Настраиваем использование DNS over HTTPS (DoH) на роутерах Mikrotik

interface31.ru/tech_it/2021/01/nastraivaem-ispolzovanie-dns-over-https-doh-na-routerah-mikrotik.html

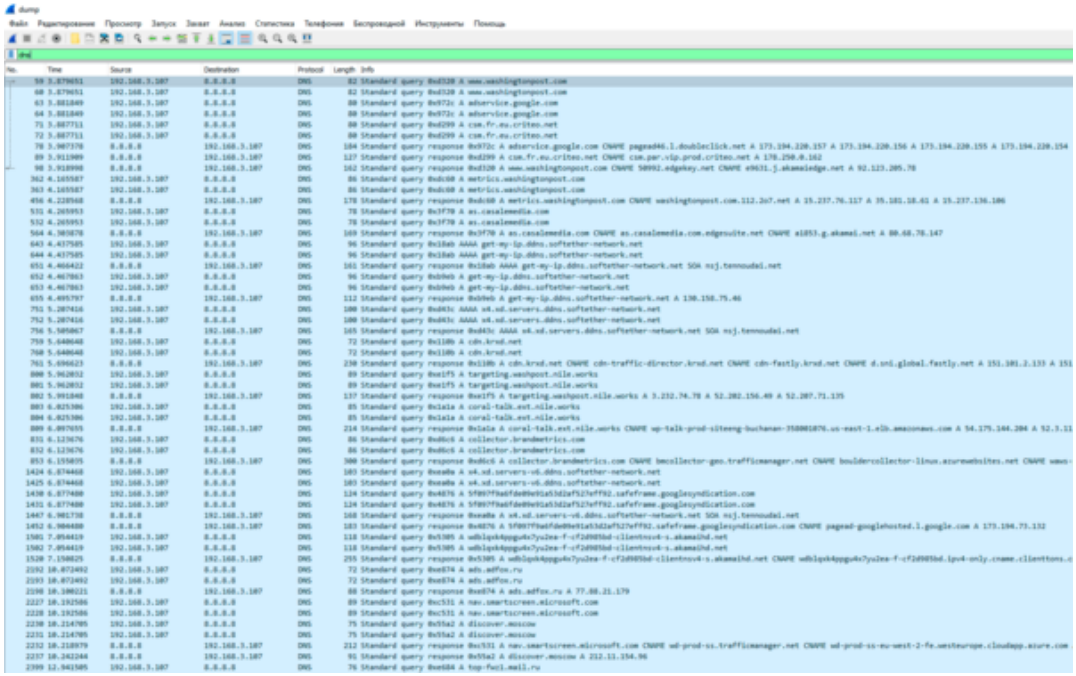
Наша жизнь с каждым днем все сильнее уходит в интернет: мы используем его для работы, проводим в нем финансовые операции, делаем покупки, общаемся с коллегами и родными. Поэтому на первый план все более выходят вопросы безопасности и конфиденциальности. Основная тенденция последних лет - переход на защищенные протоколы и уже сегодня использование HTTPS является обязательной нормой, но оставалось еще одно слабое звено - протокол DNS, данные в котором передавались открытым текстом. Устранить этот пробел призван новый протокол DNS over HTTPS (DoH), поддержка которого появилась в RouterOS.

Онлайн-курс по MikroTik
Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Чтобы понять суть проблемы незащищенного DNS немного углубимся в историю: на заре формирования глобальной сети интернет в том виде, в каком мы ее знаем встал вопрос использования простых и запоминающихся имен вместо цифровых адресов. Для того чтобы решить эту задачу был создана система DNS, которая должна была хранить соответствия имен цифровым адресам и сообщать их, получив запрос по специальному протоколу. Со временем возможности DNS росли и расширялись, но основной функцией по-прежнему остается сопоставление доменных имен IP-адресам, это одна из ключевых служб современного интернета, обойтись без нее невозможно.

В далеком 1987 году, когда принимались первые спецификации DNS вопросы безопасности были далеко не на первом месте и поэтому протокол дожил до наших дней практически в первозданном виде, передавая данные без какой-либо защиты. Чем это чревато? Давайте посмотрим.

Мы развернули в нашей виртуальной лаборатории небольшую сеть, которая выходит в интернет через виртуальный роутер Mikrotik. Вышестоящим узлом для него (читай - провайдером) является наш домашний роутер, с которого мы сняли дамп проходящего трафика. Даже беглого взгляда хватает, чтобы понять - вся интернет жизнь абонента как на ладони.



При этом, обратите внимание, абонент не использовал DNS-сервера провайдера, а работал с публичными серверами Google, но все равно провайдер имеет полную картину запросов пользователя. Эта же самая информация доступна каждому промежуточному узлу, через который проходит абонентский трафик.

- Позвольте, - скажет иной пользователь, - но мне нечего скрывать!

К сожалению, это не так. Информацию на основе ваших DNS-запросов могут использовать в рекламных целях и далеко не факт, что это будет ненавязчивая реклама в браузере. Кроме того, она позволяет составить достаточно наглядную картину вашей интернет-деятельности и далеко не все ее эпизоды вы захотите сделать общественным достоянием. Причем речь тут даже не о каких-то порочащих моментах, но вряд ли широкой общественности надо знать, что вы храните деньги в банке А и регулярно делаете покупки на площадке Б.

Поэтому сокрытие данной информации - это вопрос личной цифровой безопасности, а не попытка скрыть какие-либо неприглядные факты, тем более что провайдер может легко сопоставить такие запросы с реальной личностью: IP-адрес - номер договора - ФИО - адрес - паспортные данные.

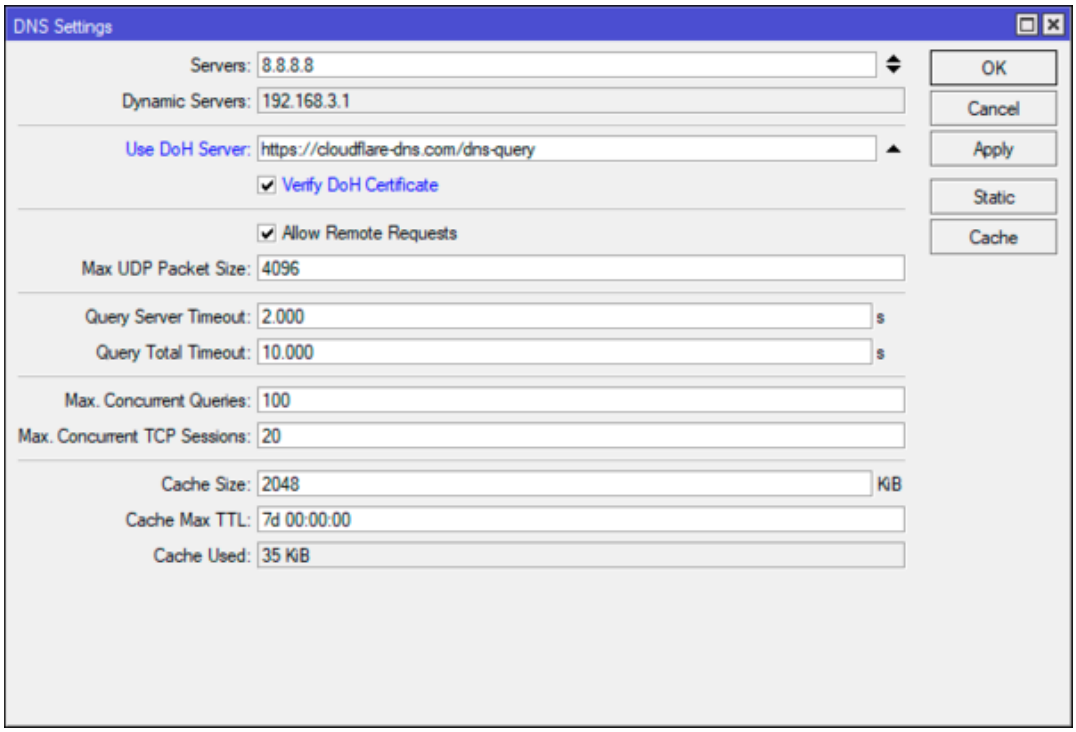
Чтобы избежать раскрытия данных о DNS-запросах был реализован протокол **DNS over HTTPS** (*DoH*), который осуществляет взаимодействие с DNS-серверами по защищенному HTTPS-каналу, что исключает перехват запросов, теперь о вашей интернет активности будете знать только вы и DNS-сервер.

В RouterOS возможность использовать DoH появилась начиная с версии 6.47, но в ней имеется ряд уязвимостей, которые могут привести к утечке DNS, поэтому минимальной версией для DoH следует считать 6.47.1.

Следующий вопрос - какие сервера DoH использовать? Мы рекомендуем крупных публичных провайдеров, благо есть из чего выбирать, ниже приведены провайдеры и URL-адреса DoH серверов:

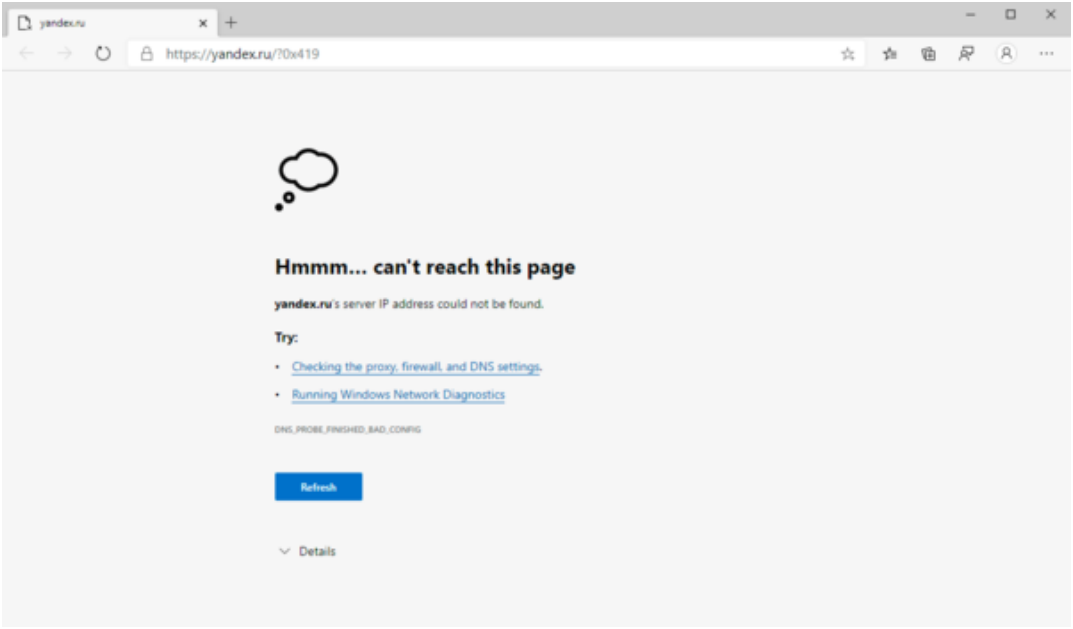
OpenDNS - https://doh.opendns.com/dns-query
Quad9 - https://dns.quad9.net/dns-query
Cloudflare - https://cloudflare-dns.com/dns-query
Google Public DNS - https://dns.google/dns-query

Для настройки DNS over HTTPS перейдем в **IP - DNS** и внесем в поле **Use DoH Server** URL-адрес одного из DoH-серверов, в нашем случае это Cloudflare. Также обязательно установим флаг **Verify DoH Certificate**.



Здесь возникает один интересный парадокс: DoH-сервер указан в виде URL, и чтобы достичь его нам нужно будет выполнить разрешение имен на обычном DNS-сервере. Поэтому в настройках выше у вас должен быть указан хотя бы один DNS-сервер. Наиболее правильно будет не трогать текущие настройки DNS, так как при указании DoH все запросы будут автоматически направляться к нему. Таким образом ваш провайдер будет знать, что вы используете DoH, но ваша интернет активность будет от него полностью скрыта.

Вроде бы все настроено правильно, но после применения данных настроек доступ в интернет на клиентах пропадет. А в качестве причины будет указана невозможность разрешения DNS-запросов.



В чем же дело? А дело в флаге **Verify DoH Certificate**, который предписывает роутеру проверить предъявляемый DoH сертификат. Можно, кончено, обойтись и без проверки, но это позволит любому злоумышленнику перехватить запрос и отправить собственный ответ, который будет принят роутером, что сведет на нет весь смысл защиты DNS с помощью HTTPS.

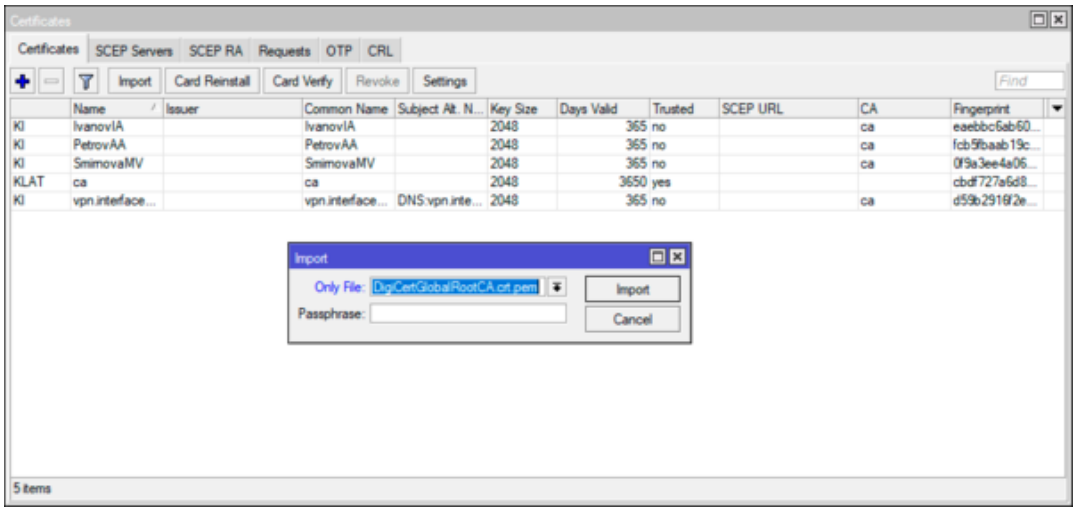
Но почему сертификат не проходит проверку? Да потому что RouterOS не имеет возможности ее выполнить. Для того чтобы проверить валидность сертификата нам потребуется **корневой сертификат центра сертификации** (CA), во "взрослых" ОС такие сертификаты хранятся в защищенном системном хранилище и обновляются средствами системы, в RouterOS нам нужно добавить такие сертификаты самостоятельно.

Для работы с Google Public DNS нам потребуется корневой сертификат **GlobalSign Root CA - R2**, а для остальных провайдеров - **DigiCert Global Root CA**, формат скачиваемых сертификатов - **PEM**.

GlobalSign Root CA - R2
SHA-256:
69:E2:D0:6C:30:F3:66:16:61:65:E9:1D:68:D1:CE:E5:CC:47:58:4A:80:22:7E:76:66:60:86:C0:10:72:41:EB

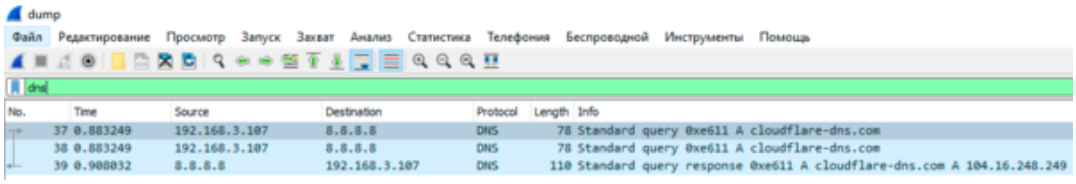
DigiCert Global Root CA
SHA-256:
43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61

Данные сертификаты следует скопировать на Mikrotik и находясь в **System - Certificates** выполнить их импорт.



Корневые сертификаты CA не являются секретными, но именно они отвечают за доверие ко всем выпущенным этим удостоверяющим центром сертификатам, поэтому скачивайте их только с официальных источников (на нашем сайте ссылки именно оттуда) и обязательно проверяйте контрольные суммы, которые отображаются в колонке **Fingerprint** на Mikrotik.

После того, как мы импортируем корневой сертификат доступ во всемирную сеть появится. А что теперь у нас видит провайдер? Снова снимем дамп трафика на промежуточном роутере и изучим его. На этот раз не густо, единственное что можно узнать - это то, что мы используем DoH от Cloudflare.



Как видим - настроить DoH не сложно, но это позволить поднять защиту приватной информации на качественно новый уровень. Надеемся, что данный материал окажется вам полезен, также всегда готовы к вашим вопросам в комментариях.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.