Содержание

General BRAS setup for L2/L3 modes

FastDPI L3 BRAS setup

You need to create services and policies, which will later be transmitted using the Radius attributes from billing. An example of setting up a policy (tariff plan) and Captive Portal, which are the minimum required to start.

1. Create a file aslocal.bin (or correct this file if it already exists). The aslocal file contains those ranges of private IP addresses that are used in the provider's local network. Any of the range 64512 - 65534 is indicated for them as an autonomous system number.

```
vi aslocal.txt
10.0.0.0/8 64512
172.16.0.0/12 64512
192.168.0.0/16 64512
cat aslocal.txt | as2bin /etc/dpi/aslocal.bin
```

FastPCRF authorizes only the local users. The fact whether the user is local or not is determined according to the fact of belonging his IP-address to the list of local autonomous systems.

2. Next, create the asnum.dscp file (or modify it if it already exists). The *local* numbers of autonomous system should be specified in this file, so the authorization will take place for them. Typically these are autonomous systems for the gray IP addresses specified in the aslocal.bin file, plus the white IPs allocated to the provider, if these white IP addresses are used on the local network, that is, they require authorization. Authorization will be done for all the autonomous systems IP addresses marked as local in the asnum.dscp file.

```
vi asnum.txt
64512 local
cat asnum.txt | as2dscp /etc/dpi/asnum.dscp
```

3. To enable authorization in **/etc/dpi/fastdpi.conf**:

```
enable_auth=1
```

4. Set the fastPCRF servers list:

```
auth_servers=127.0.0.1%lo:29002;192.168.10.5%eth1:29002
```

The format for specifying a single server: `ip%dev:port`, here `ip` is the server IP address, dev is the local device by wich the connection can be established. FastDPI connects to the first available fastpcrf server from the list.

Do not forget to activate the user property store:

```
udr=1server
```

IPv6

In order to enable IPv6 addresses authorization you should activate the IPv6 support. Actually, the Stingray SG authorizes a whole subnet with a predefined prefix length (by default it equals to /64) rather than particular individual IPv6 address. For example, if there are incoming packets sent from 2001:1::1 and 2001:1::10 addresses, only one of these addresses will be subject to authorization, so the returned authorization parameters will be applied to all the addresses from 2001:1::/64 subnet.

There is no analog of the `aslocal.bin` file for IPv6, since there are no private addresses. You must mark the AS numbers that require authorization as `local` in the `asnum.dscp` file.

IPv6 authorization is automatically enabled if fastdpi.conf has:

```
ipv6=1
enable_auth=1
```

Starting from SSG version 8.1.4, it is possible to forcibly disable IPv6 address authorization by specifying in fastdpi.conf:

```
enable_auth_ipv6=0
```

Other authorization settings

Implementing of the BRAS authorization

The process of implementing a new features is always a long and thorny path especially with regard to the BRAS authorization since it requires to configure not only the fastdpi/fastpcrf but also the Radius server which handles the main part of the subscriber authorization along with the all backend data behind the Radius server which includes the data bases, billing system and so on. Below we will refer to some approaches to implement the authorization.

Test bed

Simple and reliable way to implement the BRAS authorization is to organize a test bed. Pros: it will not affect the real subscribers. Cons: it requires the additional equipment. So it is not always possible to organize a full-fledged test bed.

Separate autonomous system

As described earlier the authorization is done by using just the local IP addresses. Locality of the IP address is specified by the `local` flag for the autonomous system. Hence, one can allocate the test range of IP addresses then to set the corresponding autonomous system from the private range of

numbers(64512..65534) and to define the autonomous system as local. So the only IP addresses belonging to this local autonomous system will be authorized. "Live" subscribers will not be affected until the autonomous system with corresponding IP addresses is not defined as local. It allows you to configure the authorization on the live fastDPI.

Diagnostic IP address

So the third approach is to define that the authorization should be performed just for the specified IP addresses. For this purpose there is the `auth_trace_ip` option in the fastdpi.conf that allows you to set one or two (but not more than two) IP addresses:

```
auth_trace_ip=192.168.20.11,192.168.30.58
```

The specified IP addresses must be local (i.e. these IP addresses should be within the autonomous system declared as local, please see above). If the `auth_trace_ip` option is used so the authorization will be performed just for the IP addresses specified therein.

«« back to BRAS authorization

Authorization settings

You can specify the following authorization options in fastdpi.conf in addition to describedearlier:

`auth_resend_timeout` - is the timeout of authorization requests resending to the fastpcrf, in seconds. The default value is 60. If the fastDPI doesn't receive a response from the fastpcrf during this period, the authorization request will be repeated.

`auth_expired_timeout` - is the authorization lifetime, in minutes. The default value is 60 minutes. Zero value corresponds to unlimited authorization lifetime. This option is applied only in case the Radius response does not contain the `Session-Timeout` attribute specifing the session lifetime. Note that the Access-Reject also can contain the `Session-Timeout` attribute. Once that time has elapsed, a second authorization request is sent.

 `auth_expired_timeout=0` (unlimited authorization lifetime) may result in subscriber being rejected in authorization (Access-Reject) will remain in "unauthorized" state permanently. The subscriber "unauthorized" state can be altered just by CoA notification to reauthorization, by the fastDPI restart or manually using the fdpi_ctrl.

`auth_pcrf_reconnect` - the timeout of reconnect to the fastpcrf, in seconds. The default value is 1 second.

Diagnostic settings

`auth_trace` - is the boolean flag enabling the authorization tracing, is not specified by default. Note that the authorization tracing significantly affects the performance of the fastDPI and causes the large number records being written to the logs, so it should not be enabled unless you have to.

`auth_trace_ip` - the list of IP addresses (no more than two) to be authorized. The list is empty by default. Example:

```
auth_trace_ip=192.168.10.20,192.168.30.45
```

This list can be applied at the authorization implementing stage and when configuring the Radius servers: the authorization will only be performed for the specified local IP addresses (typically testing subscribers are used) without affecting "real" subscribers.

«« back to BRAS authorization

FastDPI L2 BRAS setup

The activation of the fastDPI BRAS features is done according to **the mandatory settings** defined in the **fastdpi.conf** configuration file:

- `bras_enable=1` – the common flag to enable the BRAS
- `bras_arp_ip` – specifies the BRAS IPv4 address. You are allowed to set a fake IP addres, which is not connected to any network interface. The main requirement is that the IP address should be unique, i.e. it should not correspond to any user.
- `bras_arp_mac` – the BRAS MAC address in the following format: XX:XX:XX:XX:XX:XX, for example, a0:00:b1:01:4e:cc. This MAC address have to be unique within the whole local network; fake MAC can be used instead, it should not be connected to any network card, but in order to avoid an accidental match with other MAC address of client's equipment we strongly recommend to use the real dna card MAC address instead.
- `auth_servers` - specifies the list of the fastPCRF servers. FastPCRF server is responsible for interaction with Radius servers. Used format to specify the server: `ip%dev:port`, here ip - is the server IP address, dev - the local device used to establish connection. FastDPI establishes connection with the first available fastPCRF server from the list.

In order the fastDPI BRAS to work properly BRAS have to be enabled UDR (user data repository is the internal database containing user properties): the **fastdpi.conf** should contain the following line

```
udr=1
```

Example:

```
udr=1
auth_servers=127.0.0.1%lo:29002
bras_enable=1
bras_arp_ip=192.168.1.255
bras_arp_mac=a0:00:b1:01:4e:cc
```

When choosing the `bras_arp_mac` parameter, it is very convenient to use the existing MAC address of the card port. But it was noticed that some advanced cards

(for example, 25G cards on the XXV710 chip, i40e driver) can destroy some packets (for example, ARP) if `bras_arp_mac` is equal to the MAC address of the card port. The reason for this behavior is not clear, therefore, in order to avoid packet loss, we advise you to select the `bras_arp_mac` value purely virtual, not matching the MAC address of the port.

Some special fastDPI BRAS features are enabled by corresponding advanced settings described further, but without the `bras_enable=1` flag the special features will be unavailable.

«« back to BRAS