

Содержание

Subscriber authorization attributes	3
<i>VasExperts-Policing-Profile</i>	4
1. Preconfigured Profile	4
2. Policing with absolute values (simplified format)	4
3. Policing with Absolute Value Transmission (Extended HTB Format)	5
<i>VasExperts-Service-Profile</i>	6
Example 1. NAT Connection	7
Example 2. Configuring the Whitelist	7
Example 3. Overriding Traffic Classes and Policing	7
<i>VasExperts-Enable-Service</i>	8
<i>VasExperts-Multi-IP-User</i>	8
<i>VasExperts-UserName</i>	9
<i>VasExperts-Restrict-User</i>	9
<i>VasExperts-Enable-Interconnect</i>	9
Optional Radius attributes	10
<i>Session-Timeout</i>	10
<i>Acct-Interim-Interval</i>	10
<i>Idle-Timeout</i>	10
<i>Class</i>	10

Subscriber authorization attributes

The main data, in addition to the key point, i.e. whether the user is authorized or not, needed to the fastPCRF to form the response to the Access-Request properly, are the following:

- Subscriber IP address
- User policing profile
- User profiles according to the fastDPI services
- Services that are activated for the particular user
- User type: how many IP addresses are assigned to the user, whether it one or more than one
- User login is one of the following attributes: User-Name, CUI or VasExperts-UserName

The Stingray Service Gateway supports both IPv4 and IPv6 subscriber addressing. In case of IPv4 subscribers, the response should contain the Framed-IP-Address attribute specifying the IPv4 address, but this address has to match the one specified in the Access-Request. If the Framed-IP-Address values in the request and response differ, this is considered an error.



Some billing systems cannot give the Framed-IP-Address attribute to Access-Accept in L3 authorization mode. For such cases `fastpcrf.conf-option radius_framed_ip_from_request=1` is provided: with this value, if the Framed-IP-Address attribute is missing in the response, the fastPCRF takes it from the authorization request.

The following attributes are supported in the Access-Accept/Reject for IPv6 subscribers:

- Framed-IPv6-Address specifies the subscriber IPv6 address. The attribute value within response has to match the corresponding value within request.
- Framed-IPv6-Prefix specifies the IPv6 subscriber subnet prefix. Prefix size, as well as its value within the response have to match the ones within the request.
- Framed-IPv6-Pool is the pool name. It is optional attribute. If this attribute is specified in the response, it will be sent in all the Accounting-Request packets.

In case of IPv6, the response has to contain one of the Framed-IPv6-Address or Framed-IPv6-Prefix attributes (or both). However, the SSG interprets Framed-IPv6-Address attribute as a subnet prefix without taking into account the least significant bits of the address (remember that the SSG currently can handle only equal sized prefixes, specifying by the [ipv6_subnetwork](#) parameter).



The SSG implies that the IPv6 addresses are **necessarily** bound to the subscriber login, so the response should contain one of the attributes specifying the subscriber login.

The dual stack subscribers are also supported: the Access-Request is always sent using either IPv4 or IPv6 address, but the response can contain both addresses in the Framed-IP-Address and Framed-IPv6-Address/Framed-IPv6-Prefix attributes. This means that the subscriber is assigned both an IPv4 address and an IPv6 prefix. At the same time, such a subscriber is not considered by default a multi-bind subscriber: the SSG implies that each subscriber, even single-

binded, can be bound to the pair: IPv4 address and IPv6-prefix.

The policing profile and the list of activated services are sent in the [26] Vendor-Specific attribute contained in the responses.

VENDOR	VasExperts	43823	
BEGIN-VENDOR	VasExperts		
ATTRIBUTE	VasExperts-Policing-Profile	1	string
ATTRIBUTE	VasExperts-Service-Profile	2	string
ATTRIBUTE	VasExperts-Enable-Service	3	string
ATTRIBUTE	VasExperts-Multi-IP-User	4	integer
ATTRIBUTE	VasExperts-UserName	5	string
ATTRIBUTE	VasExperts-Restrict-User	7	byte или integer
END-VENDOR	VasExperts		



Need to create services and policing that will transfer using Radius attributes from billing. [Example of setting up policing \(tariff plan\) and Captive Portal, which are minimally required for startup.](#)

VasExperts-Policing-Profile

The VasExperts-Policing-Profile attribute is included in the Access-Accept response and is responsible for applying policing rules.



The Access-Accept response must contain **no more than one** VasExperts-Policing-Profile attribute.

Profile configuration options:

1. Preconfigured Profile

A string attribute that specifies the name of the [policing profile](#):

```
VasExperts-Policing-Profile = "50Mbps"
```

2. Policing with absolute values (simplified format)

```
VasExperts-Policing-Profile = "BV##100000#100000#+++--++"
```

where:

- BV — By Value, the HTB algorithm is used, where the ceil for each class is equal to the root rate
- ##100000 — limit from the Internet to the subscriber (download), kbps

- #100000 — limit from subscriber to Internet (upload), kbps
- #+++-++++ — permission for classes cs0 ... cs7, rate(cs3)=0 — class cs3 is blocked, other classes use root speed with the possibility of borrowing (HTB)

3. Policing with Absolute Value Transmission (Extended HTB Format)

SSG DPI uses [two types of policing](#) — HTB (Hierarchical Token Bucket) and TBF (Token Bucket Filter). The examples below use the **HTB** algorithm with a minimum (rate) and maximum (ceil) speed limit for each class.

The policing profile defines the overall rate (root) and the rate for each traffic class (cs0 ... cs7)

It allows you to set the rate and ceil parameters for each class separately and contains 36 parameters.



Zero values are not passed

Format (displayed as a single line without line breaks):

```
VasExperts-Policing-Profile =
"BR##4#<RIN><ROUT><CIN><COUT><RIN0><ROUT0><CIN0><COUT0><RIN1><ROUT1><CIN1><C
OUT1><RIN2><ROUT2><CIN2><COUT2><RIN3><ROUT3><CIN3><COUT3><RIN4><ROUT4><CIN4>
<COUT4><RIN5><ROUT5><CIN5><COUT5><RIN6><ROUT6><CIN6><COUT6><RIN7><ROUT7><CIN
7><COUT7>
```

where:

- BR — By Rates
- ##4# — HTB is used; the rate and ceil are transmitted for inbound and outbound traffic
- <RIN> — kbps root rate (#8192k), the total rate for all classes for inbound traffic (download)
- <ROUT> — kbps root rate (#8192k), total speed for all classes for outbound traffic (upload)
- <RIN0> ... <RIN7> — kbps class rate, minimum speed by class for inbound traffic (download)
- <CIN0> ... <CIN7> — kbps ceiling rate, maximum speed per class for inbound traffic (download)
- <ROUT0> ... <ROUT7> — kbps class rate, minimum speed per class for outbound traffic (upload)
- <COUT0> ... <COUT7> — kbps ceiling rate, maximum speed (ceiling) by class for outbound traffic (upload)



The sum of the rates by class must be \leq root rate
The ceiling of each class must be \leq root rate

Example

For convenience, it has been broken into lines, but it must be sent as a single line.

```
VasExperts-Policing-Profile = "BR##4#  
8192k8192k65M65M  
1024k1024k8192k8192k  
1024k1024k8192k8192k  
1024k1024k8192k8192k  
1024k1024k8192k8192k  
1024k1024k8192k8192k  
1024k1024k8192k8192k  
1024k1024k8192k8192k  
1024k1024k8192k8192k"
```

DPI Test

```
sudo fdpi_ctrl list --policing --ip <ip> | sed 's/\s/\n/g'
```

Sample output:

```
htb_inbound_root=rate 8192kbit  
htb_inbound_class0=rate 1024kbit ceil 8192kbit  
htb_inbound_class1=rate 1024kbit ceil 8192kbit  
htb_inbound_class2=rate 1024kbit ceil 8192kbit  
htb_inbound_class3=rate 1024kbit ceil 8192kbit  
htb_inbound_class4=rate 1024kbit ceil 8192kbit  
htb_inbound_class5=rate 1024kbit ceil 8192kbit  
htb_inbound_class6=rate 1024kbit ceil 8192kbit  
htb_inbound_class7=rate 1024kbit ceil 8192kbit  
  
htb_root=rate 8192kbit  
htb_class0=rate 1024kbit ceil 8192kbit  
htb_class1=rate 1024kbit ceil 8192kbit  
htb_class2=rate 1024kbit ceil 8192kbit  
htb_class3=rate 1024kbit ceil 8192kbit  
htb_class4=rate 1024kbit ceil 8192kbit  
htb_class5=rate 1024kbit ceil 8192kbit  
htb_class6=rate 1024kbit ceil 8192kbit  
htb_class7=rate 1024kbit ceil 8192kbit
```

VasExperts-Service-Profile

A string parameter that specifies the profile name for a specific fastDPI service.
String format:

```
service_id:profile_name
```

Where:

1. `service_id` — a number, [fastDPI service identifier](#);

2. `profile_name` — a string, [the profile name for the service](#).



The authorization response may contain zero or more `VasExperts-Service-Profile` attributes—one attribute for each service.

Example 1. NAT Connection

NAT connection (service 11) using the "cgnat" profile.

```
VasExperts-Service-Profile="11:cgnat"
```

Example 2. Configuring the Whitelist

Configuring [Whitelist and Captive Portal, HTTP redirect](#) (16 services) with the redirect page parameters set to "<http://info.com>" and the allowed IP address list set to `/var/lib/dpi/ip_list.bin`.

```
VasExperts-Service-Profile =  
"16:BV##/var/lib/dpi/ip_list.bin#http://info.com"
```

Example 3. Overriding Traffic Classes and Policing

[Service 18 \(Session-Based Policing\)](#) is used to override traffic classes (cs0 ... cs7) and configure session-based policing for a specific subscriber.

The profile defines the distribution of DPI protocols across traffic classes. Classes are assigned individually for each subscriber.

Format:

```
VasExperts-Service-Profile =  
"18:BP##profile_name#/share/#IMSI_number.dscp#IMSI_number.tbf"
```

where:

- 18 — traffic class reclassification and per-session policing
- BP — By Parameters
- ##`profile_name` — profile name, created dynamically, displayed in the GUI and CLI
- `/share/` — directory on fastPCEF. Accessible over the network; only the filename is passed, while the file itself is read from the original directory. Contains source (.txt) files (not converted to binary) for easy verification
- `#IMSI_number.dscp` — protocol and traffic class mapping file. Determines which class (cs0 ... cs7) the traffic is placed in. Supports the **drop** flag for blocking
- `#IMSI_number.tbf` — a file containing session-level policing parameters. Sets policing rules for individual protocols. Used to limit speed at the session level

Example:

```
VasExperts-Service-Profile  
=18:BP##250019500475292#/share/#250019500475292.dscp#250019500475292.tbf
```

VasExperts-Enable-Service

A string parameter that specifies whether to activate/disable a specific service not requiring any profile. String format :

```
service_id:flag
```

here:

- `service_id` - the number, the fastDPI service identifier
- `flag` - the flag indicating the activating/disabling of the service. The valid values are:
 - 1, on, enabled - corresponds to activated service
 - 0, off, disabled - corresponds to disabled service

The example of the service to be activated: 5: on

The example of the service to be disabled: 5: off

You should use this attribute in order to disable the service in CoA. For example, to disable service 5 you should specify: `VasExperts-Enable-Service="5:off"`. Whereas to activate the service 5 with `my_white_list` profile you should specify: `VasExperts-Service-Profile="5:my_white_list"`



Important: There is the rule "all the stuff not activated explicitly is disabled by default" applied to the services, so if the service is not marked as enabled (or if the corresponding profile is not specified) the service is treated as disabled. But in case of service 4 ([black list](#), prohibited traffic filtering) there is more stringent rule applied: this service have to be explicitly disabled for the user, so the `VasExperts-Enable-Service="4:off"` attribute should be presented in the Radius server response in order to disable the service 4 "black-list".

By default, the activation of the service 4 "black-list" is managed by the [global fastDPI configuration](#). Service 4 is usually globally activated in order to comply with the federal law.

VasExperts-Multi-IP-User

This attribute shows whether there are many IP addresses assigned for this subscriber or only just one. This attribute can be presented either by a byte or by a 32-bit number. A value of 1 means that several IP addresses can be assigned to this subscriber (corporate client), value 0 corresponds to only one IP-address. If the `VasExperts-Multi-IP-User` attribute is not presented in the PDU, it is considered that only one IP address is assigned to the subscriber.

If the `VasExperts-Multi-IP-User=1` attribute is set to the user so the features (active services and policing) are applied to all subscribers IP addresses and the key is a subscriber login. Note that the Stingray SG authorizes **each** subscriber IP address: for example, if 10 IP addresses are associated with the subscriber, an Access-Request authorization request will be sent for **each** of the addresses. It is expected that the response to each IP address of a multi-IP subscriber will contain the same set of active services and the same profiles. The response to the authorization of each of the 10 IP-addresses mentioned above will be applied to the subscriber **login**, so all the IP addresses within this login will be assigned the same set of services along with the same policing.

VasExperts-UserName

The subscriber name (login).

This attribute is introduced for some billing systems that aren't able to response with the User-Name attribute within the Access-Accept/Reject response, but are able to response with any VSA attribute.



If both the User-Name and VasExperts attributes are present in response, then the value of VasExperts-UserName will be preferred.

VasExperts-Restrict-User

The attribute to identify the subscriber is blocked.

For the SSG the Access-Accept response means that the subscriber is not blocked, but for blocked subscribers Access-Reject containing special subscriber attributes specifying some restrictions have to be responded. But some implementations of radius clients do not have the ability to return the Access-Reject containing subscriber attributes. For such implementations the VasExperts-Restrict-User attribute is provided :

- value 0 - means that the subscriber is not blocked
- value 1 - means that the subscriber is blocked

In case of the `VasExperts-Restrict-User=1` the SSG handles the Access-Accept as Accept-Reject.

VasExperts-Enable-Interconnect

The attribute indicating enabling/disabling local interconnect for the subscriber.

This attribute corresponds to [L2 BRAS](#). By default, if the local interconnect is enabled, L2 BRAS interconnects any two local subscribers. You can disable interconnect using this attribute: `VasExperts-Enable-Interconnect=0`. So a packet from one local subscriber to another will be dropped if the local interconnect is disabled at least for one of the subscribers.

By default, `VasExperts-Enable-Interconnect=1` and if `bras_terminate_local=1` is set in `fastdpi.conf`, then interconnect is allowed. This attribute can be used to disable interconnect for a specific subscriber by specifying `VasExperts-Enable-Interconnect=0`.

Optional Radius attributes

In addition to the mentioned above VSA attributes the Stingray Service Gateway supports the following standard Radius-attributes within the Access-Accept/Access-Reject. All of them are optional.

Session-Timeout

It specifies the duration of the subscriber authorization, in seconds. At the expiry of this time the SSG will send a second request for Access-Request to authorize.

By default, the session duration is specified in the `fastdpi.conf` using the `auth_expired_timeout` option (in **minutes**).

Acct-Interim-Interval

Specifies the time interval for updating Accounting statistics (in seconds) for the subscriber.

Interim interval is specified by default in the `fastpcrf.conf` using the `radius_acct_interim_interval` option.



Explicitly setting `Acct-Interim-Interval = 0` in the RADIUS response disables sending Interim-Update.

Idle-Timeout

Specifies the interval over which the accounting data is unchanged, when it expires the accounting session is considered to be closed caused by the subscriber inactivity. Idle timeout is set by default by the `fastpcrf.conf` `radius_acct_idle_timeout` option. A way to determine the subscriber inactivity is specified by the `acct_check_idle_mode` option defined in the `fastpcrf.conf`. The description of the parameters can be found in the section [FastPCRF settings](#).

Class

This attribute will be added to all Accounting-Request PDUs if it is set. The SSG does not analyze the value of this attribute.

Access-Reject peculiarities