Содержание

12 BRAS related questions

Authorization is not working

 Please check if authorization is enabled in the fastdpi.conf settings

 Is there local subscribers traffic? Let us recall that authorization is performed only when a packet from a local subscriber is received.

 If fastDPI and fastPCRF are running on different servers, first of all check the firewall: whether the fastPCRF TCP port of fastDPI → fastPCRF connection (default 29002) can be accessed from the fastDPI server. Similarly, ensure it works the other way round, i.e. that the fastDPI TCP control port (29000 by default) can be accessed from the fastPCRF server.

 Check if there is a fastDPI → fastPCRF connection. If the connection suddenly broken, then the following message will be written to the fastdpi_ap0.log:

```
[INFO    ][2018/06/09-19:46:58:603824] auth_server::close_socket: client
socket fd=27 closed
```

When a connection is established, the following message will be written to the log file:

```
[INFO    ][2018/06/09-19:45:46:843710] auth_server::accept: accepted client
connection from 127.0.0.1:53498, fd=27, slot=1
```

 Check whether the connection to the Radius server is alive. If there are connection errors with the Radius server, the following messages in the fastdpi_ap2.log will indicate this situation:

```
[ERROR   ][2018/06/09-19:57:44:168053] rad_auth[0]::on_conn_error: fd=24,
port=54189: errno=111 'Connection refused'
[INFO    ][2018/06/09-19:57:44:168062] rad_auth[0]::close_connection: fd=24,
port=54189, reqs=1
```

Also the connection errors might be indicated by a lot of records about the resending requests to the Radius server.

When establishing connection to the Radius server, you will see something similar in the fastpcrf_ap2.log:

```
[INFO    ][2018/06/09-20:01:44:190499] rad_auth[0]::init_connection: new
connection to X.X.X.X%eth0:1812, fd=18, port=40510, connection count=1
```

Check your Radius server: whether the requests from the fastPCRF reach the Radius server (if not, the possible reason is that the firewall blocks the Radius UDP ports), and whether the Radius secret is specified properly.

radius_unknown_user (unknown_user) – is a string, the user login, if the real login is unknown to the fastdpi. Default value: `VasExperts.FastDPI.unknownUser`. This is the value of the Access-Request User-Name attribute in case the `radius_user_name_ip = 0` and the user login is unknown. It is assumed that the radius server will send in the Access-Accept response the real user login determined by its IP address being extracted from the Framed-IP-Address attribute and will send VasExperts.FastDPI.unknownUser; in the Wireshark you can see the "User-Name = ip", and in the logs:

```
[TRACE   ][2018/07/04-15:10:34:011126] auth_server::process: auth request:
user IP=10.12.0.146, login='<n/a>', vlan-count=0
```

Starting from VAS Experts DPI version 7.4 the following more recent parameter has been introduced: `radius_user_name_auth`, see the link Integration with the Radius server. Hence the IP appears in the User-Name, if you specify it as `radius_user_name_auth=login`, then when the login is not defined, the `VasExperts.FastDPI.unknownUser` will be used instead. This parameter should be used within the fastpcrf.conf file.

CoA requests are not accepted

Check the firewall: whether the client sending the CoA request is granted the access to the fastPCRF server via the CoA port (this is the UDP port)

Other matters

Please, consult me on issues relating to the manually authorization status management. Should the default_reject_whitelist be used if I set the following stuff manually:

```
fdpi_ctrl load --auth=0 --ip=192.168.10.1
```

?

No, it should not be used. You should either explicitly run the corresponding command on the Radius, or to activate the 5th service for the subscriber.