Разное Как сохранить анонимность в сети

Рагнар · 13.05.19

ОТВЕТИТЬ

Отслеживать

Рагнар

Администратор

Регистрация: 08.05.19 Сообщения: 49,999 Реакции: 150,157

13.05.19

Оцените: ☆☆☆☆☆ Голосов: 0 #1

В чем вообще заключается анонимизация?
Кроме нашумевшего на всех углах интернета мнения о сокрытии IP-адреса есть еще множество других деталей. По большому счету все методы и средства анонимности преследуют цель сокрытия провайдера. Через которого уже можно получить физически точное местоположение пользователя, обладая дополнительной информацией о нем (IP, «отпечатки» браузера, логи его активности в определенном сегменте сети и пр.). А также большинство методов и средств направлены на максимальное сокрытие/нераскрытие этой косвенной информации, по которой позже можно будет спрашивать у провайдера нужного юзера.
Какие есть способы анонимизации пребывания в сети?
Если говорить про обособленные единицы анонимизации (ведь есть еще схемы в виде комбинирования того или иного средства анонимности), то можно выделить следующие:

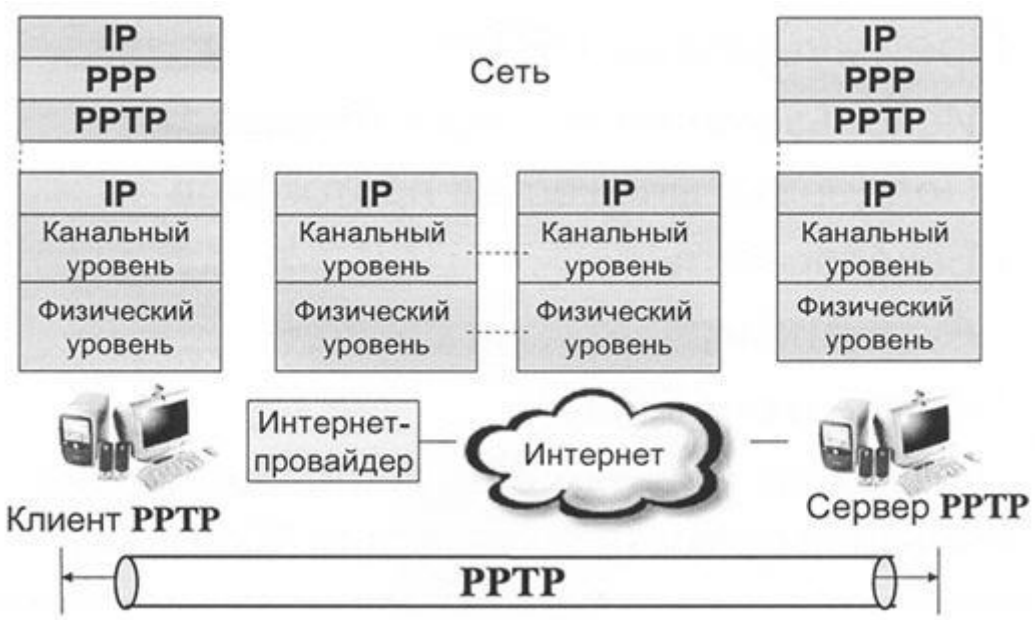
1) Прокси-серверы — бывают разных видов, со своими особенностями. Классификация прокси под спойлером.
HTTP прокси – работает по протоколу http и выполняет функцию кэширования.
Степени анонимности: прозрачные, искажающие, анонимные, элитные.
Цепочку из HTTP проксей можно построить только в том случае, если они поддерживают метод CONNECT, исключением есть построение цепочки с помощью спец. программы.
HTTPS прокси (они же CONNECT) – прокси поддерживающие HTTP 1.1, которая в свою очередь имеет две спецификации - RFC 2616 и устаревший RFC 2068. Отличаются они тем, что в спец. RFC 2616 документирован метод CONNECT.
Все эти подтипы проксей имеют одну и ту же возможность – они могут работать с использованием метода CONNECT (в дополнение к GET / POST).
Различие между подтипами состоит исключительно в настройках программ прокси-серверов:
Если в настройках прокси сервера разрешено подключение методом CONNECT к порту 443 (https:// адреса), то это HTTPS proxy;
Если в настройках прокси сервера разрешено подключение методом CONNECT к любым портам (не считая 443 и 25), то он называется CONNECT proxy (в ICQ такой прокси называется HTTP proxy);
Если в настройках прокси сервера разрешено подключение методом CONNECT к порту 25 (почтовый сервис), то его можно использовать для рассылки почты и такой прокси называется

mail-enabled, или 25 port enabled или прокси с открытым 25-м портом.
FTP прокси – работает по протоколу ftp и предназначен для анонимного управления сайтом (сервером). Все ftp прокси есть анонимными потому, что протокол FTP не предусматривает наличия прокси.
В паблике FTP прокси отсутствуют. Из FTP проксей невозможно построить цепочку.
CGI прокси (веб анонимайзер) – это страница на сайте, куда вбиваешь url, и она выводит указанную страницу. При этом адрес этой страницы (указанный в поле адреса) с точки зрения Вашего компьютера будет другой - что-то вроде

С точки зрения анонимности CGI proxy бывают такими же, как и HTTP proxy. В «смешанных» цепочках этот вид проксей может стоять только на последнем месте.
SOCKS – этот вид прокси имеет 2 спецификации:
Socks 4 работает по протоколу TCP
Socks 5 поддерживает TCP, UDP, авторизацию и удаленный DNS-запрос. Socks по своей природе есть дейсвительно анонимным (потому, что он работает напрямую с TCP). Из проксей этого вида можно построить цепь. Сокс – самый лучший способ остаться анонимным в сети.
Анонимность Прокси
Всем известно, что при взаимодействии клиента с сервером, клиент посылает серверу некую информацию (в основном ее передает браузер, но прокся тоже может добавлять туда что-то «от себя»). Имеется ввиду название и версия операционной системы, название и версия браузера, настройки браузера (разрешение экрана, глубина цвета, поддержка java / javascript, ...), IP адрес клиента (если используется proxy, то заменяется proxy сервером на IP proxy), используется ли proxy сервер (если используется proxy, то IP клиента - это IP proxy - добавляется proxy сервером), если используется proxy, то Ваш реальный IP адрес (добавляется proxy сервером) и многое другое…
Эта информация передается в виде переменных окружения (environment variables).
Я остановлюсь лишь на тех, которые имеют отношение к анонимности.
Итак, Если прокси не используется, то переменные окружения выглядят следующим образом:
REMOTE_ADDR = Ваш IP
HTTP_VIA = не определена
HTTP_X_FORWARDED_FOR = не определена
Прозрачные прокси не скрывают инфу о реальном IP:
REMOTE_ADDR = IP proxy
HTTP_VIA = IP или имя proxy (используется proxy сервер)
HTTP_X_FORWARDED_FOR = реальный IP
Анонимные прокси (anon) не скрывают того факта, что используется прокси, но меняют реальный IP на свой:
REMOTE_ADDR = IP proxy
HTTP_VIA = IP или имя proxy (используется proxy сервер)
HTTP_X_FORWARDED_FOR = IP proxy
Искажающие прокси (distorting) не скрывают того факта, что используется proxy сервер. Однако реальный IP подменяется на другой (в общем случае произвольный, случайный):
REMOTE_ADDR = IP proxy
HTTP_VIA = IP или имя proxy (используется proxy сервер)
HTTP_X_FORWARDED_FOR = случайный IP
Элитные прокси (elite, high anon) не только меняют IP, но и скрывают даже сам факт использования прокси сервера:
REMOTE_ADDR = IP proxy
HTTP_VIA = не определена
HTTP_X_FORWARDED_FOR = не определена
2) VPN-сервисы — тоже работают по разным протоколам, которые предлагают провайдеры на выбор.
3) SSH-туннели, изначально создавались (и функционируют по сей день) для других целей, но также используются для анонимизации. По принципу действия довольно схожи с VPN’ами, поэтому в данной теме все разговоры о VPN будут подразумевать и их тоже.

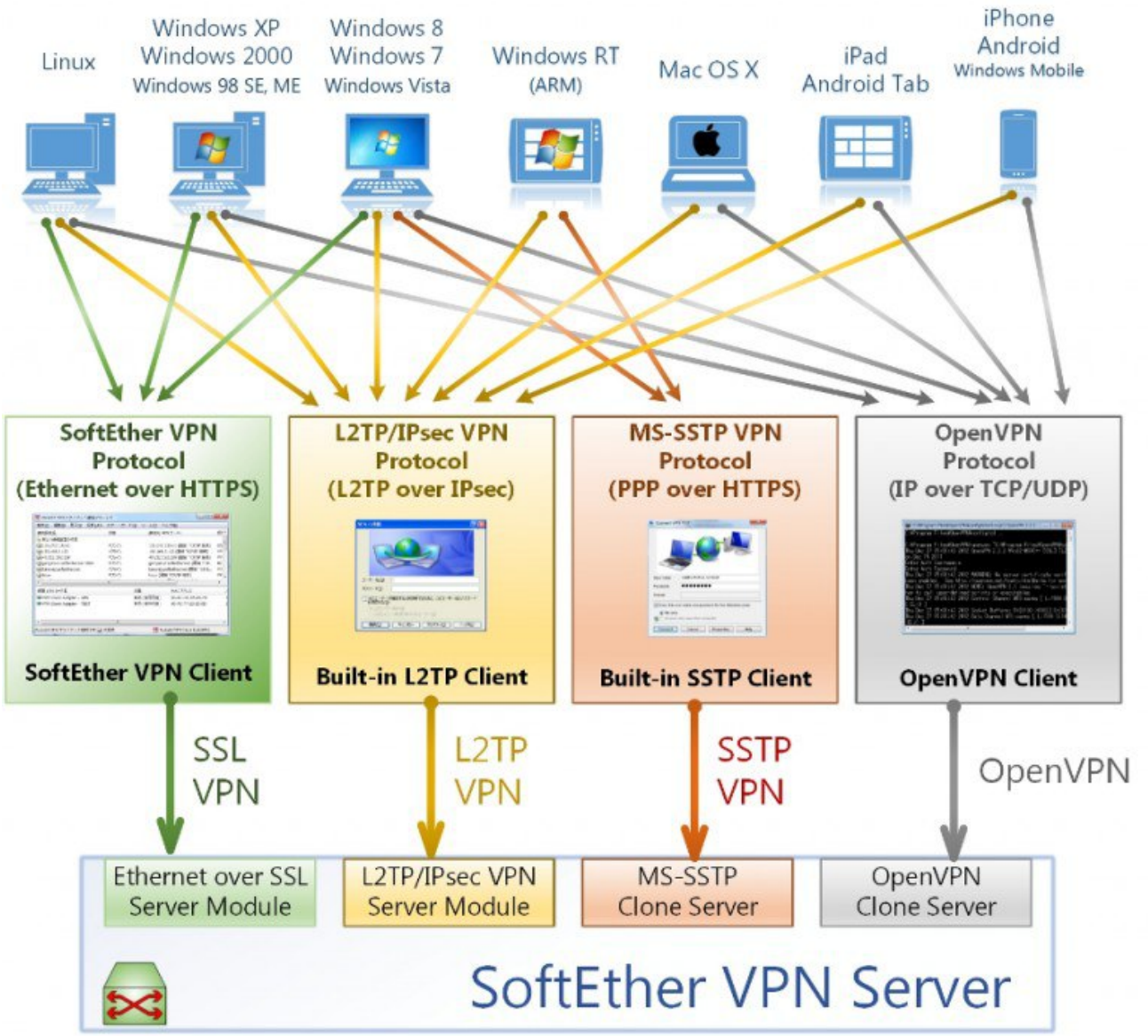
4) Dedicated-серверы — самое основное преимущество в том, что пропадает проблема раскрытия истории запросов узла, с которого проводились действия (как это может быть в случае с VPN/SSH или прокси).
5) Tor;
6) I2P — анонимная, децентрализованная сеть, работающая поверх интернета, не использующая IP-адресацию.
7) Иные средства — анонимные сети, анонимайзеры и др. В силу пока недостаточной популярности они еще не изучены (а следовательно не имеют относительной гарантии надежности) сообществом, но достаточно перспективны.
Что стоит скрывать, или какие есть деанонимизирующие данные и методы их получения?
Хочу обратить внимание на один интересный ресурс, который посвящен вопросам, какую информацию мы оставляем о себе в сети, заходя в разных устройств:
1) IP-адрес, или самый популярный идентификатор в интернете. Дает возможность найти провайдера юзера и узнать у него точный адрес через тот же IP.
2) IP DNS провайдера, который можно «потерять» через метод, называемый DNS leaks (утечки DNS). Важно отметить, что эта утечка может произойти при связке HTTP/SOCKS4 (5 в некоторых случаях) + Tor! Поэтому тут надо быть особенно внимательными.
3) Если большая часть траффика долго выходит в интернет через один узел, например, тот же Tor, то можно провести так называемое профилирование — отнести определенную активность к определенному псевдониму, который можно сдеанонить через другие каналы.
4) Прослушивание трафика на выходном узле или Mitm-атаки (man in the middle).
5) Одновременное подключение к анонимному и открытому каналам может в некоторых ситуациях создать неприятности, например, при обрывании соединения у клиента, оба канала перестанут функционировать, и на сервере можно будет определить нужный адрес, сопоставив время отсоединения пользователей (правда, это довольно геморный и далеко неточный способ деанонимизации).
6) Деанонимизирующая активность в анонимном сеансе — пользование публичными сервисами, особенно теми, на которых уже есть информация об этом пользователе.
7) MAC-адрес, который получает WiFi точка при подключении к ней (или он может быть бэкапнут коммутаторами одной из локальных сетей, через которую был осуществлен выход в интернет).
8) Информация из браузеров:
Cookies — это текстовые файлы с какими-либо данными (как правило, уникальными для каждого пользователя), хранимые приложением (часто — браузером) для разных задач, например, аутентификации. Часто бывает, что клиент сначала посетил ресурс из открытого сеанса, браузер сохранил cookies, а потом клиент соединился из анонимного сеанса, тогда сервер может сопоставить cookies и вычислить клиента;
Flash, Java, Adobe Reader — первые три плагина вообще можно выделить, как отдельные приложения на базе браузера. Они могут обходить прокси (DNS leaks), засвечивать IP (IP leaks), создавать свои подобия долгоживущих cookies и др. Также все три (в особенности этим грешит Flash) часто служат подспорищем для эксплуатации каких-нибудь 0-day или 1-day уязвимостей, позволяющих порой проникнуть в саму систему;
JavaScript — исполняется на стороне клиента, не обладает таким широким спектром возможности в плане деанона, хотя может предоставить точную информацию об ОС, виде и версии браузера, а также имеет доступ к некоторым технологиям браузера, которые могут также, например, слить IP-адрес.
Browser fingerprint или отпечаток браузера — совокупность данных, которые браузер постоянно предоставляет серверу при работе с ним, что может сформировать достаточно уникальный «цифровой отпечаток», по которому можно будет найти юзера даже в анонимном сеансе или позже, по выходу из него;
Чем VPN отличается от прокси?
1) Трафик между клиентом и прокси передается в открытом виде, при использовании VPN уже идет шифрование.
2) Стабильность — при создании VPN соединения как правило постоянная, редко создаются разъединения, у прокси они происходят относительно чаще. Но все зависит от провайдера.
3) Кроме шифрования соединения VPN предоставляет более анонимный сервис в том плане,

что используются DNS сервера VPN сервиса и не может произойти раскрытия приватных данных типа DNS leak, что ни чуть не хуже, чем раскрытие IP-адресаю Правда у SOCKS5 и SOCKS4a-прокси есть такая же возможность переложить DNS сервис на прокси-сервер.
4) VPN сервисы не ведут журналов или ведут на очень короткие сроки и неподробно (по крайней мере они так говорят), большинство прокси-серверов не дают таких обещаний.
Насколько эффективна цепочка из прокси-серверов?
Скорее она неэффективна, если ориентироваться по соотношению прироста времени деанонимизации на уменьшение скорости соединения от конечного ресурса к клиенту. К тому же, почти все недостатки деанонимизации, присущие прокси-серверам не исчезают при построении из них подобных цепочек. Поэтому можно сделать вывод, что данным методом при достижении анонимности лучше не пользоваться.
В FAQ'е про прокси-серверы не сказано о SOCKS4a, зачем он нужен?
Это промежуточная версия между 4 и 5 SOCKS'ами, в которой все функционирует аналогично 4, за исключением того, что SOCKS4a принимает только доменное имя вместо IP-адреса ресурса и сам его резолвит.
Можно поподробнее об особенностях, плюсах и минусах аренды dedicated-серверов?
Выделенный сервер предназначается далеко не для анонимизации, а для хостинга приложений, сервисов и всего другого, что заказчик посчитает нужным. Важно отметить, что арендатору предоставляется отдельная физическая машина, что дает ему некий гарант полного контроля этого узла и создадет важное преимущество для анонимности — уверенность в том, что история запросов никуда не утечет.
Учитывая вышесказанное и другие моменты можно выделить ряд преимуществ данного средства с точки зрения анонимизации:
1) Настройка HTTP/SOCKS-прокси или SSH/VPN-соединения на выбор.
2) Контроль истории запросов.
3) Спасает при атаке через Flash, Java, JavaScript, если использовать удаленный браузер.
Ну и недостатки тоже присутствуют:
1) Сильно дорогой метод.
2) В некоторых странах априори не может предоставлять анонимность, потому что арендатор обязан предоставить о себе данные: паспорт, кредитка и др.
3) Все соединения с выделенным сервером логируются у его провайдера, так что тут возникает доверенность немного другого плана.
Через какие протоколы идет работа в VPN и какие у них есть особенности?
Лучше сразу рассматривать существующие сейчас варианты VPN, то есть какие связки и технологии предлагают провайдеры, если мы конечно не ставим цель поднять знания теории сетевых протоколов (хотя есть варианты с использованием одного единственного протокола, что мы также рассмотрим).
SSL (Secure Socket Layer) протокол защищенных сокетов — использует защиту данных с открытым ключом для подтверждения подлинности передатчика и получателя. Поддерживает надежность передачи данных за счет использования корректирующих кодов и безопасных хэш-функций. Один из наиболее простых и «низкоанонимных» протоколов для VPN-соединений, используется в основном приложениями-клиентами для VPN. Чаще является частью какой-нибудь связки при создании VPN-соединения.
PPTP (Point-to-Point Tunneling Protocol) — используется наиболее часто, довольно быстрый, легко настраивается, но считается наименее защищённым относительно других своих собратьев.



L2TP (Layer 2 Tunneling Protocol) + IPSec (часто IPSec опускают в названии, как вспомогательный протокол). L2TP обеспечивает транспорт, а IPSec отвечает за шифрование. Данная связка имеет более сильное шифрование, чем PPTP, устойчива к уязвимостям PPTP, обеспечивает также целостность сообщений и аутентификацию сторон. Есть VPN на основе только протокола IPSec или только L2TP, но, очевидно, что L2TP + IPSec дают больше возможностей в защите и анонимизации, чем по отдельности.

OpenVPN — безопасный, открытый, а следовательно, распространённый, позволяет обходить многие блокировки, но требует отдельного программного клиента. Технически это не протокол, а реализация технологии VPN. Проводит все сетевые операции через TCP или UDP транспорт. Также возможна работа через большую часть прокси серверов, включая HTTP, SOCKS, через NAT и сетевые фильтры. Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует SSLv3/TLSv1.
SSTP — такой же безопасный, как и OpenVPN, отдельного клиента не требует, однако сильно ограничен в платформах: Vista SP1, Win7, Win8. Инкапсулирует PPP-кадры в IP-датаграммы для передачи по сети. Для управления туннелем и передачи PPP-кадров данных протокол SSTP использует TCP-подключение (порт 443). Сообщение SSTP шифруется каналом SSL протокола HTTPS.



Отдельно стоит отметить сервисы, предоставляющие такие услуги как «DoubleVPN», когда перед достижением нужного узла траффик проходит 2 разных VPN-сервера в разных регионах. Или существует еще более жесткое решение — «QuadVPN», когда используется 4 сервера, которые пользователь может выбрать сам и расположить в нужном ему порядке.

Какие минусы есть у VPN?

Конечно же, не такая анонимность, как у некоторых других сервисов типа Tor'a, и не только потому, что алгоритм и схема другие. Также при использовании VPN все таки в критических ситуациях придется больше полагаться на добросовестное исполнение обязанностей этого сервиса (минимальное журналирование, работа без бэкапов трафика и пр.).

Следующий момент состоит в том, что хоть VPN и скрывает IP в большинстве случаев, а также предотвращает DNS leak, но есть ситуации, при которых и этот метод анонимизации даст сбой. А именно:

1) IP leak через WebRTC — на хроме и мозилле работает гарантированно и реализовывается через обычный JavaScript.

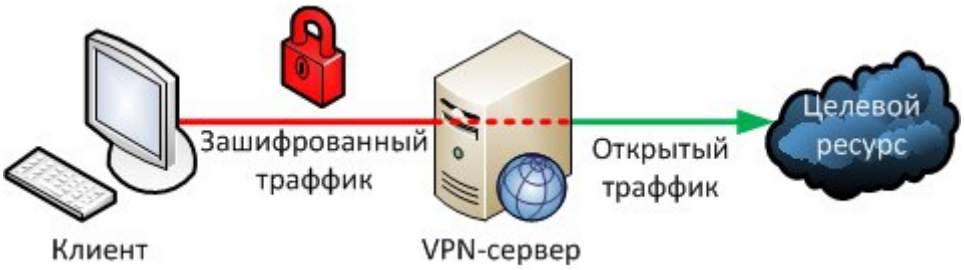
2) Утечка IP через Flash, инициировавший соединение с сервером и передавший ему IP клиента в обход VPN (правда работает не всегда);

Хотя эти случае можно предотвратить выключив у себя в браузере JS, Flash и Java.

3) При использовании клиентских настроек по умолчанию при разрыве соединения, в отличие от прокси-серверов, серфинг в сети будет продолжаться напрямую, уже не через виртуальный канал, то есть будет полное палево.

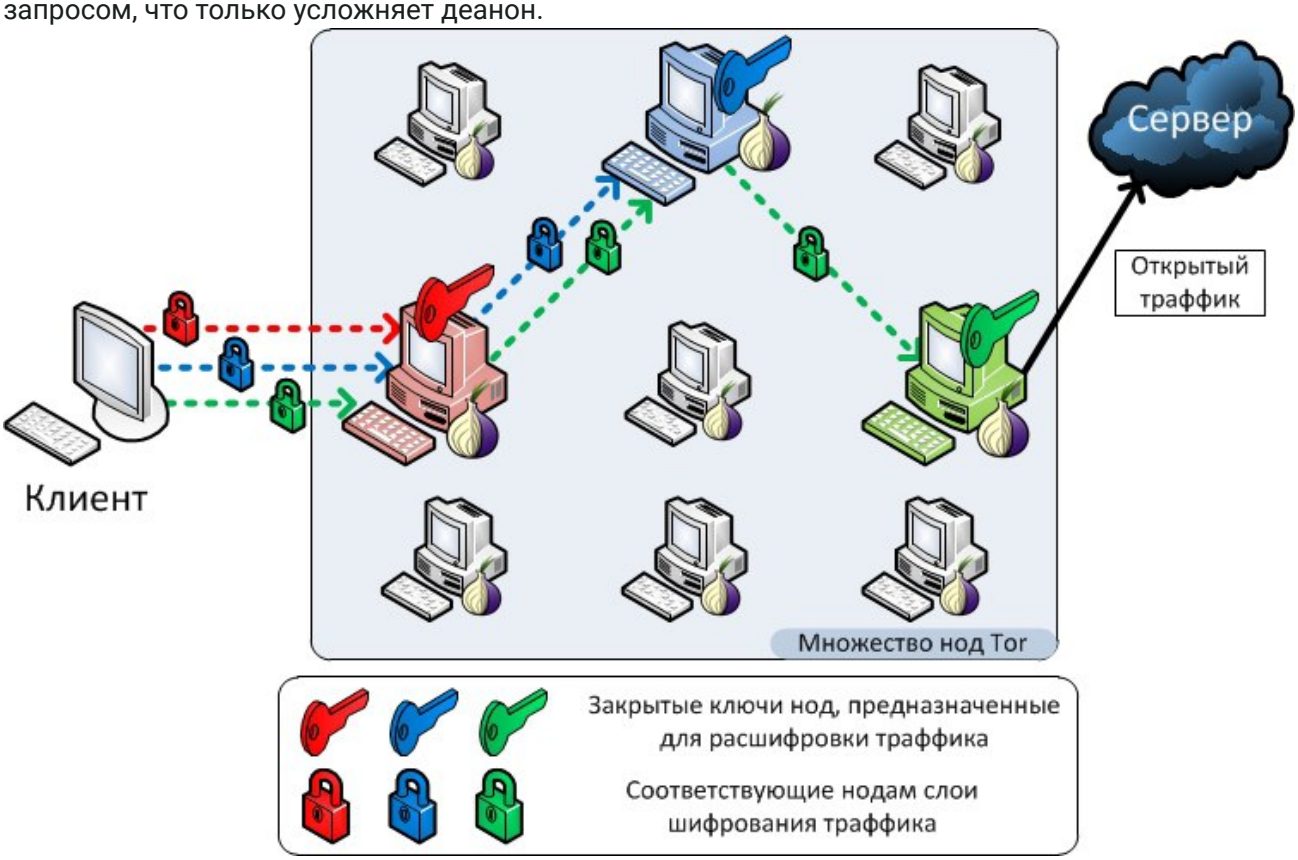
Но этого можно избежать подкорректировав таблицу маршрутизации, где в качестве основного шлюза по умолчанию указать только шлюз VPN-сервера или перенастроить файрвол.
В чем различие между SSH-тунелями и VPN?
SSH-туннель ни что иное, как шифруемое по протоколу SSH соединение, где данные шифруются на стороне клиента и расшифровываются у получателя (SSH-сервера). Создается для удаленного защищенного управления ОС, но как уже было написано выше, применяется еще для анонимизации.
Поддерживает 2 варианта работы: посредством реализации приложением HTTP/SOCKS-прокси для направления траффика через локальный прокси-сервер в SSH-туннель. Или происходит создание практически полноценного (можно сказать аналогичного, если брать последние версии SSH и OpenSSH) VPN-соединения.

VPN же разрабатывался в целях обеспечивать защищенный удаленный доступ к ресурсам корпоративных сетей, а следовательно компьютер, подключенный к VPN-серверу становиться частью локальной сети и может пользоваться ее сервисами.

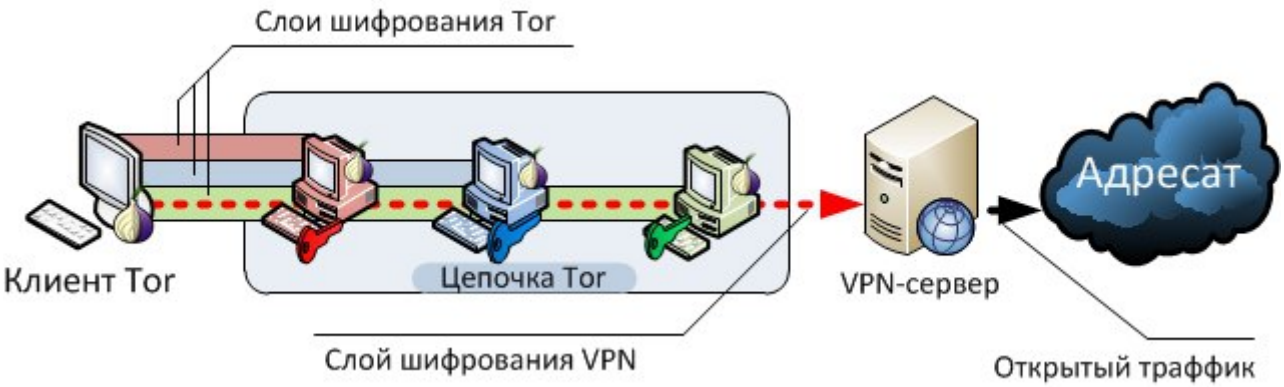


То есть кроме технических мелких аспектов принципы функционирования схожи. А основное отличие состоим в том, что SSH-туннель — это соединение точка-точка, а VPN-соединение — это соединение устройство-сеть (хотя спецы могут и перенастроить по своему усмотрению).
Как работает Tor со стороны клиента?
В сети море вариаций ответов на этот вопрос, но хочу попробовать изложить основы как можно более просто и лаконично, избавив читателя от копания в горах аналитической и сложной информации.
Tor — система маршрутизаторов, доступных только клиентам самого Tor'а, через цепочку которых клиент соединяется с нужным ему ресурсом. При дефолтных настройках количество узлов — три. Tor использует многоуровневое шифрование. Опираясь на эти особенности, можно кратко описать общую схему доставки пакета данных от клиента к запрашиваемому ресурсу через 3 узла (то есть при настройках по умолчанию): предварительно пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго и в конце, для первого. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра (как при очистки луковицы) и узнаёт, куда отправить пакет дальше. Второй и третий сервер поступают

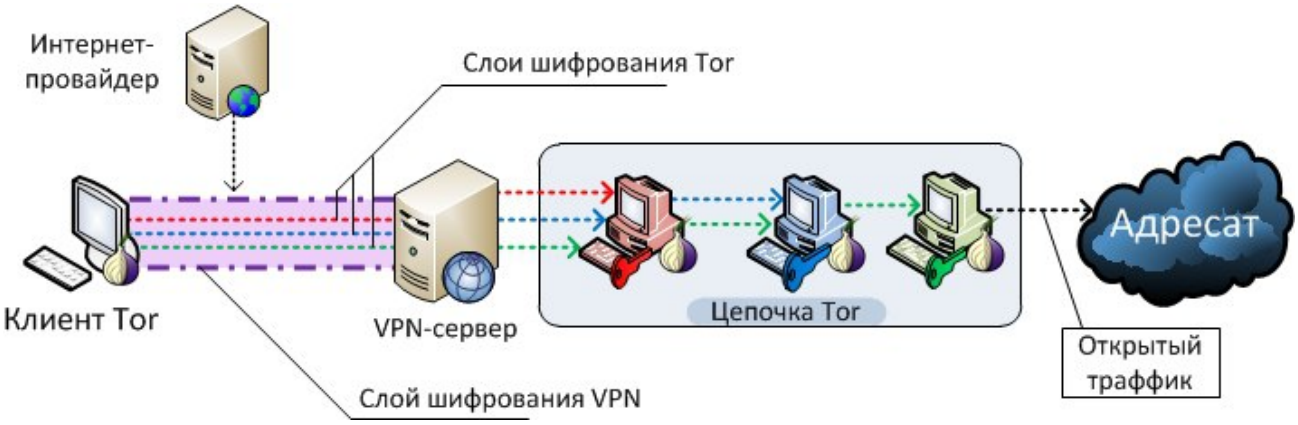
аналогичным образом. А передача зашифрованных данных между промежуточными маршрутизаторами осуществляется через SOCKS-интерфейсы, что обеспечивает анонимность в купе с динамичным переконфигурированием маршрутов. И в отличие от статических прокси-цепочек, конфигурации луковых маршрутизаторов может меняться чуть ли не с каждым новым запросом, что только усложняет деанон.



Какие преимущества и недостатки есть у Tor'а?
Из преимуществ стоит выделить:
1) Один из самых высоких уровней анонимности (при должной конфигурации), особенно в комбинации с другими способами типа VPN.
2) Простота в использовании — скачал, пользуйся (можно даже без особых настроек).
Недостатки:
1) Относительно низкая скорость, так как трафик идет через цепочку узлов, каждый раз происходит расшифровка и может проходить вообще через другой континент.
2) Выходной трафик может прослушиваться, а если не использовать HTTPS, то и прекрасно фильтроваться для анализа.
3) Может не спасти при включенных плагинах — Flash, Java и даже от JavaScript'а, но создатели проекта рекомендуют эти дела отключать.
4) Наличие управляющих серверов.
Если сайт детектит Tor, то я никак не могу зайти на этот сайт анонимным используя его?
Попасть на такой сайт можно двумя способами. При помощи более изощренной схемы, которая де-факто делает это посещение еще более анонимным: связка Tor ⇢ VPN, можно Tor ⇢ Proxy, если не нужна дополнительная анонимность, а только факт сокрытия использования Tor для сервера сайта, но надо использовать именно в этой последовательности. Так получается, что сначала запрос идет через луковые хосты, затем через VPN/Proxy, а на выходе выглядит, как будто просто VPN/Proxy (или вообще обычное соединение).
Но стоит заметить, что взаимодействие этих связок вызывает бурные обсуждения на форумах, вот раздел о Tor и VPN на сайте лукового проекта.

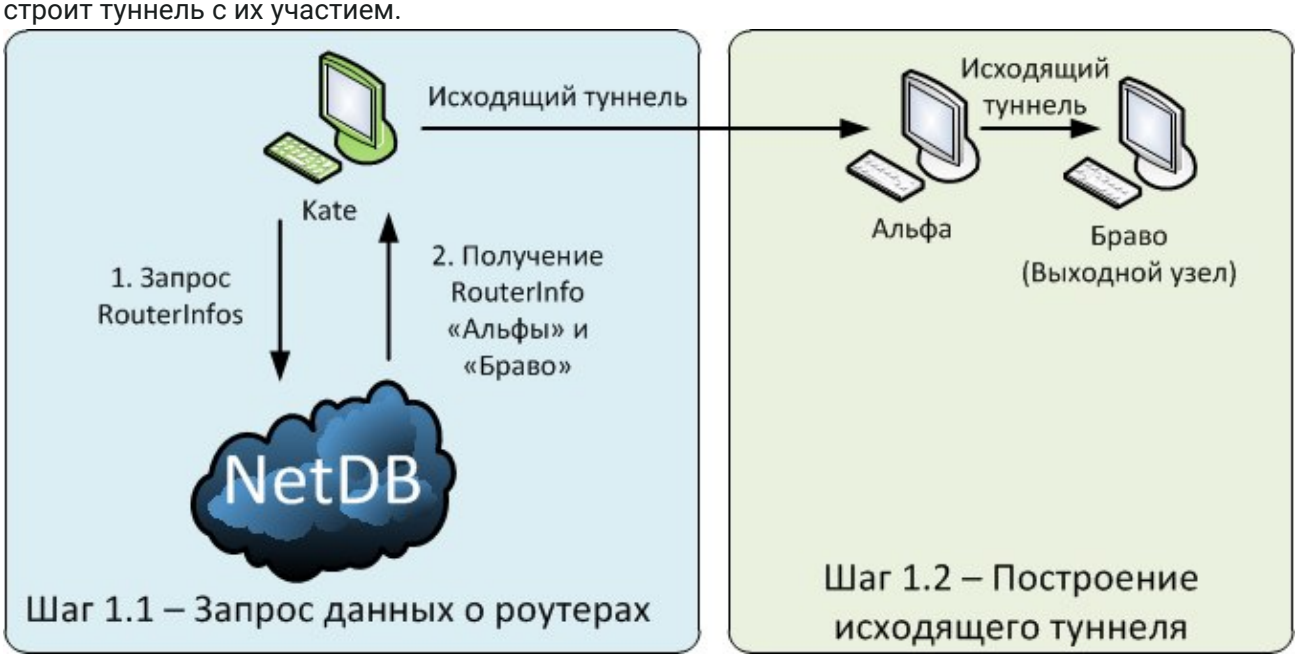


Либо можно использовать так называемые мосты (bridges) — это узлы, не занесенные в центральный каталог Tor'a, как их настраивать можно посмотреть здесь.
Можно ли как-то скрыть от провайдера факт использования Tor'a?
Да, решение будет почти полностью аналогичное предыдущему, только схема пойдет в обратном порядке и VPN соединение «вклинивается» между клиентов Tor'a и сетью луковых маршутизаторов. Обсуждение реализации такой схемы на практике можно найти на одной из страниц документации проекта.

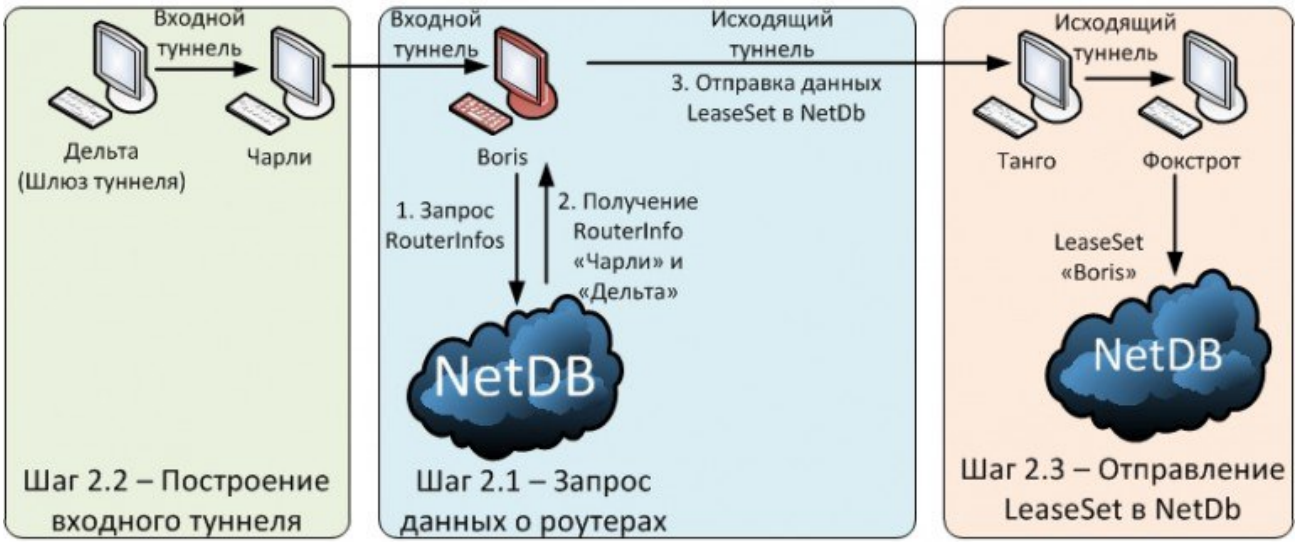


Что следует знать о I2P, и как эта сеть работает?
I2P — распределенная, самоорганизующаяся сеть, основанная на равноправии ее участников, отличающаяся шифрованием (на каких этапах оно происходит и какими способами), переменными посредниками (хопами), нигде не используются IP-адреса. В ней есть свои сайты, форумы и другие сервисы.
В сумме при пересылке сообщения используется четыре уровня шифрования (сквозное, чесночное, туннельное, а также шифрование транспортного уровня), перед шифрованием в каждый сетевой пакет автоматически добавляется небольшое случайное количество случайных байт, чтобы ещё больше обезличить передаваемую информацию и затруднить попытки анализа содержимого и блокировки передаваемых сетевых пакетов.
Весь трафик передается по туннелям — временные однонаправленные пути, проходящие через ряд узлов, которые бывают входящими или исходящими. Адрессация происходит на основе данных из так называемой сетевой базы NetDb, которая распределена в той или иной мере по всем клиентам I2P. NetDb содержит в себе:
RouterInfos — контактные данные роутеров (клиентов), используются для построения туннелей (упрощая, они представляют собой криптографические идентификаторы каждого узла);
LeaseSets — контактные данные адресатов, используются для связи исходящих и входящих туннелей.
Принцип взаимодействия узлов этой сети.
Этап 1. Узел «Kate» строит исходящие туннели. Он обращается к NetDb за данными о роутерах и

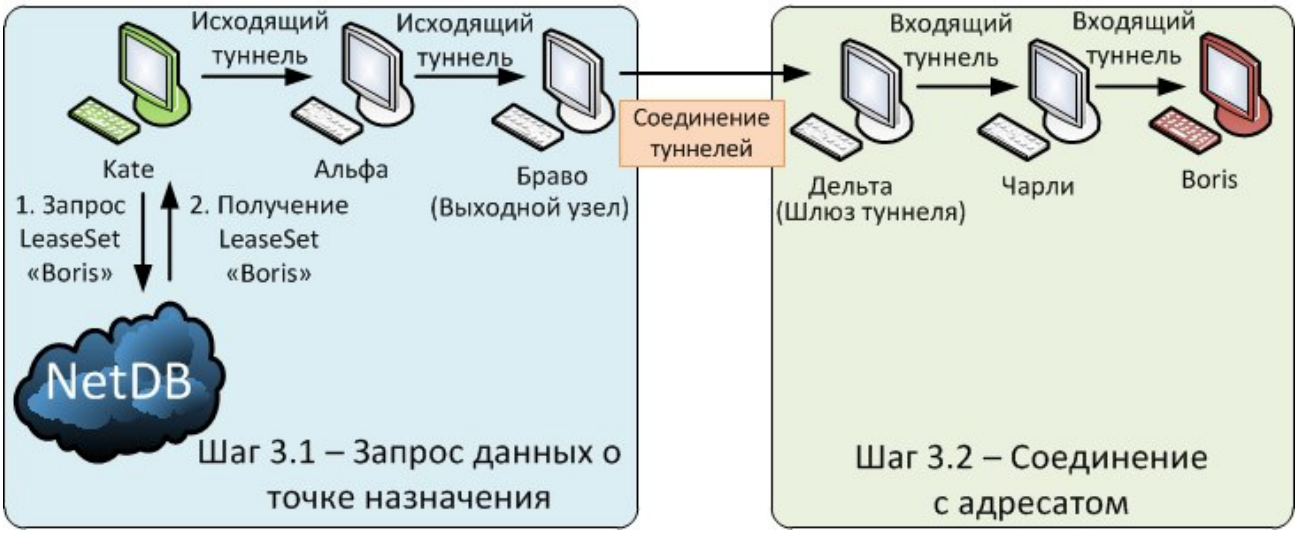
строит туннель с их участием.



Этап 2. «Boris» строит входной туннель аналогично тому, как и строится исходящий туннель. Затем он публикует свои координаты или так называемый «LeaseSet» в NetDb (здесь отметьте, что LeaseSet передается через исходящий туннель).

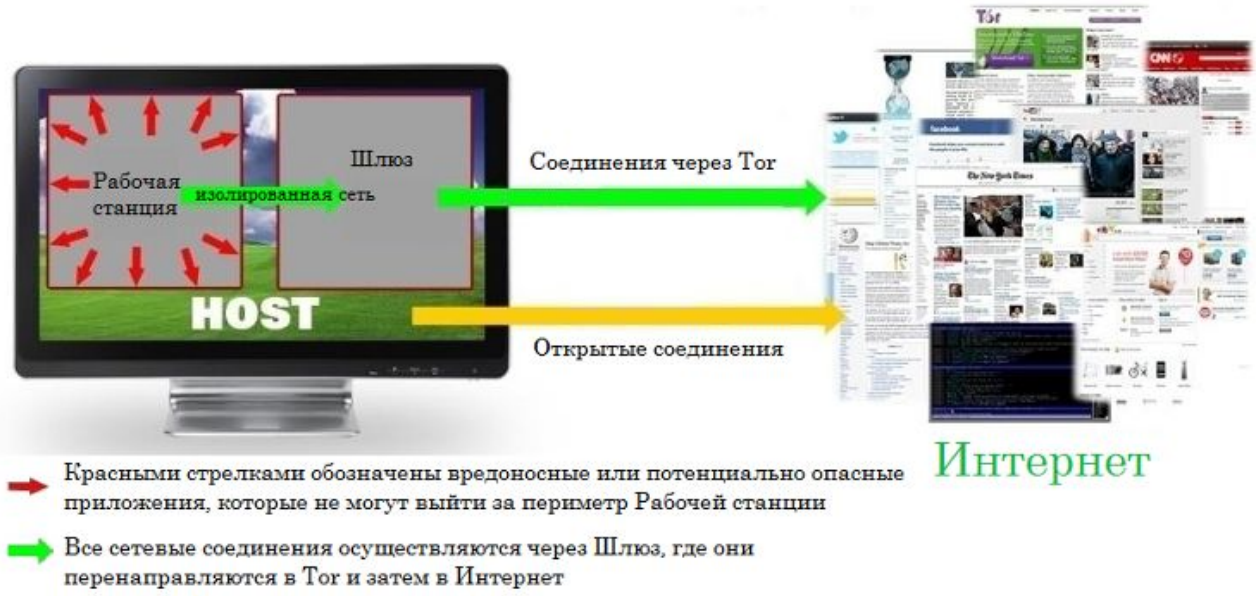


Этап 3. Когда «Kate» отправляет сообщение «Boris'у», он запрашивает в NetDb LeaseSet «Boris'а». И по исходящим туннелям пересылает сообщение к шлюзу адресата.



Еще стоит отметить, что у I2P есть возможность выхода в Интернет через специальные Outproxy, но они неофициальные и по совокупности факторов даже хуже выходных узлов Tor. Также внутренние сайты в сети I2P доступны из внешнего Интернета через прокси-сервер. Но на этих входных и выходных шлюзах высока вероятность частично потерять анонимность, так что надо быть осторожным и по возможности этого избегать.
Какие есть преимущества и недостатки у I2P сети?
Преимущества:
1) Высокий уровень анонимности клиента (при любых разумных настройках и использовании).
2) Полная децентрализация, что ведёт к устойчивости сети.
3) Конфиденциальность данных: сквозное шифрование между клиентом и адресатом.
4) Очень высокая степень анонимности сервера (при создании ресурса), не известен его IP-адрес.
Недостатки:
1) Низкая скорость и большое время отклика.
2) «Свой интернет» или частичная изолированность от интернета, с возможностью туда попасть и повышением вероятности деанона.
3) Не спасает от атаки через плагины (Java, Flash) и JavaScript, если не отключить их.
Какие еще есть сервисы/проекты по обеспечению анонимности?
Freenet — одноранговая сеть распределенного хранения данных.
GNUnet — скоординированный набор софта для peer-to-peer соединения, не нуждающегося в серверах.
JAP — John Donym, в основу взят Tor.
RetroShare — кроссплатформенный софт для бессерверного обмена письмами, мгновенными сообщениями и файлами с помощью шифрованной одноранговой F2F (friend-to-friend) сети.
Perfect Dark — японский клиент под винду для файлового обмена. Анонимность сети Perfect Dark базируется на отказе от использования прямых соединений между конечными клиентами, неизвестности IP-адресов и полном шифровании всего, что только можно.
Следующие 3 проекта особенно интересные тем, что их цель — скрыть пользователя реализуется путем освобождения от провайдерской зависимости при интернет-соединении, за счет построения беспроводных сетей. Ведь тогда интернет станет еще более самоорганизованным:
Byzantium
Netsukuku — Networked Electronic Technician Skilled in Ultimate Killing, Utility and Kamikaze Uplinking.
B.A.T.M.A.N — Better Approach To Mobile Ad-hoc Networking.
Есть ли какие-то комплексные решения по обеспечению анонимности?
Кроме связок и комбинаций различных методов, вроде Tor+VPN, описанных выше можно воспользоваться дистрибутивами линукса, заточенными на эти потребности. Преимущество

такого решения в том, что в них уже есть большинство этих комбинированных решений, все настройки выставлены на обеспечение максимального количества рубежей для деанонимизаторов, все потенциально опасные службы и софт вырезаны, полезные установлены, в некоторых помимо документации есть всплывающие подсказки, которые не дадут поздним вечером потерять бдительность.
По своему опыту и некоторых других знающих людей я бы выбрал дистрибутив Whonix, так как он содержит в себе самые новые техники по обеспечению анонимности и безопасности в сети, постоянно развивается и имеет очень гибкую настройку на все случаи жизни и смерти. Также имеет интересную архитектуру в виде двух сборок: Gateway и Workstation, которые в функционируют в связке. Основное преимущество этого состоит в том, что если в результате появления какой-нибудь 0-day в Tor или самой ОС, через которую попробуют раскрыть прятавшегося пользователя Whonix, то будет «деанонимизирована» только виртуальная Workstation и атакующий получит «очень ценную» информацию типа IP 192.168.0.1 и Mac address 02:00:01:01:01:01.



Но за наличие такого функционала и гибкости в настройке надо платить — этим обуславливается сложность конфигурации ОС из-за чего ее порой ставят в низ топа операционок для анонимности.
Более легкие в настройке аналоги — это довольно известные Tails, рекомендованный Сноуденом, и Liberte, которые также можно с успехом использовать в этих целях и которые обладают очень хорошим арсеналом для обеспечения анонимности.
Есть еще какие-нибудь моменты при достижении анонимности?
Да, есть. Существует ряд правил, которых желательно придерживаться даже в анонимном сеансе (если стоит цель достичь практически полной анонимности, конечно) и мер, которые необходимо предпринять перед входом в этот сеанс. Сейчас о них будет написано подробнее.
1) При использовании VPN, Proxy и пр. всегда в настройках устанавливать использование статических DNS-серверов провайдера сервиса, дабы избежать утечек DNS. Или выставлять должные настройки в барузере или межсетевом экране.
2) Не использовать постоянные цепочки Tor, регулярно менять выходные узлы (VPN-серверы, прокси-серверы).
3) При пользовании браузером отключать по возможности все плагины (Java, Flash, еще какие-нибудь Adobe'вские поделки) и даже JavaScript (если задача полностью минимализировать риски деанона), а также отрубать использование cookies, ведение истории, долгосрочного кэширования, не разрешать отправлять HTTP-заголовки User-Agent и HTTP-Referer или

подменять их (но это специальные браузеры для анонимности нужны, большинство стандартных не позволяют такую роскошь), использовать минимум браузерных расширений и т. д. Вообще есть еще один ресурс, описывающий настройки для анонимности в различных браузерах, к которому тоже при желании стоит обратиться.
4) При выходе в анонимном режиме в сеть следует использовать «чистую», полностью обновленную ОС с самыми последними стабильными версиями ПО. Чистая она должна быть — чтобы было сложнее отличить «отпечатки» ее, браузера и другого софта от среднестатистических показателей, а обновленная, чтобы понижалась вероятность подхватить какую-нибудь малварь и создать себе определенных проблем, ставящих под угрозу работу всех сосредоточенных для анонимизации средств.
5) Быть внимательным при появлении предупреждений о валидности сертификатов и ключей, для предотвращения Mitm-атак (прослушки незашифрованного трафика).
6) Не допускать никакой левой активности в анонимном сеансе. Например, если клиент из анонимного сеанса заходит на свою страницу в соц. сети, то его интернет-провайдер об этом не узнает. Но соц. сеть, несмотря на то, что не видит реальный IP-адрес клиента, точно знает, кто зашел.
7) Не допускать одновременного подключения к ресурсу по анонимному и открытому каналу (описание опасности было приведено выше).
8) Стараться «обфусцировать» все свои сообщения и другие продукты авторского интеллектуального производства, так как по жаргону, лексике и стиллистике речевых оборотов можно с довольно большой точностью определить автора. И уже есть конторы, которые делают на этом целый бизнес, так что не надо недооценивать этот фактор.
9) Перед подключением к локальной сети или беспроводной точке доступа предварительно менять MAC-адрес.
10) Не использовать любое недоверенное или непроверенное приложение.
11) Желательно обеспечить себе «предпоследний рубеж», то есть какой-то промежуточный узел до своего, через который вести всю активность (как это делается с dedicated-серверами или реализовано в Whonix), чтобы в случае преодоления всех предыдущих преград или заражения рабочей системы третие лица получали доступ к болванке-посреднику и не имели особых возможностей продвигаться в вашу сторону дальше (или эти возможности были бы крайне дороги или требовали затраты очень большого количества времени).

Материал может быть удален по просьбе правообладателя

На это отреагировал(а) rexar

Жалоба Мне нравится Цитата Ответить

Напишите Ваш ответ...

Прикрепить файлы Вставить цитаты... ОТВЕТИТЬ ПРЕДПРОСМОТР

Поделиться:

Russian (RU)

@ 2019-2020 Infobiza.Net - Платное теперь бесплатно! Сливы складчин, инфопродукты. #лучшедома

Служба поддержки Условия и правила Помощь