# Содержание

# Версия 11.0 Foundation

Обзор версии 11 на Rutube:

11.0 Foundation [1)]

Не проводите обновления ядра Linux. В новых версиях ядра может быть нарушена бинарная совместимость с Kernel ABI и сетевой драйвер после обновления не загрузится. Если вы все-таки произвели обновление, то на время решения проблемы настройте в загрузчике GRUB загрузку прежней версии ядра (в файле `/etc/grub.conf` установите параметр `default=1`).

## Изменения в версии 11.0

1. Добавлена поддержка сигнатур, определяемых пользователями на основе SNI, IP[:PORT] или SUBNET.
2. Добавлена запись трафика в СХД ("закон Яровой").
3. Добавлены протоколы FACETIME, NORD_VPN, EXPRESS_VPN, PRIVATETUNNEL_VPN, VPNUNLIMITED, PSIPHON3, CLUBHOUSE, TLS_UNKNOWN, QUIC_IETF, SPEEDTEST.
4. Изменено: по 12 услуге пишутся данные в pcap и после детектирования закрытия сессии.
5. [DPI engine] Добавлен настраиваемый таймаут перепроверки IP-адреса.
6. [SORM engine] Новая конфигурация `prmt` для объема `meta_parser`.
7. Изменено: Если задан параметр `ssl_reply` — в версию протокола ставится значение из протокола `content_type=0x16`.
8. Изменено: определение протоколов `ssl_unknown` и `tls_unknown` определяется как: `sni` пусто и `cname` пусто — сморим версию заголовка ServerHello (из первых пяти байтов). Если версия ⇐0x0300 — это `ssl_unknown`, иначе это `tls_unknown`. Если задан параметр `tls13_unknown` — всегда смотрим ServerHello и если там версия 0x0304 — это всегда протокол `tls_unknown` (независимо от `sni`/`cname`).
9. Исправлено: в файлах `layout` в поле `flags` ставится значение: 2 — если это служебная запись или не определено еще flow иначе устанавливаем 1 — `dir_data`.
10. Изменено: если задан параметр `ssl_parse_reply`, происходит поиск `cname`.
11. Изменено: В формат `ajb_save_sslreply_format` добавлены 3 новые поля `tphost` (тип хоста — всегда 2), `host` (`cname`), `evers` — версия из Extensions (определяется только если задан параметр `tls13_unknown=1`, иначе 0).
12. Изменено: Формат `clickstream` передачи `ssl-reply`. Добавлены поля: 1011 — `type_host` — число лежит в `host` — всегда 2 и 1005 `cname`.
13. Изменено: сообщения при трассировке вида DPI(DEF_PROTO, CHANGE_PROTO, STORED_PROTO) — добавлено поле `cntr_fin`, `direction`.
14. Исправлено: после закрытия соединения не помещалась запись в short очередь для TCP.
15. Добавлено: при трассировке для TCP соединений сообщения добавлено сообщение об изменении очереди (short/long).
16. Изменено: формат вывода команды `fdpi_cli dump flow cache`.
17. Добавлено: параметр `ajb_save_fragment` — задает запись фрагментированных пакетов

в pcap.
18. Изменено: разбор протокола TLS.
19. [PCRF][DHCP] Исправлено: передача `opt82 circuit/remote id` в аккаунтинг.
20. Добавлено: для `storage_agent` параметр `engine_bind_cores`, который задает привязку потоков записи к ядрам.
21. [BRAS][DHCPv6] Исправлено: падение на пакете DHCP-Confirm без указания IPv6-адресов в IA_NA-опции.
22. Исправлено: режим `tap_mode=1` — не должно быть отправки пакетов.
23. Исправлено: крах при разборе L2-заголовков для `eher_type=0xFFFF`.
24. [PCRF][framed-pool] Исправлено: при добавлении в уже существующую опцию `opt125` не учитывалось, что `dhcp_poolname_opt=0` — это то же самое, что и `dhcp_poolname_opt=2`. Это приводило к добавлению `opt125` для VasExperts при `dhcp_poolname_opt=0`.
25. [BRAS][ARP] Добавлено: поддержка режима сегментирования абонентов в общем VLAN на сети доступа (изоляция абонентов на коммутаторе, то есть абонентам не доставляется трафик между друг другом даже в одном vlan). Добавлен `fastdpi.conf` — параметр `bras_arp_vlan_segmentation`: Учитывается только при установленном флаге 1 в `bras_arp_proxy` для ARP-запросов от одного абонента другому. off (типичный случай) — абоненты A и B в одном VLAN могут взаимодействовать между собой напрямую, CKAT не обрабатывает ARP-запрос от абонента A "who has target abonent B IP" on — на коммутаторе включена изоляция абонентов, находящихся в одном VLAN, поэтому CKAT должен сам ответить на ARP-запрос от абонента A "who has target abonent B IP".
26. [CFG] Исправлено: не учитывалось значение параметра `set_packet_priority` в `fastdpi.conf`.
27. Изменено: статистика SDS_AGENTS_ — добавлено суммарное количество ошибок и процент.
28. Изменено: поддержка нескольких очередей SDS_AJB.
29. Добавлено: параметры `sds_ajb_num` — количество очередей `sds_ajb (default 1)` `sds_ajb_bind_cores` — задает ядра, к которым надо привязывать потоки. Если не задан — ядра назначаются автоматом. Пример: `sds_ajb_bind_cores=1:1:2:2`.

## Изменения в версии 11.1

1. [fastPCRF] Исправлено: передача `opt82` в аккаунтинг при L3 auth
2. [PCRF] Исправлено: передача значения атрибута `opt82 remoteId` в аккаунтинг
3. [PCRF] Добавлено: возможность задания атрибутов для `opt82`. Новые параметры в `fastpcrf.conf`: `attr_opt82_remoteid=vendorId.attrId`, где `vendorId` — id вендора. Если `vendorId != 0`, то значение передается в VSA-атрибуте. Если `vendorId == 0`, то значение передается в обычном Радиус-атрибуте (не-VSA) `attrId` — id атрибута, число от 1 до 255. Если эти параметры не заданы, то `opt82` передается в следующих атрибутах: `acct: circuitId: ADSL VSA 3561.1, remoteId: ADSL VSA 3561.2 auth: circuitId: VasExperts VSA 43823.39, remoteId: VasExperts VSA 43823.33`
   Пример задания: `attr_opt82_remoteid=15.34 attr_opt82_circuitid=15.35`.
4. [DPI] Добавлены протоколы ZOOM, NETFLIX, TIKTOK, TWITCH, INSTAGRAM, TWITTER, LINKEDIN, AMAZON VIDEO, APPLE STORE, APPLE ICLOUD, APPLE UPDATES, APPLE PUSH, APPLE SIRI, APPLE MAIL
5. [DPI] Название протокола GOOGLEVIDEO изменено на YOUTUBE
6. [DPI] Улучшена надежность диссектора HTTP протокола при большом количестве потерь/ретрансмиссий

7. [DPI] Исправлена ошибка `reload` при настройке LAG.

## Изменения в версии 11.2

1. [DPI] Поддержка декодирования SNI в протоколе QUIC IETF (HTTP/3).
2. [DPI] Улучшена сигнатура Telegram TLS.
3. [PCRF] Добавлен новый VSA-атрибут в Acct-Stop: [26] VasExperts-Acct-Terminate-Cause [integer] — внутренний код acct stop. Может быть полезен при анализе логов Радиуса.
4. [PPPOE] Добавлено удаление из БД PPPoE-сессий при окончании работы.
5. [PPPOE] Исправлено: при загрузке не учитывались опции `bras_pppoe_ac_name` и `bras_pppoe_service_name`.
6. [PCRF] Исправлено: при переключении на другой Радиус-сервер посылаем Acct-On от имени всех fastdpi-серверов. Если PCRF обслуживает несколько fastDPI, будет посылаться несколько Acct-On, — для каждого fastDPI отдельный Acct-On.
7. [DHCPv6] Исправлено: отправка запросов Renew/Rebind на Радиус до истечения `expired timeout`, что приводило к закрытию текущей acct-сессии и старту новой.
8. [CoA] Исправлено: CoA Disconnect мог закрыть "зависшую" сессию, созданную после отправки CoA Disconnect.
9. [PCRF] Добавлено: атрибут `NAS-Port-Id` добавляется и для single-VLAN сетей и содержит строку "`0/vlan`".
10. [CoA] Изменено: CoA Disconnect теперь приводит к закрытию всех acct-сессий по указанным реквизитам.
11. [fastPCRF] Исправлено: ошибка при обработке L3 auth по IPv6.

## Изменения в версии 11.3

1. Существенно переработана поддержка CG-NAT: клиенты на одном белом адресе будут активнее переиспользовать сессии друг друга.
2. Добавлена поддержка резервирования BRAS в режиме L2 (переключение осуществляется через службу `vrrp/keepalived`).
3. [fastPCRF] Исправлено: при переключении на другой Радиус-сервер посылаем Acct-On от имени всех fastDPI-серверов. Если PCRF обслуживает несколько fastDPI, будет посылаться несколько Acct-On, — для каждого fastDPI отдельный Acct-On.
4. [DHCPv6] Исправлено: отправка запросов Renew/Rebind на Радиус до истечения expired timeout.
5. [CoA] Исправлено: CoA Disconnect мог закрыть "зависшую" сессию, созданную после отправки CoA Disconnect.
6. [PCRF] Добавлено: атрибут NAS-Port-Id добавляется и для single-VLAN сетей и содержит строку "0/vlan". Для single-VLAN сетей также добавляется, как и раньше, атрибут NAS-Port, содержащий VLAN.
7. [CoA] Изменено: CoA Disconnect теперь приводит к закрытию всех acct-сессий по указанным реквизитам.
8. [fastPCRF] Исправлено: ошибка при обработке L3 auth по IPv6.
9. [Router] Исправлено: удаление маршрута при завершении PPPoE сессии.
10. Исправления в работе CG-NAT по результатам эксплуатации BETA1.
11. Добавлены новые протоколы HUAWEI CLOUD, WOT WARGAMING, PUBG KRAFTON, RIOTGAMES, FORTNITE EPIC. 🤣

12. Исправлена работа 5 услуги на VCHANNEL.
13. [Router][LAG] Исправлено: выбор следующего девайса из LAG в случае link down текущего.
14. [PCRF] Если в ответе авторизации задан Framed-Pool и IP-адрес — игнорируем Framed-Pool. Это касается авторизации PPP, DHCP, DHCPv6.
15. [PPP] Исправлено: если в ответе авторизации Радиус содержатся выданные IP-адреса вместе с Framed-Pool, — игнорируем атрибуты Framed-Pool и не передаем их в PPPoE BRAS. Наличие framed-pool в PPPoE BRAS меняет логику PPPoE — BRAS начинает контролировать время лизы и посылать DHCP Renew на DHCP-сервера. В случае явно выданного IP-адреса это может привести к закрытию PPPoE-сессии, если DHCP-сервер ответит NAK.
16. [DHCP6] Исправлено: отправка acct даже если не включена услуга 9.

## Изменения в версии 11.4

1. Добавлена услуга 15 (Special Subscriber): при подключении услуги для трафика абонента устанавливается приоритет из настроечного параметра `special_dscp` (по умолчанию 0).
2. Добавлен параметр `nat_gcache_slice_k100`, который задает, сколько портов выделять на каждый slice (по умолчанию 125).
3. Добавлен `seqno` в `clickstream`.
4. Улучшена обработка "пустого" ответа Radius.
5. Добавлены vchannels на основе IP/CIDR.
6. [Router] Добавлено: если включен режим терминации по AS (`bras_term_by_as=1`), то роутер (маршрутизация) применяется только для тех абонентских AS, которые терминируются. Если AS не терминируется — роутер к пакету не применяется. То же самое относится и к анонсам абонентских адресов: если адрес относится к нетерминируемой AS, такой адрес не анонсируется.
7. [Router] Добавлено: деанонсирование Framed-Route подсетей при деанонсировании абонента.
8. Переход на DPDK 21.11 LTS.
9. Проверена установка на ROSA Linux Chrome и VEOS 8.6.
10. Увеличено число поддерживаемых портов до 24.
11. Исправлено: CLI команда `router fib dump` показывает подсети меньше /24.
12. [Router] Исправлено падение при внеплановой очистке ARP-кеша роутера.
13. [BRAS][L3-auth] Исправлено: удалена отправка Acct-Start с резервного fastDPI при L3-авторизации на основном fastDPI.
14. Исправление размера пакетного буфера для DPDK 21.11 с драйвером Mellanox.

## Изменения в версии 11.4.1

1. Исправлена поддержка TAP интерфейсов.
2. [BRAS][PPPOE] Добавлен новый conf-параметр `bras_ppp_padi_recreate_timeout` Интервал времени (секунд), в течение которого входящие от абонента повторные запросы создания сессии (PADI) не приводят к созданию новой сессии (используется уже созданный объект сессии). Данный параметр призван обезопасить от шторма PADI-запросами от абонента и пересоздания объектов сессий. Некоторые роутеры посылают несколько PADI при создании сессии, не дожидаясь ответа от BRAS. По умолчанию: 5. Значение 0 — нет контроля.
3. [PCRF][ACCT] Исправлено: Обращение к удаленным данным.

4. [PCRF][ACCT][CLI] Добавлен вывод типа ожидаемого ответа для acct-записи.
5. [BRAS][CoA] Исправлено: поиск по логин в CoA update. Если в CoA update (изменение профиля абонента — подключение или отключение услуг) заданы login и IP, и абонент по логину не найден — пытаемся отыскать по IP. Ранее поиск по логину был самым приоритетным, если не абонент найден — CoA update не обрабатывался.
6. [PCRF] Обновлен словарь атрибутов radius.

# Изменения в версии 11.4.2

1. Изменено: при подключении 15 услуги отключается фильтрация по черным спискам канала (или по умолчанию).
2. Изменено: `tbf rate 8bit` оптимизирован до `drop`.
3. Улучшено распознавание протоколов RTP и SIP.
4. Изменено: общий и канальный полисинг теперь применяется в read only режиме.
5. Изменено: услуга 12 применяется после канального и абонентского полисинга.
6. Добавлен кэш для белого адреса: при экспорте данных nat трансляций при освобождении белого порта используются реальные данные из кэша (ранее значение не передавалось, т.е. =0), настроечный параметр `nat_dstaddr_cache_size` задает количество хранимых `dst_ip:dst_port` в рамках белого адреса для UDP. По умолчанию `0xffff * 2` (для TCP не актуально).
7. Изменено: при блокировке ресурса освобождение flow производится быстрее (flow перемещается в "короткую" очередь).

[1)]

Стабилизация основания для дальнейшего развития: мобильные сети, аналитика, DDOS защита, LI, AI