Преимущества и недостатки собственного сервера для туннелирования трафика

Арс Либрев 03.07.2025

Существуют разные методики туннелирования трафика. Одна из их целей — сокрытие метаданных, т.е. сведений о том, кто с какими ресурсами соединяется. Осуществляется это за счет пропускания запросов через промежуточные узлы. То есть, пользователь не напрямую подключается к какому-то сайту, а через промежуточный сервер. В этом случае провайдер и иные следящие системы не видят, к какому ресурсу обращается пользователь, а видят его обращение к этому серверу. Ресурс же не видит, кто обращается к нему, а видит запрос с данного сервера. Пожалуй наиболее известным является использование для этого VPN. Как не сложно заметить, в такой схеме, уже этот сервер видит и то, кто обращается и куда обращается. Поэтому одним из очень популярных решений является настройка собственного сервера для туннелирования, для чего, как правило используется арендованный сервер. Считается, что у этого подхода сплошные преимущества и свой сервер решает все проблемы, которые имеются у не своего. Даже иногда утверждается, что это надежнее, чем соединение с ресурсами через цепочку узлов, неподконтрольных непосредственно вам. Так ли это? В этом сегодня постараемся разобраться.

Считается, что при настройке своего сервера для туннелирования, в частности VPN-сервера, с него станет невозможным слить никакую информацию о ваших Интернет-прогулках, ведь вы его контролируете. Вы можете настроить его так, что он не будет собирать логи — информацию о том, к каким ресурсам вы подключались. На самом деле, хоть вы и контролируете то, что происходит на сервере, но соединения, идущие к нему и от него, также доступны тому, кто дал вам сервер в аренду, ведь это его сервер и его инфраструктура. И даже если он сам не собирает такую информацию, она имеется у провайдера, который подключает его сервера — в том числе арендованный вами — к Интернету. Таким образом, метаданные вашего соединения будут точно также доступны третьему лицу, как и в случае, если вы просто купите услугу VPN-соединения, или даже подключитесь к какому-то бесплатному серверу.

Кто-то может возразить, но ведь такой — неподконтрольный вам — сервер может не только видеть метаданные, но и собирать данные. То есть не только сведения о том, к каким ресурсам вы подключаетесь, но и что именно вы передаете, например, при общении, или что именно вы просматриваете на конкретном ресурсе. В общем это верно. Однако, чтобы обезопасить это,

используется шифрование на уровне соединения с целевым ресурсом, с сайтом. Сейчас большинство сайтов применяют шифрование. Что касается немногочисленных ресурсов, которые не используют шифрование, то тут речь идет о данных, которые и так лежат публично, а чтобы скрыть факт вашего обращения к ним можно использовать цепочку узлов. Еще раз повторяю, метаданные нельзя спрятать как таковые, в отличии от данных, которые можно скрыть за сквозным шифрованием или в криптоконтейнере (об этом далее). Их можно лишь запутать — сделать так, чтобы не было узла, который знал бы одновременно и то, кто осуществляет запрос, и то куда этот запрос. Для этого применяется не один перевалочный узел, а цепочка нод. Если же говорить об инструментах для общения, то сейчас все они также применяют шифрование на уровне протокола, о котором говорилось до этого. К тому же, большинство таких инструментов применяет также сквозное шифрование, то есть информация шифруется непосредственно на вашем устройстве, и даже сервер, осуществляющий взаимодействие общающихся, не знает содержимое их разговоров. Это имеется не у всех средств для общения, например этого нет в соц. сетях. Но серьезные инструменты все же используют это. Разумеется для общения желательно применять именно их.

Но ведь шифрование можно вскрыть, может быть поэтому лучше контролировать узел? Если уж на то пошло, точно также взломать можно и ваш собственный сервер. Большинству пользователей вряд ли стоит опасаться такого серьезного внимания недоброжелателей. Если же у вас есть основание предполагать, что вас будут настолько целенаправленно и настойчиво разрабатывать, то рациональней озаботиться не контролем своего сервера, который — повторяю — также можно взломать, а передавать информацию, завернув ее в криптоконтейнеры. При этом может быть даже стоит создать двойной контейнер. К примеру зашифровать данные в контейнере LUKS, а этот контейнер поместить в еще один, например VeraCrypt. В этом случае дыры разных типов шифрования будут взаимно погашены. Проломить такое будет непомерно сложнее.

Итак, насколько видно из сказанного, использовать необходимо именно цепочку узлов, поскольку отдельный узел, каким бы он ни был, не способен скрыть метаданные — не способен дать анонимности. Для подключения через цепочку удобнее всего применять сеть Tor — распределенную сеть серверов с луковой маршрутизацией. Сервера держаться различными организациями, университетами и энтузиастами по всему миру. Таким образом, нет единого поставщика, который бы держал информацию обо всех подключениях в сети. Корневые сервера обеспечивают предоставление узлам информации друг о друге, а отдельные узлы контролируются разными людьми и организациями,

подключенными к разным провайдерам в разных странах. Я не буду здесь подробнее останавливаться на том, как работает эта сеть, какие методы деанонимизации в ней существуют и разбирать мифы о ней. Все это я уже делал в иных публикациях.

Но может быть при использовании цепочки имеет смысл включить в нее свой собственный сервер? В том, чтобы создать свой сервер VPN перед Tor действительно есть преимущества. Это позволяет предотвратить деанонимизацию в случае усиленной разработки, когда у тех, кто ее проводит есть возможность определить приблизительно ваше местонахождение, к примеру до города. В этом случае, они могут узнать у провайдера, кто подключался к Tor, если видят, что действия производятся через Tor, и определить корреляции активности. Однако, в случае использования VPN перед Tor, это не сработает. Поскольку провайдер не будет видеть, что вы подключаетесь к Tor. И соответственно, это не станет известно. Такая схема позволяет препятствовать его идентификации провайдером и другими следящими системами. Однако у Tor есть собственные механизмы, препятствующие такой идентификации. Зачастую эта проблема не менее эффективно решается с помощью простых обфусцированных мостов самого Tor. Уж точно этой меры будет достаточно тем, кто просто просматривает сайты или осуществляет общение с теми, кого знает лично. Использование дополнительного VPN, тем более собственного, может иметь реальный смысл только для тех, кто публикует что-то и у него есть основания считать, что его могут серьезно разрабатывать. Также стоит понимать, что по сегодняшним временам такие протоколы как VPN тоже требуют маскировки, и не всегда она оказывается надежнее, чем та, которую способны обеспечить инструменты Tor. Поэтому при настройке своего сервера также необходимо озаботится ими.

Кроме того, при имеющихся преимуществах, необходимо учитывать вот какой момент. Вашему провайдеру будет видно, что вы подключаетесь к некоему серверу. Если вы маскируете его протокол, он не увидит сходу, что это VPN. Ему не будет известно, арендованный ли это вами сервер или какой-то сайт, размещенный на нем. Однако для аренды вам придется его оплатить. И если кто-то начнет вас серьезно разрабатывать, он сможет проверить ваши платежи и это обнаружит, проверит подключения у провайдера и сможет предположить, что это ваш личный VPN. К тому же, если вы с этого VPN подключаетесь к Tor напрямую, то это также может выяснится, если провайдер этого VPN-сервера, или точнее, в случае вашего собственного сервера, провайдер того сервиса, на чьем сервере, вы развернули свой VPN, сольет данные о производимых с него подключениях, или эти данные будут получены путем взлома. Напомню, отсутствие логов может помочь лишь в тех случаях, в которых ломается сам

сервер, но если взаимодействие идет с поставщиком — с арендодателем хостинга — или напрямую с его провайдером, это не поможет. Поэтому даже при использовании такого сервера, для подключения к Tor лучше использовать обфусцированные мосты.

Разумеется многие возразят, можно ведь оплачивать криптовалютой. Во-первых, если мы говорим о России, то здесь оплачивать что-либо криптовалютой незаконно, и если сей факт вскроется могут быть большие проблемы. И тот факт, что сервис заграницей не спасет, если вы сами при оплате находитесь на территории России. Правда, когда я написал об этом после изучения юридических материалов, говоря о том, почему нет возможности финансовой поддержки проекта, мне возразили, что на самом деле якобы при оплате криптовалютой зарубежных сервисов никаких претензий не будет — главное не оплачивать что-либо на территории самой страны. Это противоречит тому, что я узнал в ходе изучения иных материалов, хотя заявление и исходило, насколько можно судить, от профессионального юриста. Кто прав не знаю. Имейте ввиду.

Во-вторых, криптовалюта не анонимна. Цепочки транзакций вполне поддаются раскрутке, если речь идет об обычных наиболее популярных валютах. Конечно, есть анонимные криптовалюты — те, которые имеют специальные механизмы для анонимизации транзакций. Однако и их также можно раскрутить, хотя методы для этого, конечно значительно сложнее. Но самое главное, что вероятно этого и не придется делать.

В-третьих, криптовалюту нужно где-то достать. Где? Намайнить самому? По сегодняшним временам с обычного компьютера не выйдет. Кроме того майнинг также вводится в тиски законодательства. Остается покупка за обычные деньги. С обычных счетов. Привязанных к личным данным. Схемы с подставными счетами, это уже совсем жуть — незаконная, замороченная и оставляющая следы, которые почти невозможно замести.

В общем, когда вам приходится иметь дело с оплатой чего-либо, это всегда риск, всегда слабый момент в любой схеме. Любая необходимость иметь дело с финансовыми потоками, снижает анонимность. Да, это противоречит распространенной позиции, что большая анонимность требует больших денег. Я утверждаю — деньги негативно сказываются на анонимности. Какую бы деятельность вы не вели, пока вы не касаетесь финансов, вероятность того, что вас не заметят очень велика. Но как только вы начинаете касаться денег, это становится интересно и гос. структурам и злоумышленникам. Затраты на сервер могут быть оправданы только в очень узких, определенных ситуациях. Если у вас есть стойкая уверенность, что вами так и так заинтересуются, то может иметь смысл подключаться к оплаченному серверу перед остальными

узлами цепочки анонимизации. Это может затруднить попытки недоброжелателей добраться до вас. Но как будет показано далее, это буквально единственная ситуация, где аренда сервера для своего узла туннелирования может иметь смысл.

Также иногда можно встретить рекомендацию развернуть на арендованном сервере свою выходную ноду Tor. Обосновываться это может тем, что на выходной ноде трафик расшифровывается, и она может собирать данные. А в случае вашего контроля ее, этого можно не опасаться. От прослушивания на выходной ноде спасает шифрование, о котором уже было сказано достаточно. Никакой необходимости контролировать ноду для своей безопасности нет. Что касается сбора метаданных, то он здесь также безвреден, поскольку эта нода не знает кто именно производит обращения к тем или иным сайтам. И даже если вы будите ее контролировать, метаданные все равно будут доступны арендодателю, у которого вы арендуете сервер, и его провайдеру. То есть они в любом случае будут кому-то доступны. Больше того, использование своей ноды может только негативно сказаться на анонимности, ведь вы всегда будите использовать один и тот же узел, и если в сети появится глобальный пассивный наблюдатель, ему будет легче вычислить вас — легче провести корреляции трафика, чем в случае, если бы этот узел менялся, как иные узлы в цепочке. Кроме того, к этой ноде будите подключаться не только вы, а любой пользователь Tor. И поскольку именно с этой ноды происходит обращение к ресурсам, если кто-то совершит через нее какие-то действия, которые не понравятся власть имущим, то проблемы могут быть у вас. Известны случаи, когда владельцев выходных нод арестовывали за то, что пользователи использовали их ноды для незаконных действий. И тут мы снова возвращаемся к вопросу оплаты сервера, ведь именно она является наиболее прямым выходом на вас. Об этом выше уже сказано достаточно, насколько стоит доверять анонимным криптовалютам, решать вам. По мне это не очень надежный вариант в таком серьезном деле. Безусловно польза от своей выходной ноды есть. Она в том, что ей вы поддержите сеть. Но в отношении вашей собственной безопасности она принесет больше проблем, чем пользы.

Еще иногда может встретиться рекомендация подключаться к VPN за Tor. Это может иметь смысл поскольку такая схема позволяет скрыть от сайтов факт использования Tor. Иногда рекомендуется подключать для этих целей также свой сервер. Или утверждается, что платные будет более надежны, чем общедоступные бесплатные. Но при использовании таких серверов, вы предоставляете им свои данные, и соответственно смысл подключения к ним через Tor пропадает. Даже если для авторизации сервер не требует личные данные все равно остается проблема с оплатой, о которой уже говорилось

выше. Но есть и еще одна, куда более важная проблема. Дело в том, что при длительном использовании одного VPN, он может собирать на вас статистику, что даже в случае обезличенного подключения негативно сказывается на приватности. Подчеркну еще раз, что даже если сервер настроили вы сами, статистику по подключениям может копить арендодатель или его провайдер. Также и ресурсы, которые вы регулярно посещаете смогут сопоставить вашу активность с конкретным ip такого VPN. Соответственно, в разных сеансах вы и будете идентифицированы как один и тот же пользователь. Это еще одна причина, по которой не стоит для таких целей использовать платные, авторизованные VPN или собственные, настроенные на арендованном сервере. Лучше всего использовать бесплатные короткоживущие VPN. И только в исключительных случаях, когда действительно есть проблемы с подключением к сайту. Также в качестве альтернативного метода, сайт, отказывающийся открываться через Tor можно открывать в Web-архиве. Сайты с динамическим содержимым, препятствующие доступу к себе через Tor, лучше не посещать.

Таким образом, наиболее рациональной методикой для большинства пользователей является обычное подключение к Tor через обфусцированные мосты. Для случаев когда сайт отказывается корректно открываться через Tor можно применять за ним VPN — бесплатные и общедоступные. Это не привяжет вас к конкретному серверу, дополнительно растворит среди пользователей, поскольку не вы один будите его использовать, и не будет иметь следов к вам, поскольку вы не оставляете их ни в виде авторизационных данных, ни в виде оплаты. В случае же если у вас есть повод опасаться серьезного вычисления вас, можно использовать VPN перед Tor, но также с обфускацией соединения с ним и обфускацией подключения от него к Tor. Поскольку такой VPN необходимо, чтобы был стабильным и быстрым, бесплатные короткоживущие здесь не подойдут, вероятно вам так или иначе придется его покупать, т.е. производить оплату. А раз так, то действительно в этом случае надежнее использовать свой VPN.

Настроить такое подключение можно с использованием связки виртуальных машин. Наиболее надежным инструментом является Whonix. В этом случае виртуальная машина, используемая в качестве шлюза, все соединения заворачивает в Tor, к которому можно подключаться через обфусцированные мосты. А в виртуалке, из-под которой осуществляется Интернет-активность — соединенной со шлюзом по виртуальной локальной сети и получающей Интернет с нее — можно подключить VPN, который пройдет через цепочку Tor и соединиться с сервером за ним. Если же нужен VPN перед Tor, то его можно настроить на хосте с которого раздается Интернет на шлюз по технологии NAT.

И вот тут имеет место еще один миф. Чтобы его разобрать необходимо

обратиться к одной методике анонимности, которую иногда предлагают как самую надежную.

В сети можно найти методики анонимности, предлагающие организовывать такую схему, в которой для VPN перед Tor используется свой сервер, для выходной ноды Tor также используется свой сервер и для VPN за Tor используется свой сервер. Однако поводом для таких подключений является не попытка контролировать определенные узлы.

Автор таких схем опасается, что при создании такой цепочки с помощью Whonix, трафик будет идти не последовательно, а параллельно. То есть прямые соединения с хоста будут идти через VPN, а те, что идут по NAT — из виртуалки, со шлюза — будут идти в обход него. Это не так. При создании VPN-соединения на хосте, трафик из Whonix будет идти также через него. Это можно легко проверить, если сделать такое соединение на хосте, затем по NAT подключить любую виртуалку, без инструментов туннелирования и посмотреть ip. Если трафик идет параллельно, то в виртуалке будет ваш ip. Если последовательно, то ip VPN-сервера. И я вас уверяю, вы увидите именно его. Даже без специальных настроек фаервола. Многие VPN-клиенты, реализующие отключение от Интернета, в случае обрыва VPN-соединения, чтобы трафик не пошел в голую, используют для этого настройку пользовательских цепочек iptables (кто не знает, это фаервол в системах GNU/Linux) и они также заворачивают в VPN-соединения, подключения как из самой системы (хоста), так и по NAT. Теоретически можно создать комплект правил, чтобы соединения из NAT обходили VPN, но сомневаюсь, что какой-либо VPN-клиент станет его реализовывать. В этом просто нет смысла. Докучи, для создания цепочек Tor через VPN подключать VPN на хосте, рекомендуют сами разработчики Whonix, об этом прямо говорится на их официальном сайте, причем в нескольких местах. Что же они не знают, как работает их инструмент? Или специально дают вредительсткие рекомендации? Вряд ли кто-то станет такое утверждать всерьез. Кроме того, у них же говорится, что имеются проблемы с таким соединение при использовании некоторых VPN-клиентов, реализующих отключение от Интернета в случае обрыва VPN-соединения, и системы виртуализации QEMU/KVM. Если бы таких соединений вообще не происходило, то такие оговорки бы не появились. А так они возникают, есть еще эта, и эта.

То есть реализация, которую дает Whonix намного удобнее и надежнее. Этот же метод, с тремя своими серверами, вобрал в себя все проблемы, которые были здесь расписаны. Как бы я ни старался, у меня не получается увидеть ситуацию, в которой этот подход был бы более удачным.

Короче говоря, применение схемы с подключением к Tor без своих серверов,

лишь с использованием обфусцированных мостов и в некоторых случаях VPN за Tor с помощью системы Whonix подойдет большинству пользователей. Для каких-то серьезных ситуаций можно использовать VPN перед Tor, настроенный на своем сервере, также применяющий обфускацию. Все остальные усложнения и подключение иных своих серверов только снизит анонимность и безопасность. Для приватности эти действия ничего не дают.