Автор: adm
28.01.14 16:48 -

Тонкая настройка Tor Btowser

Как правило, стандартных настроек, которые реализованы в оболочке Vidalia вполне достаточно для полноценной анонимной работы в Интернет. Однако возможны случаи, когда могут потребоваться дополнительные изменения параметров Tor. Такие изменения производятся редактированием *конфигурационного файла* Tor и называются тонкой настройкой.

Конфигурационный файл - обычный текстовый файл. Он носит имя **torrc** (без расширения) и находится:

- при использовании сборки Tor Browser - в каталоге *..<Каталог Tor Browser>DataTor*

- в инсталлированных пакетах - *<Documents and Settings<пользователь>Application DataVidalia*

- в ОС Ubuntu Linux - в каталоге */etc/tor*

Программа Tor при загрузке (перезагрузке) первым делом считывает конфигурационный файл и устанавливает рабочие параметры в соответствии со значениями команд в файле **torrc**.

Редактирование файла torrc можно производить в простейшем текстовом редакторе: Блокнот, AkePad и т.д. Желательно перед правкой сохранить первоначальный файл torrc в той же папке. Например, прибавив к имени расширение *.bak, *.001 и т. д.

Чтобы изменения вступили в силу нужно перезагрузить всё ПО системы Tor!

1. Фиксирование выходного или входного узла сети Tor

Напомним, что выходные сервера в Tor постоянно меняются случайным образом. Для пользователя это означает, что его IP не стабилен. С точки зрения посещаемого ресурса пользователь в любой момент может превратиться из француза, скажем, в японца, или ещё кого хуже. При работе с сайтами, фиксирующими сессию пользователя, такой вариант совершенно неприемлем.

Есть возможность прямо указывать, какой сервер (нод) должен быть выходным. IP в этом случае будет постоянным. Для этого в **torrc** дописываем две строчки:

ExitNodes <имя узла>

StrictExitNodes 1

Где:

Переменная *ExitNodes* – указывает использовать определённый сервер в качестве выходного узла

StrictExitNodes 1 – указание в случае недоступности выбранного сервера не пытаться подключиться к другому, а выводить ошибку.

Допускается записывать **несколько узлов** через запятую или, например, указав **ExitNodes {de}**
- получим только немецкие сервера в качестве выходных. ("Закосим" под немца!)

Найти необходимый сервер можно на: http://torstatus.kgprog.com/ или https://torstat.xenobite.eu/

Аналогично фиксируется и входной узел:

EntryNodes <имя узла>

StrictEntryNodes 1

Есть ещё одна полезная настройка из этой серии - **TrackHostExits** фиксирует выходной узел (host) для заданных доменов, что позволяет сохранять сессию для тех серверов, которые проверяют IP клиентов. Синтаксис записи такой:

TrackHostExits host,.domain,...

2. Исключение подозрительных узлов

Для исключения не вызывающих доверия узлов (Например - российских, украинских и белорусских) нужно добавить в **torrc** строку:

ExcludeNodes {ru}, {ua}, {by}

Или можно указать конкретный список имён.

Теперь если пытливые ребята с серенькими глазками в РФ, УА или РБ додумаются сделать подставной Tor-сервер и попытаются прослушивать выходные данные, то мы никак не сможем попасть на такой сервер.

Есть полезное свойство файла **torrc**. Это комментарий. Tor не выполняет строки в файле torrc если строка начинается с символа "#". Благодаря комментариям вы можете хранить в файле **torrc** заготовки, и при необходимости быстро включать их, убрав "#".

3. Прописывание прокси-сервера в Tor

Добавить следующие строки в конец конфигурационного файла Tor с заменой <адрес прокси> и <номер порта> (а также <логин> и <пароль>, если они есть) на конкретные значения прописываемого http или https прокси-сервера.

 # Force Tor to make all HTTP directory requests through this host:port (or

 # host:80 if port is not set).

HttpProxy <адрес прокси>:<номер порта>

 # A username:password pair to be used with HTTPProxy.

HttpProxyAuthenticator <логин>:<пароль>

 # Force Tor to make all TLS (SSL) connectinos through this host:port (or

 # host:80 if port is not set).

HttpsProxy <адрес прокси>:<номер порта>

 # A username:password pair to be used with HTTPSProxy.

HttpsProxyAuthenticator <логин>:<пароль>

После правки и сохранения файла **torrc** необходимо перезапустить Tor.

Для проверки настроек можно использовать графическую оболочку Vidalia или Tor-анализатор (зайти на http://check.torproject.org).

Список некоторых команд (настроек) Tor

EntryNodes nickname,nickname,...

Список серверов, которые предпочтительно использовать в качестве "входных" для установления TCP/IP-соединения с узловой цепочкой маршрутизаторов Tor, если это возможно.

ExitNodes nickname,nickname,...

Список серверов, которым предпочтительно отводить роль замыкающего звена в узловой цепочке маршрутизаторов Tor, если это возможно.

ExcludeNodes nickname,nickname,...

Список узлов, которые вовсе не следует использовать при построении узловой цепочки.

StrictExitNodes 0|1 Если установлено в 1, Tor не будет использовать какие-либо узлы, кроме тех, которые присутствуют в списке выходных узлов в качестве посредников, устанавливающих соединение с целевым хостом и, соответственно, являющихся своеобразным замыкающим звеном в цепочке узлов.

StrictEntryNodes 0|1

Если данному параметру присвоено значение 1, Tor не будет использовать какие-либо узлы, кроме тех, которые присутствуют в списке входных узлов для подключения к сети Tor.

FascistFirewall 0|1

Если данному параметру присвоено значение 1, Tor при создании соединения будет обращаться исключительно на Луковые Маршрутизаторы, у которых для осуществления подключения открыты строго определённые номера портов, с коими позволяет устанавливать соединение Ваш файрволл (по умолчанию: 80-й (http), 443-й (https), см. FirewallPorts). Это позволит Tor, запущенному на вашей системе, работать в качестве клиента за файрволлом, имеющим жёсткие ограничительные политики. Обратное утверждение неверно, поскольку в этом случае Tor не сможет исполнять обязанности сервера, закрытого таким файрволлом.

FirewallPorts ПОРТЫ

Список портов, к которым Ваш файрволл позволяет подсоединяться. Используется только при установленном значении параметра FascistFirewall. (По умолчанию: 80, 443) (Default: 80, 443)

LongLivedPorts ПОРТЫ

Список портов для сервисов, которые имеют склонность устанавливать особо длительные соединения (к ним относятся преимущественно чаты, а также интерактивные оболочки) Узловые цепочки из маршрутизаторов Tor, которые используют эти порты, будут содержать только узлы с наиболее высоким аптаймом (характерным временем присутствия в сети), с целью уменьшения вероятности отключения узлового сервера от сети Tor до закрытия потока. (По умолчанию: 21, 22, 706, 1863, 5050, 5190, 5222, 5223, 6667, 8300, 8888).

MapAddress адрес:новый_адрес

Когда к Tor придёт запрос на указанный адрес, луковый маршрутизатор изменит адрес перед тем, как приступить к обработке запроса. Например, если вы хотите, чтобы при соединении с www.indymedia.org была использована цепочка узлов Tor с выходом через torserver (где torserver – это псевдоним сервера), используйте "MapAddress www.indymedia.org www.indymedia.org.torserver.exit".

NewCircuitPeriod ЧИСЛО

Каждые ЧИСЛО секунд анализировать состояние соединения и принимать решение о том, нужно ли инициировать построение новой узловой цепочки. (По умолчанию: 30 секунд)

MaxCircuitDirtiness ЧИСЛО

Разрешить повторное использование цепочки, в первый раз собранная в определённом составе своих звеньев - самое большее - ЧИСЛО секунд назад, но никогда не присоединять новый поток к цепочке, которая обслуживала данный сеанс в течение достаточно продолжительного времени. (По умолчанию: 10 минут)

NodeFamily псевдоним,псевдоним,...

Именованные сервера Tor (закономерным образом, для повышения степени прозрачности иерархии сети Tor) объединяются в "семейства" по признаку общего или совместного администрирования, так что следует избегать использования любых 2-х из таких узлов, "связанных родственными узами", в одной и той же цепочке анонимных маршрутизаторов Tor. Специальное задание опции *NodeFamily* может понадобиться только тогда, когда сервер с данным псевдонимом сам не сообщает о том, к какому "семейству" он себя причисляет, что на стороне сервера OR должно быть продекларировано путём указания параметра MyFamily в файле
torrc
. Допускаются множественные указания этой опции.

RendNodes псевдоним,псевдоним,...

Список узлов, которые по возможности желательно использовать в качестве точек рандеву (встречи).

RendExcludeNodes псевдоним,псевдоним,...

Список узлов, которые ни в коем случае не следует использовать при выборе точек рандеву (точек встречи).

SOCKSPort ПОРТ

Известить Tor о том, что на этом порту должны прослушиваться соединения, устанавливаемые приложениями, использующими SOCKS-протокол. Обнулите этот параметр, если Вам вовсе ни к чему, чтобы приложения устанавливали соединения по SOCKS-протоколу посредством Tor. (Значение по умолчанию: 9050)

SOCKSBindAddress IP[:ПОРТ]

Установить привязку к данному адресу для прослушивания запросов на соединение от приложений, взаимодействующих по SOCKS-протоколу. (По умолчанию: 127.0.0.1). Также Вы можете указать порт (например, 192.168.0.1:9100), который, разумеется, на целевой машине должен быть "открыт" посредством соотв. настройки файерволла. Определение этой опции может быть повторено многократно для осуществления одновременной ("параллельной") привязки ко множеству различных адресов/портов.

SOCKSPolicy политика,политика,...

Задаёт политики входа на данный сервер с целью ограничения круга клиентских машин, которым разрешено подключаться к SOCKS порту. Описание этих политик вводится аналогично тому, как это делается для политик выхода (см. ниже).

TrackHostExits хост,.домен,...

Для каждого из значений в разделённом запятыми списке, Tor проследит недавние соединения для хостов, соответствующих этому значению и попытается использовать один и тот же выходной (замыкающий) узел для каждого из них. Если очередной элемент списка предваряется символом ".", то его значение будет трактоваться, как соответствующее домену в целом. Если один из элементов списка состоит из одной только "точки", то это указывает на его "универсальное" соответствие всем путевым именам. Эта опция может оказаться полезной, если Вы часто устанавливаете соединение с серверами, которые аннулируют все записи о пройденной Вами аутентификации (т.е. принуждают выйти и зарегистрироваться снова) при осуществлении попытки переадресации TCP/IP-соединения, установленного с одним из таких серверов, на Ваш новый IP-адрес после его очередной смены. Обратите особое

внимание на то, что использование этой опции невыгодно для Вас тем, что это позволяет серверу напрямую ассоциировать историю соединений, запрашиваемых определённым IP, с Вашей пользовательской учётной записью. Хотя в принципе, если кому-то и понадобится собрать всю информацию о Вашем пребывании на сервере, желающие в любом случае смогут сделать это посредством cookies или других специфичных для используемого протокола обмена средств.

TrackHostExitsExpire ЧИСЛО

Поскольку серверы, являющиеся выходными звеньями узловой цепочки, имеют право начинать работу и завершать её по собственному усмотрению, т.е. так или иначе – произвольным, случайным образом, желательно, чтобы ассоциация между хостом и выходным узлом автоматически потеряла свою силу по истечении некоторого ЧИСЛА секунд полного отсутствия сетевой активности со стороны сервера. По умолчанию – 1800 секунд (30 минут).

Существующий набор команд Tor достаточно велик. Рассмотрение их всех выходит за рамки настоящего обозрения. Здесь были приведены лишь несколько наиболее типичных вариантов редактирования и лишь часть команд. Полный список и синтаксис команд (на английском языке) можно найти на сайте разработчиков Tor.

источник: http://www.redov.ru

{jcomments on}

Автор: adm
28.01.14 16:48 -