Содержание

Инструкции по установке СКАТ по схеме на зеркало трафика

1. Установите и запустите СКАТ. Требования по установке.
2. Установите IP адрес.
3. В Service Desk подайте заявку на установку лицензии и fastDPI.
4. После их установки необходимо внести следующие параметры:

Настроить прием зеркала и ответ:

Изменение настроек осуществляется с помощью редактирования файла конфигурации **`/etc/dpi/fastdpi.conf`**. Допустим, СКАТ подключен следующим образом:

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

Для настройки DPI в режиме 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=
```

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

Указать, что необходимо сбрасывать vlan:

```
strip_tap_tags=1
```

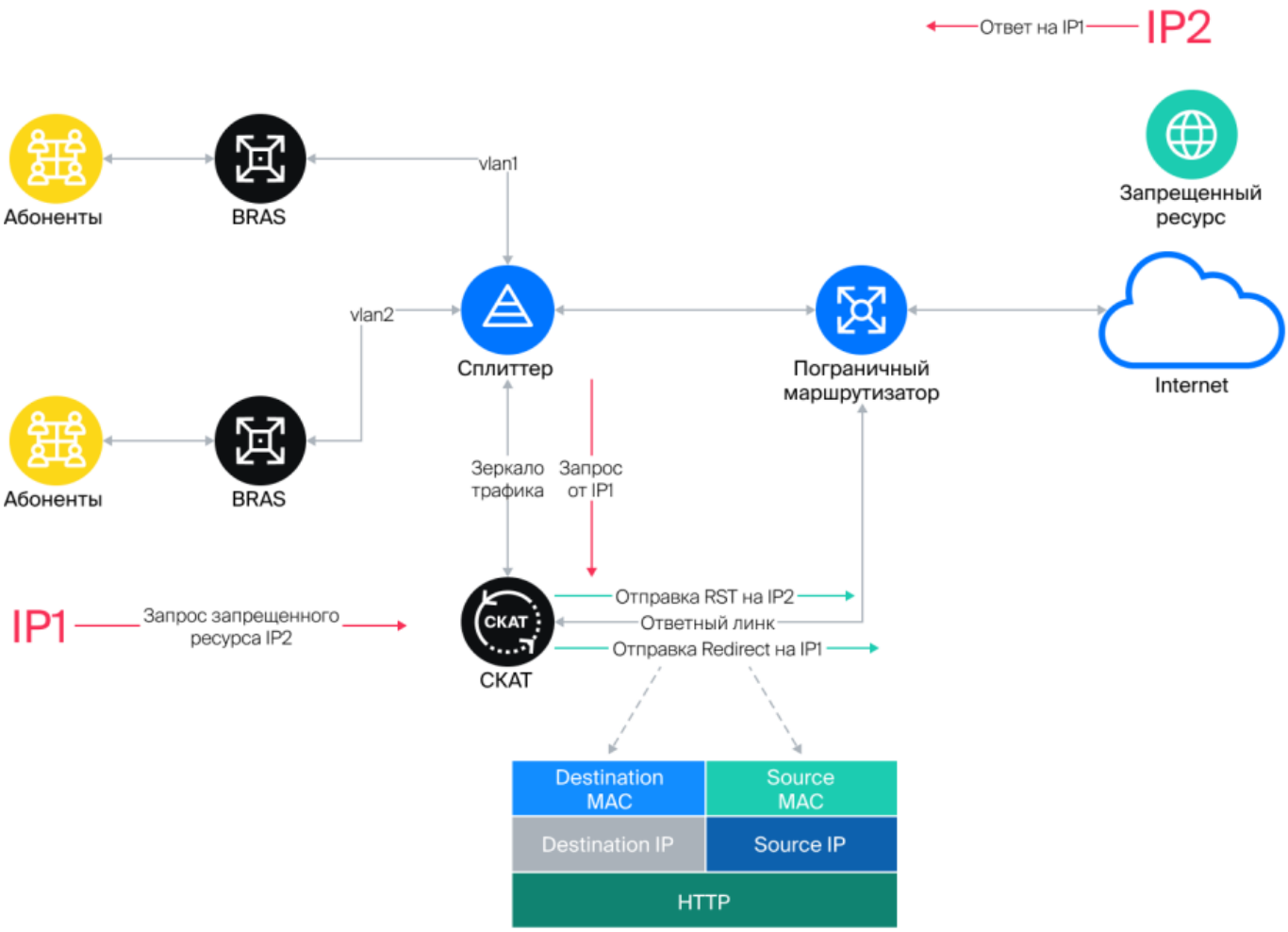
Прописать смену MAC:

```
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
```

Установить количество повторов, если есть потери в сети:

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

Схема реализации и описание работы



При обнаружении запроса на запрещенный ресурс CKAT отправляет в сторону абонента (IP1) HTTP Redirect для переадресации запроса на страницу-заглушку. В сторону запрещенного ресурса (IP2) направляется пакет TCP RST, который сбрасывает соединение. Блокировка (HTTPS) и переадресация (HTTP) происходит, так как CKAT отвечает на запрос от IP1 быстрее чем IP2.

Заголовок ответного IP 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.

Пример настройки маршрутизатора

Порт на маршрутизаторе, куда включен ответный линк от СКАТ, должен быть сконфигурирован как обычный L3 порт. Задача принять пакет от СКАТ 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;
  }
}
```

Сбор статистики

```
http_parse_reply=1

netflow=8
netflow_full_collector_type=2
netflow_dev=eth3
netflow_timeout=20
netflow_full_collector=172.18.254.124:1500
netflow_rate_limit=30
netflow_passive_timeout=40
netflow_active_timeout=120

#URL upload
ipfix_dev=eth3
ipfix_tcp_collectors=172.18.254.124:1501
ipfix_observation=127

#SIP
ipfix_meta_tcp_collectors=172.18.254.124:1511
rlimit_fsize=32000000000
```

Дальнейшие настройки производятся в зависимости от того, какие компонеты планируется использовать и расписаны в разделе 3 в соответствующих компонентах.