Table of Contents

Version 13.0 Congo

13.0 Congo [1)]

You can check the current installed version with the command:

```
yum info fastdpi
```

Rollback to 12.4:

```
yum downgrade fastdpi-12.4-0 fastpcrf-12.4-0
```

After an update or version change, a restart of the service is required:

```
service fastdpi restart
```

If PCRF and/or Radius are used, they should also be restarted. The following order is preferred for restarting PCRF:

```
service fastdpi stop
service fastpcrf restart
service fastdpi start
```

Do not perform Linux kernel upgrades. Newer versions of the kernel may break binary compatibility with the Kernel ABI and the network driver will not load after the upgrade. If you do upgrade, set the GRUB boot loader to load the previous version of the kernel: set the `default=1` parameter in the `/etc/grub.conf` file while the problem is being resolved.

If the update displays a message that the update was not found or there are dependency issues, run the command before updating:

```
yum clean all
```

Changes in version 13.0

DPI

1. On-stick support for LAG/LACP. Description
2. Transition to DPDK 23.11
3. Modified: for QUIC and QUIC_IETF: if no SNI is detected - check by AS
4. Modified: when analyzing STUN, AS from Facebook is checked - define FACEBOOK_VIDEO, not WHATSAPP_VOICE
5. Setting RSS hash flags for UDP and TCP
6. Modified: openvpn protocol definition
7. Fixed: SIGHUP processing only if fastDPI is fully initialized. Possible crash if SIGHUP is received

during fastDPI startup process
8. Trace/debug packet recording moved to new API
9. Added: wechat protocol support for UDP
10. Support for additional markup of autonomous systems `mark1`, `mark2`, `mark3`. Description
11. Prioritize SNI detection in custom signatures for autonomous systems marked as `mark1`. Description
12. Prioritize more specific custom SNI signatures.
Example: for host `a.b.c.d`, if the signatures `*.d`, `*.c.d` and `*.b.c.d` are present, the protocol defined by the signature `*.b.c.d` will be selected works only for signatures with `*`. Description
13. Support for hard locks (despite hostname/SNI) - set in an additional field in the address blacklist, example: `1.1.1.1 443 hard`. Description
14. Improved detection of YOUTUBE, SIGNAL
15. Added the DPITUNNEL protocol, which includes traffic anomalies commonly used for DPI traversal
16. Updating dpiutils
17. New protocols VK_CDN_VIDEO, META_CHAT
18. Improved signatures of FACEBOOK_VIDEO, META_CALLS protocols
19. Fixed protocol name VK_CDN_VIDEO
20. Fixed: SNI decoding in QUIC IETF and possibility of crusting in exceptional cases
21. Fixed: clearing search structures when deleting CUSTOM protocols
22. Added ability to add comments (#) and blank lines in input files for utilities lst2dscp, lst2tbf
23. Added protocols QUIC_UNKNOWN - QUIC without SNI and QUIC_UNKNOWN_MARKED - QUIC without SNI and AS labeled MARK2. Description
24. Fixed: stun character definition for TCP
25. Modified: if the stun packet viewing limit is reached - set this protocol with AS in mind
26. Updated utilities to support new protocols
27. Improvements in QUIC_UNKNOWN, QUIC_UNKNOWN_MARKED, SIGNAL, DpiTunnel protocols
28. SNI/HOST embedded protocol definitions are cloud-based, SNI/IP prioritization is supported
29. Modified: SNI comparison is case-insensitive
30. Added LANTERN_WEAK protocol signature
31. Improved IMAP protocol recognition
32. Corrects LPM when selecting channel by IP/CIDR
33. Added: to DNS text file record format - format vchnl - virtual channel number.
34. Added: to the IPFIX data transfer template for DNS channel number. Description
35. Fixed: crash on DNS trace
36. Improved VIBER_VSTREAMS protocol definition
37. Fixed: fastDPI does not accept or process any ctl requests during fastDPI stop process
38. Added SSTP protocol (49296)
39. Added ANYDESK protocol (54273)
40. LANTERN recognition improved

BRAS

1. Added: accounting of DHCP packets from subscriber in billing statistics: subscriber CPE (i.e. Wi-Fi router) without clients (e.g. at night) - sends only license renewal requests. Since these requests were intercepted by BRAS and were not included in the accounting, the session was terminated by idle timeout
2. Corrected: actions when QinQ/VLAN is changed for a subscriber

3. Fixed: `framed-pool renew`
   In some cases, incorrect DHCP responses were generated. Added trace to DHCP packets log for `framed-pool renew`.
4. Fixed: receiving packets from relay. Previously it was checked that relay was on the fc::/7 network. Now this check is unnecessary and has been removed - relay can have any address.
5. Fixed: DHCPv6 options parsing from Radius
6. The `subs prop show active` command has been added. The command outputs a dump of L2 properties of all active (not-expired) subscribers. Description
7. Modified: Prohibit calling CLI commands while stopped
8. Fixed: idle-timeout for session. For PPPoE sessions idle timeout should be taken from the `bras_ppp_idle_timeout` setting if not explicitly set in the authorization response (Idle-Timeout attribute).
9. Added priority forwarding with DSCP translation. Description
10. Corrected: Adding unnecessary option 61 (Client-Id) to fastDPI response when distributing address from Framed-Pool
11. Fixed: Logging of DHCP server IP addresses
12. Fixed: Enabling services with profiles. The `VasExperts-Service-Profile` attribute (service profile name, implicitly enables the service) has higher priority than `VasExperts-Enable-Service` (enabling/disabling a service without specifying a profile).
13. Added `ping inet` command on behalf of subscribers through the entire BRAS/NAT/ROUTER processing chain. The prompt is `fdpi_cli ping inet ?`. Description
14. Fixed: call of subscriber IP address deanounce when acct idle. Added new flag to router option `router_subs_announce`: `0x10000` - deanounce L3 subscriber at acct idle (closing acct session by idle timeout). Description
15. Added support for specifying the profile of service 18 during authorization. Enabling service 18 in the Access-Accept Radius response is set in the usual way for a service with a mandatory profile (here `serv18` is the profile name):

    ```
    VasExperts-Service-Profile = "18:serv18"
    ```

16. A search by MAC and `subs_id` has been added to the `subs prop show` command. The result of a search by MAC or `subs_id` can be multi-valued - several different entries for the same MAC/`subs_id`. The result of the `subs prop show active` command has been changed, which may be critical when parsing the command's json wiggle. Description
17. Fixed: setting link up/down flag for ports that do not support link up/down interrupts (e.g. af_packet)
18. The return code of the uptime command. The CLI command `uptime` can be used to check if fastDPI is fully started: it returns `result=0` (Success) only when fastDPI is fully initialized and all worker threads are started. Upon receiving a response from fastDPI to the `fdpi_cli uptime` command, the fdpi_cli utility itself checks the result of the execution and if `result!=0` - sets a non-zero return code.
19. Corrected: If VRF (service 254) was present in Access-Accept, the packet was incorrectly logged as invalid.
20. Restoring UDR operation after calling a command with a large number of parameters

NAT

1. Added a `checknat` utility to check the distribution of white addresses. Description
2. Fixed online change of `nat_private_cidr` parameter

Load Balancer

1. Added L2 traffic balancer mode. This enhancement allows to use SSG as a traffic balancer based on IP addresses owned by AS and defined as `local` in `asnum.dscp`. Description
2. Added mqrx_lb_engine, which is activated when dpdk_engine=2. Description

Router

1. Mempool allocation for emit packets: we do not allow the pool to be completely exhausted, there should be at least 256 free elements in the pool
2. The error of route deletion `errno=3` (No record found) has been moved to TRACE to avoid clogging the log
3. Fixed the order of router components termination
4. Changed: system error when clearing route tables. Cleaning of route tables (deleting all entries added by SSG) is done at stop and start of fastDPI. During cleaning process EBUSY error may occur, which is fatal for netlink socket, socket should be closed.
5. Fixed: TAP link down in LAG. If a port enters a lag, TAP this port to Link down state only when ALL LAG ports are down.
6. Fixed: control of selfgen mempool exhaustion
7. Optimization of data readout from TAP
8. Fixed LAG+On-stick: put TAP in link down state. TAP is set to link down only when all ports in LAG are in down state. If there is at least one port in Up state - TAP should be in Link Up state.
9. Corrected: Traffic diversion in router for on-stick device in LAG. When forming VRF topology, it was not taken into account that the LAG includes the base (physical) device, and the on-stick (virtual) device is specified in the router description.
10. Fixed: Read all data from TAP device. At fastDPI startup there were possible situations when router is not fully initialized yet and TAP is already monitored but not read out.
11. The router_subs_announce option is made hot (hot)
12. Fixed: mbuf leak on fastDPI startup

SDS

1. The `storage_tag` value is set based on directional priority or protocol priority

Radius

1. Added the ability to work with standard linux interfaces using `libpcap`. Description

Changes in Version 13.1

Warning! An error has been detected in version 13.1. PPPoE sessions do not close when `idle_timeout` expires.
The fix is planned for the next release.

DPI

1. Global code refactoring - discontinued support for `pf_ring`
2. Added: service 19 - DNS response substitution. Description
3. Modified: minimum PCAP file size to 100 MB. PCAP file rotation on reload Description
4. Modified: improved DROP event tracing
5. Fixed: erroneous ERROR level message appearing for certain `fdpi_ctrl` requests
6. Fixed: incorrect TLS (SNI) parsing when multiple 'ALPN Protocols' are specified
7. Modified: mechanism for updating AS and IP compliance lists. Description

BRAS

1. Fixed: subscriber activity control via unicast ARP Request. Previously, it was a broadcast ARP Request, which is not optimal for the network. Description
2. Added: SHCV (Subscriber Host Connectivity Verification) — DHCP subscriber activity control. Considered scenario for an already "closed" record to prevent repeated SHCV trigger and increase in the 'SHCV: session closed by inactivity' counter. Description
3. Added: ARP Proxy for known routes (router mode only). This feature is applied only if the ARP request initiator is a known subscriber. A new flag - 0x0004 has been added to the `bras_arp_proxy` option. Description
4. Fixed: help() for IPv6 addresses in the `subs prop show` command
5. Fixed: error in parsing parameters for the `subs prop del` command, which resulted in the inability to delete properties by IP with the error

   ```
   ERROR: Result code=9: No subscriber IP address
   ```

6. Added: CLI command `dhcp disconnect`. This is a CLI analog of CoA Disconnect. The disconnect mode is set by the `bras_dhcp_disconnect` option.
   1. `dhcp disconnect all` - disconnect all DHCP sessions
   2. `dhcp disconnect [ mac=X | ip=X ]` - disconnect specified session
7. Fixed: sending L3 reauth for L2 subscriber in advance, not waiting for session timeout
8. Added: number of sessions closed due to inactivity (SHCV) in the `dhcp show stat` CLI command
9. Fixed: error in intercepting and processing ICMPv6 packets, checksum not recalculated in some cases when modifying ICMPv6 packet

NAT

1. Modified: tracing in `vdpi_new_flow_nat_ipv4` is always output
2. Fixed: based on the value of `nat_exclude_private`, additionally checking the pair CHECK_AS_LOCAL or CHECK_AS_PEER for AS in local interconnect

Router

1. Added: ARP management. Description
2. Fixed: port selection for recording in a pass-through LAG. If LAG passes through fastDPI, port selection for recording from TAP should consider the Link Up/Down state of both bridge sides of the port

3. Fixed: announcing NAT profile subnets upon addition
4. Added: CLI command `router vrf dump`. The command outputs the list of VRFs set in the system and their properties
5. Fixed: do not consider term by AS when announcing NAT subnets. The `term_by_AS` mode applies to subscribers, not to NAT profiles, hence it should **not** be considered when announcing a NAT subnet
6. Fixed: order of packet interception from the general processing pipeline
7. Fixed: increased number of `mbuf` in `selfgen mempool` if router enabled: if router disabled: `mempool size=512 * number_of_slaves_in_cluster`, if router enabled: `mempool size=8 * 1024 * number_of_slaves_in_cluster`

LAG

1. Fixed: zeroing the array when building a new list of active ports. The error leads to array overflow and memory corruption
2. Added: logging of the "no mbuf" error when sending LACP

Changes in version 13.2

1. [BRAS][PPPoE] Fixed: ping of inactive client via Echo requests
2. Added: support for service profile 19 (DNS response substitution). For service 19, it is possible to specify AAAA records and use * for domains. Description
3. Fixed: service profile 18 no longer requires setting both DSCP and TBF simultaneously. Description
4. Fixed: IP:PORT takes priority over IP and CIDR for custom protocol definitions. Description
5. Changed: user-defined protocol priority is now higher than cloud-defined ones. Description
6. Fixed: AAAA record length in service 19
7. Added: `block_options` parameter, mask 8 — do not generate RST packets for blocking and redirection for direction inet→subs. Description
8. [DPI] Improved: analysis of out-of-order packets (now you can set number of buffers for out-of-order handling), decryption of fragmented QUIC. Also eliminated buffer exhaustion for out-of-order packets. Description
9. [DPI] Fixed: DOT recognition
10. [CTRL] Added: new output format for policing. Description

```
fdpi_ctrl list profile --policing --profile.name htb_6 --outformat=json2
```

11. [CTRL] Added: loading policing profiles with the new format (includes value and unit). Description
12. [BRAS][IPv6] Added: when client sends DHCPv6 confirm and session is absent in BRAS DB, reply with `NotOnLink` status
13. [FastPCRF][DHCPv6] Fixed: issue that caused current IPv6 accounting session to close and reopen when handling client's DHCPv6 lease renew requests
14. [DPI] Added: update of `asnum.bin` from the cloud, `asnum_download` parameter matches `federal_black_list` in values. Description
15. Added: `mem_ssl_savebl` parameter (cold). Sets number of saved buffers for SSL packet parsing. Description
16. Added: statistics for SSL parsing buffer usage. Description

17. [BRAS][DHCPv6] Added: ability to extract option 37 and option 38 from client packet
18. [Router][tap] Fixed: bridge status initialization at fastDPI start. TAP device for LAG passthrough is Up if at least one LAG port is Up and its peer bridge port is also Up. Previously bridge status was determined only on link Up/Down events. This patch initializes bridge status at router start based on port states.
19. [BRAS] Fixed: allow local interconnect only if srcIP belongs to a known subscriber. Previously, srcIP was not verified, which could allow IP spoofing and local DDoS with forged subscriber IPs.
20. Added: CLI command `permit`.
21. [CLI][Ping] Changed: error message when subs IP not found
22. [CLI] Added: boolean flag `on_stick` in JSON output of `dev xstat` command
23. [CLI] Changed: JSON output of `dev info` for on-stick devices.
    Previously:

    ```
    "pci_address": "on-stick based on 82:00.3"
    ```

    Now:

    ```
        // base device address
        "pci_address": "82:00.3"
        // on-stick flag
        "on-stick": "true|false"
    ```

24. Removed fake Yandex SNI from TELEGRAM_TLS
25. Added: `mem_quic_ietf_savebl` parameter. Sets number of buffers for parsing `quic_ietf` requests (multi-packet). Default is 15% of `mem_ssl_parsers`. Description
26. [DPI] Added protocols

    ```
    "HLS VIDEO"              49298
    "ICMP TUNNEL"            49299
    "DNS TUNNEL"         49300
    "FORTICLIENT_VPN"        49301
    "CISCO_ANYCONNECT_VPN"   49302
    "SHADOWSOCKS_VPN"        49303
    "NOT_DNS"                49304
    ```

27. Added: support for sending DNS query over IPFIX
28. [DPDK] Added read-only engines: RSS and port dispatcher
29. [BRAS][SHCV] Fixed: SHCV was called before pipeline fully started, which could happen in multi-port configs with long pipeline init time
30. [DPDK] Added mempool type output on fastDPI start
31. [Router] Added TAP device statistics to CLI command `router vrf show` — number of packets/bytes read from TAP, written to port, transmitted to TAP, number of events and errors
32. [Router] Changed: packets from TAP now use same thread for 5 seconds to reduce reordering under high load
33. [DPI] Improved detection of DNS TUNNEL, CISCO_ANYCONNECT_VPN, SHADOWSOCKS_VPN, DPITUNNEL, FORTICLIENT_VPN
34. Changed log level for telemetry requests to INFO regardless of outcome
35. [fastPCRF][ACCT] Fixed: Interim-Update sent properly when switching to backup RADIUS server
36. [BRAS][CLI] Fixed: subscribers closed via SHCV are no longer shown by `fdpi_cli subs prop show active`
37. [BRAS][Auth] Optimized service attach/detach

38. [FastRadius] Config file parsing migrated to new engine
39. [BRAS][DHCP] Offer now sent first to bcast 255.255.255.255
40. [BRAS][CLI] Fixed: `dhcp show stat vrf` supported only in Radius proxy mode (previously crashed in DHCP Relay mode)
41. [DPI] Improved recognition of DNS Tunnel and Shadowsocks
42. [Utils] Improved tools. `checkproto`: if IP and SNI are set, result will reflect MARK1 and priority. `ascheckip`: shows DSCP and MARK1
43. [Utils] Added support for hostnames ending with `:` in url2norm — allows "any port" for HTTP
44. [CLI] Fixed: `dhcp disconnect` command
45. [DPI] Fixed: allow protocol change via CUSTOM SNI even after builtin signature match
46. [DPI] Added integrity check for AS list file from cloud
47. [DPI] Fixed loading of black and white lists from cloud
48. [utils] Added support for new formats in bin2ip for converting black/white lists
49. Fixed potential core crash
50. Support for 128-core CPUs Description

Changes in version 13.3

1. [DPI] Added protocols:

```
BIGOTV          49305
SAYHI_CALL      49306
AZARLIVE        49307
LINE_CALL       49308
QQ_CALL         49309
VYKE_CALL       49310
VEEGO_STREAMS   49311
BHABI_CAM       49312
WEPARTY         49313
```

2. [DPI] Improved Viber recognition
3. [DPI] Reduced false positives for DPI TUNNEL
4. [DPI] Increased packet inspection depth for BIGOTV detection
5. [DPI] Changed FACETIME protocol
6. [DPI] Changed: if protocol is matched by ip/sni/cname, it is no longer overridden by built-in signatures
7. [DPI] Streamlined protocol priority enforcement to avoid unnecessary switching
8. [DPI] Fixed: searching both '*' and ':' in HTTP domains
9. [DPI] Fixed: virtual channel IP removal on reload
10. [DPI] Fixed: drop ignored when `smartdrop` is set during SSL parsing errors
11. [BRAS][PPP] Fixed: `bras_pppoe_trace_mac` now respected for DHCPv6 packets in pcap. Previously only `bras_dhcp_trace_mac` was used
12. [DPI] Fixed: errors assigning vchannel by IP/CIDR
13. [DPI] Fixed: blocking by IP for DNS over TCP
14. [DPI][PCRF] Changed log level from INFO to WARNING for start/stop messages
15. [DPI Utils] Fixed: `checkproto` when IP protocol is Unknown
16. [Utils] Fixed: `checkproto` now respects MARK1 and port presence. `checkproto 8.8.8.8 443 www.google.com` vs `checkproto 8.8.8.8 www.google.com` may give different results
17. [Utils] `bin2as` now accepts multiple input files

18. [Utils] `ascheckip` supports group checks from `stdin`
19. [Utils] `bgp2bin` is a `as2bin`-like tool but:
    - only accepts /24 and larger subnets
    - supports IP1-IP2 range as in RIPE records
    - later entries take precedence
    - output is slightly larger than `as2bin` but contains no overlapping ranges
20. [BRAS] L3-auth improvements:
    - On Reject for IP bound to multi-bind login: first unbind IP, then assign services (whitelist, policing)
    - On successful Access-Accept with a login for unbound IP: unbind all services before linking IP with new login
21. [BRAS][PPP] Fixed: mixed dual-stack where one address is specified, the other via framed-pool
22. [BRAS][PPP] Fixed: silently drop broadcast packets
23. [PCRF] Added syslog support. New param `syslog_level` in fastpcrf.conf — controls alert log to syslog. `0` disables (default)
24. Added: hot param `smartdrop = 1` — if drop set for protocol, it's delayed until TLS is parsed or error occurs
25. Fixed: adding HTTP domains ending with ':' (port number)
26. Changed: ASNUM path from VAS Cloud (cloud.vasexperts.ru)
27. Blocking by blacklist in GTP tunnel (with `detect_gtp_tunnel` enabled)
28. Fixed: https blocking with `hard` option
29. IPv6 AS reload support
30. Initial alert log to syslog support. Enable with `syslog_level=7`. Default is off. Notes:
    1. rsyslog replaces tab/newline with codes. To disable, add in `/etc/rsyslog.d/fastdpi.conf`:

       ```
       global(parser.escapeControlCharactersOnReceive="off")
       ```

       or use `journalctl`. Example:

       ```
       journalctl -t fastdpi -p 4 --since "1 hour ago" -o verbose --output-fields PRIORITY,MESSAGE
       ```

    2. Logs can be forwarded remotely. Example from `/etc/rsyslog.conf`:
        1. on fastdpi server:

           ```
           *.*  action(type="omfwd" target="192.0.0.1" port="10514" protocol="tcp"
                       action.resumeRetryCount="100"
                       queue.type="linkedList" queue.size="10000")
           ```

        2. on remote server:

           ```
           input(type="imptcp" port="10514"
                 ruleset="writeRemoteData")
           ruleset(name="writeRemoteData"
                   queue.type="fixedArray"
                   queue.size="250000"
                   queue.dequeueBatchSize="4096"
                   queue.workerThreads="4"
                   queue.workerThreadMinimumMessages="60000"
                  ) {
           ```

```
    action(type="omfile" file="/var/log/fastdpi.log"
           ioBufferSize="64k" flushOnTXEnd="off"
           asyncWriting="on")
```

1) Cradle of mankind: humans have lived here for over 50,000 years