

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 была 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.

No.	Time	Source	Destination	Protocol	Length	Info
58	5.877051	192.168.3.187	192.168.3.187	DNS	82	Standard query 8d128 A www.sashingspost.com
68	5.877051	192.168.3.187	8.8.8.8	DNS	82	Standard query 8d128 A www.sashingspost.com
69	5.881049	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d72c A adservice.google.com
68	5.881049	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d72c A adservice.google.com
71	5.887711	192.168.3.187	8.8.8.8	DNS	88	Standard query 8d209 A csa.fr.eu.critico.net
72	5.887711	192.168.3.187	8.8.8.8	DNS	88	Standard query 8d209 A csa.fr.eu.critico.net
76	5.887715	192.168.3.187	192.168.3.187	DNS	124	Standard query response 8d72c A adservice.google.com CNWE pagad46.1.doubleclick.net A 173.194.226.157 A 173.194.226.156 A 173.194.226.155 A 173.194.226.154
89	5.912090	8.8.8.8	192.168.3.187	DNS	127	Standard query response 8d209 A csa.fr.eu.critico.net CNWE csa.pw.cip.prod.critico.net A 178.258.8.162
90	5.912090	8.8.8.8	192.168.3.187	DNS	162	Standard query response 8d209 A www.sashingspost.com CNWE 58901.edgekey.net CNWE e9811.1.akamaiedge.net A 92.123.285.76
102	6.120587	192.168.3.187	8.8.8.8	DNS	86	Standard query 8d108 A metrics.sashingspost.com
103	6.120587	192.168.3.187	8.8.8.8	DNS	86	Standard query 8d108 A metrics.sashingspost.com
496	6.228568	8.8.8.8	192.168.3.187	DNS	178	Standard query response 8d108 A metrics.sashingspost.com CNWE sashingspost.com 112.207.net A 15.217.76.127 A 15.182.18.61 A 15.217.136.186
512	6.269551	192.168.3.187	8.8.8.8	DNS	78	Standard query 8d170 A as.casalemedia.com
512	6.269551	192.168.3.187	8.8.8.8	DNS	78	Standard query 8d170 A as.casalemedia.com
564	6.380378	8.8.8.8	192.168.3.187	DNS	169	Standard query response 8d370 A as.casalemedia.com CNWE as.casalemedia.com edgecube.net CNWE al851.g.akamai.net A 88.48.78.147
643	6.427585	192.168.3.187	8.8.8.8	DNS	96	Standard query 8d1ab AAAA get-my-ip.dns.softhether-network.net
644	6.427585	192.168.3.187	8.8.8.8	DNS	96	Standard query 8d1ab AAAA get-my-ip.dns.softhether-network.net
651	6.466422	8.8.8.8	192.168.3.187	DNS	161	Standard query response 8d1ab AAAA get-my-ip.dns.softhether-network.net SOA ncj.temmodel.net
652	6.467063	192.168.3.187	8.8.8.8	DNS	96	Standard query 8d1ab A get-my-ip.dns.softhether-network.net
653	6.467063	192.168.3.187	8.8.8.8	DNS	96	Standard query 8d1ab A get-my-ip.dns.softhether-network.net
655	6.495797	8.8.8.8	192.168.3.187	DNS	112	Standard query response 8d1ab A get-my-ip.dns.softhether-network.net A 138.158.75.46
702	5.287426	192.168.3.187	8.8.8.8	DNS	188	Standard query 8d1c1 AAAA vk.ud.servers.dns.softhether-network.net
702	5.287426	192.168.3.187	8.8.8.8	DNS	188	Standard query 8d1c1 AAAA vk.ud.servers.dns.softhether-network.net
756	5.588067	8.8.8.8	192.168.3.187	DNS	165	Standard query response 8d1c1 AAAA vk.ud.servers.dns.softhether-network.net SOA ncj.temmodel.net
759	5.588068	192.168.3.187	8.8.8.8	DNS	72	Standard query 8d180 A cbr.krud.net
760	5.588068	192.168.3.187	8.8.8.8	DNS	72	Standard query 8d180 A cbr.krud.net
761	5.588068	192.168.3.187	8.8.8.8	DNS	238	Standard query response 8d180 A cbr.krud.net CNWE cbr-traffic-director.krud.net CNWE cbr-fastly.krud.net CNWE d.us.globe.fastly.net A 151.181.2.133 A 151.181.2.132 A 151.181.2.131 A 151.181.2.130
888	5.962852	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d175 A targeting.sashpost.sile.works
889	5.962852	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d175 A targeting.sashpost.sile.works
892	5.991848	8.8.8.8	192.168.3.187	DNS	137	Standard query response 8d175 A targeting.sashpost.sile.works A 3.232.74.79 A 52.282.156.49 A 52.287.71.115
893	6.025386	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d1a1 A coral-talk.net.sile.works
894	6.025386	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d1a1 A coral-talk.net.sile.works
899	6.087655	8.8.8.8	192.168.3.187	DNS	214	Standard query response 8d1a1 A coral-talk.net.sile.works CNWE up-talk-prod-citeng-buchanan-358881876.us-east-1-elb.amazonaws.com A 54.175.144.284 A 52.3.11.11
911	6.121676	192.168.3.187	8.8.8.8	DNS	86	Standard query 8d1b6 A collector.broadmetrics.com
912	6.121676	192.168.3.187	8.8.8.8	DNS	86	Standard query 8d1b6 A collector.broadmetrics.com
913	6.135875	192.168.3.187	8.8.8.8	DNS	388	Standard query response 8d1c1 A collector.broadmetrics.com CNWE bccollector-go.trafficmanager.net CNWE bccollector-linux.azurewebsites.net CNWE www.broadmetrics.com
1424	6.877488	192.168.3.187	8.8.8.8	DNS	187	Standard query 8d40e A vk.ud.servers-vk.dns.softhether-network.net
1425	6.877488	192.168.3.187	8.8.8.8	DNS	187	Standard query 8d40e A vk.ud.servers-vk.dns.softhether-network.net
1438	6.877488	192.168.3.187	8.8.8.8	DNS	124	Standard query 8d476 A 578077ba6fd6b6a1a3d2af527ff92.safeframe.googleyndication.com
1451	6.877488	192.168.3.187	8.8.8.8	DNS	124	Standard query 8d476 A 578077ba6fd6b6a1a3d2af527ff92.safeframe.googleyndication.com
1467	6.887578	8.8.8.8	192.168.3.187	DNS	118	Standard query response 8d776 A 578077ba6fd6b6a1a3d2af527ff92.safeframe.googleyndication.com CNWE pagad-googletexted.1.google.com A 178.194.73.132
1468	6.888488	8.8.8.8	192.168.3.187	DNS	183	Standard query response 8d776 A 578077ba6fd6b6a1a3d2af527ff92.safeframe.googleyndication.com CNWE pagad-googletexted.1.google.com A 178.194.73.132
1585	7.094419	192.168.3.187	8.8.8.8	DNS	118	Standard query 8d385 A whlqpkqgqgq7y2ce-f-c2d88bd-clientnoc-s.akamaihd.net
1586	7.094419	192.168.3.187	8.8.8.8	DNS	118	Standard query 8d385 A whlqpkqgqgq7y2ce-f-c2d88bd-clientnoc-s.akamaihd.net
1538	7.158825	8.8.8.8	192.168.3.187	DNS	255	Standard query response 8d385 A whlqpkqgqgq7y2ce-f-c2d88bd-clientnoc-s.akamaihd.net CNWE whlqpkqgqgq7y2ce-f-c2d88bd-clientnoc-s.akamaihd.net
2292	18.873492	192.168.3.187	8.8.8.8	DNS	72	Standard query 8d674 A sds.adfox.ru
2293	18.873492	192.168.3.187	8.8.8.8	DNS	72	Standard query 8d674 A sds.adfox.ru
2298	18.188221	192.168.3.187	8.8.8.8	DNS	88	Standard query response 8d674 A sds.adfox.ru A 77.88.21.179
2227	18.182586	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d311 A nav.smartscreen.adirsoft.com
2228	18.182586	192.168.3.187	8.8.8.8	DNS	89	Standard query 8d311 A nav.smartscreen.adirsoft.com
2238	18.214795	192.168.3.187	8.8.8.8	DNS	79	Standard query 8d5a2 A discover.asomex
2239	18.214795	192.168.3.187	8.8.8.8	DNS	79	Standard query 8d5a2 A discover.asomex
2252	18.218979	8.8.8.8	192.168.3.187	DNS	212	Standard query response 8d311 A nav.smartscreen.adirsoft.com CNWE wd-prod-us-trafficmanager.net CNWE wd-prod-us-west-2-fx.sourcerise.cloudapp.azure.com
2257	18.242284	8.8.8.8	192.168.3.187	DNS	89	Standard query response 8d5a2 A discover.asomex A 232.11.134.96
2399	12.941385	192.168.3.187	8.8.8.8	DNS	76	Standard query 8d68A A top-fucl.mel.ru

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.

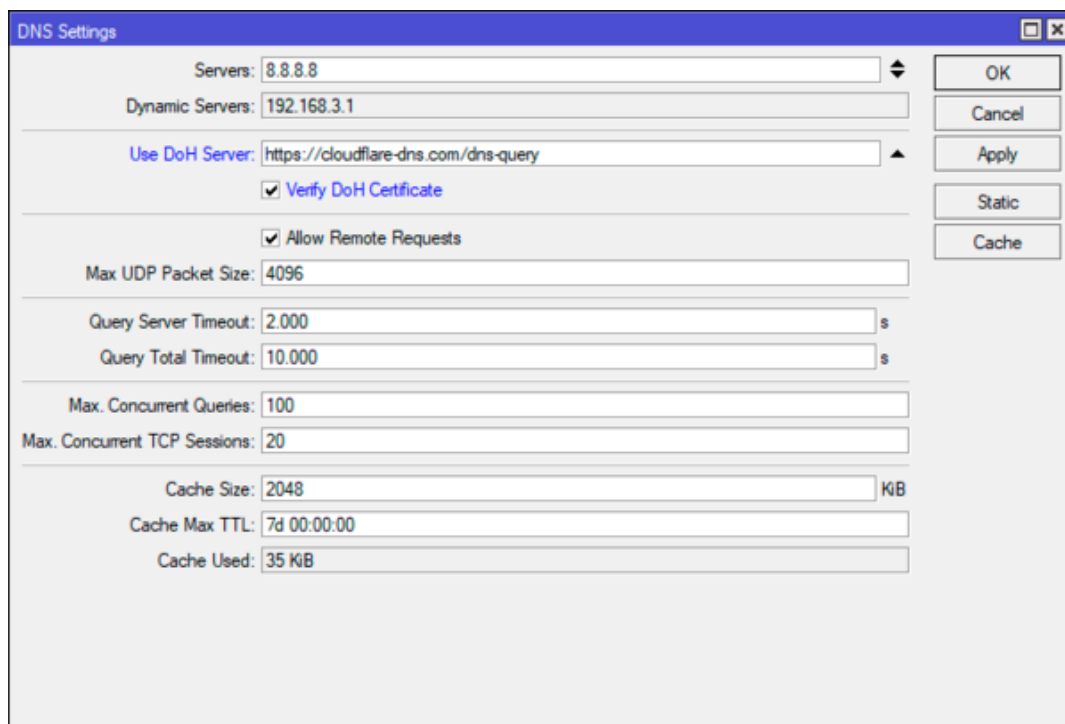
Чтобы избежать раскрытия данных о DNS-запросах был реализован протокол **DNS over HTTPS (DoH)**, который осуществляет взаимодействие с DNS-серверами по защищенному HTTPS-каналу, что исключает перехват запросов, теперь о вашей интернет активности будете знать только вы и DNS-сервер.

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:

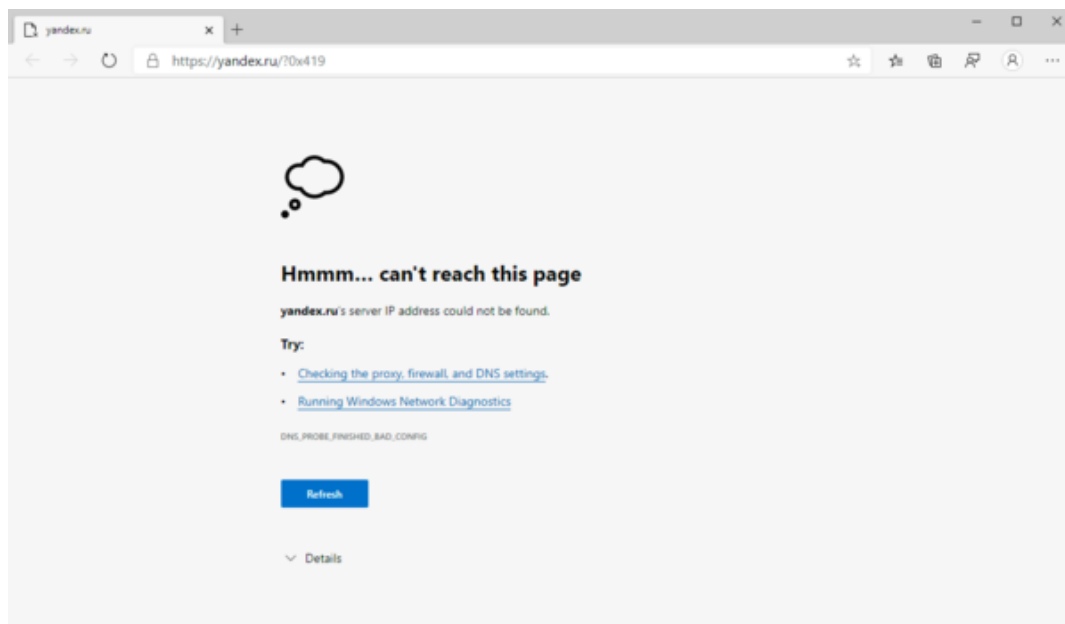
OpenDNS - <https://doh.opendns.com/dns-query>
Quad9 - <https://dns.quad9.net/dns-query>
Cloudflare - <https://cloudflare-dns.com/dns-query>
Google Public DNS - <https://dns.google/dns-query>

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, конечно, 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:

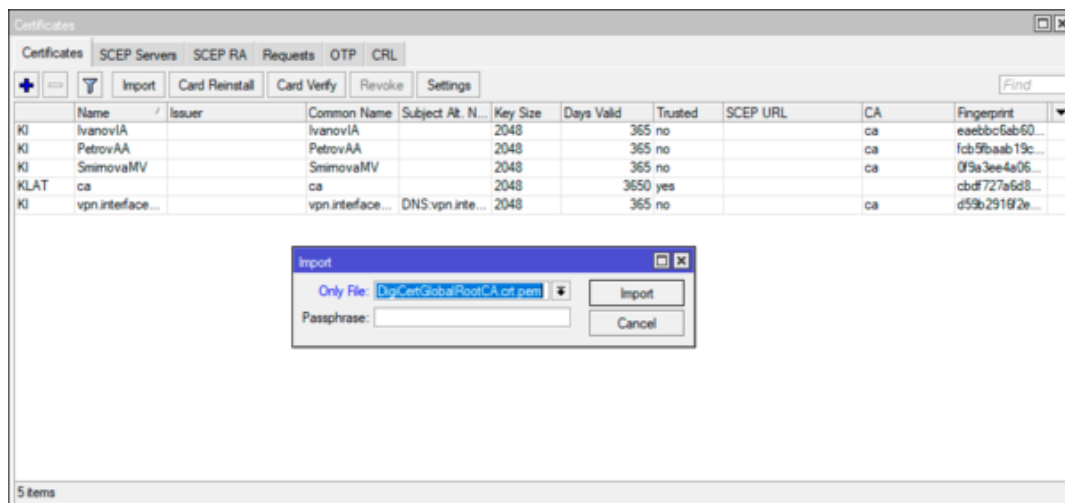
69:E2:D0:6C:30:F3:66:16:61:65:E9:1D:68:D1:CE:E5:CC:47:58:4A:80:22:7E:76:66:60:86:C0:10:72:41:EB

DigiCert Global Root CA

SHA-256:

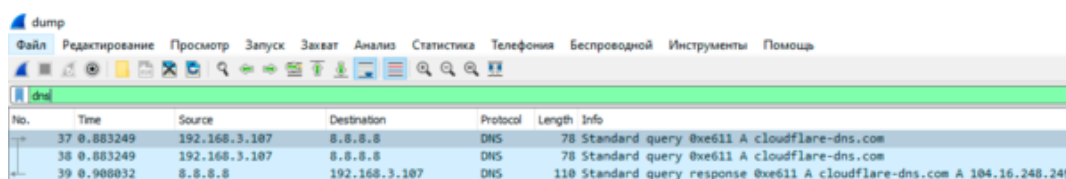
43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61

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 позволяет 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.