Защищенное пребывание в сети и признаки безопасных сетевых технологий (2xTor+TorBrowser+I2P+Tox)

Владимир

После того, как «**Интернет**» получил «**Массовое распространение**», большинство людей радовались открывшимся новым возможностям поиска «**Информации**». Но через определенный «**Промежуток времени**», когда эта функция «**Интернета**» стала для всех «**Привычной**», его начали стремиться «**Максимально эффективно**» использовать для получения «**Личной выгоды**» из-за большой «**Аудитории**» пользователей «**Интернета**». Это стало новым периодом развития для «**Интернета**». Появилась необходимость в навыках «**Защищенного**» использования «**Интернета**» и «**Прививки правильных ориентиров**» при подборе «**Безопасных сетевых технологий**».

Первым делом, предлагаю «**Попытаться осилить**» двух часовой «**Обзорный ролик**», который позволит понять, как «**Правильно**» подбирать «**Безопасные технологии**», по каким «**Критериям выбора**». Кроме этого, он покажет «**Существующие**» решения. Их можно использовать уже «**Сегодня**». Выделим следующие «**Перспективные**» технологии: «**Hyperboria**», «**Tribler**». Подробнее: «**Hyperboria: Интернет 2.0**», «**Hyperboria: Как все устроено**», «**Hyperboria: Маршрутизация**», «**Tribler сделал торрент-трекеры архаизмом**».

https://www.youtube.com/watch?v=Tiohs-bvEZw https://www.youtube.com/watch?v=cK73sYM3g0Q

Далее будет рассмотрен «**Метод**», который «**Рекомендуется**» использовать для обеспечения «**Повышенной защищенности выхода**» в «**Интернет**», он позволяет «**Компенсировать**» некоторые недостатки сетей «**Tor**»: «**Уязвимости защиты входных соединений из-за перебора конечного множества известных открытых ключей**» (необходимо увеличить количество «**Промежуточных узлов**»), «**Повышенную вероятность попадания в цепочку одних и тех же популярных узлов, особенно при включенной функции выбора узла с быстрой скоростью**» (необходимо увеличить количество «**Промежуточных узлов**»), «**Отслеживание трафика на входе и выходе**» («**Джиттер**» может таким образом носит более «**Непредсказуемый**» характер, но эффективнее «**Зашумить**» трафик) и т.п. Наиболее «**Простой**» способ добиться подобного «**Эффекта**» будет рассмотрен далее.

«**Рекомендуется**» использовать компьютер с «**Безопасной сборкой**» системы «**Linux**» без доступа в «**Интернет**» и без драйверов для «**Устройств Интернета**», по возможности, «**Отключить аппаратно**». В данную «**Базовую ОС**» необходимо установить среду «**Виртуализации**» с «**Открытым кодом**», например, «**VirtualBox**». Создать в ней «**Две**» «**Виртуальные машины**»: «**Whonix Gateway**» и «**Parrot Security OS**». «**Whonix Gateway**» с выходом в «**Интернет**» через модульную «**USB Сетевую карту**» и доступом к внутренней сети «**Whonix**». «**Parrot Security OS**» только с доступом во внутреннюю сеть «**Whonix**».

Для того, чтобы «**VirtualBox**» смог подключать любые «**USB устройства**» напрямую в «**Виртуальную машину**», в некоторых «**Linux**» необходимо добавить «**Пользователя**» системы в группу «**Vboxusers**» и «**Перезагрузить**» компьютер.

Настройка «Tor» шлюза «Whonix Gateway» (Первый уровень защиты)

Виртуальная машина с «**Whonix Gateway**» предоставляется максимально настроенной для ее безопасного использования, поэтому нужно будет внести только небольшие изменения в конфигурацию системы. Данная система не предназначена для работы в ней и служит только для защиты.

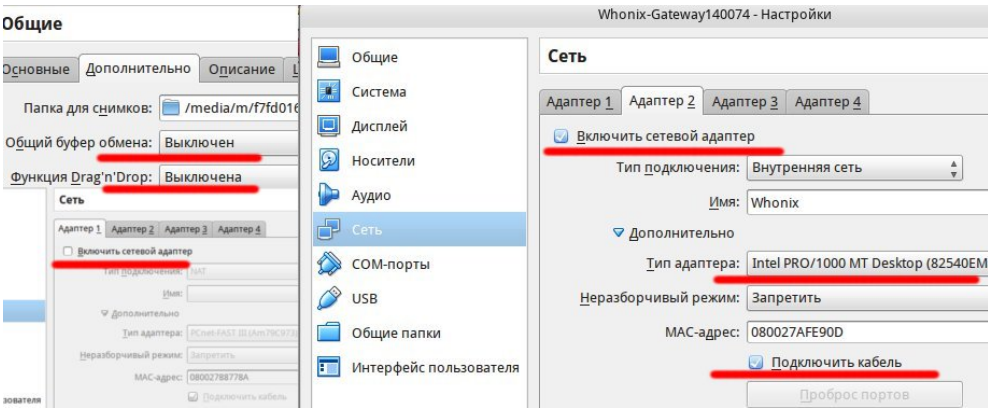
После распаковки «**Whonix Gateway**» рекомендуется обязательно внести следующие изменения:

- выключить «**Общий буфер обмена**»;

- выключить «**Функцию Drag'n'Drop**»;

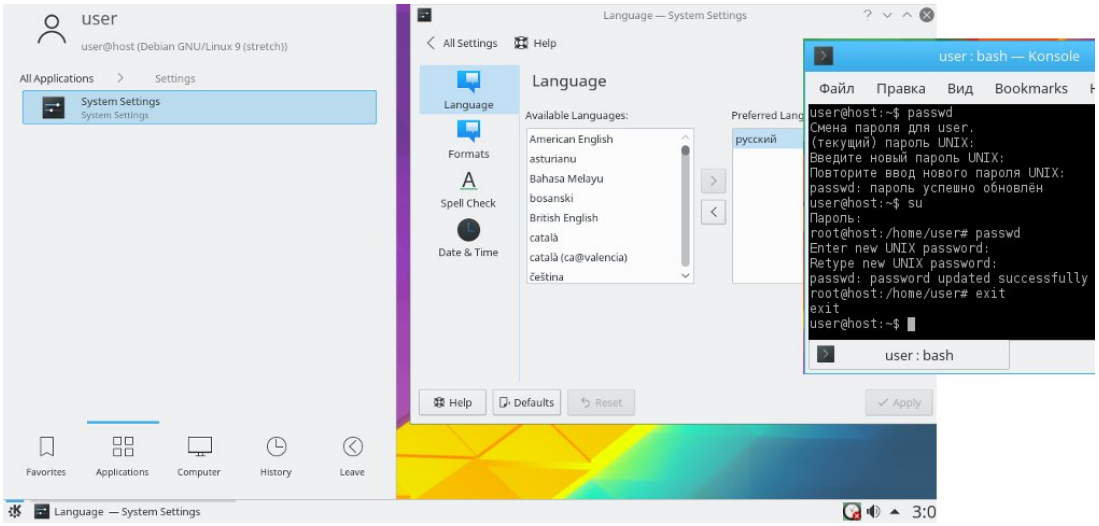
- выключить «**Сетевой адаптер в режиме NAT**», потому что в реальной ОС предполагается, что доступа в «**Интернет**» нет на программно-аппаратном уровне и он возможен только через модульную «**USB Сетевую карту**»;

- сменить эмулятор сетевой карты для внутренней сети на «**Intel PRO/1000 MT**», сетевая карта должна включаться при запуске «**Виртуальной машины**» (режим «**Подключить кабель**»).



После запуска «**Whonix Gateway**» доступ в «**Интернет**» будет невозможен, потому что в системе не установлены по умолчанию службы подключения сменных устройств и интернет соединений, как во многих других пользовательских «**Linux**». Кроме этого, к сожалению, данная ОС позволяет устанавливать только обновления системы «**Linux**», на которой основан дистрибутив «**Whonix Gateway**», но версию дистрибутива, пока что, не удалось обновить автоматически, без скачивания нового образа «**Whonix Gateway**», не смотря на то, что все необходимые репозитории «**Whonix Gateway**» подключены. Надеюсь, в будущем это исправят.

Первым делом, рекомендуется сменить пароль «**Пользователя**» и «**Root**» со стандартного пароля: «**changeme**» и изменить язык системы на русский.

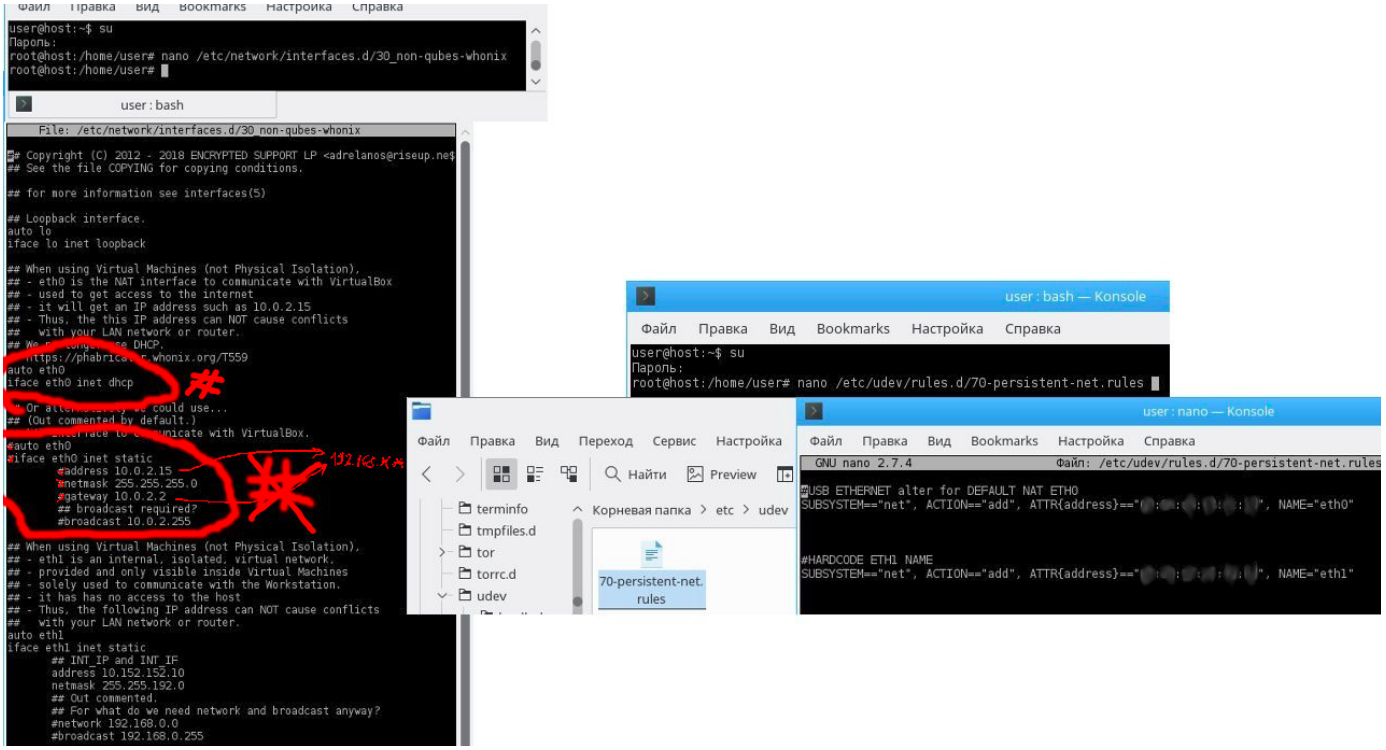


«**USB Сетевую карту**» в такой системе необходимо подключать в самом начале ее запуска. Для этого необходимо подключить данное устройство и прописать в фильтрах USB устройств, чтобы происходило автоматическое переключение сразу при запуске «**Whonix Gateway**». В реальной системе рекомендуется удалить драйверы и, как минимум, отключить автоматическое подключение к сети и автоматическое получение адресов «**IPv4**», «**IPv6**» и т.п.

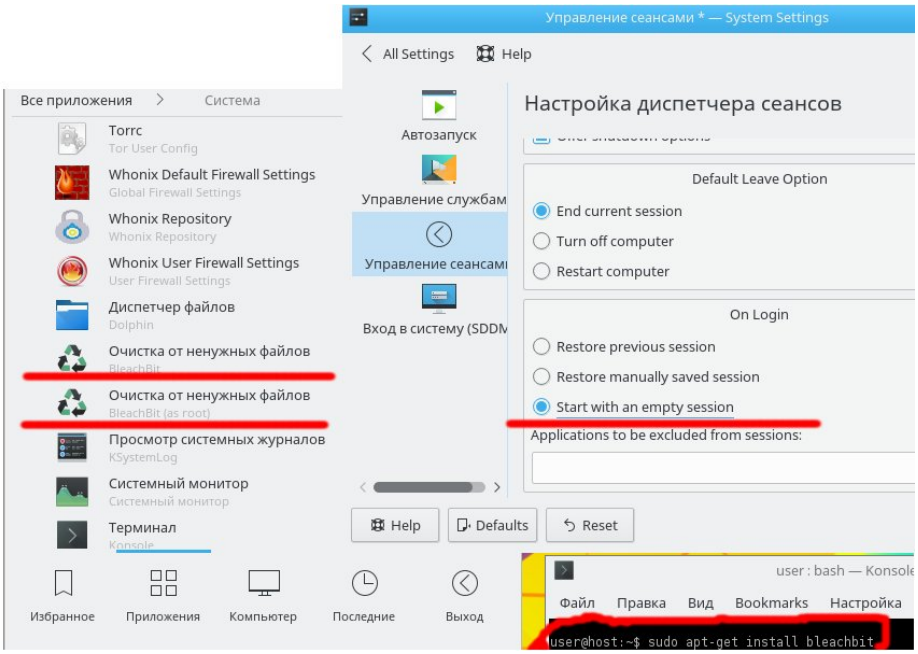
Из-за того, что мы изменили способ выхода в «**Интернет**» через «**USB Сетевую карту**», а не «**NAT через реальный компьютер**», то нам необходимо не статически, а динамически получать параметры у «**DHCP**» маршрутизатора *(В новой версии разработчики удалили пакеты обслуживающие «**DHCP**», поэтому прописываем статически)*. Поэтому, раскомментим необходимые строки в файле «**/etc/network/interfaces.d/30_non-qubes-whonix**» только в отношении «**eth0**». Параметры «**eth1**» можно не менять, но необходимо запомнить, они пригодятся при настройке внутренней сети в «**Parrot Security OS**».

(*Прим. ред.* Хотя, в «**Parrot Security OS**» достаточно программ, чтобы не запоминать эту информацию)

Теперь, жестко пропишем параметры сетевых устройств: «**eth0**» - для «**USB Сетевой карты**», «**eth1**» - для внутренней сети. Почему это необходимо делать? Во первых, при подключении «**USB Сетевой карты**» система может присвоить ей имя отличное от «**eth0**», во вторых в «**Whonix Gateway**» в межсетевой экран внесены особые настройки относительно имен «**eth0**» и «**eth1**», поэтому названия должны сохраниться, чтобы не менять все остальное. Для этого необходимо отредактировать файл «**etc/udev/rules.d/70-persistent-net.rules**».



Рекомендуется, после настройки и обновления системы, очистить ее, например программой «**Bleachbit**» и сделать снимок для постоянного сброса состояния системы до исходного после работы в ней. При возникновении обновлений, повторить процедуру: запустить из снимка, обновить, почистить и сделать новый снимок виртуальной машины и только потом запускать для работы. Также, рекомендуется выключить в «**Whonix Gateway**» сохранение сессии рабочего стола (например, расположения окон на рабочем столе).



В ходе персональных исследований технология «**Tor**» проявляла признаки ее не безопасности. Даже при всех перечисленных здесь способах серьезного повышения надежности технологии «**Tor**» организационными и конфигурационными мерами. Но подобная система, тем более, правильно сконфигурированная серьезно усложняет слежение за вами.

Действительно анонимное и безопасное пребывание в сети, то что обычно ожидается при использовании системы «**Tor**» можно получить только в следующих случаях:

1) «**2xTor**»+«**I2P**» для организации безопасного «**Интернет**» (от настроек «**I2P**» и доверия к соседним внесенным узлам тоже серьезно меняется уровень надежности данной технологии, но в целом, сочетание двух технологий позволяет получить что-то действительно приближенное к понятию безопасности).

2) «**2xTor**»+«**Tox**» позволяет получить серьезный уровень безопасности для «**VoIP**» технологии. При условии, что логин вносится вручную в виде открытого ключа и получается непосредственно у контактируемого человека, либо из доверенных или перепроверенных по другим каналам источников. Рекомендуется для особо важных файлов применять дополнительное их шифрование перед передачей.

Не мало важной в повышении надежности «**Tor**» является конфигурация параметров данной технологии в файле «**torrc**». Данных параметров много, но рекомендуется активно использовать следующие:

- «**ExcludeNodes**», «**ExcludeExitNodes**» для исключения по стране, участников цепочек «**Tor**», например, тех стран, где активно отслеживают весь трафик. Главное не переборщить и не использовать данные параметры на всех уровнях «**Tor**» (например, в «**TorBrowser**» рекомендуется не исключать никаких узлов, иначе могут возникнуть проблемы разрешения имен внутренних сайтов «**.onion**», а в «**Whonix Gateway**» и «**Parrot Security OS**» можно импровизировать, практически как угодно и это повысить уровень безопасности);

- «**HardwareAccel 1**» позволяет использовать аппаратное ускорение для шифрования, если это возможно;

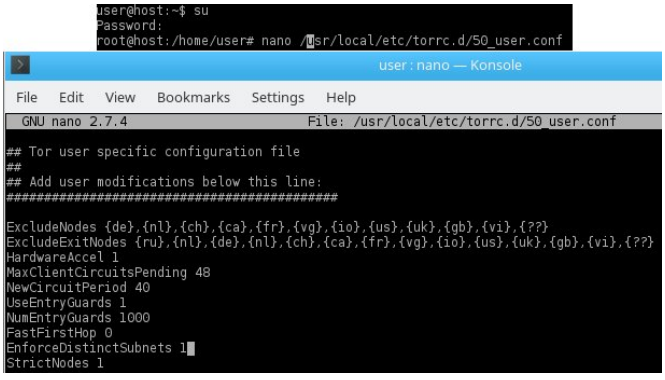
- «**MaxClientCircuitsPending**», «**NewCircuitPeriod**» максимальное количество одновременных цепочек для разных программ(вкладок) пользователя и временной интервал для построения новой цепочки в секундах;

- «**UseEntryGuards 1**», «**NumEntryGuards**» включение долгосрочных узлов в качестве входных для повышения безопасности и количество таких узлов (рекомендуется не придерживаться определенных узлов в «**Whonix Gateway**» и «**Parrot Security OS**», но придерживаться таковых в «**TorBrowser**»;

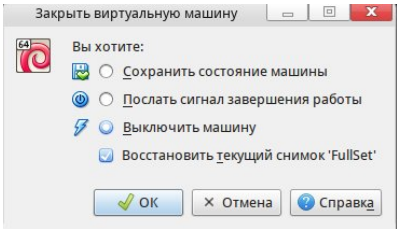
- «**FastFirstHop 0**» выключение позволяет не принимать наиболее скоростной узел, как приоритетный, что увеличивает вероятность использования одних и тех же скоростных узлов;

- «**EnforceDistinctSubnets 1**» для того, чтобы в цепочках не повторялись страны, даже если повторяются, то это происходить гораздо реже и обязательно узлы находятся в разных подсетях;

- «**StrictNodes 1**» обязательное исполнение введенных вами настроек для узлов.



Рекомендуется после работы, все время сбрасывать систему до исходного настроенного состояния и изменять снимок только в случае обновления системы.



Настройка «Parrot Security OS» (Второй уровень защиты)

После запуска Parrot Security OS необходимо включить режим Anon Surf и запустить Tor-browser для серфинга в Интернете. Задать необходимые настройки безопасности данного браузера. Конфигурацию Tor в Whonix Gateway и Anon Surf (etc/tor) рекомендуется изменить в torrc на наиболее эффективную и безопасную (пример конфигурации ниже).

Настройка «TorBrowser», «I2P» и «Tox» (Третий уровень защиты)