случайный IP-адрес):

```
89.116.243.206:443 TLS handshake failed: EOF
89.116.243.207:443 TLS handshake failed: EOF
89.116.243.208:443 ----- Found TLS v1.3 ALPN CN=caprover.com,O=CapRover.com,L=V
89.116.243.209:443 TLS handshake failed: EOF
89.116.243.210:443 ----- Found TLS v1.3 ALPN CN=patentpath.io
89.116.243.211:443 ----- Found TLS v1.3 ALPN CN=vps3.gecon.pl
89.116.243.212:443 TLS handshake failed: EOF
89.116.243.213:443 TLS handshake failed: EOF
89.116.243.214:443 TLS handshake failed: EOF
```

```
89.116.243.215:443 TLS handshake failed: read tcp 192.168.136.132:55142->89.116.243.215:443: read: connection reset by peer
89.116.243.216:443 ----- Found TLS v1.3 ALPN CN=localhost,OU=none,O=none,L=Some
89.116.243.217:443 TLS handshake failed: EOF
89.116.243.218:443 TLS handshake failed: EOF
89.116.243.219:443 TLS handshake failed: EOF
89.116.243.220:443 TLS handshake failed: EOF
89.116.243.221:443 TLS handshake failed: EOF
89.116.243.222:443 ----- Found TLS v1.3 ALPN
89.116.243.223:443 ----- Found TLS v1.3 ALPN CN=milapanel.milahosting.com
89.116.243.224:443 ----- Found TLS v1.3 ALPN CN=vps-us.workx.dev
89.116.243.225:443 ----- Found TLS v1.3 ALPN CN=www.google.com
89.116.243.226:443 ----- Found TLS v1.3 ALPN CN=www.bookifynow.com
89.116.243.227:443 ----- Found TLS v1.3 ALPN CN=next.tasosv1.cc
89.116.243.228:443 TLS handshake failed: EOF
89.116.243.229:443 ----- Found TLS v1.3 ALPN CN=alpaca-dreams.com
89.116.243.230:443 TLS handshake failed: EOF
```

Если сканер нашел какие-то домены - попробуйте сходить на них браузером - должен открыться соответствующий сайт без каких-либо ошибок сертификатов. Если не открывается, или лезут ошибки - такой домен нам не подходит, а если открывается и ошибок нет - можно попробовать маскироваться под него.

Задержки 1100-1800 ms для Нидерландского сервера это норм для XTLS-Reality?
Скорость не падает.

Да, норм. Два важных отличия от других технологий: 1) в отличие от VPN, где подключение к VPN-серверу устанавливается один раз и все, в случае с прокси, на каждое исходящее подключение из клиентского софта устанавливается новое подключение к прокси-серверу (если только не используется мультиплексирование) 2) поскольку через прокси невозможно послать ICMP-пинг, большинство клиентов меряют задержку не пингом, а выполнением HTTP-запроса.

Вот и считайте: когда вы запускаете тест, сначала устанавливается TCP-соединение с прокси-сервером (уже как минимум один, а то и два round-trip). Потом поверх него происходит TLS-хендшейк (ещё один round-trip), и в процессе него прокси-сервер ещё устанавливает TCP-соединение с reality-dest сервером и запрашивает у него сертификат. Потом прокси посылает запрос на установление TCP-соединения с тем сервером, который используется для теста. Потом, если URL указан как HTTPS, происходит ещё TLS-хендшейк с ним. Потом клиент делает HTTP-запрос и ждёт получения ответа. И только после ответа вы видите результат теста, и "задержка" - это суммарное время всего вышеописанного процесса.

Хотите минимальные задержки - маскируйтесь под какой-нибудь сервер, который находится в сети того же хостера, что и вы (см. предыдущий вопрос).

Что такое "steal from yourself"?

Это когда вы используете Reality, но прикрываясь своим же доменом. По сравнению с Reality - быстрее устанавливается соединение, вы не зависите от чужого сервера (который может отключить TLS1.3 по техническим причинам, или может забанить коннекты с IP вашего VPS, если вы его достанете), полная аутентичность (не надо маскироваться до каждой детали). По сравнению со схемой без Reality, а просто с VLESS и fallback'ом - у вашего сервера будет TLS-fingerprint как у настоящего веб-сервера (например, Nginx).

Настраивается просто: например, XRay слушает на 443 порту с Reality, в качестве "dest" у него указан "127.0.0.1:8443", а Nginx со своим сайтом с настроенным TLS слушает на 127.0.0.1 и порту 8443.

Можно ли самого XRay/Sing-box завернуть подключения в корпоративный прокси для обхода ограничений интернета в организации?

Можно ли настроить подключение через пару прокси-серверов?

XRay и Sing-box умеют делать цепочки прокси.

В Sing-box, например, можно для каждого outbound'а задать "detour" (другой прокси), и таким образом достигать до своего VLESS или Shadowsocks-сервера через корпоративный HTTP/SOCKS прокси. Если вы используете Nekobox, то нужно создать в Nekobox одно подключение типа HTTP или SOCKS (для корпоративного прокси с его адресом). Потом создать отдельно ещё одно подключение, VLESS для вашего сервера. И потом создать третье подключение типа Proxy Chain, и в него добавить первые два в нужном порядке.

Если корпоративный прокси суровый (перешифровывает TLS с подменой сертификатов), то чистый VLESS скорее всего не пропустит, но вполне может работать вариант с [websocket-транспортом](#).

Что такое port-hopping?

Пользователи из Китая писали, что когда GFW банит подключения к их прокси-серверу, ограничения часто применяются только к конкретному используемому порту. В качестве обходного пути в этой ситуации можно использовать port hopping, когда прокси-сервер слушает сразу на сотнях портов, и подключаться можно к любому - это может быть очень полезно при использовании Shadowsocks.

Сделать это можно с помощью iptables DNAT:

```
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 20000:50000 -j DNAT --to-destination 192.168.1.1:5555
ip6tables -t nat -A PREROUTING -i eth0 -p udp --dport 20000:50000 -j DNAT --to-destination 192.168.1.1:5555
```

В этом примере сервер слушает порт 555, но клиент может подключиться к любому порту в диапазоне 20000–50000.

Как понять, что у меня используется именно Shadowsocks-2022, а не старый классический Shadowsocks с уязвимостями?

В конфигурации клиента и сервера нужно использовать method который начинается с **"2022-"**, например 2022-blake3-aes-128-gcm и 2022-blake3-aes-256-gcm (это стандартные), или 2022-blake3-chacha20-poly1305, 2022-blake3-chacha12-poly1305, 2022-blake3-chacha8-poly1305 (это extra).

Для меня стало большим откровением, что современные браузеры при использовании любых прокси или VPN сливают ваш IP адрес через WebRTC

Используйте TUN-режим в клиенте.

Это все слишком сложно, можно как-то попроще?

Если все это слишком сложно - то советую [Amnezia VPN](#), он устанавливается на любой сервер двумя кликами в понятном интерфейсе, есть клиенты под все платформы, и они тоже активно работают над защитой от выявления и блокирования.

Ну либо перемещать себя в юрисдикцию, где нет блокировок по протоколам.

К чему еще стоит присмотреться кроме XRay и Sing-box?

Hysteria.

Настройка маршрутизации и клиентов

Как настроить, чтобы на российские сервера и сайты доступ шел напрямую, без прокси?

- [Shadowrocket на iOS](#)
- [Nekobox на Windows/Linux/macOS](#)
- [Nekobox Android](#)
- [Wings X / FoxRay iOS](#)
- [v2rayN Android](#)

Не могу зарегистрировать на MaxMind чтобы использовать GeoIP базы в Shadowrocket

Да, они не разрешают регистрации из России и с адресов VPS. Попросите кого-нибудь из знакомых из других стран зарегистрироваться за вас с вашим емейл-адресом или пошарить аккаунт, скачиваться должно без проблем.

Как добавлять в правила маршрутизации с кириллическими доменами? Не работает.

Используйте любой онлайн-конвертер, чтобы преобразовать их в адреса латиницей. Например, "мвд.рф" будет "xn--b1aew.xn--p1ai"

Можно ли автоматически использовать в прокси-клиенте списки "Антизапрета"?

Можно, ага. Качаете geoip.db и geosite.db вот отсюда: <https://github.com/L11R/antizapret-sing-box-geo>

И подсовываете их в ваш клиент. После этого настраиваете маршрутизацию как обычно, например, в качестве дефолтного маршрута выбираете bypass (direct), а через прокси пускаете IP-адреса по тегу geoip:antizapret и домены по тегу geosites:antizapret

Также есть очень интересные списки на <https://github.com/v2fly/domain-list-community>

Столкнулся с проблемой, что проксируется только трафик браузера, трафик терминала, например, идёт мимо прокси

Это зависит от режима работы клиента.

В режиме system проху устанавливается системный параметр, а вот использовать его или нет, зависит уже от самого приложения — браузеры его используют, а некоторые программы вообще не умеют и не хотят.

В режиме TUN заворачивается весь системный трафик, можно попробовать с ним, должно помочь.

Настроил правила роутинга в клиенте, но они, кажется, не работают - трафик все равно идет или весь напрямую, или весь на прокси, смотря что указано по умолчанию.

Надо смотреть настройки sniffинга в клиенте — во-первых он должен быть включен, и не AsIs, а что-то типа "Sniff for routing" или "Resolve Destination" (в зависимости от клиента):

Common	DNS	Simple Route
Sniffing Mode	Sniff result for routing	
Domain Strategy*	ipv4_only	
Server Address Strategy		

Все включено, но роутинг все равно не работает как надо. Конфиг писал вручную.

У XRay есть специфика, там если заданы условия, по которым будет применять тот или иной роут (например, айпи назначения из такой-то подсети, inbound такой-то, протокол такой-то), то он применит этот роут только если все условия будут выполнены.

Ну и правила применяются сверху вниз, то есть первое правило которое полностью совпало, оно и будет использоваться

Я не использую никакие правила роутинга, но некоторые сайты все равно определяют мою реальную локацию, а не локацию прокси-сервера!

Если используется TUN-режим, в клиенте не включен IPv6 (на сервере - не важно), и при этом IPv6 предоставляется вашим провайдером - есть вероятность, что трафик до IPv4-ресурсов будет идти через прокси, а до IPv6-ресурсов - напрямую.

Это не проблема конкретно V2Ray/Xray/SS, это будет для любых прокси/VPN, работающих через TUN. Решение: включить IPv6 в клиенте (даже если сервер не поддерживает), либо отключить IPv6 на сетевом устройстве (LAN или WiFi).

На Гитхабе больше нет билдов Nekoray под MacOS :(

Есть неофициальные билды под мак:

<https://github.com/aaaamirabbas/nekoray-macos/releases>

Какие из прокси/VPN можно установить не имея прав администратора в Windows?

Большинство что консольных, что GUI клиентов Shadowsocks/Trojan/VLESS не требуют установки (достаточно кинуть файлы в папку и запустить) и не требуют административного доступа. Но есть один нюанс: не получится работать через TUN-интерфейс (для установки драйвера и настройки сети нужны админские права), только через локальный прокси. Настройки прокси в винде, насколько я помню, может менять даже непривилегированный пользователь, и даже если админы запретили это делать, можно использовать браузер который не завязывается на системные настройки (например, Firefox точно так умеет).

Проблемы, ошибки, диагностика

С включенными прокси не работают аудио-видео-звонки в мессенджерах и онлайн-игры

Аудио- и видео- звонки, как и большинство игр, обычно используют передачу данных по UDP. VLESS/VMess/Shadowsocks поддерживают UDP, но у них есть проблемы с сохранением номера порта при реализации NAT, в результате чего могут быть проблемы. Для решения этих проблем разработчики XRay придумали XUDP - специальное расширение протокола, которое даст вам полноценный Full Cone NAT.

Как сделать, чтобы оно работало:

Если у вас и клиент и сервер на базе XRay свежих версий (1.8.3 и новее), то все должно работать автоматически.

Если у вас клиент на базе Sing-box (например, Nekobox), то надо явно в настройках подключения выбрать XUDP в параметре "Packet encoding".

Если у вас клиент на базе XRay, а сервер на базе Sing-box, то есть риск что ничего работать не будет, нужно менять клиент или сервер.

Клиент FoxRay на iPhone периодически вылетает, что делать?

В настройках FoxRay в меню Toolbox есть опция "reduce memory usage", возможно поможет.

Почему у клиентов теперь все предложения на YouTube, в браузере тоже хоть сбрасывай все настройки, показывает Тегеран. WTF?

Это загадка черной дыры, над которой мы долго ломали голову и так полностью и не разгадали.

У XRay совершенно точно трафик не прогоняется через какие-либо сервера ни в Иране, ни где-либо еще - это не то чтобы даже невозможно, но точно бессмысленно технически. В коде XRay ничего подобного нет.

Было подозрение что автор панели добавил в XRay какую-то отсебятину - проверили, в docker-образе оно собирается из исходников с гита, там никаких подозрительных патчей нет, и потом еще кто-то в комментариях к одной из старых статей пожаловался на такое же, только не про Иран, а про Китай :)

Для уверенности мы довольно долго смотрели в netstat и wireshark, вердикт - никаких левых подключений не делается.

Была теория, что возможно где-то в коде или конфигах захардкожены какие-нибудь региональные DNS-сервера (региональный сервер, резолвя условный гугл и ютуб, может отдать его же адреса региональных зеркал и гугл с ютубом подумают, что вы оттуда) - опять же, в коде и конфигах ничего такого не нашлось.

Но есть еще одна теория. Nekobox (возможно другие клиенты тоже, не проверял) в качестве "внутреннего" IPv6 адреса использует адрес из такого зарезервированного диапазона (ULA), где они должны генерироваться рандомно, и вероятность совпадения двух рандомных адресов ничтожна. То есть такой адрес должен быть уникальным, но в Nekobox он наоборот захардкожен один для всех случаев, и в итоге некоторые сервисы, которые могут каким-то образом получать и анализировать локальные адреса клиентов (например, Google с его телеметрией в Chrome и в Android), считают всех клиентов с таким внутренним адресом... одним и тем же клиентом, после чего сопоставляют их то ли с геолокацией, то ли с другими внутренними адресами, то ли и с тем и с тем, и в итоге в ряде случаев все пользователи Nekobox (и возможно других клиентов) для Гугла выглядят как пользователи откуда-то из Ирана, Китая или Азербайджана, вплоть до того, что со временем Гугл начинает считать публичный адрес прокси-сервера тоже иранским/китайским/etc, и это приводит к довольно забавным эффектам.

Варианты решения: не использовать TUN-режим (он же VPN mode), либо в правилах маршрутизации клиента или сервера запретить доступ до Google по IPv6, либо пропатчить клиент чтобы он использовал какой-нибудь другой внутренний адрес.

У меня FoXray не читает QR код (Shadowsocks-2022), пишет не корректные настройки. В то время этот же QR залетает в V2Box на ура. В чем может быть проблема, что я упустил?

Если пытаетесь сканировать QR из X-UI панели — можно попробовать сначала добавить подключение оттуда по ссылке в локальный Nekoray, а уже оттуда пошарить QR. Ну и проверить, что в названии конфига и параметрах нет никаких лишних символов (кириллицы, амперсантов, вопросов, точек, лишних слешей, и т.д.)

Я в настройках клиента указал свой dns сервер на adguard home. В итоге у меня на сайтах проверки dnsleaktest.com светятся помимо моих dns резолверов еще и гугловские откуда-то...

Проверьте, что у вас в `/etc/resolv.conf` :)

Настраиваю Shadowsocks, при старте клиента или сервера ругается "illegal base64 data at input byte 3"

Что-то не то с ключом. Можно еще раз регенерировать в панели (если используете панель), или с `'openssl rand -base64 16'` или `'openssl rand -base64 32'` (в зависимости от длины используемого шифра).

Пытаюсь запустить сервер, при запуске ругается "Failed to start: app/proxyman/inbound: failed to listen TCP on 443 > transport/internet: failed to listen on address: 0.0.0.0:443 > transport/internet/tcp: failed to listen TCP on 0.0.0.0:443 > listen tcp 0.0.0.0:443: bind: address already in use"

Ну ошибка говорит сама за себя: "address already in use" = на сервере на 443 порту запущен уже какой-то другой процесс. Можно посмотреть командой `'netstat -nlp'` от рута, она покажет, какой процесс слушает какой порт.

Делаю `netstat -nlp`, и судя по всему, прокся слушает только на IPv6, чэх?

В линуксе выхлоп нетстата типа `"tcp6 :::2323"` обычно означает что сокет доступен и по IPv6, и по IPv4.

Пытаюсь запустить Nekoray под Windows, ругается на какие-то ошибки в библиотеках Qt

Если у вас старая версия Windows, то нужно использовать старые версии Nekoray — в новых уже нет поддержки Windows 7 (и Windows 8 кажется тоже).

Последняя такая версия — 3.17, файл называется `"nekoray-3.17-2023-08-17-windows7-x64.zip"`.

Как точно определить, почему у меня клиент не подключается к серверу?

Увы, никак. В 99% случаев когда что-то не контактирует, это будет какое-то несоответствие конфигурации между клиентом и сервером. Сам протокол сделан так, чтобы быть максимально недетектируемым, поэтому если серверу что-то не нравится (например, не совпал ключ пользователя, или еще что), то в ответ он не пришлет никаких ошибок чтобы не демаскировать себя, а будет молчать или рвать соединение - и остается только угадывать по логам.

Сделал все по инструкции, на сервере запустилась без ошибок, но прокси не работает. Nekobox говорит: "No connection could be made because the target machine actively refused it"

Ну собственно клиент говорит как есть — он не может подключиться к серверу. Либо на сервере не запущен процесс, либо фаервол на сервере блокирует подключения, либо фаервол на клиенте блокирует подключения, либо что-то не то с настройками.

Начать расследование можно с команды "netstat -nlp", которая покажет, действительно ли ваш прокси-сервер слушает входящие подключения, на каком именно IP и на каком порту. Плюс проверьте конфигурацию фаервола согласно инструкциям для вашего дистрибутива, у некоторых дистрибутивов/хостеров по умолчанию есть правила, закрывающие все порты кроме явно разрешенных.

Также убедитесь, что вам не мешает локальный антивирус и его фаервол (например, некоторые жаловались на проблемы при наличии Касперского на клиентской машине).

В клиенте видны вот такие ошибки:

```
ERROR[0020] dns: exchange failed for mtalk.google.com. IN A: Post "https://8.8.8.8/dns-query": tls: failed to verify certificate: x509: certificate is valid for 8.8.8.8, 8.8.4.4, 2001:4860:4860::8888, 2001:4860:4860::8844, 2001:4860:4860::6464, 2001:4860:4860::64, not 8.8.8.8
```

Похоже на протухшие системные корневые сертификаты из-за очень старой ОС без обновлений. Как вариант - попробовать поменять remote DNS в клиенте с https://8.8.8.8 на просто 8.8.8.8 или 1.1.1.1 (без https).

В NekoBox 3.18 на MacOS режиме sing-box не активируется Tun Mode

<https://github.com/abbasnaqdi/nekoray-macos/issues/36> -> 'sudo /Applications/nekoray_arm64.app/Contents/MacOS/nekoray'

На Android подписки заработали с v2rayNG, а с FoxRay на iOS нет

Без SSL-сертификата и https-ссылки на подписку ничего не будет работать на iOS.

У меня сервер с XTLS-Vision или XTLS-Reality, при подключении с десктопа все работает, с мобильного устройства - нет, в чем может быть дело?

Проверьте настройки uTLS. Почему-то у многих клиентов при установке uTLS как "android" подключение фейлится, при установке uTLS как "chrome" - все работает. Не совсем понятно, это баг на стороне клиента или сервера, но баг интересный.

Использую Shadowsocks/Trojan/VLESS, и что-то скорость совсем не радует...

Настройте BBR на сервере, станет гораздо веселее:

```
echo "net.core.default_qdisc=fq" >> /etc/sysctl.conf
echo "net.ipv4.tcp_congestion_control=bbr" >> /etc/sysctl.conf
sysctl -p
```

▸ [либо более полный вариант тюнинга](#)

На некоторых системах модуль bbr может быть не загружен по умолчанию, если

```
# sysctl net.ipv4.tcp_available_congestion_control
не выдает в списке bbr:
net.ipv4.tcp_available_congestion_control = reno cubic hybla vegas yeah
необходимо добавить и ребутнуться:
echo "tcp_bbr" > /etc/modules-load.d/modules.conf
```

При использовании SS/VLESS периодически перестает работать Google, выдает "That's an error. Your client does not have permission to get URL / from this server. That's all we know."

Это известная проблема со стороны Гугла при доступе с некоторых VPS по IPv6. Стоит попробовать отключить IPv6 в клиенте, если включен (обычно в настройках TUN-режима, если используете его), также в настройках DNS/роутинга выбрать PreferIPv4 если есть такая опция. Если ничего не помогает, то последний метод - если используете TUN-режим, то попробовать обычный прокси-режим, и наоборот.

Панели

Забыл логин или пароль 3X-UI, как восстановить?

Если подключен телеграм бот, то можно сделать бэкап конфига и бд, открываем .db файл блокнотом и ищем возможные части комбинаций пароля или логина.

Как обновить X-UI? Устанавливал через Docker

А: 1) Зайти в папку cd x-ui; 2) Потом остановить контейнер: 'docker-compose down' 3) Обновить, 'docker-compose pull xui'; 4) И запустить обратно docker-compose up -d Готово. При этом тут в докер файле настройки и так хранятся в отдельном volume, поэтому ничего не сотрется.

На этом всё.

Удачи, и да прибудет с вами сила.

Если вы хотите сказать спасибо автору - сделайте пожертвование в один из благотворительных фондов: "Подари жизнь", "Дом с маяком", "Антон тут рядом". Это важно.

Теги: xray, shadowsocks, nekobox, proxy, singbox, foxray, xtls, reality

Хабы: Информационная безопасность, Системное администрирование, Сетевые технологии

Редакторский дайджест

Присылаем лучшие статьи раз в месяц

**11****0**

Карма

Рейтинг

Deleted user @Deleted-user


Так вышло

 Комментарии 172

Публикации

ЛУЧШИЕ ЗА СУТКИ


ПОХОЖИЕ


- 


UranusExplorer

12 часов назад


Надежный обход блокировок в 2024: протоколы, клиенты и настройка сервера от простого к сложному


 Простой



 36 мин

 27K

Тutorial

 +198


 444


 73
- 


Telnov_WIKI

19 часов назад


Исследование деградации Li-ion аккумуляторов в результате “быстрой” зарядки


 Простой



 4 мин

 19K

Аналитика

 +43


 48


 39
- 


Lunathecat

вчера в 12:00


115 лет прогресса: от механического осциллографа до самодельного цифрового


 Простой



 9 мин

 6.7K

Ретроспектива

 +37


 42


 13
- 


Exosphere

вчера в 12:27


Инженеры, мы в ваших руках


 Простой

 6 мин

 4.4K

+29

 25

 13

**DAN_SEA**

20 часов назад

Ещё один шаг в сторону оптических наушников



Средний



10 мин



8K

Обзор

**+27**

23



50

**madyouth**

23 часа назад

Как мы создаём редакторы документов. Ядро и его роль в кроссплатформенной разработке



10 мин



1.1K

**+27**

19



1

**iMonin**

19 часов назад

Энергетика большой страны. Почему мы все не можем отапливаться электричеством?



28 мин



10K

**+25**

36



67

**sacredtree**

22 часа назад

Почему рациональный выбор невозможен



8 мин



3.2K

**+18**

38



7

**it_union**

3 часа назад

Снижение зарплат в ИТ



2 мин



10K

**+16**

8



10



WizAlx

19 часов назад

Интеграция нативных SDK во Flutter-приложение

🕒 9 мин

👁 851

Тutorial

Перевод

📌 +15

📄 33

💬 1

А если всё рухнет при первой атаке? Почему нужно вкладываться в ИБ-обучение сотрудников

Турбо

Показать еще

МИНУТОЧКУ ВНИМАНИЯ



Из горнила конкуренции:
лучшие технобренды России



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

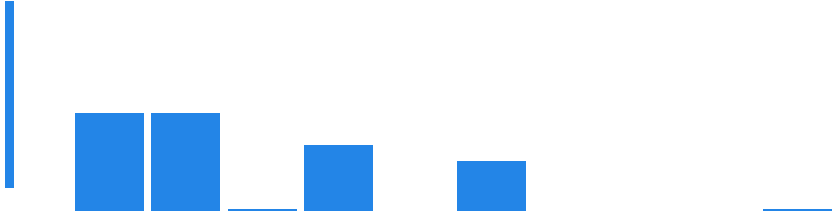


Планируй своё время и его
хватит на IT-ивенты из
Календаря

СРЕДНЯЯ ЗАРПЛАТА В IT

168 040 ₺/мес.

— средняя зарплата во всех IT-специализациях по данным из 22 229 анкет, за 1-ое пол. 2024 года. Проверьте «в рынке» ли ваша зарплата или нет!



ЧИТАЮТ СЕЙЧАС

Надежный обход блокировок в 2024: протоколы, клиенты и настройка сервера от простого к сложному

27K 73

Снижение зарплат в ИТ

10K 10

Голодные игры начались. Развитие ИИ приведёт к естественному отбору населения

43K 196

Исследование деградации Li-ion аккумуляторов в результате “быстрой” зарядки

19K 39

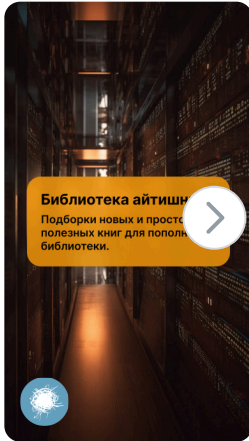
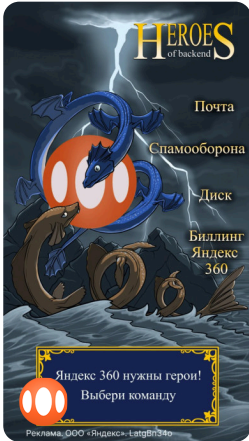
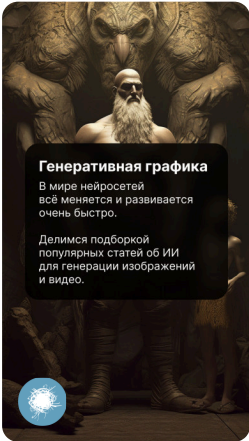
Сколько мы заработали за год на 1 товаре из Китая. Продаем коврики для ноутбука на маркетплейсах

39K 65

А если всё рухнет при первой атаке? Почему нужно вкладываться в ИБ-обучение сотрудников

Турбо

ИСТОРИИ




- GitVerse: открой вселенную кода
- Нейросети: интересное
- Что умеет калькулятор зарплат в IT
- Яндекс 360 призывает героев бэкенда
- Полезные книги для библиотеки айтишника


РАБОТА

- Системный администратор
92 вакансии
- Специалист по информационной безопасности
140 вакансий
- DevOps инженер
28 вакансий


Все вакансии

БЛИЖАЙШИЕ СОБЫТИЯ


Как решать алгоритмический блок при найме в IT?
Разбираемся на Тренировках по алгоритмам 5.0 от Яндекса




Хабр Карьера





Онлайн-курс «Delivery Manager»

Почему становится Delivery Manager'ом — плохая идея?


Открытый урок 18 марта в 20:00


 1 марта – 19 апреля


 19:00

 Онлайн



Подробнее в календаре


 18 – 24 марта

 09:00 – 23:00

 Онлайн

Подробнее в календаре

 18 марта 

 Онлайн

Подробнее в календаре

Войти	Статьи	Устройство сайта	Корпоративный блог
Регистрация	Новости	Для авторов	Медийная реклама
	Хабы	Для компаний	Нативные проекты
	Компании	Документы	Образовательные программы
	Авторы	Соглашение	Стартапам
	Песочница	Конфиденциальность	



Настройка языка

Техническая поддержка