

Содержание

Subscriber Activity Monitoring	3
<i>Monitoring Subscriber Activity and Blocking Incoming Traffic Without Terminating the Session</i>	3
Configuration	3
<i>Monitoring Subscriber Activity with Session Termination (Subscriber Host Connectivity Verification)</i>	4
Configuration	4
<i>Subscriber host connectivity verification with session termination (Subscriber Host Connectivity Verification)</i>	4
Configuration	5

Subscriber Activity Monitoring

FastDPI provides two mechanisms for monitoring subscriber activity based on outgoing traffic from the subscriber to the internet:



- Monitoring subscriber activity and blocking incoming traffic without terminating the session. This is a reactive control, performed "after the fact," i.e., when a packet arrives from the internet to the subscriber. If there is no traffic from the internet to the subscriber, there is no control; ARP ping is used to check subscriber activity. This method limits incoming traffic to the subscriber in case of inactivity without terminating the subscriber session.
- Monitoring subscriber activity with session termination (Subscriber Host Connectivity Verification) complements this control with active monitoring of open DHCP sessions and terminates the subscriber session in case of inactivity.

Both algorithms are compatible and can work together.



The activity monitoring mechanisms described here are not applied to PPPoE subscribers. PPPoE contains built-in standard mechanisms for activity checking and session termination due to inactivity.

Monitoring Subscriber Activity and Blocking Incoming Traffic Without Terminating the Session

Subscriber activity monitoring is an L2 BRAS function that blocks traffic from the internet to the subscriber if the subscriber shows no activity (no traffic from the subscriber to the internet). During its operation, L2 BRAS records the time T of the last packet received from the subscriber. Within the $T + \text{bras_subs_activity_timeout}$ activity interval, the subscriber is considered active and all packets from the internet to the subscriber are allowed. If the subscriber becomes inactive, meaning the activity interval has been exceeded since the last packet **from** the subscriber, L2 BRAS drops the incoming traffic.

Additionally, the `bras_subs_activity_ping_timeout` function can be set to ping the subscriber if they become inactive. The ping is performed by sending a unicast ARP request to the subscriber: if a response to the ARP unicast request is received, it updates the last packet reception time from the subscriber, thus considering the subscriber active.

Activity monitoring only works on outgoing subscriber traffic (from the subscriber to the internet). This control can be particularly relevant for subscribers with a static public address.

Configuration

Subscriber activity monitoring is configured with the following parameters in `fastdpi.conf`:

- `bras_subs_activity_timeout` — sets the activity interval in seconds. 0 (default) — disables activity monitoring.
- `bras_subs_activity_ping_timeout` — timeout in seconds for pinging the subscriber with an ARP request. 0 (default) — disables ARP pinging of the subscriber. If the subscriber is inactive, unicast ARP requests will be sent to them every `bras_subs_activity_ping_timeout` seconds.

Monitoring Subscriber Activity with Session Termination (Subscriber Host Connectivity Verification)

SHCV (Subscriber Host Connectivity Verification) monitors the activity of DHCP subscribers similarly to [Nokia](#) by proactively monitoring the state of the subscriber's DHCP session. If there is no traffic from the subscriber to the internet within `bras_dhcp_shcv_interval` seconds, fastDPI starts pinging the subscriber by sending unicast ARP requests on behalf of the subscriber's gateway. The ARP request response wait time is `bras_dhcp_shcv_retry_timeout` seconds. If no response is received to `bras_dhcp_shcv_retry_count` consecutive ARP requests or the ARP response contains a different MAC, the subscriber is considered inactive, and their DHCP session is terminated. Session termination mechanism:

1. Sending Acct Stop;
2. De-announce the subscriber's IP address;
3. Update the session status to "released". The reauthorization time remains unchanged to prevent parasitic L3 authorizations if the subscriber reactivates before the lease time expires and sends anything other than DHCP;
4. Delete the DHCP session (in the DHCP database).

Configuration

All options are hot.

- `bras_dhcp_shcv_interval` — subscriber inactivity interval, seconds.
Default = 0 (SHCV disabled)
- `bras_dhcp_shcv_retry_timeout` — ARP request response wait time, in seconds
Default = 3 seconds.
- `bras_dhcp_shcv_retry_count` — number of ARP requests without response.
Default = 3 requests.
- `bras_shcv_trace` — SHCV tracing.
Default = off.

Subscriber host connectivity verification with session termination (Subscriber Host Connectivity Verification)

Monitoring the activity of a static IP L2 subscriber (a subscriber for whom RADIUS returned the flag `VasExperts-L2-User=1` during L3 authorization).

If there is no traffic from the subscriber for `bras_subs_shcv_interval` seconds, fastDPI starts pinging the subscriber by sending a unicast ARP request on behalf of the subscriber gateway. The wait time for an ARP response is `bras_subs_shcv_retry_timeout` seconds. If no response is received for `bras_subs_shcv_retry_count` consecutive ARP requests, or if the ARP response contains a different MAC, the subscriber is considered inactive, their authorization status is reset, and the accounting session is terminated.

Configuration

All options are hot.

- `bras_subs_shcv_interval` — subscriber inactivity interval, seconds.
Default = 0 (SHCV is disabled).
- `bras_subs_shcv_retry_timeout` — ARP response wait time, seconds.
Default = 3 seconds.
- `bras_subs_shcv_retry_count` — number of ARP requests.
Default = 3 requests.
- `bras_shcv_trace` — SHCV tracing.
Default = off.