

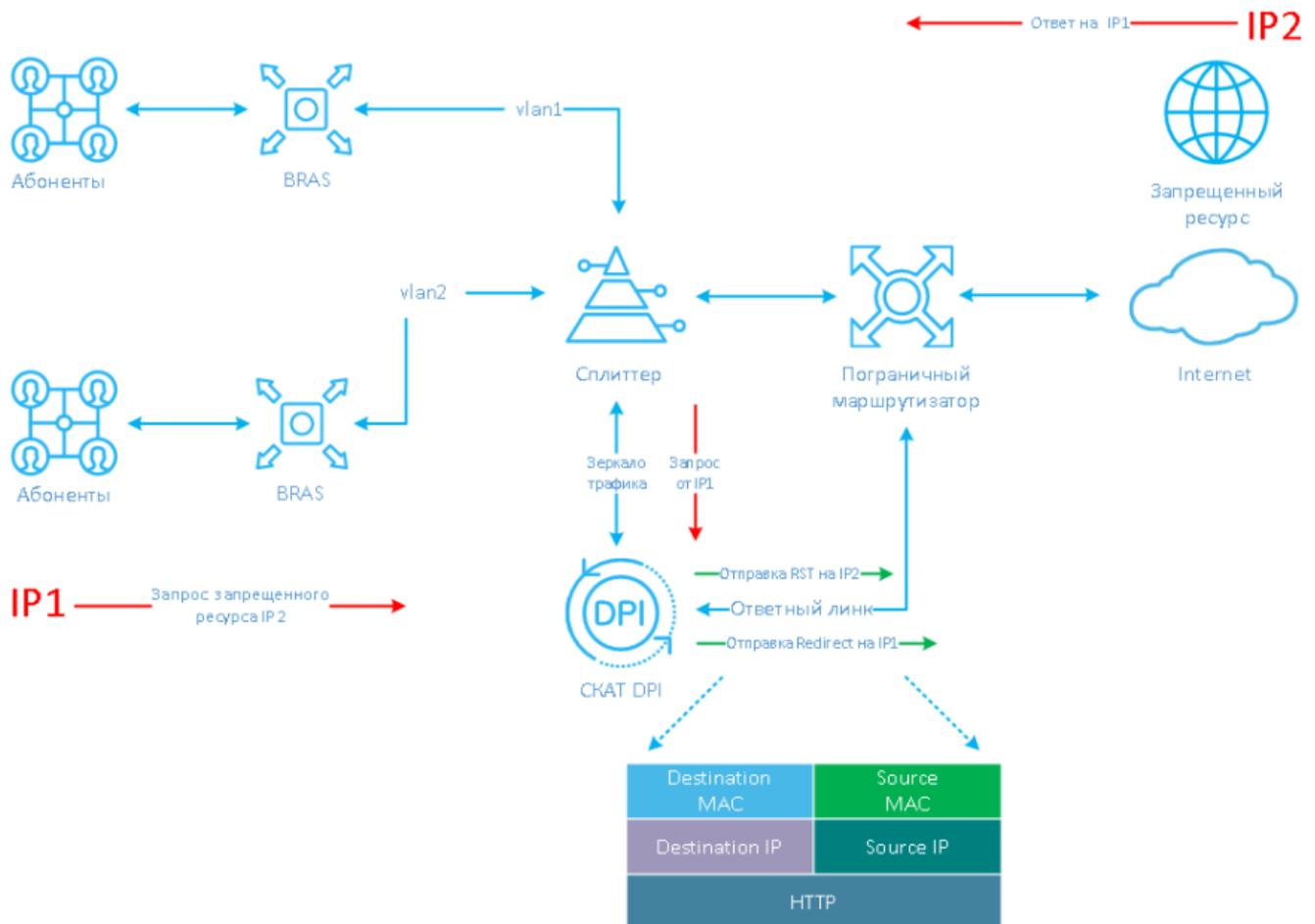
# Содержание

Схема установки СКАТ на зеркало трафика .....	3
<i>Заголовки пакета:</i> .....	3
<i>Настройка маршрутизатора</i> .....	4
Пример конфигурирования СКАТ .....	4



# Схема установки СКАТ на зеркало трафика

(SPAN порты или оптический сплиттер)



При обнаружении запроса на запрещенный ресурс СКАТ отправляет HTTP Redirect для переадресации запроса на страницу-заглушку.

## Заголовки пакета:

- Destination MAC - MAC адрес порта маршрутизатора, куда подключен ответный линк
- Source MAC - MAC адрес карты out\_dev
- Source IP - IP адрес запрещенного ресурса IP2
- Destination IP - IP адрес пользователя IP1

Номер Vlan может быть сохранен либо сброшен.

В сторону IP2 (запрещенного ресурса) направляется пакет TCP RST, который сбрасывает соединение. Блокировка (HTTPS) и переадресация (HTTP) происходит, т.к. СКАТ отвечает на запрос от IP1 быстрее чем IP2.

## Настройка маршрутизатора

Порт на маршрутизаторе, куда включен ответный линк от SKAT, должен быть сконфигурирован как обычный L3 порт. Задача принять пакет от SKAT и на основе общих таблиц маршрутизации направить его абоненту.

Пример конфигурации: В сторону Juniper MX подключен eth1

- На стороне MX настройки:
- description from\_SKAT\_redirect;
- unit 0 {
- family inet {
- address a.b.c.d/30;
- }
- }

## Пример конфигурирования SKAT

Изменение настроек осуществляется с помощью редактирования файла конфигурации **/etc/dpi/fastdpi.conf**. Допустим SKAT подключен сл. образом:

```
dna1, dna2, dna3 - принимают зеркало трафика
dna0 - подключен к маршрутизатору, который принимает и перенаправляет ответы
абонентам и в инет
```

Для настройки DPI работы в режиме работы - зеркалирования, в конфигурации нужно указать следующее:

установить в конфигурации для входящих портов, in\_dev порты, которые принимают зеркало трафика:

```
in_dev=dna1:dna2:dna3
```

установить в конфигурации для исходящих портов, tap\_dev порт на который отправляется ответ о переадресации:

```
tap_dev=dna0
```

Указать режим работы -асимметричный:

```
asym_mode=1
```

указать направление ответов tap\_dev:

```
emit_direction=2
tap_mode=2
```

указать что необходимо сбрасывать vlan:

```
strip_tag_tags=1
```

прописать смену MAC:

```
replace_source_mac=00:25:90:E9:43:59 - MAC адрес карты out_dev - dna0  
replace_destination_mac=78:19:F7:0E:B1:F4 - MAC адрес маршрутизатора, или  
маршрутизирующего коммутатора
```

Установите к-во повторов, если есть потери в сети:

```
emit_duplication=3  
где 3 - это количество повторов (дублей) пакета с редиректом или блокировкой
```

Для отправки ответов в режиме зеркалирования, правильно использовать дополнительную карту 1GbE, например, intel i350 (+ лицензию DNA), сконфигурировать в системе отдельный порт для отправки переадресации, а 10GbE порты задействовать под потоки зеркалированного трафика.