Содержание

Пример BRAS L2 DHCP Radius Proxy

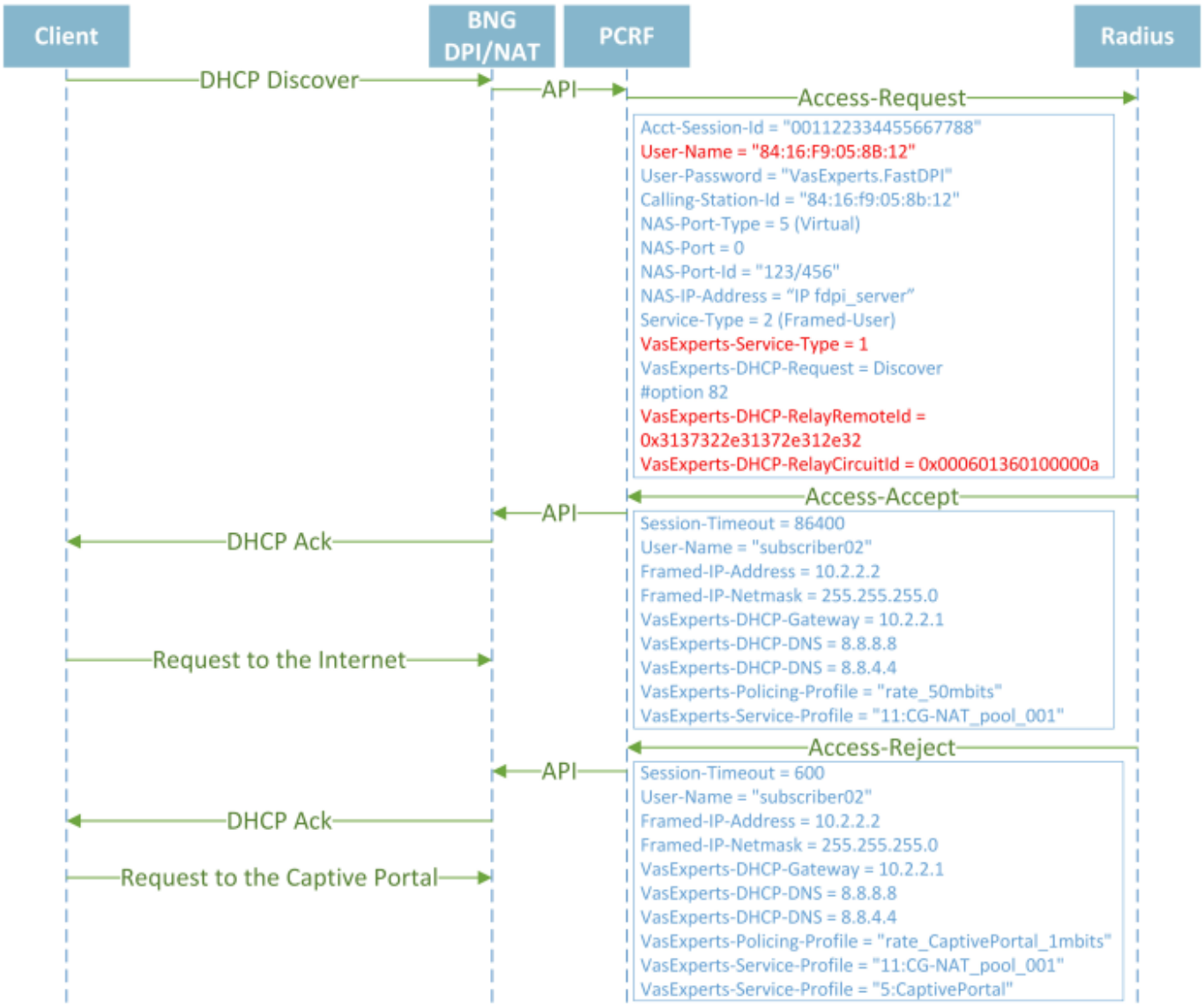
Описание схемы

BRAS DHCP L2 означает, что абонент получает IP-адрес через DHCP Proxy и проходит AAA в Биллинге. Дальше терминируется СКАТом и попадает на бордер.

Для организации работы СКАТ в режиме BRAS L2 DHCP Radius Proxy участвуют следующие элементы:

1. Клиент с типом доступа Q-in-Q
2. FastDPI - обработка трафика и применение политик
3. FastPCRF - проксирование запросов между fastDPI и Radius
4. Radius сервер - принимает запросы от fastPCRF и формирует ответы с заданными атрибутами
5. Router - отвечает за передачу пакетов в интернет и обратный маршрут, на текущий момент необходимо прописывать Static Route, т.к. в СКАТ нет поддержки OSPF и BGP

Сценарий



По DHCP запросу - В этом случае, когда BRAS фиксирует DHCP запросы со стороны абонентской сети, то формирует соответствующие Radius запросы для получения параметров DHCP-аренды которые сообщаются абоненту. Кроме того, в ответе на DHCP-аутентификацию можно, также, передать параметры сессии влияющие на прохождение трафика абонента. При передачи параметра Session-Timeout является значением временем аренды адреса (lease time). При раздельном получении параметров DHCP и трафика (IP) можно указывать различные значения Session-Timeout, что разумеется будет довольно удобно, так например выдать время аренды 6 часов, но при этом проводить реавторизацию параметров трафика каждый час. Идентификатором оборудования абонента является - MAC-адрес, номер VLAN или значения полей Option-82.

Настройка FastDPI

1. Редактирование файла конфигурации DPI

Сперва необходимо раскомментировать (добавить) следующие строчки в файл конфигурации */etc/dpi/fastdpi.conf* .

```
#включение внутренней базы данных свойств пользователей
udr=1
```

```
#активирует режим L2 BRAS
bras_enable=1
enable_auth=1

#"виртуальный" IP адрес DPI (должен быть уникальным в сети)
bras_arp_ip=192.168.1.2
#"виртуальный" MAC адрес DPI (следует использовать реальный MAC адрес любого из DNA интерфейсов)
bras_arp_mac=a0:36:9f:77:26:58

#IP адрес бордера
bras_gateway_ip=192.168.1.1
#MAC адрес интерфейса, в который подключен DPI, на бордере
bras_gateway_mac=c4:71:54:4b:e7:8a

#данные сервера, где установлен Fastpcrf (если на том же, где и Fastdpi, не изменять)
auth_servers=127.0.0.1%lo:29002

#включение режима DHCP Radius Proxy
bras_dhcp_mode=2

#терминация vlan (в данном случае тег будет вырезан)
bras_vlan_terminate=1
#подмена MAC адресов
bras_terminate_l2=1
#терминация трафика только для AS, помеченных как term (полезно, если через СКАТ также проходит трафик, который не нужно терминировать)
bras_term_by_as=1
#замыкание локального трафика
bras_terminate_local=1

#включение accounting
enable_acct=1
#статистика по биллингу абонента
netflow=4
#тайм-аут отправки статистики
netflow_timeout=60
```

Следует выставить **свои** значения для следующих параметров

- bras_arp_ip
- bras_arp_mac
- bras_gateway_ip
- bras_gateway_mac

Указание AS для терминирования

Следующим шагом следует пометить, для трафика из каких AS необходимо проводить терминацию трафика.

Список AS готовится в текстовом формате, каждая запись с новой строки в формате CIDR<пробел>номер_AS:

```
192.168.2.0/24 65550
```

Потом он преобразуется во внутренний формат утилитой as2bin и размещается в файле */etc/dpi/aslocal.bin* , где его подхватит DPI. Указанные в списке диапазоны адресов добавятся к глобальному списку.

```
cat aslocal.txt | as2bin /etc/dpi/aslocal.bin
```

Список локальных AS для терминирования подготавливается в текстовом файле в формате номер_AS<пробел>флаг:

```
65550 local
65550 term
```

Конвертирование во внутренний формат и размещение в рабочем каталоге, где настройки будут подхвачены DPI:

```
cat my_as_dscp.txt | as2dscp /etc/dpi/asnum.dscp
```

Настройка FastPCRF

Необходимо настроить FastPCRF. Для этого редактируем файл */etc/dpi/fastpcrf.conf* . Находим строчку с параметрами RADIUS сервера и изменяем

```
     #secret123 - Radius секрет
     #192.168.1.10 - IP адрес Radius сервера
     #eth0 - интерфейс, **с которого** FastPCRF "общается" с Radius сервером
   #1812 - порт, на который FastPCRF отправляет запросы авторизации
     #acct_port - порт, на который FastPCRF отправляет Accounting
radius_server=secret123@192.168.1.10%eth0:1812;acct_port=1813
```

Настройка Radius

Настройка приводится в качестве **примера** на freeRADIUS 3 и может отличаться от конфигурации Вашего Radius сервера.

Словарь VasExperts

Сперва необходимо добавить VSA словарь

- копируем словарь /usr/share/dpi/dictionary.vasexperts из дистрибутива fastpcrf в каталог $freeRadius/share/freeradius
- Добавляем в главный словарь $freeRadius/share/freeradius/dictionary строку:

```
$INCLUDE dictionary.vasexperts
```

Создание Radius клиента

Добавляем в raddb/clients.conf Radius-сервера следующие строки

```
client fastdpi1 {
    ipaddr        = 192.168.1.5
    secret        = secret123
    require_message_authenticator = yes
#   add_cui = yes
    virtual_server    = fastdpi-vs
}
```

Создание виртуального сервера

Для создания конфигурации виртуального сервера копируем файл raddb/sites-available/default, входящий в поставку FreeRadius, в raddb/sites-enabled/fastdpi-vs и затем редактируем fastdpi-vs:

- задаем имя виртуального сервера - меняем в начале файла строку server default на server fastdpi-vs
- в секции listen для auth-запросов (type = auth) прописываем, на каком IP-адресе и каком порту слушать входящие запросы (заметим, это локальный адрес Radius-сервера):

```
ipaddr = 192.168.1.10
port = 1812
interface = eth0
```

Создание учетной записи для авторизации

Добавляем в файл */etc/raddb/users* данные по абоненту (следует учесть, что FastPCRF по умолчанию в данном режиме использует в качестве логина MAC адрес источника, а в качестве пароля - VasExperts.FastDPI)

```
08:00:27:e5:9e:15      User-Password := "VasExperts.FastDPI"
       VasExperts-UserName = "L2DHCP",
       Framed-IP-Netmask = 255.255.255.0,
       VasExperts-DHCP-Gateway = 192.168.2.1,
       VasExperts-DHCP-DNS = 8.8.8.8,
```

```
       VasExperts-Policing-Profile = "100Mbps",
       VasExperts-Enable-Service = "9:on"
```

В файл */etc/raddb/users* также следует добавить две записи для FastPCRF

```
VasExperts.FastDPI.unknownUser Cleartext-Password := "VasExperts.FastDPI"
DEFAULT Cleartext-Password := "VasExperts.FastDPI"
```

Настройка Маршрутизатора

На маршрутизаторе добавляем статический маршрут в подсеть, которую обслуживает СКАТ.

```
/ip route add dst-address=192.168.2.0/24 gateway=192.168.1.2
```

Подключение тестового абонента

При подключении неизвестного абонента FastPCRF шлет Access-Request со следующим содержанием:

```
User-Name = "A0:36:9F:77:26:58"
User-Password = "VasExperts.DPI"
Calling-Station-Id = "a0:36:9f:77:26:58"
NAS-Port-Type = 5
NAS-Port = 100
NAS-Identifier = "VasExperts.FastDPI"
Service-Type = 2
VasExperts-Service-Type =1
VasExperts-DHCP-Request = Discover
VasExperts-DHCP-RelayRemoteId = 0x3137322e31372e312e32
VasExperts-DHCP-RelayCurcuitId = 0x000601360100000a
```

По умолчанию FastPCRF в поле User-Name помещает MAC адрес абонента. В кофигурационном файле FastPCRF возможно указать, что следует использовать в качестве логина (например QinQ тэг)

При успешной авторизации данного абонента FastPCRF помимо сетевых параметров также ожидает получить список необходимых услуг и тарифный для данного абонента в Access-Accept

```
Session-Timeout = 84600
User-Name = "Subscriber001"
Framed-IP-Address = 10.0.0.10
Framed-IP-Netmask = 255.255.255.0
VasExperts-DHCP-Gateway = 10.0.0.1
VasExperts-DHCP-DNS = 8.8.8.8
```

```
VasExperts-DHCP-DNS = 8.8.4.4
VasExperts-Policing-Profile = "100Mbps"
VasExperts-Service-Profile = "11:CG_NAT_POOL_1"
VasExperts-Service-Enable = "9:on"
```

Диагностика

При внедрении L2 BRAS могут возникать различные ошибки, при которых абоненты не могут быть авторизованы и, соответственно, остаться без доступа к интернету. Ниже приведены Самые распространенные проблемы:

Нет запросов на авторизацию.

Проверить, запущен ли процесс fastpcrf. Корректно ли указан адрес Radius сервера.

Не доходят запросы на авторизацию до Radius сервера.

Проверить, разрешен ли в Firewall’е порт для приема запросов на авторизацию (по-умолчанию 1812) на Radius сервере.

Пингуется DPI, но до бордера пинг не доходит.

1. Необходимо прописать статичный маршрут в сторону абонентов на бордере. Так как CKAT, пока не умеет анонсировать абонентские подсети, которые обслуживает, соответственно, необходимо указать бордеру, куда маршрутизировать трафик.
2. В случае использования NAT для абонентов необходим аналогичный маршрут для подсетей, используемых в NAT.
3. Корректно ли заданы параметры **bras_gateway_ip** и **bras_gateway_mac**

Не отправляется статистика для Accounting.

1. Проверить, разрешен ли в Firewall’е порт для приема статистики (по-умолчанию 1813) на Radius сервере.
2. Проверить, подключается ли для абонента услуга 9.
3. Проверить, включен ли accounting в настройках конфигурации DPI.
4. Проверить, корректное ли значение указано для параметра netflow.

Не доходят CoA до BRAS.

Проверить, разрешен ли в Firewall’е порт для приема CoA (по-умолчанию 3799) на сервере с FastPCRF.