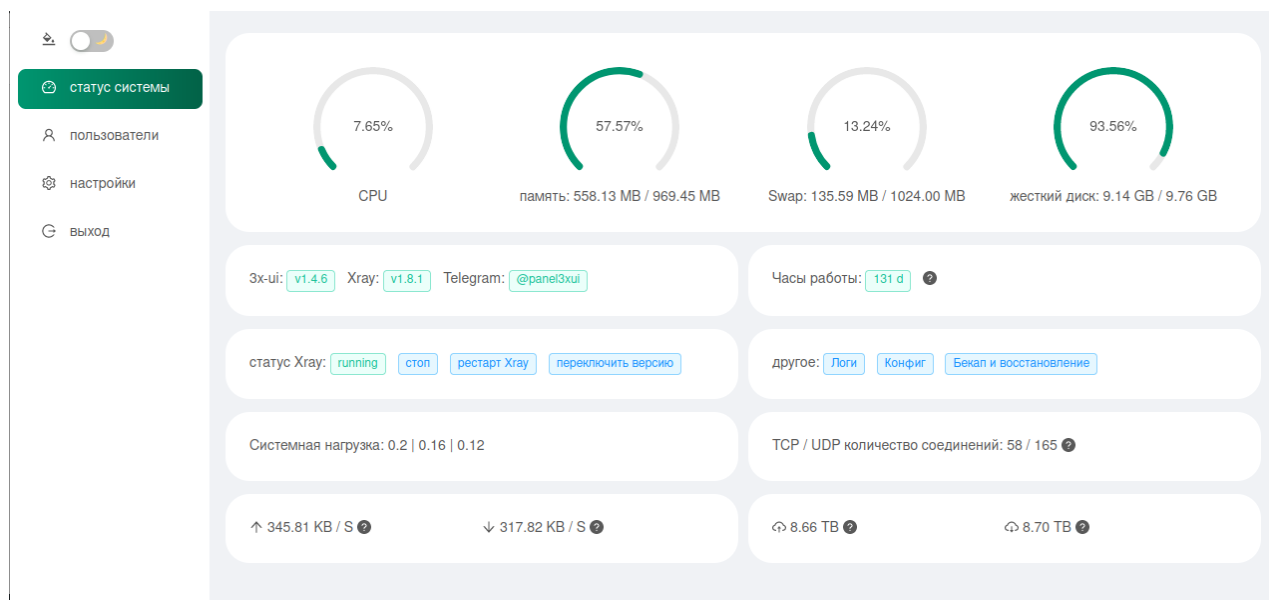


3X-UI: Shadowsocks-2022 & XRay (XTLS) сервер с простой настройкой и приятным интерфейсом

 habr.com/ru/articles/735536

Deleted user

May 18, 2023



[Deleted-user](#) 18 мая 2023 в 22:14

Простой

13 мин

557K

Тutorial

Статья опубликована под лицензией Creative Commons [BY-NC-SA](#).

В серии предыдущих статей я описывал, почему повсеместно используемые VPN- и прокси-протоколы такие как OpenVPN и L2TP [очень уязвимы к выявлению и могут быть легко заблокированы](#) цензорами при желании, обозревал [существующие гораздо более надежные протоколы](#) обхода блокировок, [клиенты для них](#), а также [описывал настройку сервера двух видов](#) для всего этого.

Многим читателям, однако, ручная настройка показалась сложной и неудобной - хотелось иметь понятный легко устанавливаемый графический интерфейс без необходимости ручного редактирования конфигов и вероятности допустить ошибки, а еще мы не поговорили про механизм "подписок", позволяющих клиентам автоматически подключать список новых серверов с настройками подключений.

Поэтому сегодня мы поговорим об установке и использовании графической панели 3X-UI для сервера X-Ray с поддержкой всего того, что умеет X-Ray: Shadowsocks-2022, VLESS с XTLS и т.д.

Почему 3X-UI? Существует, на самом деле, довольно много панелей для V2Ray/XRay: [оригинальный X-UI](#), [Marzban](#), [Libertea](#), [Hiddify](#). Проблема в том, что в процессе экспериментов у меня и ряда других хабраюзеров заставить их нормально работать с пол-пинка не получилось. Например, одним из требований была установка в Docker (чтобы не создавать бардак в системе и не запускать непонятные bash-скрипты на хосте вне контейнера), и на этом этапе отвалились уже многие панели: у каких-то установка падала еще на этапе разворачивания docker-контейнера из-за ошибок в скриптах, какие-то устанавливались, но не могли нормально запуститься (фронтенд говорил, что не может подключиться к бэкенду), какие-то в итоге запускались, и после получаса тыканья везде в попытках переключить язык с китайского или фарси хотя бы на английский выяснялось что что-то глючит или не работает.

3X-UI, который является доработанным форком оригинального X-UI, в сравнении со всем вышеописанным, почти идеален: легко устанавливается в Docker, сразу на английском с возможностью переключения на русский, имеет в себе все что надо - и главное, работает! Пара багов, конечно, тоже нашлась, но они не критичны и о них будет чуть позже.

Update: в конце мая в своем Telegram-канале автор 3X-UI написал, что возможно больше не будет работать над проектом, но есть альтернатива - еще один из форков оригинального X-UI под названием (внезапно!) [X-UI](#), который очень похож на 3X-UI и тоже работает без проблем.

Выбор домена для маскировки

Нам нужно найти сайт, под который мы будем маскироваться.

Требования довольно простые:

это должен быть иностранный сервер (вне РФ), не забаненный по домену Роскомнадзором, поддерживающий подключения по TLSv1.3 и HTTP/2, имеющий главную страницу, которая *не* переадресовывает на какой-нибудь другой домен. Если совсем упарываться, то неплохо было бы если бы IP-адрес был из диапазона того же облачного хостера, что и у вас, и чтобы сервер поддерживал Online Certificate Status Protocol (OCSP). Если вы не знаете, что вся эта фигня значит - не заморачивайтесь, выбирайте что-нибудь простое, например

- [www.samsung.com:443](#)
- [www.googletagmanager.com:443](#)
- [www.asus.com:443](#)
- [www.amd.com:443](#)
- [www.cisco.com:443](#)

- www.microsoft.com:443
- dl.google.com:443
- www.linksys.com:443
- www.nvidia.com:443

и т.д.

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

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

Далее, запускаете как-то так:

```
./RealTLScanner -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 рандомный IPшник):

```

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=Vancouver,ST=British
Columbia,C=CA,1.2.840.113549.1.9.1=#0c11696e666f40636170726f7665722e636f6d
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: i/o timeout
89.116.243.216:443      ----- Found TLS v1.3      ALPN
CN=localhost,OU=none,O=none,L=Somertown,ST=Someprovince,C=US,1.2.840.113549.1.9.1=#
0c137765626d6173746572406c6f63616c686f7374
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.tasosvl.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.

Установка панели 3-XU (X-UI)

Официальный репозиторий 3X-UI: <https://github.com/MHSanaei/3x-ui>

Официальный репозиторий форка X-UI: <https://github.com/alireza0/x-ui>

Итак, дано: VPS с IPv4 (неплохо бы иметь еще IPv6, но не обязательно) и Debian либо Ubuntu Linux (на других дистрибутивах суть будет примерно та же самая). И установленные Docker и docker-compose (если вдруг нет - [следуйте инструкциям](#) для вашего дистрибутива, у меня без проблем установилось простым "apt install docker.io docker-compose"). Ну и git в придачу.

Сначала клонируем исходники. Лучше всего использовать последнюю стабильную версию, можно проверить в "Releases" на гитхабе.

Для 3X-UI:

```
git clone https://github.com/MHSanaei/3x-ui.git
cd 3x-ui
git checkout v1.4.6
```

Для X-UI:

```
git clone https://github.com/alireza0/x-ui.git
cd x-ui
git checkout 1.4.1
```

Запускаем docker-compose:

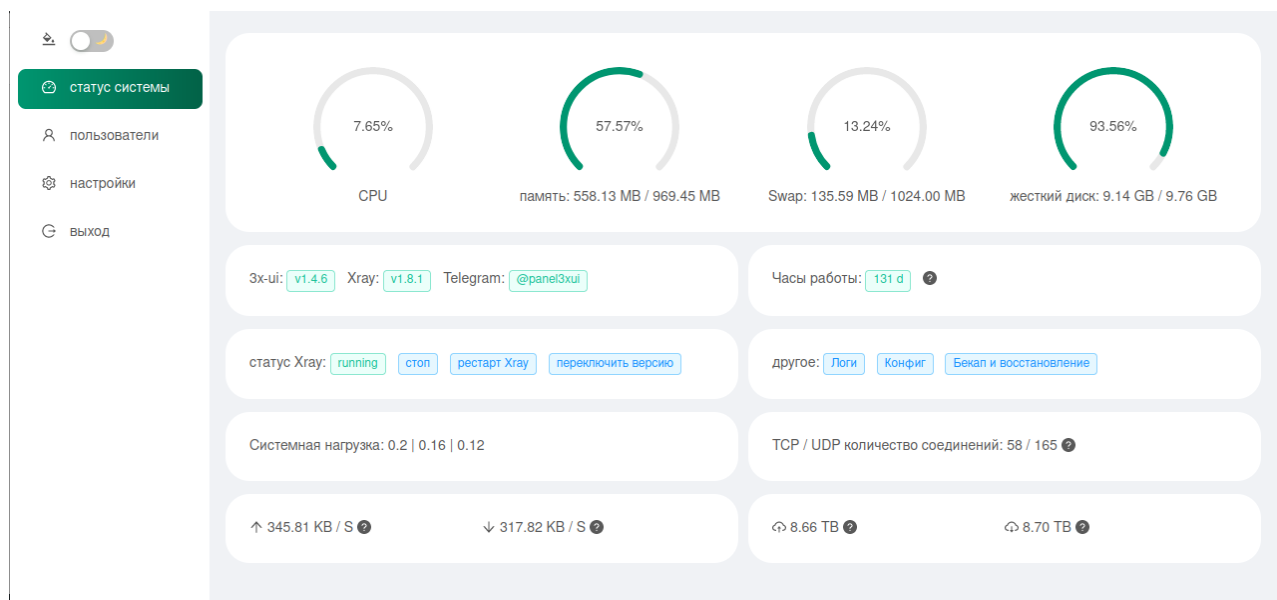
```
docker-compose up -d
```

Готово! Вы восхитительны! Я серьезно, все, панель установлена и работает.

Дело осталось за малым - настроить ее:

Для 3X-UI идем браузером по адресу <http://yourserverip:2053/panel/>, где yourserverip - IP-адрес вашего сервера или доменное имя, если оно у вас есть и настроено (обратите внимание, протокол <http://>, а не <https://>). Для X-UI нужно сначала посмотреть с помощью команды "docker logs x-ui", на каком именно порту запустилась панель.

Логинимся под стандартными реквизитами admin/admin и видим нашу прекрасную панель управления:



Первым делом я советую сделать несколько вещей. Перейти в "Settings" (настройки) и там:

1. Изменить порт на котором работает панель со стандартного 2053 на какой-нибудь другой (лучше всего где-нибудь в верхнем конце диапазона, до 65535) - **обязательно** ;

2. Изменить корневой путь URL-адреса панели с / на что-то типа /mysecretpanelroot/ - **обязательно**;
3. При желании переключить язык на русский (но имейте в виду, в русском переводе есть некоторые неточности, сбивающие с толку);
4. На второй вкладке "Настройки безопасности" изменить стандартный админский пароль на свой - **обязательно**;
5. После чего сохраняем настройки и рестартуем панель. Нужно будет изменить URL с учетом нового порта и пути, заданных в настройках.

☑️ ☐

статус системы

🔍

пользователи

⚙️

настройки

🚪

выход

Сохранить

Рестарт панели

Настройки панели

Настройки безопасности

Конфигурация Xray

Настройки Телеграм-бота

IP-порт панели

Оставьте пустым для работы с любого IP. Перезагрузите панель для применения настроек.

Порт панели

Перезагрузите панель для применения настроек.

4444

Путь к файлу публичного ключа сертификата панели

Введите полный путь, начинающийся с «/». Перезагрузите панель для применения настроек.

Путь к файлу приватного ключа сертификата панели

Введите полный путь, начинающийся с «/». Перезагрузите панель для применения настроек.

Корневой путь URL-адреса панели

Должен начинаться с «/» и заканчиваться на «/». Перезагрузите панель для применения настроек.

/secretpanel/

статус системы

пользователи

настройки

выход

СохранитьРестарт панели

Настройки панелиНастройки безопасностиКонфигурация XrayНастройки Телеграм-бота

АдминСекретный токен

Имя пользователя сейчас:

Пароль сейчас:

👁

Новое имя пользователя:

Новый пароль:

👁

подтвердить

Все вышеперечисленное необходимо для защиты от тупых скриптов и злоумышленников, которые случайно могут наткнуться на вашу панельку при массовом сканировании адресов. Другие советы по повышению безопасности я приведу в конце статьи.

Создаем подключения

Идем в раздел меню Inbounds (в русском переводе он почему-то называется "Пользователи", это неправильно и сбивает с толку). Нажимаем "Add Inbound" ("Добавить пользователя"):

Всего входящих/исходящих: 0 В / 0 В

Количество пользователей: 0

+ Добавить пользователя

☰ Общие действия

поиск

Меню	Включить	ID
------	----------	----

Появляется милое окошко. Сначала добавим возможность подключаться через Shadowsocks-2022.

"Remark" (Примечание) - ввести что угодно, это просто человекочитаемое название;

"Протокол" выбираем shadowsocks;

"Listening IP" (в русском переводе называется "Порт IP", и это тоже неправильно и запутывает) можно оставить пустым, тогда сервер будет слушать на всех IP-адресах, либо можно явно указать требуемый;

"Порт" - панель выберет рандомный.

Далее настраиваем пользователя (в момент создания inbound'a создается один, других при желании можно добавить позже):

Поле "Email" на самом деле не обязательно должно содержать email, может быть любой текст (имя пользователя) - панель генерирует рандомный набор символов, если вы хотите создавать несколько разных пользователей (например, раздать аккаунты друзьям, смотреть кто сколько накачал и при желании блокировать доступ), то лучше вбить сюда что-то человекочитаемое и понятное;

"Subscription" - пока что можно вбить тот же самый юзернейм (о подписках я расскажу чуть позже).

Дальше снова идут настройки протокола:

"Шифрование" - выбираем что-нибудь что начинается с "2022", вариант по умолчанию вполне неплох;

"Пароль" (ключ) панель сгенерирует автоматически с правильной длиной для выбранного метода шифрования.

Нажимаем "Создать" и на этом настройка для Shadowsocks закончена, им уже можно пользоваться.

примечание: включить: ☒

протокол:

порт IP [?]:

Порт:

Общий расход (GB) [?]:

Дата окончания [?]:

▼ Клиент

Email:

Password:

Subscription [?]:

Telegram ID [?]:

ограничение по IP [?]:

Общий расход (GB) [?]:

Начать со времени первого подключения: ☐

Дата окончания [?]:

Шифрование:

пароль:

Сеть:

Sniffing [?]: ☒ HTTP ☒ TLS ☒ QUIC

закрыть

Создать

Теперь переходим к настройке VLESS с XTLS-Reality. Тут все будет чуточку сложнее, но в целом так же просто.

"Remark" (Примечание) - любое название;

"Протокол" - "vless",

"Listening IP" ("Порт IP", который на самом деле не порт, а адрес) - оставляем пустым, либо задаем вручную если надо;

"Порт" - вместо randomного ставим **443**;

Добавить пользователя

×

примечание: Reality

включить: ☒

протокол: vless

▼

порт IP ? :

Порт: 443

Общий расход (GB) ? :

0

Дата окончания ? :

Select date

📅

▼ Клиент

Email : ↻ t3882vbj

ID : ↻ 17caff16-859a-4f14-ea9e-995f1dc1cb09

Subscription ? : ↻ user1

Telegram ID ? :

ограничение по IP ? :

0

Flow: xtls-rprx-vision

▼

Общий расход (GB) ? :

0

Начать со времени первого подключения: ☐

Далее переходим к настройкам клиента.

"Email" - как в и в прошлом пункте, лучше указать что-то человекочитаемое и понятное. Важно: пользователи разных подключений не могут иметь один и тот же email (например, наш новый VLESS и старый Shadowsocks созданный в

предыдущем пункте), поэтому можно добавить какой-нибудь префикс (например user1vl) для избежания конфликтов.

"Subscription" - тут наоборот, лучше будет если текст в этом поле будет совпадать с тем, что вы задали для Shadowsocks (подробности ниже). *Внимание: в отличие от 3X-UI, в X-UI поле Subscription по умолчанию не отображается, нужно сначала активировать функционал подписок в настройках панели.*

"Flow" - надо выбрать "xtls-rprx-vision". Обратите внимание, поле Flow (см. скриншот) появится только после того, как чуть ниже вы поставите галочку на пункте "Reality". То есть лучше всего настраивать так: сначала ставите галочку Reality, а потом заполняете поля с настройками пользователя.

Дальше у нас идут настройки транспорта:

"Reality" - как уже сказано выше, должно быть активно;

"XTLS" - наоборот, должно быть неактивно (это немного запутывает, не смотря на то, что Reality тоже относится к XTLS, здесь под XTLS подразумеваются только устаревшие версии протокола, и галочки "XTLS" и "Reality" в панели являются взаимоисключающими);


"uTLS" - по умолчанию "firefox", я обычно выбираю "chrome", по факту особо без разницы (главное чтобы не "android", могут быть проблемы с клиентами);

"Домен" - на самом деле это не домен, а адрес для подключения к вашему серверу. Можно оставить пустым, тогда панель автоматически подставит IP-адрес или домен, по которому вы обращаетесь в панели на сервере.

"ShortIds" - панель сгенерирует рандомный ID;



"Public Key", "Private Key" - можно кликнуть на "Get new keys", и панель сама сгенерирует новые для вас;

"Dest" и "Server names" - вот это самое интересное, это домен, под который вы будете маскироваться. По умолчанию панель предлагает маскировку под yahoo.com и www.yahoo.com с переадресацией на yahoo.com:443, но лучше выбрать какой-нибудь другой домен, как описано ранее;

Fallbacks: 

протокол передачи: TCP

AcceptProxyProtocol: ☐ HTTP маскировка: ☐

TLS: ☐ Reality : ☒ XTLS : ☐

Show: ☐ xVer: 0

uTLS: chrome

домен:


dest: yahoo.com:443


Server Names: yahoo.com,www.yahoo.com

ShortIds: c793166c

Private Key: SAHNmwubAXnenKEAcJQURUufucOXLaq;











Public Key: M8o0suSlkmwflVDNXiCXEqXm7h421cfutAN

 Get New Key

Sniffing : ☒ ☒ HTTP ☒ TLS ☒ QUIC

Сохраняем введенную форму, и - всё! Настройка завершена.

После этого на странице видим примерно вот это:

Меню	Включить	ID	Примечание	Порт	Протокол	клиенты	Трафикт l	Дата окончания
 Меню	<input checked="" type="checkbox"/>	1	SS	51258	shadowsocks		0 B / 0 B бесконечно	бесконечно
Меню	Включить	Клиент	Трафикт l	Дата окончания	Password			
   	<input checked="" type="checkbox"/>	user1ss	0 B / 0 B бесконечно	бесконечно	vQldFCVT9ADCSoUcktrRCpJCj88cMols5J0y4Cj6iy8=			
 Меню	<input checked="" type="checkbox"/>	2	Reality	20794	vless tcp Reality	1	0 B / 0 B бесконечно	бесконечно
Меню	Включить	Клиент	Трафикт l	Дата окончания	UID			
   	<input checked="" type="checkbox"/>	user1vl	0 B / 0 B бесконечно	бесконечно	b6c151e7-15b9-413e-dc56-d1aa070cbcd9			

Если ткнуть на кнопку "Меню" соответствующую нужному протоколу, можно его активировать/деактивировать, сбросить счетчики трафика, добавить пользователей (в том числе сгенерировать разом N аккаунтов по шаблону), и самое главное - раскрыв (плюсиком) список пользователей, можно посмотреть настройки подключения для вбивания в клиенты для этого пользователя.

Нажав на значок QR-кода, панель покажет QR-код, который можно отсканировать камерой в мобильных клиентах ([v2rayNG](#) или [Nekobox](#) на Android, [Wings X/FoXray](#) или [Shadowrocket](#) на iOS). Подробнее о клиентах читайте в [этой статье](#).

► ремарочка



Нажав на иконку информации (с буквой "i") можно посмотреть настройки для вбивания в десктопные клиенты, в том числе и URL, который можно скопировать и вставить.


Под дестоп я рекомендую Nekobox (есть [под Windows, Linux](#) и билды от сообщества [для MacOS](#)). Подробнее о клиентах читайте в [этой статье](#).

протокол	vless	протокол передачи	tcp
Адрес	81.35.155.2	хост	пусто
Порт	443	путь	/
reality:	включено		
reality домен:	—		

Клиент


id	17caff16-859a-4f14-ea9e-995f1dc1cb09		
flow	xtls-rprx-vision		
email	t3882vbj		
статус	включено		

использование	Общий расход	Дата окончания
0 B / 0 B (0 B)	бессрочно	бессрочно

Subscription link [http://\[REDACTED\]/secretpanel/sub/user1](http://[REDACTED]/secretpanel/sub/user1) 

URL

vless://17caff16-859a-4f14-ea9e-995f1dc1cb09@81.35.155.2:443?type=tcp&security=reality&fp=chrome&pbk=zIFm5XMXSZes7LYQ7Filzpl5faEaKwptPFB3pKFmB0A&sni=yahoo.com&flow=xtls-rprx-vision&sid=49eab435#Reality-t3882vbj

 **копировать**


► краткая настройка Nekobox

Там же вы можете найти "subscription URL". Это - специальным образом сгенерированный список подключений для клиентов. Помните, вы указывали "Subscription" при создании пользователя? При запросе по такому subscription URL, сервер выдаст список настроек (сервера, ключи) для всех подключений с этим ID в поле subscription. Многие клиенты (включая v2rayNG, v2rayN, Nekobox, и другие) умеют автоматически либо по запросу скачивать настройки с таких URL и добавлять их к себе - таким образом, если вы добавили какие-то новые протоколы или решили поменять конфигурацию, пользователи могут легко получить новые параметры с вашего сервера.

Внимание: в отличие от 3X-UI, в X-UI поле Subscription по умолчанию не отображается и вообще функционал подписок по умолчанию отключен, его нужно активировать в настройках панели.

Дополнительные настройки

В менюшках панели можно найти много интересностей, например, можно запретить клиентам качать торренты (если у вас на сервере не слишком широкий канал или есть лимит трафика), добавить фильтр доменов рекламных сервисов, запретить доступ к порносайтам (ума не приложу, кому вообще в жизни может понадобиться такая ужасная функция).

 **Эти параметры не позволят пользователям подключаться к определенным протоколам и веб-сайтам.**

Запретить использование BitTorrent

☒

Измените конфигурацию, чтобы пользователи не использовали BitTorrent. Перезагрузите панель для применения настроек.

Запрет частных диапазонов IP-адресов для подключения

☒

Измените конфигурацию, чтобы избежать подключения к диапазонам частных IP-адресов. Перезагрузите панель для применения настроек.

Бокировка рекламы

☐

Измените конфигурацию, чтобы заблокировать рекламу. Перезагрузите панель для применения настроек.

Блокировка порносайтов

☐

Измените конфигурацию, чтобы отключить подключения к порносайтам. Перезагрузите панель для применения настроек.

Блокировать сайты для проверки скорости

☐

Измените шаблон конфигурации, чтобы избежать подключения к веб-сайтам для тестирования скорости. Перезапустите панель, чтобы применить изменения.

А еще можно заблокировать доступ через сервер к IP-адресам и доменам Ирана, Китая и России (Россия здесь в отличной компании, не правда ли?) - это нужно если вы по ряду соображений настроили на клиентах доступ к российским сайтам напрямую, и хотите заблокировать их на сервере чтобы случайно не вылезти в рунет через него из-за ошибок в настройках.

Отключить подключение к диапазонам IP-адресов Ирана



Измените конфигурацию, чтобы отключить подключение к диапазонам IP-адресов Ирана. Перезагрузите панель для применения настроек.

Отключить подключение к доменам Ирана



Измените конфигурацию, чтобы отключить подключение к доменам Ирана. Перезагрузите панель для применения настроек.

Отключить подключение к диапазонам IP-адресов Китая



Измените конфигурацию, чтобы отключить подключение к диапазонам IP-адресов Китая. Перезагрузите панель для применения настроек.

Отключить подключение к доменам Китая



Измените конфигурацию, чтобы отключить подключение к доменам Китая. Перезагрузите панель для применения настроек.

Отключить подключение к диапазонам IP-адресов России



Измените конфигурацию, чтобы отключить соединения с диапазонами IP-адресов России. Перезагрузите панель для применения настроек.

Отключить подключение к доменам России



Измените конфигурацию, чтобы избежать подключения к доменам России. Перезагрузите панель для применения настроек.

► Про опцию запрета IPv6 для Google

Улучшения и баги

Сначала о паре багов.

При установке в Docker не получается посмотреть логи Xray, панель выплевывает ошибку. Иногда что-то подсмотреть и понять можно используя команду "docker logs 3x-ui", но там логи довольно куцые. Будем надеяться, что в следующих версиях это исправят (зарепортируйте им там кто-нибудь, а?).

Второй баг - не удастся создать несколько inbounds с одним и тем же портом, но разными listening IP - панель ругается. Из-за этого, например, нельзя реализовать классическую схему с XTLS-Reality слушающем на 443 порту на IPv4-адресе, и VLESS+Websockets или VLESS+gRPC для работы через CDN (как запасной вариант) на IPv6 адресе. Опять же, будем надеяться, что авторы это когда-нибудь пофиксят.

Из того, что можно улучшить при конфигурации - по умолчанию панель слушает на чистом HTTP, без шифрования. Вариантов решения несколько:

1. Если у вас есть домен (даже бесплатный от no-ip, freenom, dynu), то можно установить certbot от letsencrypt, запросить сертификат для своего домена, положить его в папку `./certs` (внутри директории, куда вы клонировали 3x-ui) или сделать туда симлинки, и указать путь к ключам в панели в виде `/root/cert/privkey.pem` и `/root/cert/public.crt`. Не забудьте добавить `post-update hook` для рестарта контейнера;
2. Другой вариант - поменять в настройках listen IP для панели на `127.0.0.1` - после этого панель станет недоступна "снаружи", но на нее всегда можно будет зайти с помощью SSH:
`"ssh -L 8080:localhost:2053 your_server_ip"` - тогда вбивая в браузере `http://localhost:8080`, подключение через SSH пойдет на локальный порт 2053 сервера, где и слушает ваша панель;
3. Третий вариант - повесить на сетевой интерфейс на сервере еще один "виртуальный" IP-адрес: прописать в `/etc/network/interfaces` что-то типа
`iface lo:1 inet static`
`address 192.88.99.1`
`network 192.88.99.0`
`netmask 255.255.255.0`
и настроить панель, чтобы она слушала только на нем. Тогда "снаружи" панель будет недоступна, но при подключении через Shadowsocks/VLESS-прокси вы сможете до нее достучаться по этому адресу.

Про работу через веб-сокеты, gRPC и CDN: [Особенности проксирования через CDN/Websocket/gRPC для обхода блокировок](#)

О VLESS

Мы настроили протокол VLESS. Иногда в интернете можно встретить утверждения, что, мол VLESS не шифрует данные, а значит он небезопасен. Это не так. 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.

О надежности

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. начало статьи).
2. Перевесьте SSH на вашем сервере 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@serveraddress -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 отрезолвте 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.

О клиентах

Весьма важно настроить на клиентских устройствах правила, чтобы доступ к внутренним (российским, если вы в РФ) ресурсам не шел через прокси-сервер.

Примеры настроек разных клиентов для этого есть в FAQ:

[FAQ по Shadowsocks/XRay/XTLS/Reality/Nekobox/etc. для обхода блокировок](#)

Там же есть ответы на многие другие частые вопросы и советы по устаранию проблем.

Telegram

И интересное напоследок. Панель может работать как Telegram-бот :)

Сначала обращаемся к боту BotFather и просим его зарегистрировать нового бота:



BotFather 
bot



/newbot 19:40 ✓✓

Alright, a new bot. How are we going to call it?
Please choose a name for your bot.

19:40

[REDACTED] 19:40 ✓✓

Good. Now let's choose a username for your
bot. It must end in `bot`. Like this, for example:
TetrisBot or tetris_bot.

19:40

[REDACTED] 19:41 ✓✓

Sorry, this username is invalid.

19:41

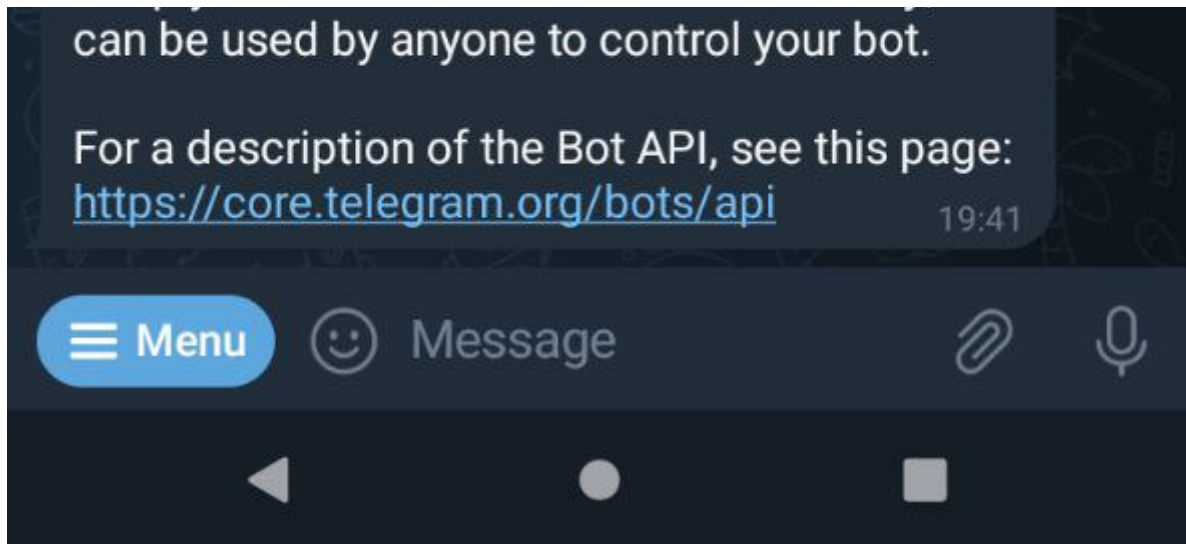
[REDACTED] 19:41 ✓✓

Done! Congratulations on your new bot. You
will find it at [t.me/\[REDACTED\]](https://t.me/[REDACTED]). You can
now add a description, about section and
profile picture for your bot, see [/help](#) for a
list of commands. By the way, when you've
finished creating your cool bot, ping our Bot
Support if you want a better username for it.
Just make sure the bot is fully operational
before you do this.

Use this token to access the HTTP API:

[REDACTED]

Keep your token secure and store it safely, it



Он сгенерирует для вас API-токен. Его надо вставить в настройки панели, и там же указать ваш ID как админа (его можно запросить у бота userinfobot):

Настройки панели	Настройки безопасности	Конфигурация Xray	Настройки Telegram-бота
Включить Telegram-бота		<input checked="" type="checkbox"/>	
Перезагрузите панель для применения настроек.			
Токен Telegram-бота		<input type="text" value="1234567890:ABCDEFghijklmnopqrstuvwxyz0123456789"/>	
Перезагрузите панель для применения настроек.			
Telegram-ID админа бота		<input type="text" value="123456789"/>	
Если несколько Telegram-ID, разделить запятой. Используйте @userinfobot, чтобы получить Telegram-ID. Перезагрузите панель для применения настроек.			
Частота уведомлений telegram-бота		<input type="text" value="@daily"/>	
Используйте формат Crontab. Перезагрузите панель для применения настроек.			
Резервное копирование базы данных		<input type="checkbox"/>	
Включать файл резервной копии базы данных с уведомлением об отчете. Перезагрузите панель для применения настроек.			

После этого можно разговаривать с панелью через Telegram - смотреть статистику, делать бэкапы конфигурации, и т.д.



bot



May 16

/start 19:42 ✓✓

Hello 🤖👋

Welcome to yourhostname management bot

I can do some magics for you, please choose:

19:42

Server Usage

Get DB Backup

Get Inbounds

Deplete soon

Commands



Hostname: yourhostname



X-UI Version: 1.4.6



IP: [172.17.0.1](#) [172.18.0.1](#)
[172.19.0.1](#) [172.20.0.1](#) [172.21.0.1](#)



IPv6: [:::ffff:::1](#)



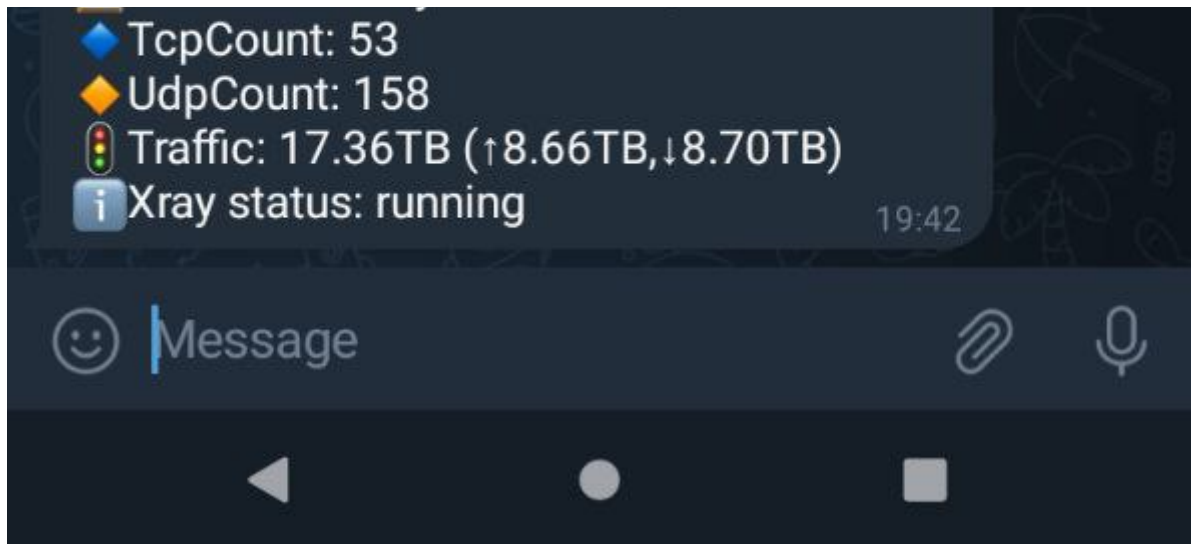
Server Uptime: 131 days



Server Load: 0.1, 0.1, 0.1



Server Memory: 543.29MB/969.45MB



На этом всё.

Удачи, и да прибует с вами сила.

Если вы хотите сказать спасибо автору — сделайте пожертвование в один из благотворительных фондов: "[Подари жизнь](#)", "[Дом с маяком](#)", "[Антон тут рядом](#)".