Содержание

Версия 14.0 Shooting Stars 3
Изменения в версии 14.0 3
Изменения в версии 14.1 6

Версия 14.0 Shooting Stars

В память о коллегах, которые внесли огромный вклад в развитие компании и ее продуктов и навсегда останутся в нашей памяти

Изменения в версии 14.0

DPI

1. [DPI] Переход на DPDK 24.11, поддержка новых сетевых карт (Intel E830 200G, Intel E610, Napatech SmartNIC). Описание
2. [DPI] Добавлены новые протоколы: AGORA_STREAMS(49314), AZAR_CALL(49315), WECHAT_CALL(49316), TEAMS_CALL(49317). Список протоколов
3. [DPI] Улучшена поддержка протоколов LINE_CALL, VYKE_CALL. Список протоколов
4. [DPI] Исправлена работа smartdrop
5. [DPI] Добавлена валидация для сложносоставных протоколов. Список протоколов
6. [DPDK] Максимальное число диспетчеров увеличено до 32. Описание
7. [DPI] Добавлены облачные протоколы с идентификаторами 55296..58367
8. [DPI] Добавлен протокол DOQ 49318 (DNS-over-QUIC)
9. [DPDK] Добавлен `dpdk_engine=6` (`mqrx-bridge`) — количество RSS диспетчеров на мост. Описание
10. [DPDK] Удалены выделенные mempool. Опция fastdpi.conf `dpdk_emit_mempool_size` объявлена устаревшей и более не используется.
11. [DPI] Понижен приоритет определения `telegram_tls`
12. [DPI] Улучшено детектирование `WECHAT` и `WECHAT_CALL`
13. [DPI] Добавлен протокол FakeTLS (49319) с валидацией
14. [VLAN-Rule] Перенос данных vlan group из UDR в SDR. Глобальные правила для vlan drop/pass/hide/permit, заданные прежней CLI-командой `vlan group`, сконвертированы и перенесены из UDR в SDR с удалением из UDR. Описание
15. До 14 версии используется только одна встроенная база данных UDR (User Data Repository) предназначена для постоянного хранения данных об услугах, полисингах и других настройках FastDPI.
    С 14 Версии вводится разделение UDR на UDR и SDR. Разделение происходит автоматически при обновлении версии.
    SDR (System Data Repository) предназначена для хранения настроек FastDPI, не связанных с абонентами. Можно считать, что SDR является продолжением fastdpi.conf. Никакой специальной активации SDR не требуется — необходимые .mdb-файлы создаются автоматически при включении соответствующего режима в fastdpi.conf.
16. [VLAN] VLAN rules — добавлены CLI-команды. Описание
17. [VRRP] Исправлено: корректная обработка изменения опции `vrrp_enable`
18. [SNMP] Создан модуль мониторинга компонентов системы по SNMP
19. [IPv6] Добавлена возможность определения направления в комбинированном трафике (IN+OUT в одном порту) на основе признака local для IP-адресов. Включается опцией `combined_io_direction_mode`
20. [VLAN-Rule] Добавлена поддержка 'any' вместо '*' при описании диапазона VLAN. Описание
21. [DPI][LOG] Сообщение о нехватке ssl парсеров пишется в slave лог не на каждое событие,

а с периодичностью 1/50000
22. [DPI] Добавлены протоколы ZALO_CALL(49320) and VK_CALL(49321)
23. [DPI] Исправлена работа блокировки в режиме hard для SSL
24. [DNS] Добавлена возможность подстановки/блокировки/отброса DNS запросов A, AAAA, MX, HTTPS. Описание
25. [DPI] Добавлен протокол BIGO_CDN(49324)
26. [DPI] Добавлена поддержка UDP для BIGOTV
27. [DPDK] Удаление устаревших настроек rx channels и связанных с ними проверок
28. [PCAP] Добавлена возможность сохранять трафик заданного vlan с помощью параметра `ajb_save_vlan`. Описание

BRAS

1. [BRAS] Поддержка DHCP-Dual. Описание
2. [BRAS] Поддержка терминации L2TP. Описание
3. [BRAS][PPP] Ключ PPP-сессий сделан составным: `l2subs_id` + `tunnel-IP`. Для PPPoE-сессий туннельного IP нет (`tunnel-IP=0`). CLI-команды, принимающие в качестве ключа `subs_id` (`subs prop show`, `l2tp show session`, `l2tp term` и пр.) теперь могут возвратить несколько записей с одинаковым `l2subs_id`. Описание
4. [BRAS][subs_grooming] Исправлено: возможное падение из-за гонки при остановке fastDPI
5. [BRAS][DHCP] Исправлено: падение при разборе ответа Framed-Pool Renew, если в ответе нет DHCP опций
6. [BRAS] Исправлена совместимость с прежним форматом 18 услуги, где было меньше протоколов и оба поля в профиле нужно было заполнять
7. [BRAS][Framed-Route] Исправлено: возможная корка при освобождении памяти
8. [BRAS] Рефакторинг связи с PCRF: в новой реализации все подключения равнозначны, ошибка на любом из них приводит к переподключению всех соединений и переходу на другой PCRF. Добавлены CLI-команды:
   1. `pcrf connect show` — вывод текущего состояния и накопленной статистики по соединениям с PCRF.
   2. Принудительное подключение к указанному PCRF `pcrf connect switch [<pcrf_index>]`, где `<pcrf_indxed>` — индекс строки соединения в параметре `auth_server`. Если `<pcrf_indxed>` не указан — полагается равным 0. Описание
9. [PCRF][PPP][Framed-pool] Добавлено: в DHCP-опцию `Client-Id` включается также `tunnel-IP` как часть идентификатора абонента. Подробнее в разделах Поддержка IPv4-пулов и Поддержка IPv6-пулов
10. [PCRF][Acct] Исправлено: отключение отправки Interim-Update. Явное задание `Acct-Interim-Interval = 0` в ответе Радиуса должно отключать отправку Interim-Update. Подробнее в разделах acct-interim-interval, PPPoE Radius Access-Request
11. [PCRF] Добавлена поддержка задания услуги 19 "Подмена DNS", профиль обязателен. Описание
12. [BRAS][DHCP] Изменено: алгоритм скользящего окна для rate limit
13. [BRAS] Исправлено: ошибка при сравнении времени при загрузке ip_prop из UDR
14. [Acct] Добавлен атрибут `VASExperts-Service-Type`. Radius acct start/interim/stop в атрибуте `VASExperts-Service-Type` передается тип авторизации. Описание
15. [PCRF][L2TP] Исправлено: атрибуты NAS для L2TP при авторизации
16. [BRAS][L2TP] Исправлено: data race при закрытии сессии
17. [BRAS][L2TP] Исправлено: data race при создании туннеля
18. [BRAS][L2TP] Исправлено: поле длины в заголовке L2TP для data-пакетов. Согласно RFC, в

data-пакетах поле len L2TP-заголовка является опциональным. Некоторые реализации client L2TP не понимают data-пакеты с полем len в L2TP-заголовке. Это исправление корректирует поведение FastDPI: если data-пакеты от абонента приходят без поля len, то и CKAT будет посылать data-пакеты без этого поля. Если же data-пакеты от абонента содержат поле len, CKAT также будет его включать.

19. [BRAS] Исправлено: отправка команд из `pending_queue`. В некоторых случаях (например, при переходе состояний pcrf-монитора `initial → connected`) не вызывалась отправка команд из `pending_queue`, что приводило к "зависанию" команды в очереди на неопределенное время (до переподключения в результате ошибки сокета).

CLI

1. [VASE_CLI] Создан универсальный CLI для управления DPI, BRAS, DHCP(KEA), ROUTER(BIRD) с поддержкой авторизации и логгирования команд в TACACS (требуется VEOS 8.x). Описание
2. [CLI] Добавлена поддержка `subs_id` в команды `dhcp show`, `dhcp reauth`, `dhcp6 show`, `dhcp6 reauth` и `dhcp disconnect`. Описание
3. В CLI-команду `dev info` добавлено имя LAG, в который входит порт. Описание
4. [CLI] Добавлены команды вывода свойств и статистики mempool

   ```
   hal mempool props
   hal mempool stat
   ```

   Для вывода статистики mempool требуется сборка DPDK с включенным сбором статистики

5. [CLI] Добавлено: команда `stat flow ip6` вывода статистики по IPv6 flow. Описание
6. [CLI] Добавлено: команда `stat flow ip4` вывода статистики по IPv4 flow. Аналог вывода в `fastdpi_stat.log`. Описание
7. [CLI] Добавлена команда `stat netflow`. Вывод общей статистики по Netflow/IPFIX (то же, что выводится в `fastdpi_stat.log` в разделе "Statistics on NFLW_export"). Описание
8. [CLI] Добавлена команда `stat firewall`. Описание

IPFIX

1. [IPFIX/Neflow] Добавлена возможность изменения параметров IPFIX/Netflow без перезагрузки fastDPI с помощью параметра `ipfix_reserved`. Описание
2. [IPFIX] Добавлена агрегация сообщений для IPFIX потоков FullFlow/DNS/META/NAT
3. [IPFIX] Добавлен параметр `ipfix_mtu_limit`, ограничивающий для udp-пакетов IPFIX максимальный размер передаваемого сообщения. Подробнее: Настройка экспорта Clickstream, Настройка экспорта Full NetFlow в формате IPFIX
4. [IPFIX DNS] В IPFIX DNS добавлены новые элементы 224 (ipTotalLength) и 43823:3206 (DNS transaction id). Описание
5. [IPFIX] Исправлены ошибки реинициализации IPFIX экспортеров
6. [IPFIX DNS] Добавлена возможность отправки DNS MX ответов по IPFIX. Включается путем установки 3 бита (4) параметра `ajb_save_dns`. Описание
7. [IPFIX] Исправлена ошибка формирования ExportTime в IPFIX Fullflow
8. [IPFIX] Добавлена настраиваемая отправка счетчиков drop octets/packets при формировании IPFIX fullflow. Описание

RADIUS

1. [FastRadius] Можно задать `bind_ipv6_address` и `bind_ipv6_subnet` одновременно. При наличии маски 128 в Framed-IPv6-Prefix она не проверяется на ограничение по значению `bind_ipv6_subnet`. Описание

Router

1. [Router] Анонсирование белых адресов абонентов для NAT 1:1 по одному и после авторизации. Описание
2. [Router] Исправлено: перехват и отвод IPv6-пакетов на tap-интерфейсы. Link-local адреса не отводились на tap, даже если это явно задано в настройках `router.subnet6`.

Утилиты

1. [DPIUTILS] Обновлена утилита checknat. Описание
2. [DPIUTILS] Обновлена утилита dns2dic с поддержкой блокировки доменов. Описание

Изменения в версии 14.1

DPI

1. [DPI][ajb_save_vlan] Исправлена ошибка при работе движка в режиме только для чтения
2. [DPDK][tap_device] Исправлено: задание длины tx-очереди опцией `dpdk_tx_queue_size`. Ранее длина tx-очереди TAP-девайса безусловно задавалась равно 256, на что VMware VMXNET3 Ethernet Controller ругался: ETHDEV: Invalid value for nb_tx_desc(=256), should be: <= 4096, >= 512, and a product of 1
3. [LAG] Исправлено: добавлена балансировка для пакетов pass
4. [DPI][ip_node stg] Добавлена статистика по заселению buckets. Новая CLI-команда `stat storage ip4 detail` выводит статистику по заполнению buckets в IPv4 node storage
5. [DPI] Добавлена валидация протоколу MULTIPROXY_STRONG
6. [DPI] Улучшена масштабируемость на 128-ядерных системах
7. [DPI][log] Улучшена подсистема логирования в случаях переполнения log файлов.
8. [DPI][tethering] Добавлено детектирование tethering. Параметр `tethering_ttl_allowed = 128:64` [hot] - определяет список допустимых значений TTL для трафика от абонента, которые не считаются tethering. Значения перечисляются через ':'. Количество значений до 256 (0-255). Описание

BRAS

1. [BRAS][framed-route] Исправлено: передача Framed-Route при изменении логина абонента. При изменении логина подсети Framed-Route оставались подключенными к старому логину, и все услуги и полисинг для подсетей Framed-Route брались от старого логина.
2. [BRAS] Добавлена опция `bras_disable_l3_auth` — явный запрет L3 auth в режиме L2 BRAS для всех абонентов. К примеру будет работать только DHCP авторизация для

абонентов с метой AS local. Значение по умолчанию: `off` (L3 auth разрешена) `bras_disable_l3_auth=off`. Данная опция имеет смысл только если `enable_auth=1`. Опция несовместима с режимом `bras_dhcp_auth_mix=0`: если задано `bras_dhcp_auth_mix=0`, то `bras_disable_l3_auth` полагается равным `off` (L3 auth разрешена) и выводится предупреждение в alert-лог.

3. [BRAS] Добавлен новый флаг для абонента — запрет L3 auth для конкретного абонента. Этот флаг можно установить/снять только через CLI: в команду `subs prop set` добавлен новый параметр `disable_l3_auth=[1:0]` (`1` - запретить L3 auth, `0` - разрешить). По умолчанию L3 auth разрешена.
4. [BRAS][srcIP spoofing] Добавлена фильтрация по флагам source AS на пути subs→inet до приема пакета в обработку для блокирования исходящего от оператора DDOS с подменой IP-адреса. Описание
5. [BRAS][PPP] В команду `ppp show stat` добавлена статистика по утилизации БД-сессий. Описание
6. [BRAS][PCEF][Policing] Добавлено конфигурирование общего полисинга из параметров переданных в атрибуте `VasExperts-Policing-Profile` с префиксом BR##
7. [BRAS][PCEF][Services] Добавлено конфигурирование персонального (`noname`) профиля пользователя для сервисов из параметров переданных в атрибуте `VasExperts-Service-Profile` с префиксом BP##
8. [BRAS][PCEF][rating-group] Новые опции (cold, требуется рестарт fastDPI):
   - `rating_group_count` — число rating group, `0` — RG отключены. Значение по умолчанию: `0`
   - `rating_group_max_subs` — max число абонентов с RG. Значение по умолчанию: (RG отключены)
     Хранилище RG инициализируется только если включена биллинговая статистика. Расчет объема памяти под RG статистику: размер счетчиков под одну RG = 32 байта. Общий размер требуемой памяти:

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

     Например, для 10 тыс. абонентов, 256 RG и 8 потоков обработки требуется 625M памяти:

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

9. [BRAS][PCEF][rating-group][RADIUS Accounting] Вывод статистики по RG в RADIUS Accounting. Статистика по RG передается в отдельных пакетах Interim-Update. Передаются данные только по ненулевым RG. Из-за ограничений на размер RADIUS-пакета в 4096 байт, RG-данные могут быть разбиты на несколько RADIUS-пакетов Interim-Update.
   Чтобы отличить Interim-Update содержит признак данных, содержащихся в нем: новый VSA `VasExperts-Acct-Type` (id=28, vendor 43823, тип integer) со значениями:
   - `0`: стандартный Interim Update Accounting
   - `1`: данные по RG
     Каждая rating-group и ее счетчики передаются в *одном* VSA, который содержит следующие атрибуты:
   - `VasExperts-Acct-Rating-Group` (новый атрибут типа short, 16-битовое целое) - номер RG;

- `VasExperts-Acct-Input-Octets-64`
- `VasExperts-Acct-Output-Octets-64`
- `VasExperts-Acct-Input-Packets-64`
- `VasExperts-Acct-Output-Packets-64`
  счетчики пакетов/байт по направлениям выводятся в соответствии с опцией `acct_swap_dir` (как в Accounting).
  Особенности передачи RG:
- RG являются опциональными данными и могут отсутствовать у абонента; соответственно и никакой передачи RG-аккаунтинга для такого абонента не будет;
- в случае неподтверждения приема RG-пакета со стороны RADIUS-сервера его повторная отправка не производится, - свежие данные отправятся в следующем Interim-Update абонента;
- если абонент имеет RG-статистику, то по окончании сессии перед отправкой Acct-Stop посылаются текущие RG-данные в пакетах Interim-Update.

10. [BRAS][PCEF][rating-group][CLI] Добавлено: CLI-команда `subs traffic stat`. Команда для указанного абонента выводит биллинговую статистику и статистику по rating group, если они подключены у абонента. Описание
11. [BRAS][PCEF][rating-group][RADIUS Accept] Добавлено: задание услуги RG при авторизации. Накопление статистики по RG может быть включено только если включена услуга 9 (bill stat) для конкретного абонента. RG задается на уровне абонента при авторизации указанием специального профиля услуги 9 с именем 'RG':

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

    Если услуга 9 отключается, отключается и накопление RG.
    Примеры заданий услуги 9 и RG:

    ```
    # service 9 enabled, RG disabled. Отправляется стандартный RADIUS
    Accounting.
    VasExperts-Enable-Service :="9:on"
    ```

    ```
    # service 9 enabled, RG enabled. Отправляются данные RG в RADIUS
    Accounting.
    VasExperts-Service-Profile :="9:RG"
    ```

    ```
    # service 9 disabled, RG disabled. Не отправляются стандартный RADIUS
    Accounting и RG.
    VasExperts-Enable-Service :="9:off"
    ```

12. [BRAS][SHCV][hot] Добавлен контроль активности static IP L2-абонента (абонента, которому при L3-авторизации RADIUS возвратил флаг `VasExperts-L2-User=1`). Описание
13. [BRAS][DHCP][hot] Для опции `bras_dhcp_check_secondary_keys` доступны новые значения 2 и 4. Полное описание опции:

    `bras_dhcp_check_secondary_keys` — контроль вторичных уникальных ключей (opt82/QinQ) [hot]
    В DHCP основными ключами выступают ClientId (opt61) или, если ClientId не указан, MAC-адрес клиента. В режиме контроля вторичных ключей если хотя бы по одному вторичному ключу найдена другая DHCP-сессия, она будет закрыта (посылается acct Stop)

    - 0 (значение по умолчанию) — не контролировать вторичные ключи.
    - 1 — контролировать все вторичные ключи — QinQ и opt82
    - 2 — контролировать только opt82
    - 4 — контролировать только QinQ
14. [BRAS][L2TP] Исправлено: падение при получении дубля out-of-order ctl-пакета
15. [BRAS][dhcp-relay] Добавлена возможность сохранения значения поля siaddr.
    Новый флаг в опции `bras_dhcp_server`: `keep_siaddr=1` — сохранять поле siaddr DHCP-пакета. Пример:

    ```
    bras_dhcp_server=188.227.73.42%eth0;arp_proxy=1;reply_port=67;keep_siaddr=1
    ```

    По умолчанию поле siaddr может быть модифицировано, чтобы скрыть реальный адрес DHCP-сервера.</code>

16. [BRAS][CLI] Добавлено: команда `subs db stat` вывода статистики по БД L2 BRAS
17. [BRAS][DHCP6] Исправлено: падение при обработке DHCPv6 с некорректной длиной в UDP-заголовке

NAT

1. [CG-NAT] Добавлен `rx_dispatcher=3` — метод с равномерной балансировкой по произвольному количеству потоков с поддержкой NAT 1:1 с возможностью назначения конкретных Публичных адресов, без требования назначения конкретного Приватного адреса на абонента. Описание
2. [CG-NAT] Учет времени жизни трансляции в команде `fdpi_ctrl list status --service 11 --login UserName (--ip IP)`. В выводе команды появились дополнительные поля: `active_sess_tcp` — количество активных NAT-трансляций для TCP и `active_sess_udp` — количество активных NAT-трансляций для UDP. Активность трансляции определяется временем ее последнего использования и параметром времени жизни, задаваемого в опциях кластера.
3. [CG-NAT][CLI] Учет времени жизни трансляции в команде `nat show <internal_ip> [<lifetime>]`. Выводит список всех NAT трансляций для заданного серого IP. Запись трансляции выглядит следующим образом:
    - nat_type - тип NAT (0 - CGNAT, 1 - NAT 1:1),
    - protocol - протокол уровня L4 (0 - TCP, 1 - UDP),
    - internal_ip - серый IP,
    - internal_port - серый порт,
    - dest_ip - IP назначения,
    - dest_port - порт назначения,
    - external_ip - белый IP,
    - external_port - белый порт,
    - active - флаг активности трансляции (true если активна)
      Активность трансляции определяется временем ее последнего использования и параметром времени жизни, задаваемого в опциях кластера. Если задан `<lifetime>` (в секундах), то используется его значение в качестве времени жизни трансляции.

CLI

1. [CLI] Добавлена команда `subs bind show` просмотра списка IP-адресов, привязанных к логину `<login>`. Описание
2. [CLI] Добавлено: CLI-команда `stat http`. Эта команда выводит внутреннюю статистику, аналогичную выводу в fastdpi_stat.log. Описание
3. [CLI] Фикс команд `list status --service 11` (NAT) и `nat show`

IPFIX

1. [IPFIX] Хранение информации о TTL из заголовка IP-пакетов. Описание
   В статистику Full NetFlow в формате IPFIX добавлены:
   - TTL пакетов, id 192. Поле используется для обоих направлений: subs2inet и inet2subs
   - Rating group, id 2020
2. [IPFIX] Исправлена ошибка конвертирования времени в unix формат
3. [IPFIX] В Full NetFlow IPFIX добавлены новые 64-bit поля. Описание
   `service_flags` - информация о метках, которые получил flow в DPI. Детектированный tethering сообщается по IPFIX в бите 1 поля service_flags. Доступны 63 бита для дальнейшего использования.
   `detection_flags` - зарезервировано под метод детекции.
   `action_flags` - зарезервировано под передачу какие действия были с flow.
4. [IPFIX] В Full NetFlow IPFIX исправлена передача TTL в одном поле с идентификатором 192 в зависмости от направления. Описание

Утилиты

1. [utils] Добавлена утилита name2custom для просмотра списка протоколов, загруженных из облака (в отличие от встроенных)

RADIUS

1. [FastRADIUS] Добавлена поддержка записи в syslog. Новый параметр `syslog_level` в fdpi_radius.conf — уровень записи сообщений из alert-лога в syslog. `0` — запись в syslog отключена (значение по умолчанию).
2. [FastRADIUS] Добавлено извлечение RADIUS атрибута 3GPP User Location Info и его отправка в IPFIX