

Содержание

4 Minimum FastDPI configuration for L3-connected BRAS 3

4 Minimum FastDPI configuration for L3-connected BRAS

Creating a configuration describing the locality of client IP network prefixes

L3-connected BRAS authorizes Users using the FastPCRF component.



Once received the network packet from the previously unknown IP address, the FastDPI will send a request to FastPCRF in order to authorize the User. It makes sense when the User IP address is **local** in relation to the FastDPI.

Address Locality Settings

The locality of the User IP address is defined under the two following **mandatory** conditions:

1. The element of the user IP addresses numbered list should belong to the local Autonomous Systems (AS) list specified in the [aslocal.bin](#) file. It has to be filled with information on private IP addresses ranges being used in the Provider local network. Any number within the 64512 - 65534 range should be used as the Autonomous System (AS) number.
2. The local autonomous system item within the numbered list should be listed in the [asnum.dscp](#) file. You should specify the numbers of local Autonomous Systems (AS) in this file because they will be used in the authorization procedure. Authorization will be performed for all the Autonomous System (AS) IP addresses marked as local in the [asnum.dscp](#) file.

Authorization enabling

An example demonstrating how to enable authorization and specify the list of fastpcrf servers in the fastdpi.conf configuration file is shown below:

```
enable_auth=1
auth_servers=127.0.0.1%lo:29002;192.168.10.5%eth1:29002
```

The format of the single server record looks like this: `ip%dev:port`, here `ip` is the server IP address, `dev` is the local device used to establish a connection, `port` is the tcp port. FastDPI establish connection with first available fastpcrf server from the list.

Enabling of user properties storage

To do so you should add the following entry in the fastdpi.conf configuration file:

```
udr=1
```

Additional authorization options

You can specify the following additional authorization parameters in the `fastdpi.conf` file:

`auth_expired_timeout` - authorization lifetime, in minutes. This parameter will be applied only if there is no `Session-Timeout` attribute in the `Access-Accept` or `Access-Reject` RADIUS responses. It specifies the session lifetime. Once that period expires, a second authorization request will be sent. The default value is 60.



A zero value (unlimited session lifetime) can lead to a situation when the Subscriber who has been denied access (`Access-Reject`), will reside in the "unauthorized" state forever. The subscriber can be withdrawn from this state only by the following ways: using CoA-notification to re-authorize, restarting the FastDPI or using the command line utility `fdpi_ctrl` (manually).

`auth_resend_timeout` - timeout to resend authorization requests to the FastPCRF, in seconds. If FastDPI did not receive a response from the FastPCRF during this time, the authorization request will be repeated. The default value is 60.

`auth_pcrf_reconnect` - timeout for reconnecting to the FastPCRF, seconds. The default value is 1.

Authorization tracing



Authorization tracing significantly decrease the fastDPI performance and quickly consumes disk space. It should only be used during initial solution setup.

`auth_trace` - enables authorization tracing.

Test authorization mode

`auth_trace_ip` - a list of IP addresses to authorize. It can contain at most two IP addresses. It does not have a default value. When configuring, authorization is performed only for the specified IP addresses.



Configuration example:

```
auth_trace_ip=192.168.20.11,192.168.30.58
```

Enabling IPv6 support

To authorize [IPv6 addresses](#) you should enable IPv6 support. Actually, the VAS Experts DPI authorizes

not an individual IPv6 address, but a whole subnet with a given prefix length (default is /64). For example, if there are packets from addresses 2001:1::1 and 2001:1::10, then only one of these addresses will be sent for authorization, and the returned authorization parameters will be applied to all the addresses from the 2001:1::/64 subnet.