## Содержание

Описание и настройка	3
Схемы работы	3
Рекомендуемая схема: Прием трафика RADIUS Accounting на выделенный Linux-	
интерфейс не связанный с FastDPI	3
Минимальная Настройка FastRADIUS	4
Альтернативная схема: Отвод трафика RADIUS Accounting с DPDK-интерфейсов	
FastDPI	5
Настройка ТАР интерфейсов	5
Настройка отведения трафика из FastDPI в FastRADIUS	
Дополнительные Настройки Radius Monitor	
Подлючение NAT на основе CIDR	7
Поддержка IPv6	8
Идентификация абонентов в мобильных сетях	8
Дополнение имен абонентов (LOGIN) префиксами регионов	

# Описание и настройка

FastRADIUS (Монитор событий RADIUS) предназначен для создания в DPI связки IP-LOGIN в сетях с динамической выдачей IP-адресов на основании RADIUS Accounting (Mapping IP-LOGIN). FastRADIUS поддерживает в FastDPI следующие команды:

1. Поддержка абонентов с одиночным IPv4 адресом и IPv6 подсетью Связывание IP-адреса с LOGIN:

```
fdpi_ctrl load --bind --user user_name:ip_aдpec
```

Удаление связки IP ↔ login:

```
fdpi_ctrl del --bind --login user_name
```

2. Поддержка абонентов с несколькими IP

Связывание IP-адреса или блока IP-адресов с LOGIN:

```
fdpi ctrl load --bind multi --user user name:ip адрес или блок
```

Удаление одного из IP, связанных с LOGIN:

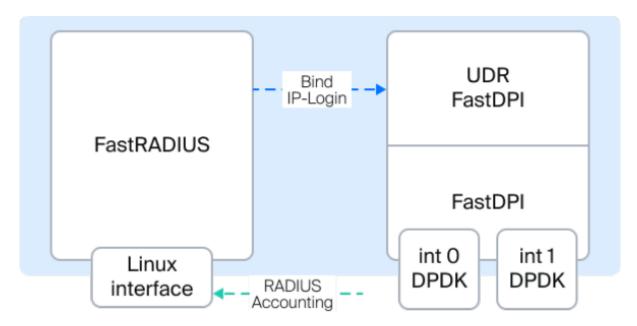
```
fdpi_ctrl del --bind_multi --ip ip_адрес
```

Также возможно назначение CG-NAT (11 услуги) по заданным параметрам.

# Схемы работы

# Рекомендуемая схема: Прием трафика RADIUS Accounting на выделенный Linux-интерфейс не связанный с FastDPI

RADIUS Accounting передается на FastRADIUS на стандартный Linux-интерфейс, указанный в конфигурационном файле (in\_dev), путем зеркалирования существующего RADIUS трафика, либо с использованием RADIUS proxy (например FreeRADIUS). В данном случае FastRADIUS только принимает зеркало и никак не отвечает RADIUS серверу. Работа со стандартными интерфейсами Linux осуществляется с помощью libpcap.



#### Минимальная Hacтройка FastRADIUS

Настройки находятся в файле /etc/dpi/fdpi radius.conf.

Для применения конфигурации необходимо перезапустить сервис:

#### systemctl restart fastradius

- in\_dev=eth0 имя прослушиваемого Linux-интерфейса
- rad\_acct\_port=1813,1814,1815 номер прослушиваемого порта (или список портов через запятую) с пакетами Radius Accounting
- save\_pdu\_proto=0 сохранять в рсар формате PDU для анализа. Задается битовой маской:
  - ∘ 0x00 ничего не писать
  - ∘ 0x01 битые/не разобранные RADIUS пакеты
  - ∘ 0x02 все RADIUS пакеты
  - ∘ 0x04 битые/не разобранные DIAMETER пакеты
  - ∘ 0x08 BCE DIAMETER
  - ∘ 0x10 битые TACACS+ пакеты
  - ∘ 0x20 все TACACS+ пакеты
- rad\_check\_code\_pdu=2:4 анализировать PDU с кодом 2 и 4
- rad check acct status type=1:3 анализировать PDU со статусом 1 и 3
- mem\_preset=1 инициализировать память при старте
- fdpi\_servers=127.0.0.1:29000,123.45.67.85:29000 список DPI серверов, на которые отправлять данные, где 29000 управляющий порт по умолчанию

#### Настройка обработки потоков



Рекомендуется использовать приведенные значения

- num threads=1
- rx bind core=0

- services bind cores=0
- engine bind cores=0
- fifo bind cores=0
- snaplen=2000
- timeout alarm=5
- dbg\_log\_mask=0x31

#### Настройка экпорта RADIUS-событий на внешний коллектор

- ipfix\_dev=eno8 имя Linux-интерфейса, с которого идет отправка IPFIX. Форматы шаблона выгрузки IPFIX из FastRADIUS
- ipfix tcp collectors=172.32.0.239:1502 адрес IPFIX коллектора

# Альтернативная схема: Отвод трафика RADIUS Accounting с DPDK-интерфейсов FastDPI

RADIUS Accounting необходимо подать в порты устройства DPI вместе с сетевым трафиком. Реализовать это возможно через зеркалирование портов, к которым подключен RADIUS сервер. В данном случае FastRADIUS только принимает зеркало и никак не отвечает RADIUS серверу.

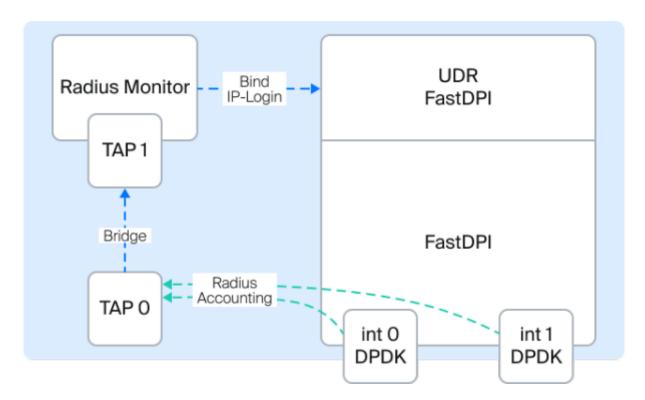
#### Настройка ТАР интерфейсов

FastRADIUS может быть запущен на том же сервере, что и FastDPI или вынесен на внешний сервер. Для выделения нужного трафика используются два виртуальных интерфейса TAP0 и TAP1.

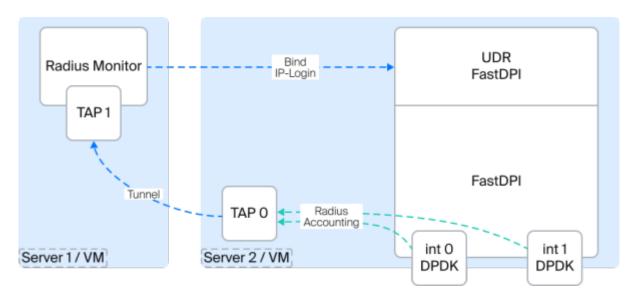
В конфигурации необходимо указать порт:

in dev=tap1

Размещение Radius монитор на том же сервере. Используется Bridge:



#### Размещение Radius монитор на внешнем сервере. Используется Tunnel:



- ТАРО используется для отведения трафика
- TAP1 слушает Radius Monitor
- Между TAP0 и TAP1 создается Bridge или Tunnel для передачи трафика.
- На интерфейсе TAPO отключается mac learning

#### Из консоли выполнить следующие команды:

```
ip tuntap add tap0 mode tap
ip tuntap add tap1 mode tap

ip link set dev tap0 up
ip link set dev tap1 up

ip link add br0 type bridge
```

```
ip link set tap0 master br0
bridge link set dev tap0 learning off
ip link set tap1 master br0

ifconfig tap0 192.168.4.20 up
ifconfig tap1 192.168.4.21 up
ifconfig br0 up
```



ВНИМАНИЕ: ТАР интерфейсы необходимо стартовать после перезагрузки сервера!

#### Настройка отведения трафика из FastDPI в FastRADIUS

Подключить на FastDPI услугу отведения трафика:

```
fdpi_ctrl load profile --service 14 --profile.name radius --profile.json '{
"typedev" : "tap","dev" : "tap0","udp" : [ 1813,1814,1815 ] }' --
outformat=json
fdpi_ctrl load --service 14 --profile.name radius --ip 10.16.252.11
fdpi_ctrl load --service 14 --profile.name radius --ip 10.16.252.12
```

#### где:

- 1813, 1814, 1815 порты, на которых передается RADIUS Accounting
- 10.16.252.11, 10.16.252.12 IP-адреса RADIUS серверов, с которых идет RADIUS Accounting

## Дополнительные Hacтройки Radius Monitor

- rad\_auth\_port=1645 номер прослушиваемого порта (или список портов через запятую) с пакетами RADIUS Authentication
- bind\_multi=true разрешить несколько IP на одном USER-NAME смотри команду load --bind multi



Если порядок bind/unbind в RADIUS-потоке не соблюдается или есть потери пакетов (например, если это зеркало), то вероятны артефакты.

#### Подлючение NAT на основе CIDR

Создание на FastDPI именованных профилей NAT:

```
fdpi_ctrl load profile --service 11 --profile.name nat_profile_all --
profile.json '{ "nat_ip_pool" : "5.200.43.0/24,5.200.44/25",
```

```
"nat_tcp_max_sessions" : 2000, "nat_udp_max_sessions" : 2000 }'
```

В конфигурационном файле FastRADIUS /etc/dpi/fdpi\_radius.nat указываются диапазоны адресов и соотвествующие им имена профилей NAT пример:

```
0.0.0.0/0 nat_profile_all
10.0.0.0/8 nat_profile_1
10.1.1.0/24 nat_profile_2
```

Когда указан более специфичный (конкретный) профиль для адреса, то выбирается он.

## Поддержка IPv6

В конфигурационном файле /etc/dpi/fdpi\_radius.conf указываются настроечные параметры связки адреса и подсетей с абонентом:

- bind ipv6 address
  - 0 не связывать адрес с абонентом (по умолчанию)
  - $\circ$  1 связывать

Связывание аналогично команде bind в fdpi\_ctrl). Адрес берется из RADIUSатрибута Framed-IPv6-Address(168)

- bind\_ipv6\_subnet
  - ∘ 0 не связывать (по умолчанию)
  - ∘ 64 связывать только для подсетей /64
  - ∘ -1 связывать для любых подсетей.
    Подсеть берется из RADIUS-атрибута Delegated-IPv6-Prefix(123)

Абонент идентифицируется RADIUS-атрибутом User-Name или Calling-Station-ID (в зависимости от настройки login replace)



В текущей реализации поддерживаются только IPv6 подсети фиксированной длины (по умолчанию /64), поэтому связывание подсетей меньшей длины приведет к ошибке.

## Идентификация абонентов в мобильных сетях

- login\_replace=1 в этом случае для идентификации абонента используется RADIUSатрибут Calling-Station-ID (IMSI) вместо User-Name, если он присутствует в RADIUS.
- ipfix\_extra\_gsm=1 включить поддержку отправки по IPFIX дополнительных атрибутов из RADIUS Accounting.

### Дополнение имен абонентов (LOGIN) префиксами регионов

Используется когда RADIUS монитор и CKAT обслуживают несколько регионов, а user-name

может в разных регионах пересекаться с другими регионами, таким образом их можно развести по разным login

- 1. Включить настройку rad\_prefix\_info=1
- 2. В файл /etc/dpi/prefixes.info добавить:

```
172.17.76.1 MSK-
172.17.76.2 MSK-
172.17.76.3 SPB-
172.17.76.4 SPB-
172.17.76.5 SPB-
```

#### где:

- первое поле NAS-IP-Address из RADIUS-пакета
- второе поле префикс, который будет добавлен к Login