ОБНОВЛЕНО 16 МАР

Что нового в DosGate

Раздел содержит изменения в системе DosGate. Обновления веб-интерфейса SP Spider вынесены отдельно.

- История версий SP Spider

Версия 3.9.0

Дата релиза: 29.08.2025

Новые возможности

Совпадения по портам *port* Проверяет одновременно порты источника и назначения и срабатывает, если указанный порт встречается в любом направлении (TCP/UDP/SCTP).

Действие *DNSAUTH*
Аутентифицирует входящий DNS-трафик, имитируя ответ сервера с флагом **TC** и вынуждая источник повторить запрос по **TCP**. Применяется против атак типа **DNS Flood**.

Метка *HMARKC*
Служебная метка источника, доступная для чтения. Используется для реализации временных чёрных и белых списков.

Параметр *cpu-count* в конфигурации арены
Используется для корректного расчёта размеров *percpu-lru* карт в зависимости от количества CPU.

Версия 3.8.0

Дата релиза: 10.03.2025

Новые возможности

Отслеживание адреса правила
Добавлено отслеживание адреса правила во время обработки пакета.

Расширенный заголовок UH
В заголовок добавлена информация об адресе правила, по которому пакет был отброшен.

Дополнительные данные BPF
Добавлена служебная информация BPF для аудита через API.

Новые возможности сессионного модуля

Поддержка JA4-TLS
Добавлена поддержка JA4-TLS для более точной классификации зашифрованного трафика и улучшенной детекции аномалий.

Формат захвата pcap-ng
Добавлена поддержка формата pcap-ng.

Комментарии в дампах сброшенных пакетов
В дампы добавляется номер правила, по которому пакет был отклонён.

Управление прерываниями
Добавлена возможность отключать управление прерываниями через конфигурацию.

Улучшенные эвристики прерываний
Оптимизирована работа в режиме non-MSI и при совместном использовании векторов прерываний.

Обновление статистик
Статистики pbuf/seg удалены. Управление этими данными перенесено в библиотеку.

Исправления

Исправления ошибок
Исправлены выявленные проблемы.

Версия 3.7.4

Отрицание совпадений по протоколу
Добавлена возможность отрицать совпадение по протоколу.

Объединение совпадений
Реализовано объединение выбранных совпадений в одно.

Приоритеты для ToS и TC
Добавлено совпадение по приоритету IPv4 ToS / IPv6 TC и действие PRIORITY.

Фильтрация по стране GeoIP
Добавлена фильтрация меток по стране GeoIP в CLI и API.

Audit-команда
Добавлена команда для просмотра BPF-тегов программ и идентификаторов.

Улучшения

Обработка списков протоколов
Улучшена работа со списками протоколов при преобразовании из/в строки.

Оптимизация структуры совпадений
Совпадения разделены на протокольные и специфичные части. Протокольные совпадения объединены в один блок, что сокращает количество проверок и ускоряет пропуск нерелевантных правил.

Оптимизация порядка совпадений
Совпадения упорядочены по сложности. Простые проверки выполняются первыми, позволяя быстрее завершать обработку правила.

Парсинг и кеширование TCP-опций
TCP-опции разбираются в прологе BPF:

- уменьшена сложность основного блока;
- ошибки в TCP-опциях приводят к отказу разбора;
- кеширование уменьшает сложность для BPF-верификатора.

Параметр strict-check
Добавлен конфигурационный параметр `strict-check` с перечнем дополнительных проверок на этапе разбора протокола.

Валидация IPv4-опций
Добавлена валидация IPv4-опций (включается флагом `ipv4-options` в `strict-check`).

Перенос очистки flow-записей
Очистка flow-записей перенесена из кода совпадений в пролог арены для снижения сложности критичного участка.

Исправления

Исправлена работа негативного кеширования prefix-set
Исправлено некорректное использование отрицательного результата поиска.

Исправлены ошибки и улучшена стабильность
Внесены корректировки и исправлены выявленные проблемы.

Версия 3.6.0

Дата релиза: 12.08.2024

Новые возможности

Реализован экспорт кадров для сессионной защиты
Добавлена поддержка экспорта кадров.

Трассировка BPF-кода
Добавлена система трассировки для анализа нагруженных участков BPF.

Перенаправление трафика на набор CPU
Реализовано перенаправление трафика на заданный набор CPU. Используется хеш кадра от сетевой карты, а при его отсутствии выполняется собственный расчёт хеша. Кадры распределяются по целевому набору CPU по принципу RSS, без нарушения целостности потоков.

Обновлённое действие PASS
Действие PASS теперь поддерживает перенос трафика на другие CPU.

Проверка совместимости ядра
Запуск запрещён на ядре ниже допустимого ABI. Для Ubuntu 22.04 минимальная версия — Linux 5.15.0.

Новые возможности сессионного модуля

Экспорт через libxskexp
Добавлена поддержка экспорта кадров и TLS Hello-сообщения через libxskexp.

Событие полного получения данных
Зафиксирован момент получения корректного TLS Hello-сообщения.

Трассировка и перенос отладочных данных
Реализована система трассировки. Механизмы debug и dump перенесены в неё.

Подтверждение соединений
Для TCP подтверждение требует валидного ACK с корректным номером последовательности.

Статистика на уровне протоколов
Добавлена поддержка сбора статистики на уровне сетевых протоколов.

Дефрагментация TLS-handshake
Реализована сборка фрагментированного TLS-handshake.

Подсистема событий
Реализована новая подсистема событий.

Замена offenders
Механизм offenders удален. Его функциональность заменена подсистемой событий.

Поддержка yes/no/auto для zero-copy
Логика выбора режима zero-copy приведена в соответствие с поведением ядра.

Выбор размера буфера кадров для старых карт
Добавлена возможность выбирать размер буфера кадров для старых сетевых карт.

Поддержка внешних источников кадров
Переработана логика очередей fill/comp с учётом возможного поступления кадров от внешних источников.

Автоматическое определение режима zero-copy
Теперь система считывает отчёт ядра о привязке сокета, чтобы определить режим zero-copy, и включает перенаправление только при необходимости.

Старт TCP-соединения с SYN+ACK
Добавлена возможность открывать соединение с SYN+ACK в однонаправленном режиме.

Корректная обработка ICMP Unreachable
Улучшена обработка ICMP-ошибок для отслеживаемых TCP- и UDP-соединений.

Дополнительные метрики TLS
Добавлены новые метрики для использования в системе событий.

Исправления

Исправления ошибок
Исправлены выявленные проблемы.

Версия 3.4.2-1

Дата релиза: 23.02.2024

Новые возможности

Новый механизм TCP-авторизации
Реализована TCP-авторизация на основе синхронизации TCP ISN. Поддерживаются два агентных модуля с разными алгоритмами хеширования и набором протоколов.

Расширенные возможности меток
Добавлены таймеры для записей в метках и новые операторы сравнения. Теперь можно проверять время появления записи и использовать значение таймера в правилах. Поддерживается хранение до 100 млн записей до одного года.

Поддержка новых драйверов
Добавлена поддержка ixgbe и virtio, частичная поддержка vmxnet3.

Опция null в tcpopts
Добавлена возможность указывать отсутствие TCP-опций.

Оптимизация побайтового сопоставления
Ускорено сопоставление по параметру `-m seq`.

Поддержка веб-интерфейса
Добавлена совместимость с веб-интерфейсом версии 3.9.9.

Исправления

Исправления и обновления по запросам
Внесены улучшения по feature-request'ам и исправлены выявленные ошибки.

Версия 3.2.3-3

Дата релиза: 21.09.2023

Улучшения

Оптимизация работы сокета
Выполнены улучшения для ускорения работы сокета и взаимодействующего с ним веб-интерфейса

Версия 3.2.3-2

Дата релиза: 01.09.2023

Исправления

Исправления ошибок
Внесены общие исправления.

Версия 3.2.3-1

Дата релиза: 28.06.2023

Новые возможности

Обновлённый побайтовый поиск
Изменён алгоритм сопоставления для `-m seq`.

Настройка размеров таблиц данных
Добавлена возможность модифицировать размеры таблиц данных.

Обработка и экспорт FLOW
Добавлена обработка потоков и экспорт в лог-файлы, BSD syslog, stderr/stdout и IPFIX.

Улучшения

Оптимизация системы
Повышена производительность.

Исправления

Исправления ошибок
Исправлены выявленные проблемы.

Версия 3.2.2-5

Исправления

Исправления ошибок
Исправлены проблемы, связанные с prefix-set, GeoIP и метками.

Версия 3.2.2-4

Исправления

Исправления побайтового поиска
Исправлены ошибки, связанные с `-m seq`.

Версия 3.2.2

Дата релиза: 5.04.2023

Новые возможности

Сессионная защита
Добавлены функции отслеживания соединений, проверка TLS, дефрагментация, проверка checksum, поддержка TLS cipher-suite и JA3-отпечатков.

Гибкая загрузка базы GeoIP
Система пытается загрузить GeoIP из `/etc/dosgate/GeoLite2-Country.mmdb`, при ошибке — использует файл дистрибутива из `/usr/share/dosgate`.

Новое действие RETURN
В чейне возвращает выполнение к правилу после GOTO. В профиле работает как ACCEPT.

Новое действие CAPTURE
Помечает кадр для записи. Работает при активном сессионном модуле.

Обновление действия PASS
Действие PASS теперь может передавать обработку в сессионную защиту с указанием приложения и профиля.

Улучшение TCPAUTH
Таймауты стали раздельными по направлениям, обновлена логика greylist-аутентификации.

Оптимизация больших prefix-set
Ускорена работа prefix-set с размером более 10K записей.

Реализовано кеширование ключей map
Повышена скорость всех совпадений и действий, использующих map.

Ускорение hmark-кэша
Увеличена скорость поиска за счёт разделения id на линейный индекс.

Команда для просмотра внутренних статистик
Добавлена CLI-команда для вывода внутренних статистик.

Ранний сброс кеша меток при обработке ответов
Кэш очищается до изменения пакета, чтобы избежать использования неверных ключей и обеспечить корректную обработку ответов.

Оптимизация сопоставления адресов
Вместо набора немедленных констант используются статические таблицы значений и масок, что снижает сложность сопоставления и уменьшает число ветвлений.

Кеширование запросов к prefixset и GeoIP
Реализовано кеширование запросов prefixset. Это особенно полезно при повторных проверках GeoIP, когда для разных стран применяются разные политики. В таком случае выполняется только один запрос к map.

Глобальные методы для оптимизации BPF
Часть логики вынесена в глобальные методы, что сокращает количество путей выполнения и снижает нагрузку на BPF-верификатор.

Глобальные методы для правил
Правила переведены на обработку через глобальные методы, что снижает сложность кода и контролирует рост путей выполнения.

Оптимизация сопоставления TCP-флагов
Переход на сопоставление по 4-байтовому слову вместо устаревших BSD-бита, что повышает скорость и снижает сложность BPF-кода.

Сохранение и загрузка состояния демона через API
Добавлена возможность сохранять и загружать состояние. Состояние хранится в `/var/lib/dosgate/state/<name>`, формат совместим назад. Требуется корректная синхронизация времени.

Поле arena id в конфигурации
Добавлено поле `id` в конфигурации арены — требуется для работы сессионного модуля.

Полный API для работы с чейнами
Добавлен API для создания, изменения и управления чейнами.

Улучшения

Перенос flush-логики для flow-записей
Очистка перенесена из кода совпадений в пролог арены — критическая секция стала проще.

Исправления

Исправления ошибок и повышение стабильности
Внесены корректировки для улучшения стабильности и уменьшения нагрузки на BPF-верификатор.

Версия 3.2.1-4

Дата релиза: 22.02.2023

Исправления

Исправления ошибок
Исправлены выявленные проблемы.

Версия 3.2.1

Дата релиза: 26.12.2022

Новые возможности

Использование percpu LRU для меток и ratelimit
Карты меток и ratelimit переведены на percpu LRU для повышения производительности.

Фильтрация по регулярным выражениям
Добавлена возможность фильтровать списки профилей и чейнов по регулярным выражениям.

Поддержка нового метода загрузки BPF
В конфигурацию добавлен объект `daemon` с параметром `xdp-mode`. Доступные режимы:

- `auto` — автоматический выбор (попытка drv, затем fallback в skb),
- `drv` / `hw` — принудительный режим drv,
- `skb` / `sw` / `generic` — принудительный режим skb. При смене режима возможны ошибки, если программа не выгружена принудительно.

Улучшения

Улучшенный вывод статусов в CLI
Обновлён формат отображения состояния объектов.

Консольная блокировка CLI
Добавлена система рекомендационной блокировки CLI по сессии консоли.

Дополнительные обходные решения для ALU32 и BPF-verifier
Добавлены улучшения для повышения стабильности и совместимости.

Исправления

Исправления ошибок
Исправлены известные проблемы.

Версия 3.2.0

Дата релиза: 2.08.2022

Новые возможности

Split-карты для повышения производительности
Добавлена поддержка split maps. Технология распределяет нагрузку между несколькими объектами за счёт хеширования ключей и выбора целевого объекта по хешу. Это снижает конкуренцию между CPU и повышает производительность по сравнению с глобальным LRU.

Минимальный объём памяти — 8 ГБ
Увеличение размеров карт требует не менее 8 ГБ RAM.

Оптимизация TCPAUTH
Карты TCPAUTH переведены на percpu LRU для работы при высокой нагрузке. Возможность переключиться на split-карты сохранена.

Именованные счётчики
Добавлены именованные счётчики. Поддерживаются одновременно со старым форматом.

Новое действие RATE
Добавлен механизм оценки скорости трафика с состояниями conform, exceed и cooldown. Работает на интервальном анализе и позволяет детектировать всплески нагрузки.

Начальная реализация inline-режима
Добавлена базовая поддержка inline-обработки: прозрачная работа ARP и IPv6 multicast, управляемое переключение L2-трафика, поддержка LACP.

Передача link-local multicast в ОС
STP, GVRP и другие link-local L2-протоколы всегда передаются в ОС.

Надёжная идентификация системы
Добавлен механизм аппаратной идентификации и защита от подмены.

Новая система лицензирования
Введены типы лицензий Package, Admin, Operator. Поддержано добавление, удаление и просмотр через API. Добавлена поддержка сертификатов на этапе сборки.

Управление интерфейсами
Интерфейсы настраиваются через interface_set. Включение promisc при inline-записях, отключение VLAN RX offload.

Новые оптимизации для LLVM-13 и современных ядер
Переработаны функции работы с памятью для прохождения BPF-валидации.

Обновлённый match_sequence
Переведён на новый API. Оставлены ограничения по сложности — допускается примерно три правила на профиль.

Обновлённый match_tcpopt
Добавлено сопоставление по конкретной последовательности заголовков. Поддерживаются оба типа проверок.

Режим passthrough
Добавлен лёгкий контекст для прозрачной передачи трафика без анализа. Статистика передается в collectd и доступна через API/CLI.

Улучшения

Рефакторинг системы статистик
Статистики вынесены на отдельный уровень, команды переработаны.

Исправления

Исправления ошибок
Внесены улучшения стабильности и исправлены выявленные проблемы.

Версия 3.1.3

Исправления

Корректная работа batch-операций с map
Исправлены ошибки, возникавшие при почти заполненных batch-операциях. Они приводили к сбоям, некорректному выводу меток и нарушению синхронизации map.

Исправление падения при удалении профиля
Исправлен segfault, возникавший из-за синхронизации карт роутера и выхода за границы memset.

Исправление утечки памяти в mapdiff
Устранена утечка памяти в механизме сравнения карт.

Корректная обработка прослушивающих сокетов
Исправлена логика accept — теперь обрабатываются все доступные сокеты, а не только один на событие.

Упрощение обработки сокетов
Обновлена логика работы с сокетами для упрощения и очистки кода. Исправлен segfault при получении EOF.

Обновление API libdt и libaevent
Обновлены интерфейсы библиотек.

Единая система обработки ошибок
Создан внутренний API обработки ошибок. Большинство функций переведено на него, что позволяет передавать любые ошибки в JSON API.

Переписаны основные подсистемы
Переработаны lib, prog_lib, prog_set и interface_set. Упрощена структура кода, исправлена проблема с обновлением tag программы после пересборки и улучшена синхронизация program maps.

Исправление маркировки RX-программы
Исправлена ошибка, из-за которой RX-программа не помечалась как dirty при удалении некоторых записей switchtable.

Обновление логики TCP-авторизации
Аутентификация ограничена одной TCP-сессией на хост. Другие получают состояние invalid до завершения или таймаута выбранной.

Новые возможности

Цепочки правил и API для них
Реализованы цепочки правил и добавлен API для их управления

Команда replace для prefix-set
Добавлена команда, полностью заменяющая содержимое prefix-set новым набором данных.

Завершённые работы

Исправления ошибок
Исправлены дополнительные проблемы, влияющие на корректность работы системы.

Версия 3.1.2

Дата релиза: 22.04.2022

Новые возможности

GeoIP в списках меток
Добавлена поддержка GeoIP в выдаче меток через API.

Редактирование профилей
В API добавлены операции переименования профиля и изменения его описания.

Автоматическая отправка статистики в collectd
Реализована автоматическая выгрузка статистики.

Новый таргет stats
В API появился target stats для работы со статистикой.

API: поддержка URL
Добавлена работа с URL в API.

TCP Reverse Auth
Добавлена обратная TCP-аутентификация.

GeoIP
Добавлена работа с GeoIP.

Prefix-set
Добавлена поддержка prefix-set.

Исправления

Исправления ошибок
Исправлены выявленные проблемы.

Версия 3.1.1

Новые возможности

Табличные методы TCP-аутентификации
Добавлена поддержка табличных методов TCP-авторизации.

Исправления

Исправления ошибок
Исправлены проблемы предыдущих версий.

Версия 3.1.0

Дата релиза: 21.02.2022

Новые возможности

Улучшение Full API
Расширены возможности полного API.

Расширенная справка для RATELIMIT
Обновлено описание действия RATELIMIT.

Полная переработка DNS
Реализована поддержка всего заголовка DNS.

Переработанная обработка фрагментов
Добавлена поддержка нескольких состояний фрагмента в одном правиле.

Улучшенный разбор IPv6
Исправлена обработка повреждённых IPv6-пакетов и фрагментов.

Новая логика host-marks
Зависимости протоколов перенесены в helpers. Правила и совпадения работают без привязки к протоколу

Batch-операции с map
Реализована поддержка пакетных операций с map.

Резервное копирование и восстановление в dgadm
В dgadm добавлены функции резервного копирования и восстановления конфигурации.

Улучшения

Косметические правки
Улучшена читаемость и внешний вид некоторых частей системы.

Исправления

Исправления ошибок
Исправлены обнаруженные проблемы.