Содержание

Обработка DNS-запросов и подмена DNS-ответов	. 3
Назначение	. 3
Схема работы услуги	. 3
Настройка	. 4
Управление	4

Обработка DNS-запросов и подмена DNSответов

Назначение

Услуга подмены DNS-ответов позволяет изменять IP-адреса, возвращаемые DNS-сервером для определенных доменных имен. Это позволяет влиять на ответы DNS-серверов, переопределяя IP-адреса в ответах сервера для определённых типов DNS-запросов, указанных в настройках услуги.

Эта услуга эффективна для контроля DNS-запросов клиентов и перенаправления их на альтернативные IP-адреса. Используется для балансировки трафика определенных ресурсов между разными серверами на основании IP адреса.

Описание настройки экспорта DNS-запросов и DNS-ответов.

Схема работы услуги

- 1. Клиент выполняет определенный тип запроса к DNS-серверу (например, тип A).
- 2. DPI анализирует все DNS-запросы и проверяет, назначена ли услуга подмены для этого клиента (IP sourse) на конкретный ресурс. В случае если настроена блокировка данного запроса, то DPI только отбрасывает DNS-запрос с конкретным типом записи.
- 3. Если услуга назначена, DPI отбрасывает оригинальный DNS запрос клиента и формирует ответ DNS-сервера, в зависимости от указанных правил в услуге.
- 4. DPI перенаправляет модифицированный ответ клиенту. При этом клиент не замечает модификации и считает ответ легитимным.

Поддерживаемые типы DNS-записи:

- A IPv4-адрес (длина 32 бита);
- AAAA IPv6-адрес (длина 128 бит);
- HTTPS тип записи предназначен для предоставления информации о доступных сервисах, работающих по протоколу HTTPS. Он позволяет указывать альтернативные endpoints, поддержку HTTP/3, шифрование ClientHello и нестандартные порты TCP/UDP;
- MX txt-запись, которая содержит информацию о почтовых серверах, обрабатывающих почту.

Возможные действия с DNS-запросами:

- ya.ru HTTPS #drop DPI отбрасывает DNS-запрос с HTTPS типом записи
- ya.ru HTTPS #nxdomain DPI отвечает домен не сущетсвует на DNS-запрос с типом записи HTTPS
- ya.ru A #nxdomain DPI отправляет ответ об отсутствии домена с типом записи А
- mail.ru MX smtp.googlemail.com в данном случае на запрос mail.ru с типом MX должен быть получен ответ что домен mail.ru имеет почтовый сервер по адресу smtp.googlemail.com с preference равным 10.

Настройка

1. Создать текстовый файл и добавить в него правила обработки DNS-запросов, указав: доменное имя, тип DNS-записи, или действие, или IP-адрес или домен для записи с типом МХ, который будет указан в ответе для данного домена. Поддерживается указание * для доменов.

```
vi test.txt
google.com A 192.0.2.1
test.ru A #nxdomain
example.com AAAA 2001:db8:85a3::8a2e:370:7334
ya.ru HTTPS #drop
*.fb.com A 203.0.113.5
mail.ru MX smtp.googlemail.com
```

2. Утилитой dns2dic конвертировать текстовый файл в бинарный формат, понятный для DPI:

```
cat test.txt|dns2dic test.bin
```

Обратная конвертация утилитой dic2dns.

3. Поместить полученный бинарный файл в директорию, откуда его будет читать DPI:

```
cp test.bin /var/lib/dpi/dns.bin
```

4. Создать профиль услуги:

```
fdpi_ctrl load profile --service 19 --profile.name test_193 --
profile.json '{ "dns_list" : "/var/lib/dpi/dns.bin" }'
```

 $max_profiles_serv19$ — настройка максимального количества профилей. По умолчанию — 32.



DNS ответ по умолчанию направляется в тот интерфейс с которого пришел запрос (IN интерфейс из которого пришел запрос от абонента). Отправка в OUT интрефейс актуальна для асимметричного режима работы DPI (только на исходящем трафике). Настраивается в fastdpi.conf параметром emit_direction=2

Управление

Формат команды:

```
fdpi_ctrl [команда] --service 19 [список опций] [login или vchannel]
```

Подключение услуги:

```
fdpi_ctrl load --service 19 --profile.name test_193 --login test
#или
fdpi_ctrl load --service 19 --profile.name test_193 --vchannel 1
```

Отключение услуги:

```
fdpi_ctrl del --service 19 --profile.name test_193 --login test
#или
fdpi_ctrl del --service 19 --profile.name test_193 --vchannel 1
```

Поиск абонентов, которым подключена услуга с заданным именем профиля:

```
fdpi_ctrl list all --service 19 --profile.name test_193
```

Удаление именованного профиля (не должно быть абонентов, которые его используют):

```
fdpi_ctrl del profile --service 19 --profile.name test_193
```

Изменение настроек (профиля) услуги (новые настройки применятся ко всем абонентам с заданным профилем услуги):

```
fdpi_ctrl load profile --service 19 --profile.name test_193 --profile.json
'{ "dns_list" : "/var/lib/dpi/dns.bin" }'
```