Содержание

1 Mobile Networks Support		3
---------------------------	--	---

11 Mobile Networks Support

```
<html>
</html> <html>
</html>
```

Stingray SG can detect GTP-C traffic and extract subscriber parameters for the subscriber's IP and login binding from the GTP session creation requests. GTP-C versions 1 and 2 are supported. GTP support is enabled by parameters in fastdpi.conf:

```
# bras enable=1
   # GTP processing mode
   # Values:
   # 0 - (default) GTP processing is disabled
        1 - [bind mode] In this mode, BNG/BRAS processes GTP-C packets of
the session start and end,
            binding the IP-address issued to the subscriber with the login
(IMSI or MSISDN is used as the login).
            At the end of the session, the login-IP connection is broken.
        2 - [auth mode] authorization of GTP sessions is enabled. In this
mode, BNG/BRAS processes GTP-C session start and end packets.
            Upon successful start of the GTP session, BRAS sends an L3
authorization request to PCRF,
            transmitting the subscriber's IP address, IMSI, MSISDN, IMEI and
other parameters.
            At the end of the session, the login-IP connection is broken.
   #
            SSG does not terminate GTP sessions, all GTP-C packets are
dropped.
      3 - [passive bind mode] Similar to mode 1 [mirror bind mode], but
GTP-C packets are not dropped.
           The SSG should be in a gap on the S11 or S5 interface.
        4 - [passive auth mode] Similar to mode 2 [mirror auth mode], but
GTP-C packets are not dropped.
           The SSG should be in a gap on the S11 or S5 interface.
#bras gtp mode=0
```

Creating a session (bind IP-LOGIN) on responses:

```
#Response to Create PDP Context Request for GTPv1:
Create PDP Context Response

#Response to Create Session Request for GTPv2:
Create Session Response
```

Deleting a session (bind IP-LOGIN) on responses:

```
#Response to Delete PDP Context Request for GTPv1:
Delete PDP Context Response

#Response to Delete Session Request for GTPv2:
Delete Session Response

#Response to Delete Bearer Request for GTPv2:
Delete Bearer Response
```

The Stingray SG connection point is set by the parameter:

```
# Where the SSG is connected (which GTP-C is fed to the SCAT)
# Valid values:
# 0 - S5 protocol (SGW <-> PGW). This is the default
# 1 - S11 protocol (MME <-> SGW)
bras_gtp_mountpoint=0
```

In mirror mode (bras_gtp_mode 1 or 2), SSG drops all incoming GTP-C packets. In passive mode (bras gtp mode 3 or 4) SSG passes GTP-C traffic through itself.

You should also set the maximum size of active GTP-sessions internal database in fastdpi.conf

```
# Max number of concurrent GTP-sessions
# We recommend setting this parameter 1.5-2 times more than the actual
max number of sessions
# Default value: 10000 sessions, minimum value: 10000
#bras_gtp_session=10000
```

After receiving a request to create a GTP-C session, SSG waits for a packet of successful session creation. Only at this moment, upon receiving a successful response and issuing an IP address to the subscriber, connects the login and IP. The response timeout is set by a parameter in fastdpi.conf:

```
# Max time to wait for a response to a GTP session creation, seconds
# Default = 3 seconds
#bras_gtp_pending_timeout=3
```

IMSI or MSISDN can be used as a login, which is set by a parameter in fastdpi.conf:

```
# What is the subscriber's login for GTP:
# 0 - IMSI (by default)
# 1 - MSISDN
#bras_gtp_login=0
```



Using MSISDN (phone number) as a login, although more familiar to everyone, is not safe: MSISDN may not be present in GTP-C session creation packets. In this case, SSG will use IMSI as a login. As a result, it will not be clear what the login is - MSISDN or IMSI. Therefore, we recommend using only IMSI as a login

To detect GTP-U, you have to enable tunnel parsing:

```
# enable the tunnels parsing by dispatchers
check_tunnels=1
  # enable the detection and parsing of GTP-U
detect_gtp_tunnel=1
```

When you enable parsing of GTP-U tunnels, SSG will work with the real IP-address of the subscriber, and not with the IP-address of the tunnel. That means that it becomes possible to apply filtering, services and policing to the GTP-subscriber.

SSG does not terminate GTP-U tunnels.

The internal database of GTP-sessions can be controlled with a special set of CLI-commands.