Настраиваем двойной горизонт DNS (Split DNS) на роутерах Mikrotik

Записки IT специалиста

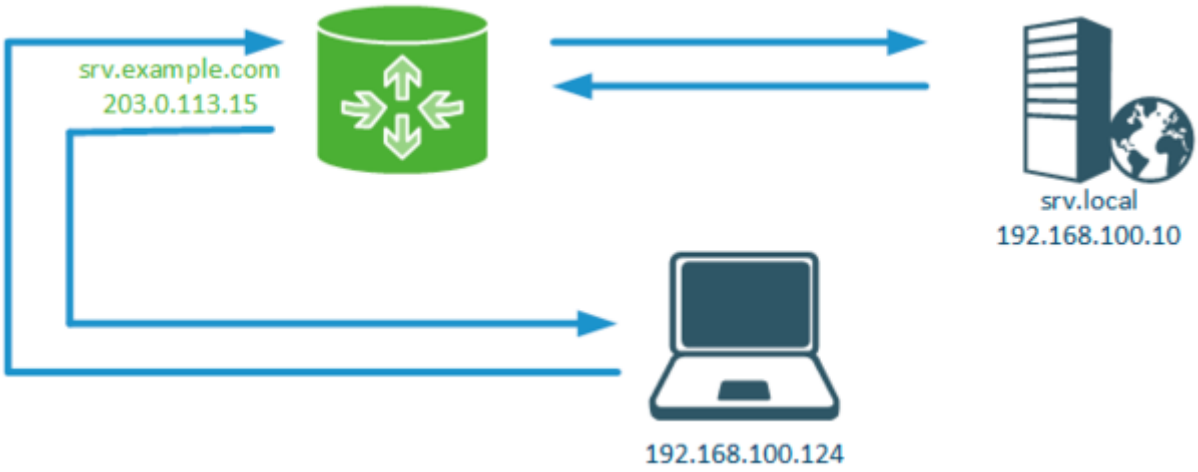
Технический блог специалистов ООО"Интерфейс"

- Главная
- Настраиваем двойной горизонт DNS (Split DNS) на роутерах Mikrotik

Двойным горизонтом DNS (Split DNS, разделенный DNS) называется такая организация системы доменных имен, когда различным клиентам предоставляется различные наборы информации в зависимости от некоторых условий. Например, в зависимости от исходного адреса DNS-запроса или запрашиваемого домена. Это простой, но в тоже время удобный инструмент, позволяющий гибко управлять пространством имен с минимальной нагрузкой на оборудование. В данной статье мы рассмотрим, как настраивать двойной горизонт DNS на роутерах Mikrotik.

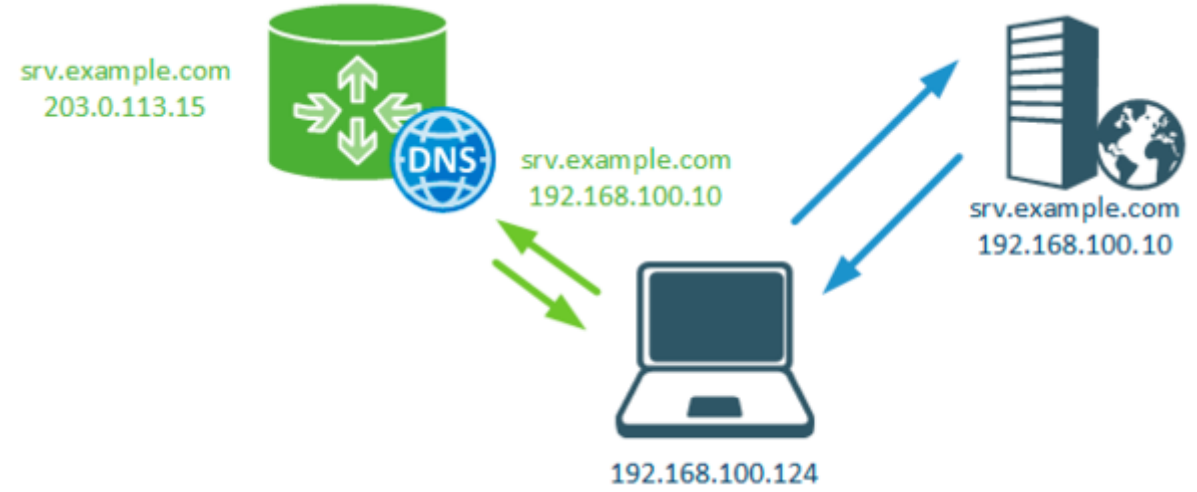
Важно! В роутерах Mikrotik DNS over HTTPS (DoH) имеет **приоритет** над встроенным DNS-сервером и при его включении ничего из описанного ниже **работать не будет**!

Итак, двойной горизонт DNS, что это такое и для чего нужно? Давайте представим себе простую ситуацию, во внутренней сети у нас есть сервер, который одновременно доступен снаружи по публичному доменному имени. И есть мобильные клиенты, которые могут подключаться к этому серверу как снаружи, так и внутри периметра. Так как имя сервера разрешается во внешний IP-адрес, то для нормальной работы внутри периметра обычно настраивается Hairpin NAT, который позволяет обеспечить правильное прохождение пакетов от клиента к серверу вне зависимости от его расположения.

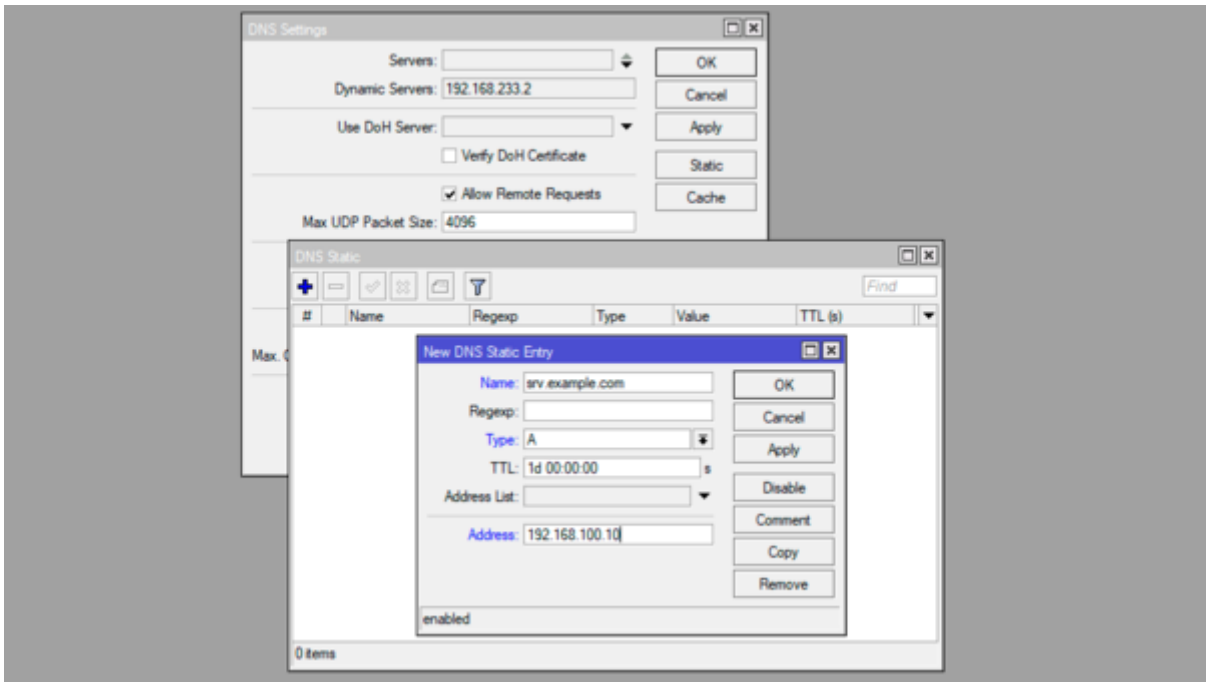


Эта схема полностью рабочая, но имеет один существенный недостаток: весь трафик между клиентами и сервером, находящимися в одной локальной сети **все равно проходит через роутер**, создавая лишнюю нагрузку на оборудование.

Как можно этого избежать? Очень просто, настроим на локальном DNS-сервере статическую запись, которая на запрос адреса сервера будет отдавать его внутренний адрес. Теперь, оказавшись внутри периметра локальный клиент будет общаться с сервером напрямую, минуя роутер. При этом везде за пределами локальной сети адрес сервера по-прежнему разрешается во внешний адрес. Это и есть двойной горизонт DNS.



Как реализовать это в роутерах Mikrotik? Переходим в **IP - DNS - Static** и добавляем запись типа **A** в которой указываем внешнее доменное имя сервера и его внутренний адрес.



Либо выполните в терминале:

```
/ip dns static
add address=192.168.100.10 name=srv.example.com
```

Это самый простой вариант системы с двойным горизонтом, но Mikrotik позволяет реализовывать и более сложные схемы, связанные с пересылкой запросов к разным доменам на разные DNS-сервера.

Допустим у нас есть локальный домен **interface31.lab**, который обслуживает DNS-сервер **192.168.72.8,** и мы хотим все запросы к адресам локального домена направлять ему, а остальное - вышестоящим DNS-серверам (публичным или провайдерским).

Снова переходим в **IP - DNS - Static** и добавляем запись типа **FWD** со следующим содержимым:

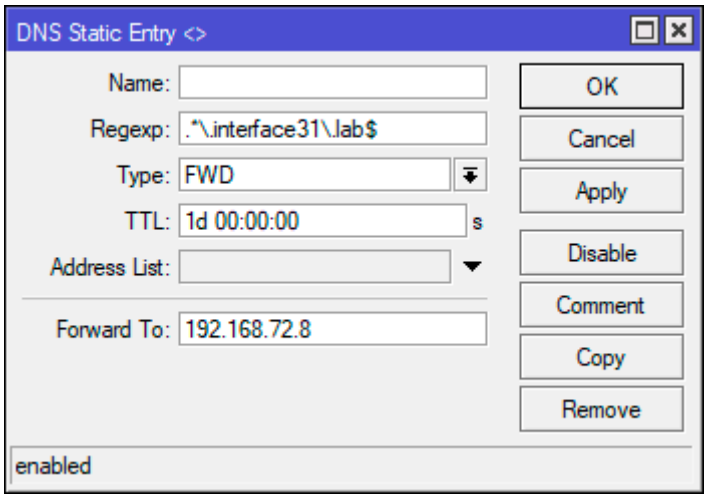
- **Regexp** - .*\.interface31\.lab$
- **Type** - FWD
- **Forward To** - 192.168.72.8

В терминале это можно сделать следующей командой:

```
/ip dns static
add forward-to=192.168.72.8 regexp=".*\\.interface31\\.lab\$" type=FWD
```

При работе с регулярными выражениями в Mikrotik следует помнить, что они **регистрозависимые**, в то время как **DNS-запросы не чувствительны к регистру**, поэтому Mikrotik автоматически переводит все DNS-запросы в нижний регистр и все регулярные выражения нужно составлять именно в нем.

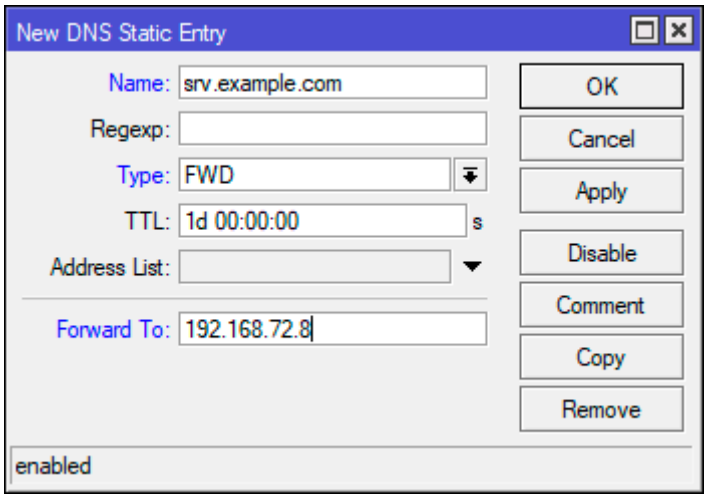
А как быть, если нам нужно перенаправить запрос только к единственному доменному имени? Просто впишите его в поле **Name**:



Команда для терминала:

```
/ip dns static
add forward-to=192.168.72.8
name=srv.example.com type=FWD
```

Стоп, скажет внимательный читатель, а чем это отличается от A-записи, которую мы добавляли в начале статьи? По сути ничем, но позволяет реализовать централизованный подход к управлению пространством имен. Если вы решили изменить внутренний IP-адрес для узла **srv.example.com**, то это нужно будет сделать на единственном вышестоящем сервере. В противном случае вам придется изменять настройки на каждом из роутеров.



Теперь о приоритетах. Любая A-запись имеет больший приоритет, чем FWD. Любая запись с использованием регулярных выражений имеет приоритет над записью с простым указанием имени. Т.е. сначала обрабатываются A-записи с Regexp, потом A с Name, потом FWD с Regexp и уже после них FWD с Name. Учитывайте это при создании записей.

Это же позволяет исключить отдельные имена из перенаправления по регулярному выражению - просто создайте для них A-записи.

Надеемся это материал окажется вам полезен и позволит в полной мере раскрыть все возможности вашего роутера Mikrotik.

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.