Содержание

7 Checklist for L3-Connected BRAS configuring

L3-Connected BRAS Diagnostic Procedure

- Check if authorization is enabled in fastdpi.conf settings
- Is there traffic from local subscribers? Remember that authorization takes place only after the packet from a local subscriber is received.
- If FastDPI and FastPCRF are installed on different servers, then you should first check the firewall settings: whether you have configured FastPCRF server to allow access from the FastDPI server to the TCP port for establishing fastDPI → fastPCRF connection (by default 29002). Similarly, in order to establish the opposite direction connection, the FastDPI server should be configured to allow access from the FastPCRF to the TCP management port (by default 29000).
- Check if there is a fastDPI → fastPCRF connection available. If the connection suddenly fails, then the following message will be written to the fastdpi_ap0.log log file:

[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 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 an active connection with the Radius server. The following messages in fastdpi_ap2.log indicate that there are problems with Radius server connection:

```
[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 indicated by multiple records about re-sending requests to the Radius server. When you establish a connection with the Radius server, you will see something like this 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: does it receive requests from the FastPCRF (possible reason is the firewall is configured to block connections to the Radius UDP ports), and is the Radius secret specified correctly.

The radius_unknown_user paremeter (unknown_user) is a string, user login, in case the real login is unknown to the fastdpi. The default value is `'VasExperts.FastDPI.unknownUser'`. It corresponds to the value of the `User-Name` attribute within the Access-Request request in case the `radius_user_name_ip` equals to zero and the user login is unknown. Предполагается, что radius-сервер в ответе Access-Accept сообщит истинный логин пользователя, определенный по его IP-адресу, взятому из атрибута Framed-IP-Address и вышлет VasExperts.FastDPI.unknownUser, в разобранных Wireshark'ом пакетах видно User-Name = ip, в логах:

```
[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
```

начиная со СКАТ 7.4 появился такой параметр, более свежий: radius_user_name_auth, см. по ссылке Интеграция с Радиус Сервером отсюда и появляется IP в User-Name, если его задать как radius_user_name_auth=login, то при отсутствии логина будет браться VasExperts.FastDPI.unknownUser

это параметр для fastpcrf.conf