Содержание

8 BRAS L2 DHCP Radius Proxy Example

Description

BRAS DHCP L2 mode means that the subscriber recieves an IP-address via DHCP Proxy and proceeds to AAA in the Billing system. Then the subscriber is terminated by VAS Experts DPI and transferred to border equipment.

The following elements are involved in the VAS Experts DPI operation scheme in BRAS L2 DHCP Radius Proxy mode:

1. Client with Q-in-Q access type
2. FastDPI - traffic processing and policing
3. FastPCRF - proxying requests between fastDPI and Radius
4. Radius server - accepts requests from fastPCRF and generates responses with specified attributes
5. Router - is responsible for packets transmission to the Internet and the backward routing. It is necessary to specify the Static Route, since VAS Experts DPI does not support OSPF and BGP at the moment.

Scenario

FastDPI Setup

Editing the DPI Configuration File

First, you need to uncomment (add) the following lines to the /etc/dpi/fastdpi.conf configuration file.

```
# enable internal database of user properties
udr=1
# activates L2 BRAS mode
bras_enable=1
enable_auth=1

# DPI "virtual" IP address (must be unique on the network)
bras_arp_ip=192.168.1.2
# "virtual" DPI MAC address (you should use the real MAC address of any of
the DNA interfaces)
bras_arp_mac=a0:36:9f:77:26:58

#border IP-address
bras_gateway_ip=192.168.1.1
#MAC address of the border’s interface to which DPI is connected
```

```
bras_gateway_mac=c4: 71: 54: 4b: e7: 8a

# server data where Fastpcrf is installed (if the same server, do not
change)
auth_servers=127.0.0.1% lo: 29002

# enable DHCP Radius Proxy mode
bras_dhcp_mode=2

# vlan termination (this value means tag will be removed)
bras_vlan_terminate=1
# MAC-addresses replacement
bras_terminate_l2=1
# traffic termination only for AS, marked as "term" (useful if traffic that
does not need to be terminated also passes through DPI)
bras_term_by_as=1
# local traffic interconnection
bras_terminate_local=1

# enable accounting
enable_acct=1
# subscriber billing statistics
netflow=4
# timeout for sending statistics
netflow_timeout=60
```

You should set **your own** values for the following parameters

- bras_arp_ip
- bras_arp_mac
- bras_gateway_ip
- bras_gateway_mac

AS Specification for Termination

The next step is to mark the AS traffic that has to be terminated.

The AS list is prepared in text format, each entry on a new line in the format CIDR<space>AS_number:

```
192.168.2.0/24 65550
```

Then it is converted into an internal format by the as2bin utility and placed in the file */etc/dpi/aslocal.bin*, where DPI will pick it up. The address ranges specified in the list will be added to the global list.

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

The list of local AS to be terminated is prepared in a text file in the format AS_number<space>flag:

```
65550 local
65550 term
```

To convert into internal format and place into the main directory, where the DPI will pick the settings up:

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

FastPCRF Setup

To configure FastPCRF, edit the file */etc/dpi/fastpcrf.conf*. Find the line with the RADIUS server parameters and change

```
     #secret123 - Radius secret
     #192.168.1.10 - IP address of Radius server
     #eth0 - the interface from which FastPCRF communicates with the Radius
server
     #1812 - the port to which FastPCRF sends authorization requests
     #acct_port - the port that FasPCRF sends Accouting to
radius_server=secret123@192.168.1.10%eth0:1812;acct_port=1813
```

Radius Setup

The setup is given as **an example** on freeRADIUS 3 and may differ from the configuration of your Radius server.

VasExperts Dictionary

First you need to add a VSA dictionary

- Copy the dictionary /usr/share/dpi/dictionary.vasexperts from the fastpcrf distribution into $freeRadius/share/freeradius directory
- Add the following line to the main dictionary $freeRadius/share/freeradius/dictionary:

```
$INCLUDE dictionary.vasexperts
```

Creating Radius Client

Add the following lines to raddb/clients.conf of the Radius server

```
client fastdpi1 {
    ipaddr        = 192.168.1.5
```

```
    secret        = secret123
    require_message_authenticator = yes
#   add_cui = yes
    virtual_server    = fastdpi-vs
}
```

Creating a virtual server

To create a virtual server configuration, copy the included in the FreeRadius file raddb/sites-available/default, to raddb/sites-enabled/fastdpi-vs. Then edit fastdpi-vs:

- set the name of the virtual server - change the 'server default' line at the beginning of the file to 'server fastdpi-vs'
- in the 'listen' section for auth requests (type = auth), set IP-addresses and ports that will listen to the incoming requests (note that this is the local address of the Radius server):

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

Creating an account for authorization

Add subscriber data to the file */etc/raddb/users*

```
testuser        Cleartext-Password := "VasExperts.FastDPI"
        Framed-IP-Address = 192.168.2.199,
        VasExperts-DHCP-DNS = 8.8.8.8,
        VasExperts-Enable-Service = "9:on",
    VasExperts-Policing-Profile = "100Mbps"
    VasExperts-Service-Profile = "11:user_nat"
```

Two more lines for FastPCRF should also be added to the file */etc/raddb/users*

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

Router Setup

On the router, add a static route to the subnet served by the VAS Experts DPI.

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

Connecting a Test Subscriber

When an unknown subscriber is connected, FastPCRF sends an Access-Request with the following

content:

```
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
```

By default FastPCRF puts the subscriber's MAC address in the User-Name field. In the FastPCRF configuration file it is possible to specify what should be used as a login (for example, QinQ tag)

При успешной авторизации данного абонента FastPCRF помимо сетевых параметров также ожидает получить список необходимых услуг и тарифный для данного абонента в Access-Accept When the subscriber is authorized successfully, FastPCRF expects to receive a list of necessary services and a tariff for this subscriber in Access-Accept in addition to other network parameters.

```
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"
```

Troubleshooting

When implementing L2 BRAS, some errors may occur, when the subscribers cannot be authorized and connected to the Internet. Below are the most common problems:

There are no authorization requests

Check if fastPCRF process is running and if the server Radius address is specified correctly.

Authorization requests do not reach the Radius server

Check if the Firewall's port is allowed to receive authorization requests (by default 1812) on the Radius server.

I can ping DPI, but the ping does not reach the border

1. It is necessary to set a static route towards the subscribers on the border. Since DPI is not able to announce the subscriber subnets that it serves yet, it is necessary to indicate the border where to route the traffic.
2. In the case of using NAT for subscribers, a similar route is required for the subnets used in NAT.
3. Check if the parameters **bras_gateway_ip** and **bras_gateway_mac** are set correctly.

Statistics for Accounting is not sent

1. Check if the port for receiving statistics is allowed in the Firewall (by default 1813) on the Radius server.
2. Check if service 9 is activated for the subscriber.
3. Check if accounting is enabled in DPI configuration settings.
4. Check if the correct value is specified for the Netflow parameter.

CoA does not reach BRAS

Check if the port for receiving CoA (3799 by default) is allowed in the Firewall on the server with FastPCRF.