Содержание

Quick Start: Tariff Plan and Captive Portal

Introduction

To implement BRAS, this section provides an example of creating two tariff plans (policing):

- **rate_10M** - basic tariff plan that is used after subscriber authorization.
- **blocked** - a tariff plan that is used to block a subscriber and provide access only for certain protocols. His name must be passed to the Radius-Reject.

After blocking, the subscriber is assigned (Service 5) **my_white_list** - Allow list of resources to which he has access to pay for the service. It also redirects HTTP resources to the Captive Portal.

The names of these profiles must be passed in the corresponding message attributes Radius-Accept, Radius-Reject.

Traffic distribution by class for the tariff plan

To mark the priorities, use the option Assigning priorities depending on the protocol.

1. Create a **protocols.txt** file with a description of the protocol groups that we want to separate from the general traffic, and the priorities (classes) assigned to them:

```
dns cs0
ICMP cs0
http cs0
https cs0
QUIC cs1
default cs2
bittorrent cs7
```

where

- cs0 corresponds to priority 0, class0 respectively
- cs1 - priority 1, class1
- cs7 - priority 7, lowest class

The classes highlighted in this way can be used in the description of tariff plans, introducing separate restrictions for them, in addition, in accordance with them, the protocols will be prioritized in the strip.

2. We convert it to DSCP format, which fastDPI understands

```
cat protocols.txt | lst2dscp /etc/dpi/protocols.dscp
```

3. Apply the settings

```
service fastdpi reload
```

Creating a tariff plan

To organize the subscriber bandwidth according to the tariff plan, use the option Distribution of the access channel between subscribers.

1. For each tariff plan of the subscriber in the billing, create a configuration file with a description of its settings for DPI.

Convenient agreement: make the names of the configuration files, describing the setting of the tariff plan for DPI, the same as the name of the tariff plan in the billing.

An example of a description for the 10mbit tariff, the name in the billing "rate_10M"

Create a file rate_10M.cfg

```
htb_inbound_root = rate 10mbit
htb_inbound_class0 = rate 4mbit ceil 10mbit
htb_inbound_class1 = rate 3mbit ceil 10mbit
htb_inbound_class2 = rate 8bit ceil 10mbit
htb_inbound_class3 = rate 8bit ceil 10mbit
htb_inbound_class4 = rate 8bit ceil 10mbit
htb_inbound_class5 = rate 8bit ceil 10mbit
htb_inbound_class6 = rate 8bit ceil 10mbit
htb_inbound_class7 = rate 8bit ceil 10mbit
htb_root = rate 10mbit
htb_class0 = rate 4mbit ceil 10mbit
htb_class1 = rate 3mbit ceil 10mbit
htb_class2 = rate 8bit ceil 10mbit
htb_class3 = rate 8bit ceil 10mbit
htb_class4 = rate 8bit ceil 10mbit
htb_class5 = rate 8bit ceil 10mbit
htb_class6 = rate 8bit ceil 10mbit
htb_class7 = rate 8bit ceil 10mbit
```

Notes:

- htb_class0-1 - have a guaranteed speed of 4Mbps and 3Mbps, respectively
- htb_class7 - the minimum bandwidth is 8bit, which means that it can be clamped at 0 Mbps (0 - cannot be specified, reserved)

2. Create a tariff plan named **rate_10M**

```
fdpi_ctrl load profile --policing /path/to/rate_10M.cfg --profile.name
rate_10M
```

3. So that our settings for subscribers, which we will make in the future, do not disappear when the DPI is rebooted, we connect UDR database

```
udr=1
```

4. Apply settings via fastDPI restart

```
service fastdpi restart
```

Preparing Captive Portal, for zero balance and access to payment systems

Service 5 (Allow lists and Captive Portal) regulates access to TCP-based protocols only. In order to restrict access to other resources using various protocols, you must use the appropriate profile of the tariff plan, which allows traffic only of certain classes.

1.Create a description of the tariff plan for subscribers in blocked.cfg blocking. Allow only cs0 traffic (see the list in item 1).

```
htb_inbound_root=rate 10mbit
htb_inbound_class0=rate 1mbit ceil 10mbit
htb_inbound_class1=rate 8bit ceil 8bit
htb_inbound_class2=rate 8bit ceil 8bit
htb_inbound_class3=rate 8bit ceil 8bit
htb_inbound_class4=rate 8bit ceil 8bit
htb_inbound_class5=rate 8bit ceil 8bit
htb_inbound_class6=rate 8bit ceil 8bit
htb_inbound_class7=rate 8bit ceil 8bit
htb_root=rate 10mbit
htb_class0=rate 1mbit ceil 10mbit
htb_class1=rate 8bit ceil 8bit
htb_class2=rate 8bit ceil 8bit
htb_class3=rate 8bit ceil 8bit
htb_class4=rate 8bit ceil 8bit
htb_class5=rate 8bit ceil 8bit
htb_class6=rate 8bit ceil 8bit
htb_class7=rate 8bit ceil 8bit
```

2. Create a tariff plan named **blocked** for a blocked subscriber

```
fdpi_ctrl load profile --policing /path/to/blocked.cfg --profile.name
blocked
```

3. Create a list of sites available in the Captive Portal mode. More details in the description of the Allow list option.

Create a file **my_white_list.txt** from the url of payment system sites. Each line of the file contains one url (without the http:// prefix), it is recommended to include subdomains as well, for example:

```
online.bank.com
*.online.bank.com
```

To create an Allow list for payment systems, we recommend using a prepared list.

List of payment systems
List of banks prepared by our partners.

The list is ready for uploading to SKAT. The link is updated periodically.

4. Conversion to internal format:

```
cat my_white_list.txt | url2dic my_url_list.bin
cat my_white_list.txt | url2dic my_cn_list.bin
cat my_white_list.txt | url2dic my_sni_list.bin
```

To prevent the https sites blocking, you have to prepare white list for CN, SNI with * symbol, signaling that CN and SN can be any.

5. Create a **named profile** for the Allow list

```
fdpi_ctrl load profile --service 5 --profile.name my_white_list --
profile.json '{"url_list": "/path/to/my_url_list.bin", "sni_list":
"/path/to/my_sni_list.bin", "cn_list": "/path/to/my_cn_list.bin",
"redirect": "mysite.com/block"} '
```

where

- redirect - redirect page [1) 2)]
- url_list: URL Allow list
- sni_list: SNI Allow list
- cn_list: Common Name Allow list [3)]

Integration with billing without Radius

If the network still uses Radius, but you do not intend to configure the interaction of Stingray Service Gateway with billing through it and have dynamic IP addresses, you must use Radius-monitor, which would add a thread of IP-Login in the UDR.

1. We carry out integration with billing

The integration option depends on whether the billing system has the ability to control equipment by events or not.

1a. Billing can control equipment by events: creating a subscriber, changing a tariff plan, blocking

In this case, select the type of equipment controlled via SSH / RSH [4] Or by executing local scripts and enter it into settings of the corresponding commands (or scripts) of the command for connecting (changing) the tariff plan:

```
fdpi_ctrl load --policing $ {rateplan} .cfg --ip $ {ip_address}
or
fdpi_ctrl load --policing $ {rateplan} .cfg --login $ {login}
```

where

- $ {rateplan} - variable where billing half will set the name of the subscriber's tariff plan rate_10M
- $ {ip_address} - billing will substitute the subscriber's ip address 192.168.0.1 here (for subscribers with a fixed ip)
- $ {login} - billing will substitute the login of the subscriber dom1kv2 here (for subscribers with dynamic ip, multiple ip, or we just want to manage it by login)

1b. Billing cannot control equipment by events

Let's configure the upload of data from billing on a schedule to crontab. In files with the names of_plan_name.lst, we unload the list of subscribers with the corresponding tariff plans from the billing system (the list may contain ip or login) and start loading this data into dpi

```
fdpi_ctrl load --policing rate_10M.cfg --file rate_10M.lst
fdpi_ctrl load --policing rate_20M.cfg --file rate_20M.lst
...
or (for all at once)
for rateplan in * .cfg; do fdpi_ctrl load --policing "$ rateplan" --file "$
{rateplan %%. *}". lst; done
```

2. We place the subscriber in the Captive Portal [5]

```
fdpi_ctrl load --policing blocked.cfg --ip $ {ip_address}
fdpi_ctrl load --service 5 --ip $ {ip_address}
```

3. After payment, we turn off the Captive Portal for the subscriber and restore his tariff plan

```
fdpi_ctrl load --policing $ {rateplan} .cfg --ip $ {ip_address}
fdpi_ctrl del --service 5 --ip $ {ip_address}
```

1)
Attention, if you specify an https site, then this domain must be added to the SNI list, otherwise the domain will be blocked

2)
additional parameters can be added (according to http rules) only after? or &, they must be specified in the url for the Allow list, and here you need to think for DPI, otherwise DPI would add /?

3)

check by ip: port or cname is performed if the request does not contain url or sni

4)

If necessary, you can add additional software compatible with OS Linux to dpi to expand the capabilities of remote control, for example, a telnet server.

5)

If event management is not supported, then we do it by uploading blocked and unblocked subscribers to the file blocked.lst and unblocked.lst