Содержание

Troubleshooting

Authorization does not work

Check if authorization in fastdpi.conf settings is enabled

Is there traffic for local subscribers? The authorization is carried out only when receiving a package from a local subscriber.

If fastDPI and fastPCRF are on different servers, first of all check the firewall: if the fastPCRF server has access to the fastDPI → fastPCRF TCP communication port (by default 29002) from the fastDPI server. Likewise, for feedback on the fastDPI server, access from fastPCRF to the TCP control port must be allowed (default 29000)

Check if there is a fastDPI → fastPCRF link. If the connection is suddenly cut off, then the following message is written to the log fastpcrf_ap0.log:

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

When establishing a connection, the following message is logged:

```
[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 if there is a connection with the Radius server. The following messages in fastpcrf_ap2.log indicate communication problems with the Radius server:

```
[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, problems can be signaled by many records of re-sending requests to the Radius server.

When connecting to the Radius server, you will see something similar in 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 requests from fastPCRF reach it (a possible reason - the

firewall is closed on Radius UDP ports), whether the Radius secret is specified

 radius_unknown_user (unknown_user) - string, username, if the real username is unknown fastdpi. Default value: 'VasExperts.FastDPI.unknownUser'. This is the value of the User-Name attribute of the Access-Request if radius_user_name_ip = 0 and the username is unknown. It is assumed that the radius-server in the Access-Accept response will report the true username of the user, determined by his IP-address taken from the Framed-IP-Address attribute and send VasExperts.FastDPI.unknownUser, in wiresharke I see User-Name = ip, 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 with SSG 7.4 such a parameter appeared, more recent: radius_user_name_auth, see the link Radius Server Integration. The IP appears in the User-Name here, if you set it as radius_user_name_auth = login, then in the absence of a login, VasExperts.FastDPI.unknownUser will be taken

this is the parameter for fastpcrf.conf

CoA requests are not accepted

 Check the firewall: whether the client sending the CoA request is open to the fastPCRF server on the CoA port (this is the UDP port)

Any other business

 check on Manual control of authorization status? if I set

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

by hand then default_reject_whitelist should be applied?

It should not. Either you need to give a command through the Radius, or directly activate the 5th service on the subscriber.