Table of Contents

BRAS

Product Description

1. Authorization is not working

- Check if authorization is enabled in the `fastdpi.conf` settings.
- Is there traffic from local subscribers? Note that authorization only occurs when a packet is received from a local subscriber.
- If fastDPI and fastPCRF are installed on different servers, first check the firewall: ensure that the TCP port connection from fastDPI to fastPCRF (default 29002) is open on the fastPCRF server. Similarly, for the reverse connection, the TCP management port (default 29000) must be open on the fastDPI server.
- Check if there is connectivity between fastDPI and fastPCRF. If the connection is suddenly lost, the log `fastpcrf_ap0.log` will show a message:

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

When establishing the connection, you will see a message like:

```
[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 connectivity with the Radius server. Issues with Radius server connectivity are indicated by the following messages in `fastpcrf_ap2.log`:

```
[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
```

Issues may also be indicated by numerous entries about resending requests to the Radius server.
When establishing a connection with the Radius server, you will see an entry 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: are requests from fastPCRF reaching it (possible cause - firewall blocking UDP ports for Radius), and is the Radius secret correctly specified?
- `radius_unknown_user` (`unknown_user`) — the string representing the user's login if the actual login is unknown to fastDPI. Default value: `VasExperts.FastDPI.unknownUser`. This value is for the `User-Name` attribute of the `Access-Request` message if `radius_user_name_ip=0` and the user login is unknown. The Radius server is expected to return the actual user login in the `Access-Accept` response, determined by their IP address

from the `Framed-IP-Address` attribute and send `VasExperts.FastDPI.unknownUser`. In Wireshark, you will see `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 with SSG 7.4, there is a more recent parameter: `radius_user_name_auth`, see the Radius Server Integration link.
This is where `IP` appears in `User-Name`; if set as `radius_user_name_auth=login`, then in the absence of a login, `VasExperts.FastDPI.unknownUser` will be used. This parameter is for `fastpcrf.conf`.

2. CoA requests are not being accepted

Check the firewall: ensure that the client sending the CoA request has access to the fastPCRF server on the CoA port (which is a UDP port).

3. Manual control of authorization status. If 'fdpi_ctrl load --auth=0 --ip=192.168.10.1' is manually set, will 'default_reject_whitelist' be applied?

It will not. You need to either issue the command via Radius or directly activate the 5 service on the subscriber.