Особенности настройки DNS в Nekoray

Все описанные здесь ниже познания родились в упорной борьбе с утечкой DNS (DNS-leak). Все сообщаемые сведения подходят для компьютера, моноблока, ноутбука, насколько они актуальны для смартфона, или планшета сказать не могу.

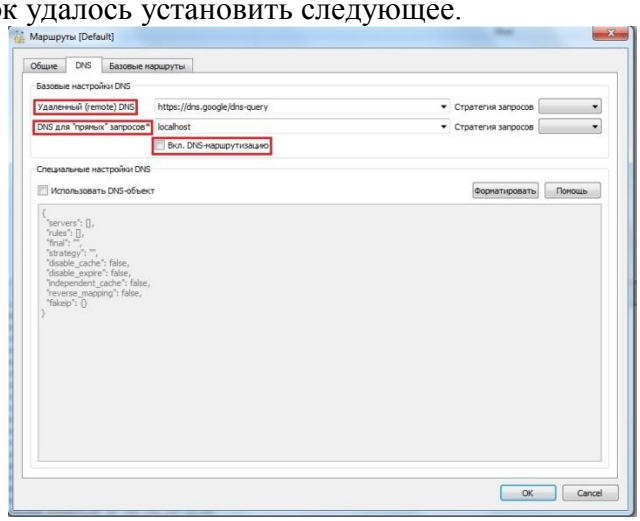
Чем нехороша утечка DNS при обходе блокировок? Мне кажется, главным образом, по двум причинам:

- оператору связи, а также цензору известны все попытки посещения запрещённых ресурсов;
- обычно в домашних маршрутизаторах разрешение имён стандартно настраивается на DNS-серверы оператора, поэтому для запрещённых сайтов могут возвращать «левые» IP-адреса, ведущие на страницы с сообщением о запрете, иногда о его причине (там, решение какого-нибудь суда и. т. п.).

Проблема утечек DNS меня интересовала со дня установки Nekoray с ядром sing-box.

Всем хороша эта программа – русскоязычный интерфейс, настройка подключения к серверу освещена во многих статьях (на Habr и других сайтах, посвящённых обходу блокировок Рунета). Вот плохо только то, что про тонкости работы DNS ни слова. Официальная помощь на китайском, переведённая с помощью Google на английский тоже света проливает мало.

Методом проб и ошибок удалось установить следующее.



Если не вдаваться в тонкости, то в окне настройки, вызываемом по «Настройки»=>«Настройки маршрутов»=>вкладка «DNS» интерес представляют три пункта, обведённые красным (см. рисунок выше). Чаще всего используется «DNS для “прямых” запросов». «localhost» указывает на использование DNS, настроенного на компьютере (где установлен Nekoray), в свою очередь, перенаправляющий запросы на разрешение имён на домашний, или корпоративный маршрутизатор. Из раскрывающегося списка можно также выбрать DoH-сервер, или обычный, принимающий UDP на 53. Все запросы тогда будут направляться непосредственно на него.

Верхний пункт «Удалённый (remote) DNS» будет использоваться только тогда, когда установлен флажок «Вкл. DNS-маршрутизацию», или активирован «Режим TUN». В этом случае, прежде чем отправить запрос на прокси-сервер, имя сайта в нём будет разрешено в IP-адрес посредством сервера, выбранного из раскрывающегося списка «Удалённый (remote) DNS». От греха подальше, в нём есть возможность указать только DoH-сервер.

В случае, если флажок, как на рисунке не установлен, все запросы на прокси-сервер уходят с неразрешёнными именами (IP-адреса для них будут запрошены средствами DNS прокси-сервера). Правда, это полезно только для «Режим системного прокси».

На мой взгляд, последнее более предпочтительно. Скрыть DNS-запросы от постороннего взгляда это не мешает, а имена в IP-адреса всего того, что ходит через прокси, пусть разрешаются на месте. Это лучше потому что:

- немало сайтов выдают разные IP-адреса в зависимости от географического положения, следовательно, сервер назначения может оказаться поближе к прокси, что существенно уменьшит задержку;
- вдруг DoH заблокируют, (по крайней мере, известные серверы, перечисленные в раскрывающихся списках Nekoray, ведь технически это сделать элементарно) - при этом всё будет работать.

Накануне я задался вопросом, возникает ли у меня утечка DNS при использовании Nekoray. Посмотрев в журнал корпоративного сервера DNS, я был неприятно удивлён – имена всех посещённых мною сайтов, в том числе и запрещённых, видны, как на ладони. Вот тебе, на!

Никакие перенастройки DNS в Nekoray ничего не давали. Как будто в корпоративном DNS для Nekoray прямо мёдом намазано! «Ломится» туда – и всё! Напропалую!

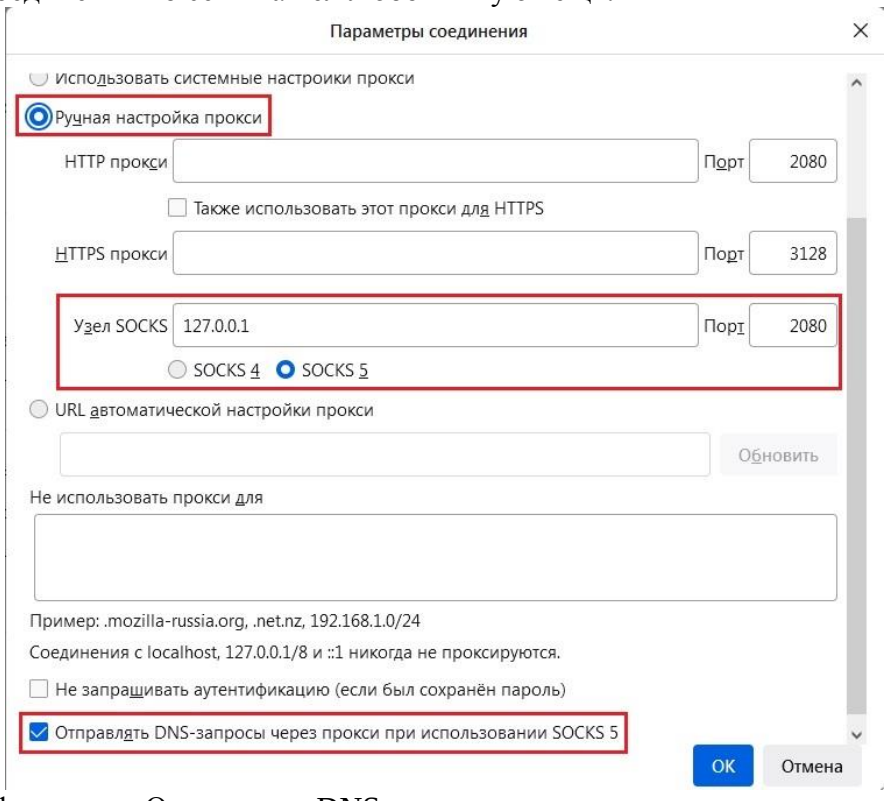
Правда, что-то подсказывало мне, что хоть тресни, но Nekoray не может быть таким дырявым, об этом бы уже где-нибудь написали. Это проделки какой-то сторонней программы. Какой? Браузер настроен на системный прокси, который в свою очередь, на Nekoray в непрозрачном режиме. Вроде бы по определению все запросы должны идти через него.

Подумал на сетевой фильтр антивируса, даже на возможного зловреда, перехватывающего сетевые соединения. Поэтому, уходя с работы, запустил сканер антивируса.

Утром показало, что всё чисто. Отключил антивирус, проблема не ушла.

И вот, по какому наитию закрыл Firefox, воспользовался стареньким Internet Explorer в Windows 7, затем Google Chrome – ни одного запроса через корпоративный DNS. Firefox – опять всё появилось! Так вот оно что. Этот хитрый своенравный огненный лис, зачем-то шлёт DNS-запросы в обход Nekoray!

Несмотря на это отказываться от Firefox не хотелось – нравится он мне по многим причинам, но и с утечкой DNS ситуация не устраивала. Конечно, в Firefox есть свой DoH, правда я его выключил после непродолжительного использования. Какой-то кривой он там. Сайты открываются с существенной задержкой. Тем более, даже самый захудалый Web-ресурс может содержать JS функции от Goolgle, и «тормоза» из-за этого возрастают кратно. Но тут в окне настройки Firefox соединения по сети нашёл любопытную вещь:



а именно, пункт с флажком «Отправлять DNS-запросы через прокси при использовании SOCKS 5». Непонятно, почему только для SOCKS 5, а не для HTTP тоже, ведь Internet Explorer и Google Chrome прекрасно это могут.

Подумав, какие всё-таки молодцы создатели Nekoray, что предусмотрели возможность соединения по SOCKS 5 «из коробки» без дополнительных настроек, я поменял «Использовать системный прокси» на «Ручная настройка прокси», вбил адрес, порт, выбрал SOCKS 5 и поставил

флажок (все настройки обведены красным на рисунке выше), в результате обнаружил полное исчезновение проблемы с утечкой DNS.

Точнее, зная вышеупомянутые настройки DNS в Nekoray, теперь стало возможным контролировать секретность любых DNS-запросов (по крайней мере, при Web-сёрфинге).

Не знаю, как другим, но я люблю, что называется, прятаться на виду. Лучше слыть для оператора связи и цензоров честным открытым пользователем Интернета, не скрывающим факт посещения всех разрешённых в РФ сайтов, а вот всякая там «запрещёнка» пусть будет недоступной для посторонних глаз.