Содержание

7 L3-Connected BRAS configuration checklist

Diagnostic Procedure for L3-Connected BRAS

- Check whether authorization is enabled in the `fastdpi.conf` file
- Is there traffic generated by local subscibers? Remember that authorization is carried out only when packet from a local subscriber has been received.
- If FastDPI and FastPCRF are installed on different servers, first you should check the firewall settings: whether the FastPCRF configured to grant access from the FastDPI server according to the fastDPI → fastPCRF connection (by default TCP port 29002 is used) . Similarly, in order to enable two-way communication, the FastDPI server should be configured to grant access from the FastPCRF to the TCP control port (be default 29000 is used).
- Check whether there is a fastDPI → fastPCRF connection alive. If the connection was 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 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 whether there is a connection with the RADIUS server. The following messages in fastdpi_ap2.log indicates communication issues 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, multiple entries about re-sending requests to the RADIUS server can be considered as an indicator of communication issues. When establishing a connection with the RADIUS server, you will see similar entries 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 requests from FastPCRF reach it (a possible reason could be that the firewall is closed to RADIUS UDP ports), along with whether the RADIUS secret is specified correctly

radius_unknown_user parameter is the string, username in case the real user login is unknown to fastdpi. Default value is `VasExperts.FastDPI.unknownUser`. This is the value of the `User-Name` attribute of the Access-Request request in case the `radius_user_name_ip` equals to zero and the user login is unknown. It is assumed that the RADIUS server will provide the real user login within the Access-Accept response and will send the VasExperts.FastDPI.unknownUser. The real user login will be identified by its IP address extracted from the Framed-IP-Address attribute and send VasExperts.FastDPI.unknownUser. You can see the User-Name=ip in the packets parsed by Wireshark, the same thing can be seen in 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 the VAS Experts DPI version 7.4 a newer `radius_user_name_auth` parameter appears, to see detailed info follow the Integration with RADIUS Server link along with that an IP appears withing the User-Name. If you specify it as `radius_user_name_auth=login` then in case the login is missed the VasExperts.FastDPI.unknownUser will be used instead.