[Виртуальные анонимы. Знакомимся с анонимизирующей операционкой Whonix](https://pikabu.ru/story/virtualnyie_anonimyi_znakomimsya_s_anonimiziruyushchey_operatsionkoy_whonix_4279926" \t "_blank)

[94 Комментария](https://pikabu.ru/story/virtualnyie_anonimyi_znakomimsya_s_anonimiziruyushchey_operatsionkoy_whonix_4279926#comments) [codeath](https://pikabu.ru/profile/codeath) в [Информационная безопасность](https://pikabu.ru/community/ibc)

583 дня назад

[анонимность](https://pikabu.ru/tag/%E0%ED%EE%ED%E8%EC%ED%EE%F1%F2%FC/hot) [операционная система](https://pikabu.ru/tag/%EE%EF%E5%F0%E0%F6%E8%EE%ED%ED%E0%FF%20%F1%E8%F1%F2%E5%EC%E0/hot) [whonix](https://pikabu.ru/tag/whonix/hot" \o "Поиск по тегу \"whonix\"" \t "_blank)[Linux](https://pikabu.ru/tag/Linux/hot) [информационная безопасность](https://pikabu.ru/tag/%E8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF%20%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC/hot) [журнал хакер](https://pikabu.ru/tag/%E6%F3%F0%ED%E0%EB%20%F5%E0%EA%E5%F0/hot) [tor](https://pikabu.ru/tag/tor/hot" \o "Поиск по тегу \"tor\"" \t "_blank) [длиннопост](https://pikabu.ru/tag/%E4%EB%E8%ED%ED%EE%EF%EE%F1%F2/hot" \o "Поиск по тегу \"длиннопост\"" \t "_blank)

[](https://cs4.pikabu.ru/post_img/2016/06/18/0/1466198866112833343.png)

Когда мы говорим об анонимности в интернете, то чаще всего подразумеваем такие проекты, как Tor, I2P, Tor Browser, DNSCrypt и Live CD TAILS, включающий в себя все перечисленное. Однако существует менее известная, но очень интересная система Whonix, использующая виртуализацию в качестве средства изоляции рабочей станции от глобальной сети и способная защитить твою анонимность даже после взлома.

**ВМЕСТО ВВЕДЕНИЯ**

Чтобы обеспечить анонимность своего пребывания в Сети, мало установить Tor и завернуть в него весь исходящий трафик. Необходимо позаботиться о таких вещах, как утечки DNS, обнаружение твоего географического положения на основе настроек часового пояса, утечки имени пользователя (через SSH, например), утечки IP-адреса, свойственные некоторым сетевым протоколам, побороть проблему идентификации машины на выходных узлах Tor путем сравнения типов трафика. Ну и в целом придется серьезно повозиться, чтобы заставить все установленные сетевые приложения использовать Tor и не выдавать данных о твоей машине.

Ты можешь сделать все это сам, но лучше взять проверенное готовое решение, а именно дистрибутив TAILS. Он включает в себя множество преднастроенных приложений, корректно настроенный Tor и брандмауэр, так что в целом это достаточно надежная в плане сохранения анонимности и приватности система, которой не гнушался пользоваться сам Эдвард Сноуден.

Однако у TAILS есть два серьезных ограничения. Во-первых, это Live CD, изначально позиционируемый как «одноразовый»: TAILS не умеет запоминать свое состояние между выключениями и не оставляет никаких следов на машине. Как средство для слива секретных документов АНБ несколько раз за всю жизнь это превосходный инструмент, как повседневно используемая система — ужасный. Во-вторых, запуская TAILS на голом железе, юзер автоматически открывает серьезную дыру в своей анонимности. Ведь конфигурация ПК тоже позволяет идентифицировать человека.

Плюс TAILS никак не защищена от компрометации системы. Любой взломавший твою машину сразу деанонимизирует и твой IP, и тебя самого. Чтобы этого избежать, запланировано размещать ключевые системные сервисы в песочницах — но только в версии 3.0, которая непонятно когда выйдет, да это и не даст стопроцентной защиты. А самое печальное, что «благодаря» необновляемости системы ты не сможешь быстро залатать дыру, с помощью которой тебя взломали, придется ждать официальный релиз свежей версии TAILS (при условии, что информация о дыре находится в открытом доступе).

Для решения всех этих проблем как раз и предназначен Linux-дистрибутив Whonix, преследующий те же цели, но достигающий их несколько иным путем.

**СИЛА ВИРТУАЛИЗАЦИИ**

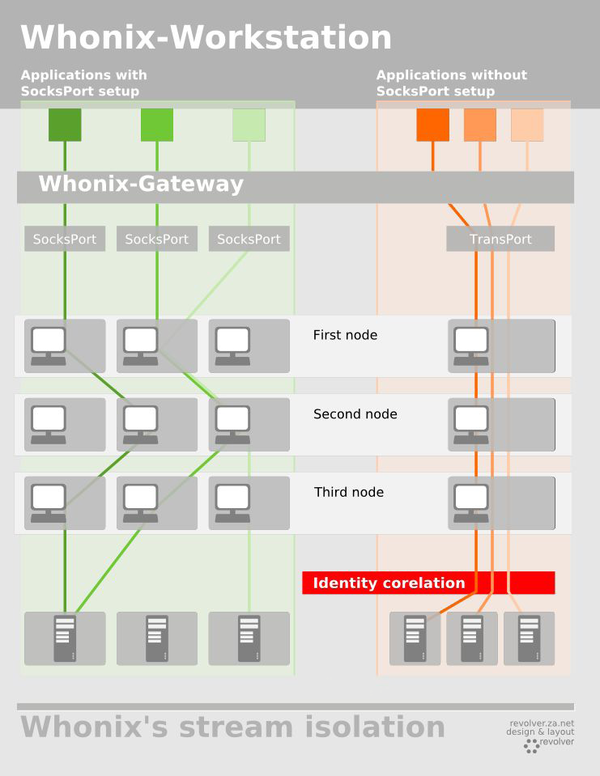
TAILS распространяется в форме немодифицируемого Live CD не только для защиты от троянов и от возможных утечек конфиденциальных данных при получении физического доступа к машине, но и для банальной «защиты от дурака». Разработчики не могут быть уверены, что пользователь корректно настроит каждое установленное им приложение и не спровоцирует утечку данных или раскрытие своего IP. А если систему нельзя менять, то и проблема пропадает сама собой.

[Whonix](https://whonix.org/), с другой стороны, изначально разрабатывался с оглядкой на возможность модификации системы и «настройки под себя», поэтому, кроме используемых в TAILS методов защиты от утечек и фингерпринтинга, здесь реализована довольно интересная архитектура с применением виртуализации. Whonix распространяется в двух образах VirtualBox: один играет роль шлюза в глобальную сеть через Tor, а второй — это рабочая машина с браузером, чат-, email-клиентами и другим софтом, в том числе тем, что можно установить из репозиториев. Оба образа основаны на Debian.

Единственный способ выйти во внешний мир для рабочей машины — это шлюз, единственный путь трафика во внешний мир из шлюза и обратно — через сеть Tor. Неважно, насколько протекающий софт ты установишь на рабочую машину, он все равно тебя не выдаст. Получить доступ к интернету в обход Tor приложение не сможет, IP-адрес увидит только локальный, именем пользователя для него будет просто user (разработчики не рекомендуют его менять), а информацией о железе — стандартная конфигурация VirtualBox. Тебя не удастся отследить даже по временной зоне, часы здесь настроены на UTC, а для синхронизации времени используются time stamp’ы HTTP-заголовков, отдаваемых случайно выбранными веб-серверами.

Самая же интересная черта системы в том, что она вовсе не требует, чтобы ты использовал именно рабочую машину Whonix. Главный компонент здесь — это шлюз, к которому можно подцепить любую другую запущенную в виртуалке ОС, будь то Ubuntu, Windows или OS X, и получить почти такой же уровень защиты от отслеживания (см. [официальную документацию](https://www.whonix.org/wiki/Other_Operating_Systems)). «Почти такой же» потому, что, кроме графического окружения и набора приложений, рабочая машина Whonix включает набор инструментов и настроек, позволяющих защитить тебя от отслеживания с помощью сравнения типов трафика на выходных узлах Tor (identity correlation through Tor circuit sharing) и определения настроек твоих часов и uptime’а через NTP и метки времени TCP/ICMP (все это подробно описано на [wiki-странице Whonix](https://www.whonix.org/wiki/Time_Attacks" \t "_blank)).

Первая задача здесь решается с помощью [изоляции потоков (stream isolation)](https://www.whonix.org/wiki/Stream_Isolation), все поставляемое в комплекте рабочей машины ПО заранее настроено на использование разных портов Tor (SocksPort) и [враппера uwt](https://github.com/Whonix/uwt" \t "_blank), перенаправляющего трафик на разные Tor-порты, если приложение само не предоставляет такой возможности (используется для apt-get, cURL, Git и других консольных инструментов). Поэтому трафик всех приложений идет через разные цепочки Tor-узлов на разные выходные узлы. Вторая проблема решается с использованием [утилиты sdwdate](https://github.com/Whonix/sdwdate), которая синхронизирует часы не через NTP, а обращаясь к случайно выбранным серверам.

[](https://cs4.pikabu.ru/post_img/big/2016/06/18/0/146619950112483794.png)

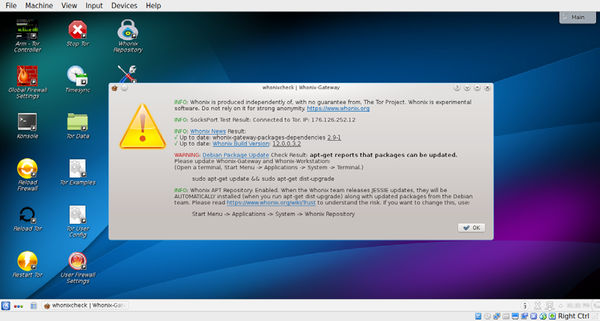
**⬆***Концепция stream isolation*

Whonix поддерживает любые виды туннелирования трафика Tor через VPN/SSH (или наоборот). Эта функция может очень пригодиться, если твой провайдер блокирует Tor (в этом случае VPN-клиент устанавливается на шлюз и Tor использует его для связи с другими узлами), или для скрытия трафика уже после того, как он покинул выходной узел Tor (VPN-клиент устанавливается на рабочую машину, так что Tor роутит уже зашифрованный трафик).

**ПРОБУЕМ**

Итак, Whonix — это два преднастроенных образа для VirtualBox или Linux KVM. Поэтому систему можно запустить в любой операционке, для которой есть официальная версия VirtualBox, а это Linux, Windows, OS X и Solaris. Все, что для этого требуется сделать, — это [скачать](https://www.whonix.org/wiki/VirtualBox#Landing) оба образа (суммарный объем 3,5 Гбайт) и затем импортировать их в VirtualBox с помощью меню File -> Import Appliance.

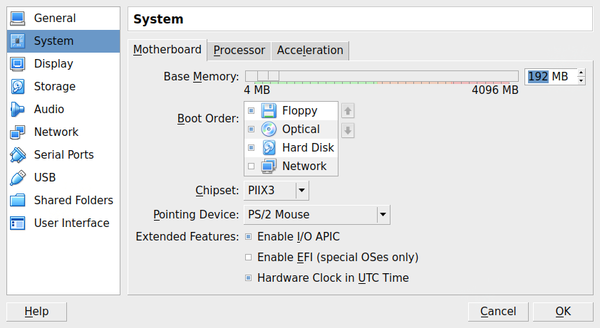
Далее запускаем Whonix-Gateway и дожидаемся его загрузки. После появления рабочего стола (да, у шлюза есть графический интерфейс, так что разберутся даже самые маленькие) система предложит согласиться с дисклеймером, запустить Tor и обновить пакеты, затем запустится утилита whonixcheck, которая проверит подключение к Tor и корректность настроек системы, одновременно с ней отработает служба синхронизации времени sdwdate.

[](https://cs4.pikabu.ru/post_img/big/2016/06/18/0/1466199664119822665.png)

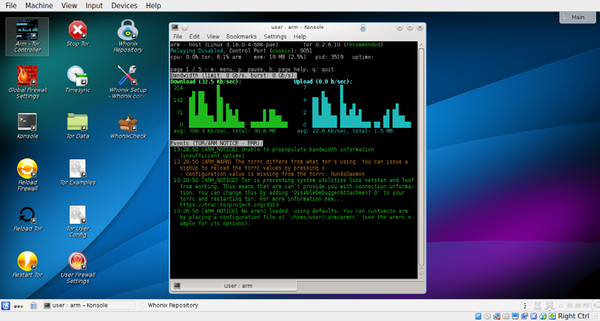
**⬆***Whonixcheck предупреждает о наличии новых версий пакетов*

Сразу скажу о двух неочевидных моментах. Шлюз и рабочая станция Whonix никогда не подключаются к интернету напрямую и используют Tor даже для обновления пакетов из сетевых репозиториев. Поэтому сразу приготовься к довольно значительному проседанию скорости (я получил невероятно медленные по нынешним меркам 500 Кбайт/с).

Второй момент — шлюз совсем не обязательно запускать с графическим интерфейсом, который будет понапрасну жрать оперативку. Более того, здесь есть механизм, автоматически загружающий шлюз в текстовом режиме, если в настройках виртуалки выделить машине 192 Мбайт. Чтобы сделать это, достаточно кликнуть правой кнопкой на Whonix-Gateway, выбрать Settings и на вкладке System сдвинуть ползунок до значения 192. В итоге ты ничего не потеряешь, так как все, что позволяет сделать графический интерфейс, — это перезапустить Tor кликом мыши, отредактировать настройки брандмауэра и запустить интерфейс мониторинга Tor под названием arm (и он текстовый).

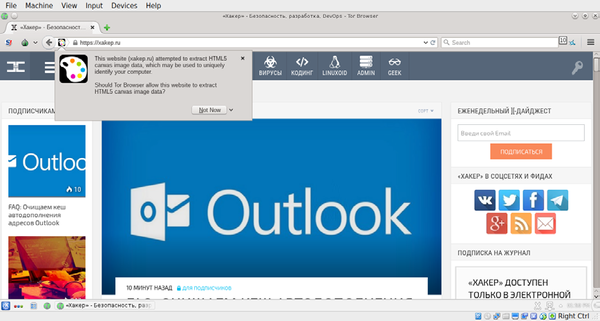
[](https://cs8.pikabu.ru/post_img/big/2016/06/18/0/1466199827178899869.png)

⬆ *Отключаем графику на шлюзе*

[](https://cs8.pikabu.ru/post_img/big/2016/06/18/0/1466199886162857511.png)

⬆ *Текстовая утилита arm*

После окончания загрузки шлюза можно запускать десктоп. Последовательность действий тут почти такая же: запускаем виртуалку, соглашаемся с дисклеймером, соглашаемся обновить пакеты, ждем окончания проверки соединения с Tor и синхронизации времени. Далее можно начать работать. Правда, предустановленных приложений тут кот наплакал. Из повседневно необходимых только Tor Browser, IRC-клиент XChat и KGpg. Причем первый даже не установлен; после клика по иконке запускается инсталлятор, который предлагает выкачать браузер через Tor.

[](https://cs4.pikabu.ru/post_img/big/2016/06/18/0/1466199948165978668.png)

**⬆** *Tor Browser*

Остальной необходимый софт ты волен ставить из репозиториев с помощью стандартной команды «sudo apt-get install приложение». В ответ на запрос пароля вводим changeme и, конечно же, меняем пароль с помощью команды passwd.

**STREAM ISOLATION**

Устанавливая сторонний софт в Whonix, ты сразу столкнешься с проблемой, называемой identity correlation through Tor circuit sharing. Не решусь перевести этот термин, просто скажу, что по умолчанию левый софт использует системные настройки SOCKS-прокси, а это единый стандартный порт Tor (TransPort). Проблема такой настройки в том, что, просто сравнивая типы трафика и их временную связь (например, ты можешь использовать Telegram одновременно с WhatsApp), выходной узел может установить связь между разными сеансами использования приложений и идентифицировать тебя (но не твой IP или географическое положение).

Для борьбы с данным типом атаки в Tor есть механизм, названный stream isolation, он позволяет разделить трафик разных приложений, направив его в разные цепочки узлов Tor. Использовать его довольно просто — надо всего лишь создать в настройках Tor несколько дополнительных портов SOCKS и настроить сами приложения так, чтобы они использовали разные порты. Whonix уже имеет такие [настройки](https://www.whonix.org/wiki/Stream_Isolation): предустановленный софт использует порты 9100–9149. Также в нем есть набор свободных портов для стороннего софта:

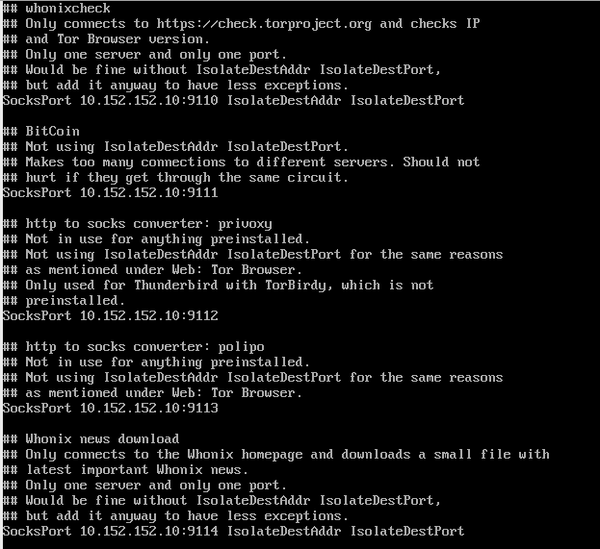
• 9153–9159 — свободные;

• 9160–9169 — свободные с опцией IsolateDestAddress;

• 9170–7179 — свободные с опцией IsolateDestPort;

• 9180–9189 — с обеими опциями.

Все, что остается, — это настроить софт на использование адреса**10.152.152.10** и любого из этих портов в качестве адреса SOCKS-сервера. Причем использовать порты с опциями IsolateDestPort и/или IsolateDestAddr я бы не рекомендовал. Они разделяют даже трафик одного приложения на основе адреса удаленного порта или адреса. В большинстве случаев это избыточно и очень накладно (представь, если торрент-клиент или веб-браузер будет использовать разные цепочки узлов Tor для всех соединений).

[](https://cs8.pikabu.ru/post_img/big/2016/06/18/0/1466200329185811808.png)

**⬆***Настройки портов для предустановленного софта*

**ВЫВОДЫ**

Whonix, при всех своих странностях и неоднозначностях, определенно стоитвнимания любого, кто хочет обеспечить свою анонимность в Сети. По умолчанию это всего лишь система для запуска Tor Browser, однако при наличии рук и свободного времени из Whonix можно сделать полноценную рабочую систему, и необходимость запуска системы в виртуалке этому нисколько не мешает. Ну и конечно же, стоит помнить, что абсолютной анонимности не существует. Если надо — тебя найдут. Следи за собой, будь осторожен.