

Содержание

Описание	3
Минимальные требования к оборудованию	3
Установка и обновление	3
Установка на отдельный сервер или VM	4
Схемы работы	4
Рекомендуемая схема: Прием трафика RADIUS Accounting на выделенный Linux-интерфейс не связанный с FastDPI	4
Администрирование FastRADIUS	4
Минимальная Настройка FastRADIUS	5
Альтернативная схема: Отвод трафика RADIUS Accounting с DPDK-интерфейсов FastDPI	6
Настройка TAP интерфейсов	6
Настройка отведения трафика из FastDPI в FastRADIUS	8
Дополнительные Настройки Radius Monitor	8
Подключение NAT на основе CIDR	8
Поддержка IPv6	9
Идентификация абонентов в мобильных сетях	9
Дополнение имен абонентов (LOGIN) префиксами регионов	9

Описание

FastRADIUS (Монитор событий RADIUS) предназначен для создания в DPI связки IP-login в сетях с динамической выдачей IP-адресов на основании RADIUS Accounting.

[Поддержка абонентов со связыванием одиночного IPv4 адреса и IPv6 подсети или динамической выдачей адресов](#)

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

и удаление связки IP ↔ login:

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

[Поддержка абонентов с несколькими IP](#)

```
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
```

Так же возможно назначение CGNAT (11 услуги) по заданным параметрам.

Минимальные требования к оборудованию

FastRADIUS может быть установлен на сервер СКАТ или на выделенный сервер или VM.

1. Процессор (CPU) — 2 ядра
2. Оперативная память (RAM) — от 1 ГБ
3. SSD — 50 ГБ
4. Операционная система — [VEOS](#)
5. Сетевая плата (NIC) — 2 порта, для управления по SSH (+ отправка IPFIX опционально) и для приема RADIUS трафика

Установка и обновление

Компонент поставляется в стандартном пакете ПО СКАТ. При использовании на том же сервере что и СКАТ дополнительная установка не требуется.

Дальнейшее обновление осуществляется стандартным образом:

```
yum update fastradius
```

Установка на отдельный сервер или VM

1. Необходимо настроить синхронизацию точного времени через сервис ntpd. Файл конфигурации ntpd: `/etc/sysconfig/ntp`. Для этого Установите службу точного времени

```
yum install chrony -y
systemctl restart chronyd
timedatectl
```



При вводе команды `timedatectl`, у параметра `System clock synchronized` должно быть значение `yes`

2. Подключите репозиторий `vasexperts`

```
rpm --import http://vasexperts.ru/centos/RPM-GPG-KEY-vasexperts.ru
rpm -Uvh
http://vasexperts.ru/centos/6/x86_64/vasexperts-repo-2-1.noarch.rpm
```

3. Установите `FastRADIUS`

```
yum install fastradius
```

4. Проверьте что сервис запускается

```
service fastradius start
```

5. Включите автозапуск сервиса при старте компьютера

```
systemctl enable fastradius
```

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`.

Администрирование FastRADIUS

Основной процесс называется `fdpi_radius` - установлен в системе как сервис и управляется

стандартными для сервиса командами. Перезапуск сервиса:

```
systemctl fastradius restart
```

Настройки FastRADIUS находятся в каталоге */etc/dpi*:

<code>fdpi_radius.conf</code>	конфигурационный файл
<code>prefixes.info</code>	настройки регионов (префиксы для login абонентов), файл отсутствует если не нужен

Параметры в настроечном файле бывают "горячие" и "холодные":

Горячие параметры можно менять в процессе работы "на лету", т.е. без перезапуска сервиса.

Холодные параметры вступят в силу только после перезапуска сервиса.

Обновление горячих настроек без перезапуска сервиса:

```
systemctl fastradius reload
```

Логи FastRADIUS находятся в каталоге */var/log/dpi*:

<code>fdr_alert.log</code>	лог информационных сообщения и ошибках
<code>fdr_stat.log</code>	лог статистической информации

Ротация логов осуществляется с помощью стандартного средства `logrotate`, по умолчанию логи хранятся в течение суток. Конфигурационный файл `logrotate`: */etc/logrotate.d/fdpi_radius*

При изменении администратором сроков хранения необходимо проследить, чтобы на диске оставалось достаточно места.

За работой процесса следит системный `watchdog`, который перезапустит его в случае падения. Конфигурационный файл `watchdog`: */etc/watchdog.d/wd_radius.sh*

В зависимости от настроек FastRADIUS может записывать в каталог */var/dump/dpi* следующую информацию

<code>spdu_*.pcap</code>	- pcap файлы с записью плохих или всех RADIUS пакетов
<code>uip_*.txt</code>	- текстовые логи с информацией о выделении и освобождении IP адресов

В этом случае необходимо самостоятельно предусмотреть очистку этой информации для предотвращения переполнения диска.

Минимальная Настройка 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 pcap 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 - все 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 экспорта RADIUS-событий на внешний коллектор:

ipfix_dev=enp8 - имя Linux-интерфейса, с которого идет отправка IPFIX

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.

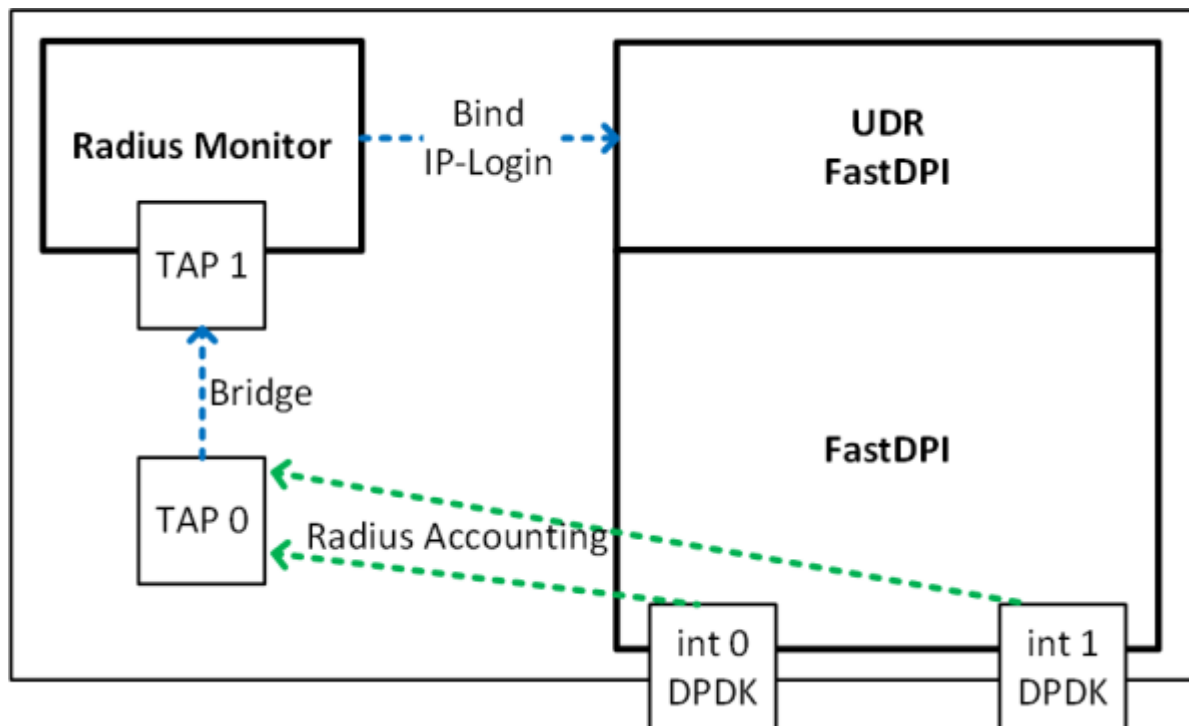
Реализовать это возможно через зеркалирование портов, к которым подключен RADIUS сервер.

В данном случае FastRADIUS только принимает зеркало и никак не отвечает RADIUS серверу.

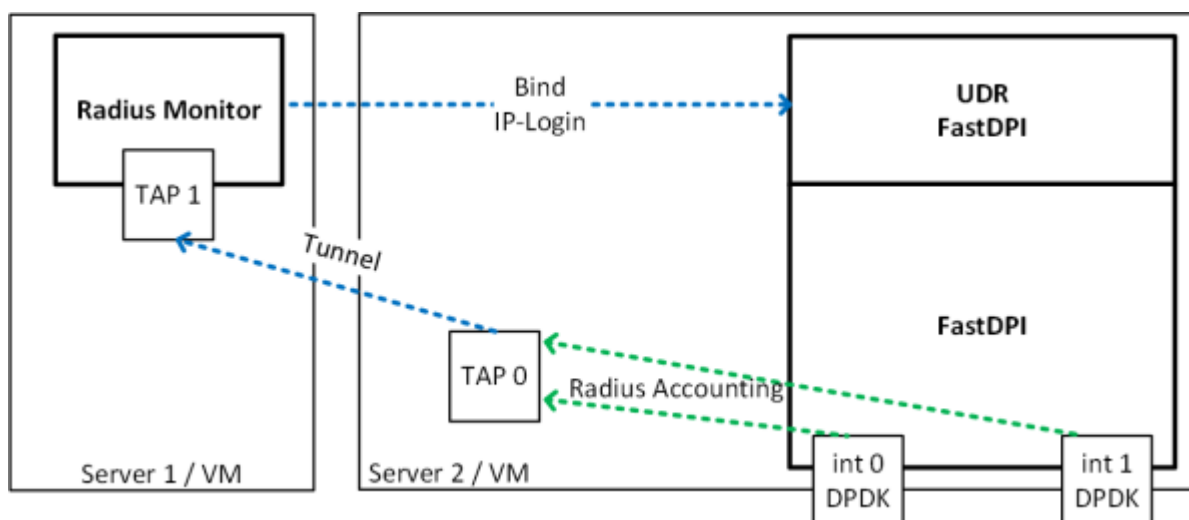
Настройка TAP интерфейсов

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
```



Размещения Radius монитор на том же сервере. Используется Bridge.



Размещения Radius монитор на внешнем сервере. Используется Tunnel.

- TAP0 - используется для отведения трафика
- TAP1 - слушает Radius Monitor
- Между TAP0 и TAP1 создается Bridge или Tunnel для передачи трафика.
- На интерфейсе TAP0 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 Настройки 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, предупреждение: если порядок bind/unbind в радиус потоке не соблюдается или есть потери пакетов (например это зеркало), то вероятны артефакты

Подключение NAT на основе CIDR

Создаем на FastDPI именованные [профили 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 соответствующие 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

```
bind_ipv6_address=0 (по умолчанию - не связывать адрес с абонентом), 1 связывать
(связывание аналогично команде bind в fdpi_ctrl). Адрес берется из атрибута радиус
Framed-IPv6-Address(168)
bind_ipv6_subnet=0 (по умолчанию - не связывать), 64 (связывать только для подсетей
/64), -1 связывать для любых подсетей. Подсеть берется из атрибута радиус Delegated-
IPv6-Prefix(123)
```

Абонент идентифицируется радиус 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 RADIUS атрибут 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 СКАТ обслуживают несколько регионов, а user-name может в разных регионах пересекаться с другими регионами, таким образом их можно развести по разным login

1. Включаем 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 - это NAS-IP-Address из RADIUS пакета

второе поле - какой префикс будет добавлен к Login