Configuring Mikrotik DNS

DNS Dynamic Servers OFF

Группа исследователей из нескольких университетов США и Китая провела исследование степени вмешательства провайдеров в транзитный DNS-трафик пользователей. Для обращения к DNS в большинстве случаев не применяются технологии аутентификации (DNSSEC) и шифрования (DNS over TLS/HTTPS), что позволяет провайдерам легко перехватывать и перенаправлять на свои сервера DNS-запросы к публичным DNS-серверам, таким как 8.8.8.8 (Google), 1.1.1.1 (Cloudflare), OpenDNS, Dyn DNS и Edu DNS. Основными мотивами перенаправления обычно является желание сэкономить трафик, снизить время отклика, обеспечить дополнительную защиту или реализовать блокировку запрещённых ресурсов.

Метод определения перехвата был основан на отправке запроса на резолвинг уникального хоста (UUID.OurDomain.TLD)) с последующей проверкой с какого DNS-резолвера поступил запрос на обслуживающий данный хост авторитативный DNS-сервер (например, о перехвате свидетельствует активность, когда клиентом был отправлен запрос резолвинга на 8.8.8.8, а к авторитативному серверу пришёл запрос от стороннего IP провайдера, а не от DNS-сервера Google).

Наибольшая активность перехвата наблюдается в Китае, в котором из 356 автономных систем перехват применяется в 61 AS (17% от всех рассмотренных в данной стране AS), в России - 44 AS (28%), в США - 15 AS (9%), Бразилии и Индонезии по 7 AS (4%).

Из методов перехвата трафика наиболее популярными являются перенаправление запросов и реплицирование ответа (оригинальный запрос и ответ не блокируются, но провайдер также направляет свой подставной ответ, который обычно приходит раньше и воспринимается клиентом). Как правило, в рамках одной автономной системы используется один метод перехвата, который применяется к конкретным внешним DNS-серверам, что свидетельствует о применении провайдером единой политики.

Наиболее часто перехватываемым публичным DNS-сервером стал сервис Google (8.8.8.8), для которого в Китае перехватывается 27.9% запросов по UDP и 7.3% по TCP. В 82 автономных системах перехватывается более 90% трафика к Google DNS. При этом в AS9808 (Guangdong Mobile) зафиксирована подмена результата для 8 запросов к Google Public DNS, в которых вместо запрошенного хоста был выдан ответ с IP рекламного сайта, продвигающего приложение China Mobile.

Проверим настройки:

```
[admin@MikroTik] > /ip dns print

servers: 8.8.8.8,8.8.4.4
dynamic-servers: 192.168.8.1,85.21.192.5,213.234.192.7
allow-remote-requests: yes
max-udp-packet-size: 4096
query-server-timeout: 2s
query-total-timeout: 10s
max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 51KiB
```

Основной сервер: `8.8.8.8,8.8.4.4`

`Динамические сервера: 192.168.8.1,85.21.192.5,213.234.192.7`

Отключение DHCP client от PeerDNS:

/ip dhcp-client set use-peer-dns=no

Отключение PPOE от PeerDNS:

/interface ppoe-client set use-peer-dns=no 0 (ввести 0 число).

Ввести ваши DNS сервера:

/ip dns set server=208.67.222.220,208.67.222.222

Обратите внимание на кэш, перезагрузите устройства подключенные к роутеру, перезагрузите роутер.

Проверим настройки:

/ip dns print

servers: 208.67.222.222,208.67.220.220
dynamic-servers:
allow-remote-requests: no
max-udp-packet-size: 4096
query-server-timeout: 2s
query-total-timeout: 10s
max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 13KiB