

Содержание

Beta-version 14.1	3
<i>Changes in version 14.1 BETA1</i>	<i>3</i>
<i>Changes in version 14.1 BETA2</i>	<i>6</i>
<i>Changes in version 14.1 BETA3</i>	<i>7</i>

Beta-version 14.1

Changes in version 14.1 BETA1

DPI

1. [DPI][ajb_save_vlan] Fixed an issue when the engine runs in read-only mode
2. [DPDK][tap_device] Fixed: setting the tx queue length via the `dpgk_tx_queue_size` option. Previously, the tx queue length of the TAP device was unconditionally set to 256, which VMware VMXNET3 Ethernet Controller complained about: ETHDEV: Invalid value for nb_tx_desc(=256), should be: <= 4096, >= 512, and a product of 1
3. [LAG] Fixed: added load balancing for pass packets
4. [DPI][ip_node stg] Added statistics for bucket occupancy. The new CLI command `stat storage ip4 detail` outputs statistics on bucket filling in the IPv4 node storage
5. [DPI] Added validation for the MULTIPROXY_STRONG protocol
6. [DPI] Improved scalability on 128-core systems
7. [DPI][log] Improved the logging subsystem in cases of log file overflow

BNG

1. [BNG][framed-route] Fixed: Framed-Route propagation when changing the subscriber login. When changing the login, Framed-Route subnets remained attached to the old login, and all services and policing for the Framed-Route subnets were taken from the old login.
2. [BNG] Added the `bras_disable_l3_auth` option — explicit prohibition of L3 auth in L2 BNG mode for all subscribers. For example, only DHCP authorization will work for subscribers with AS local meta. Default value: off (L3 auth is allowed) `bras_disable_l3_auth=off`. This option makes sense only if `enable_auth=1`. The option is incompatible with `bras_dhcp_auth_mix=0`: if `bras_dhcp_auth_mix=0` is set, then `bras_disable_l3_auth` is assumed to be off (L3 auth is allowed) and a warning is printed to the alert log.
3. [BNG] Added a new subscriber flag — prohibit L3 auth for a specific subscriber. This flag can be set/cleared only via CLI: a new parameter `disable_l3_auth=[1:0]` was added to the `subs prop set` command (1 — prohibit L3 auth, 0 — allow). By default, L3 auth is allowed.
4. [BNG][srcIP spoofing] Added filtering by source AS flags on the `subs→inet` path before a packet is accepted for processing, to block outgoing operator-side DDoS with IP spoofing. Added a new `fastdpi.conf` option `ip_filter_source_as_flags (hot)[hot]` — filtering subs traffic by AS. Bitmask of AS (autonomous systems) flags for the source IP from the subs side. Only packets whose source IP AS contains at least one of the listed flags are allowed for processing. Otherwise, the packet is dropped. AS flag values (bit mask):
 - 0 - filtering disabled (default) — `ip_filter_source_as_flags=0x0`
 - 0x0100 - pass
 - 0x0200 - local
 - 0x0400 - peer
 - 0x0800 - term
 - 0x1000 - mark1
 - 0x2000 - mark2
 - 0x4000 - mark3
5. [BNG][PPP] Added database-session utilization statistics to the `ppp show stat` command

6. [BNG][PCEF][Policing] Added configuration of global policing from parameters passed in the VasExperts-Policing-Profile attribute with the BR## prefix
7. [BNG][PCEF][Services] Added configuration of a personal (noname) user profile for services from parameters passed in the VasExperts-Service-Profile attribute with the BP## prefix
8. [BNG][PCEF][rating-group] New options (cold, requires fastDPI restart):

- rating_group_count — number of rating groups, 0 — RG disabled. Default: 0
- rating_group_max_subs — max number of subscribers with RG. Default: 0 (RG disabled)

RG storage is initialized only if billing statistics are enabled. Memory sizing for RG statistics: counter size per one RG = 32 bytes. Total required memory:

```
32 * rating_group_count * rating_group_max_subs * num_thread
```

For example, for 10k subscribers, 256 RG, and 8 processing threads, 625M of memory is required:

```
rating_group_count = 256
rating_group_max_subs = 10000
num_thread = 8
memory_required= 32 * 256 * 10000 * 8 = 625M
```

9. [BNG][PCEF][rating-group][RADIUS Accounting] Output RG statistics in RADIUS Accounting. RG statistics are sent in separate Interim-Update packets. Only non-zero RG data is sent. Due to the 4096-byte RADIUS packet size limitation, RG data can be split into multiple Interim-Update RADIUS packets.

To distinguish the Interim-Update type, it contains an indicator of the data carried inside: the new VSA VasExperts-Acct-Type (id=28, vendor 43823, integer) with values:

- 0: standard Interim Update Accounting
- 1: RG data

Each rating group and its counters are sent in *one* VSA, which contains the following attributes:

- VasExperts-Acct-Rating-Group (new short attribute, 16-bit integer) - RG number;
- VasExperts-Acct-Input-Octets-64
- VasExperts-Acct-Output-Octets-64
- VasExperts-Acct-Input-Packets-64
- VasExperts-Acct-Output-Packets-64

packet/byte counters by direction are output according to the acct_swap_dir option (as in Accounting).

RG transfer specifics:

- RG are optional data and may be absent for a subscriber; accordingly, no RG accounting will be sent for such a subscriber;
- if the RADIUS server does not acknowledge receiving an RG packet, it is not retransmitted — fresh data will be sent in the subscriber's next Interim-Update;
- if a subscriber has RG statistics, then before sending Acct-Stop at session end, the current RG data is sent in Interim-Update packets.

10. [BNG][PCEF][rating-group][CLI] Added: the CLI command `subs traffic stat`. For the specified subscriber, the command outputs billing statistics and rating group statistics, if they are enabled for the subscriber.
11. [BNG][PCEF][rating-group][RADIUS Accept] Added: setting the RG service at authorization. RG statistics accumulation can be enabled only if service 9 (bill stat) is enabled for the specific subscriber. RG is set at the subscriber level during authorization by specifying a special service

9 profile named 'RG':

```
VasExperts-Service-Profile := "9:RG"
```

If service 9 is disabled, RG accumulation is disabled as well.

Examples for service 9 and RG:

```
# service 9 enabled, RG disabled. Standard RADIUS Accounting is sent.  
VasExperts-Enable-Service := "9:on"
```

```
# service 9 enabled, RG enabled. RG data is sent in RADIUS Accounting.  
VasExperts-Service-Profile := "9:RG"
```

```
# service 9 disabled, RG disabled. Standard RADIUS Accounting and RG are not  
sent.  
VasExperts-Enable-Service := "9:off"
```

NAT

1. [CG-NAT] Added `rx_dispatcher=3` — a method with even load balancing across an arbitrary number of threads with NAT 1:1 support requiring assignment of specific addresses.
2. [CG-NAT] Accounting for translation lifetime in the `fdpi_ctrl list status --service 11 --login UserName (--ip IP)` command. Additional fields were added to the output:
`active_sess_tcp` — number of active NAT translations for TCP and `active_sess_udp` — number of active NAT translations for UDP.
Translation activity is determined by the time it was last used and by the lifetime parameter configured in the cluster options.
3. [CG-NAT][CLI] Accounting for translation lifetime in the `nat show <internal_ip> [<lifetime>]` command. Outputs a list of all NAT translations for the specified private IP. A translation record looks like:
 - `nat_type` - NAT type (0 - CGNAT, 1 - NAT 1:1),
 - `protocol` - L4 protocol (0 - TCP, 1 - UDP),
 - `internal_ip` - private IP,
 - `internal_port` - private port,
 - `dest_ip` - destination IP,
 - `dest_port` - destination port,
 - `external_ip` - public IP,
 - `external_port` - public port,
 - `active` - translation activity flag (true if active)Translation activity is determined by the time it was last used and by the lifetime parameter configured in the cluster options. If `<lifetime>` (in seconds) is specified, its value is used as the translation lifetime.
4. [NAT][CLI] Output translations for a client by private IP using `nat show`

CLI

1. [CLI] Added the subs `bind show` command to view the list of IP addresses bound to the login `<login>`:

```
subs bind show <login> [memory|udr]
```

Two modes:

- memory (default) outputs the IP-to-login binding as it is currently configured in fastDPI.
 - udr — outputs the IP-to-login binding from UDR
- The output of these two modes may differ: not all IP↔login bindings are stored in UDR; for example, for Framed-Route subnets, the login binding is created only in memory, while the Framed-Route subnets themselves are stored in UDR in a separate table, see the CLI command group `cli framed route ?`

2. [CLI] Added: the CLI command `stat http`. This command outputs internal statistics similar to the output in `fastdpi_stat.log`:
 - Detailed statistics on HTTP
 - Detailed statistics on SSL_SAVEBL
 - Detailed statistics on QUIC_IETF_SAVEBL
 - Detailed statistics on BitTorrent

IPFIX

1. [IPFIX] Storing TTL information from the IP packet header. [Description](#)
Added to Full NetFlow statistics in IPFIX format:
 - Packet TTL, id 192. The field is used for both directions: `subs2inet` and `inet2subs`
 - Rating group, id 2020

Utilities

1. [utils] Added the `name2custom` utility to view the list of protocols loaded from the cloud (as opposed to built-in ones)

Changes in version 14.1 BETA2

IPFIX

1. [IPFIX] Fixed an issue with converting time to unix format

BNG

1. [BNG][SHCV][hot] Added activity control for a static IP L2 subscriber (a subscriber for whom, during L3 authorization, RADIUS returned the flag `VasExperts-L2-User=1`).
New options (all hot):
 - `bras_subs_shcv_interval` — inactivity interval, seconds; 0 - SHCV disabled.
 - `bras_subs_shcv_retry_timeout` — ARP request response wait time, seconds; default = 3 seconds.
 - `bras_subs_shcv_retry_count` — number of ARP requests; default = 3.
 - `bras_shcv_trace` — SHCV tracing; default = off.

If there is no traffic from the subscriber for `bras_subshcv_interval` seconds, fastDPI starts pinging the subscriber by sending a unicast ARP request on behalf of the subscriber gateway. Waiting for an ARP reply is `bras_subshcv_retry_timeout` seconds. If no reply is received for `bras_subshcv_retry_count` consecutive ARP requests, or the ARP reply contains a different MAC, the subscriber is considered inactive, their authorization status is reset, and the accounting session is stopped.

2. [BNG][DHCP][hot] New values 2 and 4 are now available for the `bras_dhcp_check_secondary_keys` option. Full option description:

`bras_dhcp_check_secondary_keys` — control of secondary unique keys (opt82/QinQ) [hot]
In DHCP, the primary keys are ClientId (opt61) or, if ClientId is not specified, the client MAC address. In secondary key control mode, if another DHCP session is found by at least one secondary key, it will be closed (Acct Stop is sent)

- 0 (default) — do not control secondary keys.
- 1 — control all secondary keys — QinQ and opt82
- 2 — control opt82 only
- 4 — control QinQ only

RADIUS

1. [FastRADIUS] Added support for logging to syslog. New parameter `syslog_level` in `fdpi_radius.conf` — the log level for writing messages from the alert log to syslog. 0 — syslog logging is disabled (default).

Changes in version 14.1 BETA3

1. [DPI][tethering] Added tethering detection. Parameter `tethering_ttl_allowed = 128:64` [hot] defines the list of allowed TTL values for subscriber traffic that are not considered tethering. Values are listed separated by ':'. Up to 256 values (0-255). [Description](#)
2. [IPFIX] Added new 64-bit fields to Full NetFlow IPFIX. [Description](#)
`service_flags` - information about tags assigned to a flow in DPI. Detected tethering is reported in IPFIX in bit 1 of the `service_flags` field. 63 bits are available for future use.
`detection_flags` - reserved for the detection method.
`action_flags` - reserved to indicate what actions were applied to the flow.
3. [IPFIX] Fixed TTL export in Full NetFlow IPFIX in a single field with identifier 192 depending on direction. [Description](#)