

Table of Contents

Список изменений БЕТА-версии СКАТ	3
Изменения в версии 13.3 БЕТА1	3
Изменения в версии 13.3 БЕТА2	3
Изменения в версии 13.3 БЕТА3.2	3
Изменения в версии 13.3 БЕТА3.3	3
Изменения в версии 13.3 БЕТА3.4	4
Изменения в версии 13.3 БЕТА3.5	4
Изменения в версии 13.3 БЕТА3.6	5
Инструкция по обновлению	5

Список изменений БЕТА-версии СКАТ

Изменения в версии 13.3 БЕТА1

1. [DPI] Новые протоколы BIGOTV [49305], SAYHI [49306], AZARLIVE [49307]
2. Добавлено: горячий параметр smartdrop = 1, если для прокола задан drop, то он будет отложен, пока не будет разобран tls или ошибка разбора tls
3. Исправлено: добавление http доменов с окончанием на : (номер порта)
4. [Utils] Исправлено: checkproto проверяет с учетом MARK1, задан ли номер порта, т.е. checkproto 8.8.8.8 443 www.google.com и checkproto 8.8.8.8 www.google.com могут вернуть разный результат
5. Изменен путь загрузки ASNUM из VAS Cloud (cloud.vasexperts.ru)
6. Блокировка по черному списку в GTP туннеле (при заданной настройке detect_gtp_tunnel)
7. Исправлено: блокировка https с опцией hard

Изменения в версии 13.3 БЕТА2

1. [DPI] Улучшено распознавание Viber
2. Поддержка reload для автономных систем IPv6
3. [Utils] bin2as принимает любое количество входных файлов как аргументов
4. [Utils] ascheckip принимает адреса для групповой проверки со stdin
5. [Utils] bgp2bin аналог as2bin, но принимает только подсети /24 и крупнее, понимает формат диапазона IP1-IP2 как в записях ripe (выделяя из него подсети /24 и крупнее), последующие записи приоритетнее предыдущих, создает файл немного крупнее чем as2bin, но в нем диапазоны подсетей не пересекаются (т.к. менее приоритетные записи отфильтрованы), что позволяет передать утилите на вход данные из нескольких источников в порядке приоритета
6. [BRAS][PPP] Исправлено: разнородный dual-stack. Один адрес (IPv4 или IPv6) задан явно, для второго (IPv6 или IPv4) указан framed-pool.

Изменения в версии 13.3 БЕТА3.2

1. [DPI] Исправлено: поиск одновременно * и : в http доменах
2. [DPI] Исправлено: удаление адресов в виртуальных каналах при reload
3. [DPI] Исправлено: игнорирования drop при задании параметра smartdrop при ошибках разбора ssl
4. [BRAS][PPP] Исправлено: учет опции bras_pppoe_trace_mac при сохранение DHCPv6-пакетов в rсар. Ранее учитывалась только опция bras_dhcp_trace_mac. Теперь для DHCPv6-пакетов в PPPoE-туннеле учитывается также и bras_pppoe_trace_mac

Изменения в версии 13.3 БЕТА3.3

1. [DPI] Уменьшено число ложных срабатываний для DPI TUNNEL
2. [DPI] Исправлены ошибки при назначении vchannel по IP/CIDR

Изменения в версии 13.3 БЕТА3.4

1. [DPI] Исправлено: блокировка по IP DNS, работающего через tcp
2. [DPI] Увеличена глубина просмотра пакетов при поиске BIGOTV
3. [DPI Utils] Исправлена checkproto для случая IP протокол Unknown
4. Начальная поддержка записи alert лога в syslog. Включается настройкой `syslog_level=7` (уровень, включительно до которого дублируются сообщения в syslog), по умолчанию не писать. Замечания:
 1. По умолчанию rsyslog при записи в текстовый лог заменяет символ табуляции и переводы строк на их коды. Чтобы это отключить можно создать файл `/etc/rsyslog.d/fastdpi.conf` с настройкой

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

либо пользоваться утилитой `journalctl`. Пример:

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

2. Можно перенаправить запись логов на удаленный сервер. Пример из `/etc/rsyslog.conf`:

1. на локальном сервере с fastdpi:

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

2. на удаленном сервере:

```
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")
```

Изменения в версии 13.3 БЕТА3.5

1. [pcrf] Добавлена поддержка записи в syslog. Новый параметр `fastpcrf.conf`: Уровень записи сообщений из alert-лога в syslog, 0 - запись в syslog отключена (это значение по умолчанию) `syslog_level=0`
2. [bras][ppp] Fixed: бродкастные пакеты теперь молча дропаем

3. [bras] Доработка L3-авторизации 1. Если приходит Reject на IP-адрес, привязанный к multi-bind логину, то сначала отвязываем этот IP от логина, а затем навешиваем услуги (белый список, полисинг) на IP. 2. При успешной авторизации (Access-Асcept): если IP не имеет логина, но при авторизации (успешной) пришел логин - надо отвязать все услуги от IP, прежде чем связывать IP с новым логином.
4. [DPI] Изменено : если протокол определен по ip/sni/cname, то не происходит переопределение протокола по встроенным сигнатурам

Изменения в версии 13.3 BETA3.6

1. [DPI] Упорядочено соблюдение приоритетов протоколов, что позволяет избежать лишних переключений между протоколами в процессе анализа.

Инструкция по обновлению

Проверить текущую установленную версию можно командой

```
yum info fastdpi
```

Если у вас установлена версия CentOS 6.x или CentOS 8.x, то однократно переключите репозиторий командой:

```
sed -i -e '/^mirrorlist=http:\\\\//d' -e 's/^#  
*baseurl=http:\\\\mirror.centos.org/baseurl=http:\\\\vault.centos.org/  
/etc/yum.repos.d/CentOS-*.repo
```

и далее производите обновления как обычно.

Команда установки тестовой версии:

```
yum --enablerepo vasexperts-beta update fastdpi
```

Откат на 13.2:

```
yum downgrade fastdpi-13.2 fastpcrf-13.2
```



После обновления или смены версии требуется рестарт сервиса