servicepipe

Документация по DosGate

v3.9 / spider-4.7

СГЕНЕРИРОВАНО 26.03.2026, 07:45

dosgate v3.9 / spider-4.7

Содержание

DosGate

DosGate — адаптивная система защиты IT-инфраструктуры от DDoS-атак и сетевых угроз. Благодаря преднастроенным правилам обеспечивает многоуровневую защиту на L3-L7 уровнях, гибкую настройку фильтрации и адаптацию к новым угрозам. Высокая производительность аппаратных платформ (до 400 Гбит/с и 400 млн пакетов в секунду) обеспечивает устойчивую работу системы даже при масштабных DDoS-атаках.

Архитектура DosGate включает в себя:

- Сетевая защита — включает в себя встроенные механизмы проверок и возможность создания правил защиты, основанных на детальных комбинациях содержимого пакетов.
- Сессионная защита — обеспечивает защиту веб-приложений с помощью интеллектуального отслеживания соединений и автоматического разрыва сессий для минимизации простоя.
- Модуль Autopilot — анализирует текущий сетевой трафик и самостоятельно формирует эффективные контрмеры, позволяя мгновенно реагировать на атаки.
- Модуль RLOG — анализирует поток HTTP-логов от внешних систем. На основании полей логов позволяет формировать правила фильтрации для блокировки IP-адресов источника, обеспечивая возможность фильтрации зашифрованного L7-трафика.

Возможности системы

- **Мгновенная фильтрация всех типов DDoS-атак**
  DosGate комплексно защищает от любых флудов, амплификаций и ковровых атак на всех уровнях модели OSI (L3–L7), включая защиту для зашифрованного трафика веб-приложений.
- **Собственное ядро обработки трафика на XDP и eBPF**
  Благодаря этому система поддерживает создание до 150 млн уникальных правил обработки трафика и блокирует атаки менее чем за 1 с в режиме Always-on.
- **Обновляемая база вредоносных сигнатур**
  База сигнатур DosGate поддерживается командой аналитики Servicepipe и обновляется каждый час.

- **Удобное управление защитой**
  Правила гибко настраиваются, а отчёты создаются через единый, интуитивно понятный веб-интерфейс.
- **Полностью российское ПО**
  DosGate входит в реестр отечественного ПО. Servicepipe имеет лицензии ФСТЭК на разработку СЗИ и ТЗКИ.
- **Подключаемый анализатор**
  Система интеллектуального анализа трафика FlowCollector непрерывно отслеживает входящие и исходящие из сети пакеты, обнаруживая аномалии и переводя DDoS-атаки на фильтрацию за 100 мс.
- **Техподдержка 24/7/365**
  Круглосуточную поддержку продукта оказывают инженеры информационной безопасности с ответом в течение 5 минут по SLA.

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 програм 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.

Лицензирование

Лицензия – это файл, который импортируется в DosGate и применяется для управления фильтрацией трафика. Изменение лицензии не влияет на уже применённые правила фильтрации и обработку трафика.

Лицензия позволяет администратору системы использовать введённые правила фильтрации для обработки трафика, выполняя команду `-c commit`.

Ограничения лицензии

Лицензия может накладывать следующие ограничения:

Временные – действует только в установленный период.

По пропускной способности – ограничивает объем обрабатываемого, сбрасываемого или передаваемого трафика, измеряемый в битах и пакетах в секунду. В случае истечения срока действия лицензии или до момента её активации, существующие правила остаются в рабочем состоянии, однако их редактирование становится недоступным из-за невозможности выполнения команды `-c commit`.

Выдача лицензии

При выдаче лицензии вендору необходимо передать системный ID устройства.

Получение системного ID: После установки ПО выполните команду:

```
dosgate --id
```

Внимание!
Системный ID не меняется при замене сетевых карт, процессора, оперативной памяти, а также при переустановке операционной системы и другого ПО

Активация лицензии

Загрузка лицензии в DosGate:

```
dgctl -u license:// -c add -l file.lic

dgctl -u license:// -c commit
```

Проверка загруженной лицензии:

```
dgctl -u license:// -c list
```

Применение лицензии. Указать `arena-name` из dosgate.conf и выполнить команду

```
dgctl -u arena://arena-name -c commit
```

Стоимость лицензии

Стоимость рассчитывается индивидуально и зависит от следующих факторов:

- количества лицензий, поставляемых заказчику;
- периода действия лицензии;
- необходимой пропускной способности;
- дополнительных параметров.

Если у вас есть вопросы по стоимости или выбору лицензии, свяжитесь с нами через контактные данные, указанные на нашем сайте. Мы будем рады помочь!

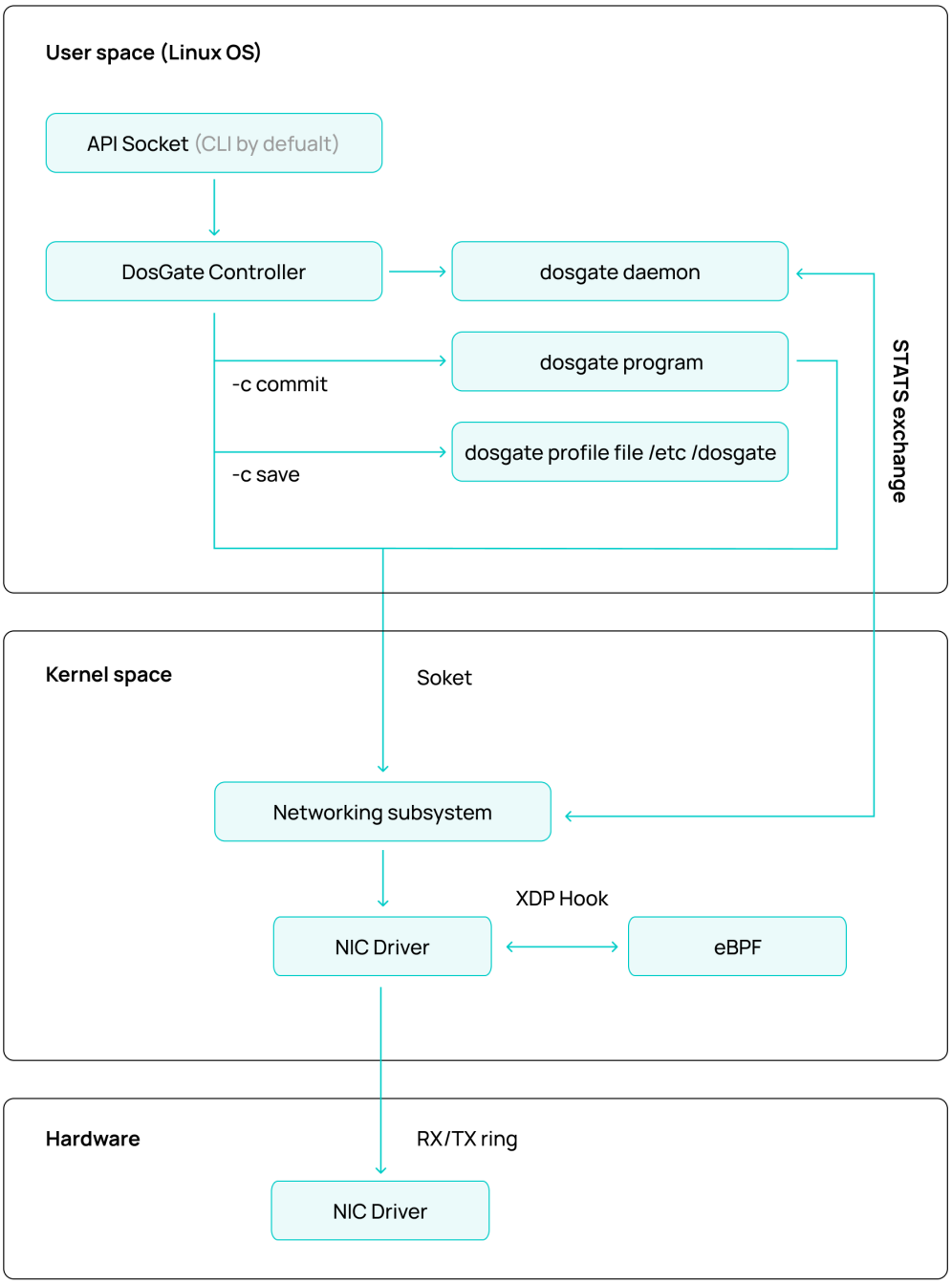
Компоненты платформы ПО

Архитектура платформы базируется на операционной системе Linux и включает в себя следующие ключевые компоненты:

DosGate Controller — программный модуль, предназначенный для трансляции пользовательских правил в машинный код, который впоследствии используется другими компонентами системы.

DosGate — ядро программы, содержащее скомпилированный машинный код, которое интегрируется в ядро Linux (Linux Kernel) посредством управления со стороны DosGate Controller.

DosGate Daemon — системный сервис, обеспечивающий сбор статистических данных и выполнение автоматического контроля. Этот компонент взаимодействует с ядром Linux, где выполняется загруженная программа DosGate.



Модули системы

DosGate содержит функционал, реализованный в виде модулей, распределённых по различным компонентам платформы:

Арена — набор сетевых интерфейсов, и применяемых к ним настроек.

Routing Program — программа, определяющая, в какой профиль должен быть направлен пакет на основании адреса назначения.

Профиль — набор правил, которые применяются к пакету, проходящему через профиль.

Пример взаимодействия модулей при обработке IP-пакета

Когда IP-пакет поступает на Сетевой интерфейс 1, система выполняет следующие шаги:

Идентификация Арены

Конфигурационный файл dosgate.conf используется для определения, к какой Арене относится данный сетевой интерфейс. После идентификации IP-пакет передается в программу маршрутизации (Routing Program) соответствующей Арены (например, Арена 1).

> **Примечание**
> DosGate Daemon использует конфигурационный файл dosgate.conf для сбора статистики. Собранные данные передаются в collectd, который обрабатывает и перенаправляет их в Graphite для последующего визуального отображения метрик.

Определение профиля защиты

На основании адреса назначения, указанного в Routing Program, выбирается профиль защиты, который должен быть применен к сетевому пакету.

Применение правил профиля защиты

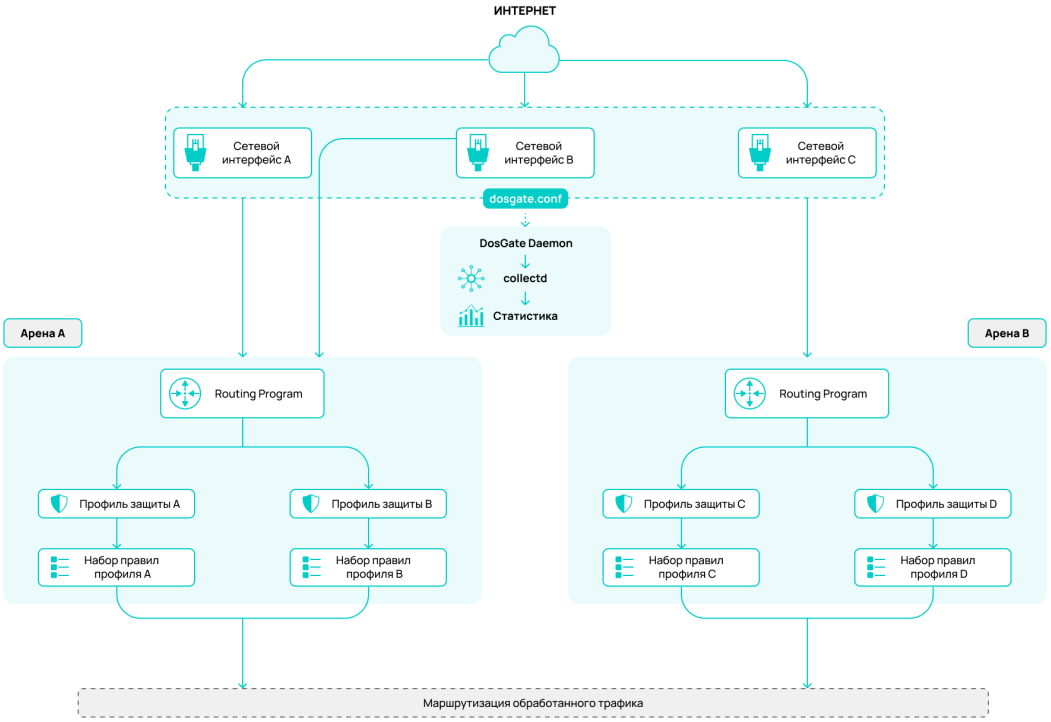
Выбранный профиль защиты содержит наборы правил фильтрации и обработки пакетов. К поступившему сетевому пакету последовательно применяются эти правила.

Результат обработки пакета

После обработки согласно заданным правилам возможны три варианта действий:

1. Отбрасывание пакета (Drop): сетевой пакет считается нежелательным и удаляется.
2. Маршрутизация пакета (Route): сетевой пакет передается далее по назначению в соответствии с таблицей маршрутизации.
3. Возврат пакета (Reply): сетевой пакет передается в предыдущий этап обработки или возвращается в систему для дальнейшей обработки.

Такой подход позволяет гибко управлять сетевым трафиком и применять фильтрацию на основе правил, определённых для конкретных профилей защиты.



Архитектуры инсталляций

В данном разделе представлены примеры архитектурных решений DosGate, включающего интерфейс управления и систему хранения данных. Допустимо использование иной формы архитектуры в зависимости от конкретных требований проекта или условий эксплуатации.

Локальная установка всех компонентов

Архитектура кластера в локальной конфигурации предполагает установку всех компонентов системы DosGate на один физический или виртуальный сервер. Основными элементами являются сервер обработки трафика, веб-интерфейс управления, а также локальное хранилище данных.

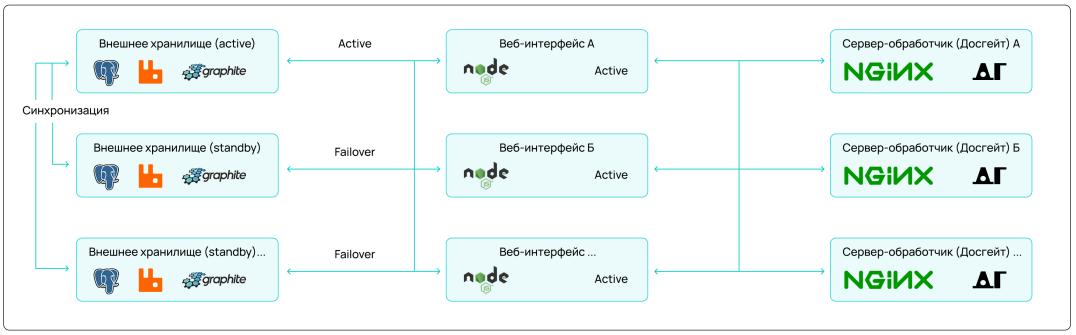
Сервер обработки DosGate выполняет функции фильтрации входящего трафика и защиты от DDoS-атак. Поскольку используется один экземпляр сервера, масштабирование системы в данной конфигурации не предусмотрено.

Веб-интерфейс управления развернут на том же сервере и обеспечивает централизованный доступ к данным и настройкам системы. Для работы интерфейса используются встроенные службы: локальная база данных PostgreSQL для хранения информации, брокер сообщений RabbitMQ для обмена событиями между компонентами и система мониторинга Graphite для сбора метрик.

Все данные сохраняются на локальном диске сервера, без подключения к внешним системам хранения. Такой подход упрощает развёртывание и администрирование системы, обеспечивая базовую защиту и мониторинг без необходимости в сложной инфраструктуре.

Инструкция по локальной установке всех компонентов

Внешнее отказоустойчивое хранилище и веб-интерфейс управления



Архитектура кластера представляет собой отказоустойчивую систему с балансировкой нагрузки, резервированием данных и возможностью горизонтального масштабирования. В её состав входят серверы-обработчики, веб-интерфейсы и внешние хранилища.

Внешнее хранилище организовано по схеме standby: с одним активным узлом и несколькими резервными. В качестве ключевых технологий используются PostgreSQL для хранения данных, RabbitMQ в роли брокера сообщений и Graphite для мониторинга и сбора метрик. Между активным и резервными узлами реализована синхронизация, что позволяет автоматически переключаться на резервный узел в случае отказа основного (failover).

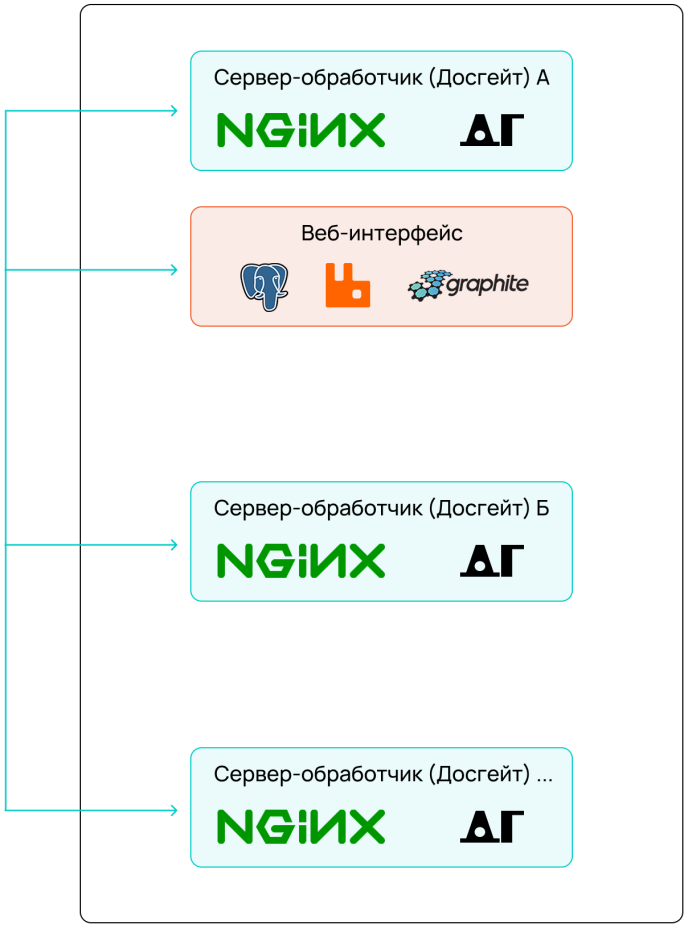
Веб-интерфейсы работают в активном режиме, обеспечивая балансировку нагрузки и доступ к данным.

Серверы-обработчики DosGate предназначены для фильтрации входящего трафика и защиты от DDoS-атак. Серверы взаимодействуют с веб-интерфейсами и перераспределяют нагрузку для повышения устойчивости системы.

Архитектура кластера обеспечивает отказоустойчивость за счёт резервирования хранилищ и механизма автоматического переключения в случае сбоя, балансировку нагрузки благодаря распределению трафика между несколькими веб-интерфейсами, а также горизонтальное

масштабирование, позволяющее без простоев добавлять новые серверы, веб-интерфейсы и хранилища. Встроенная синхронизация данных предотвращает их потерю при отказе основного узла. Преимуществами данной архитектуры являются минимизация времени простоя за счёт автоматического failover, высокая доступность системы, возможность масштабирования без значительных изменений инфраструктуры и устойчивость к сбоям и внешним атакам.

Внутреннее хранилище и веб-интерфейс управления



Архитектура кластера представляет собой распределённую систему обработки данных, обеспечивающую балансировку нагрузки и защиту от перегрузок. Основные компоненты включают серверы-обработчики, веб-

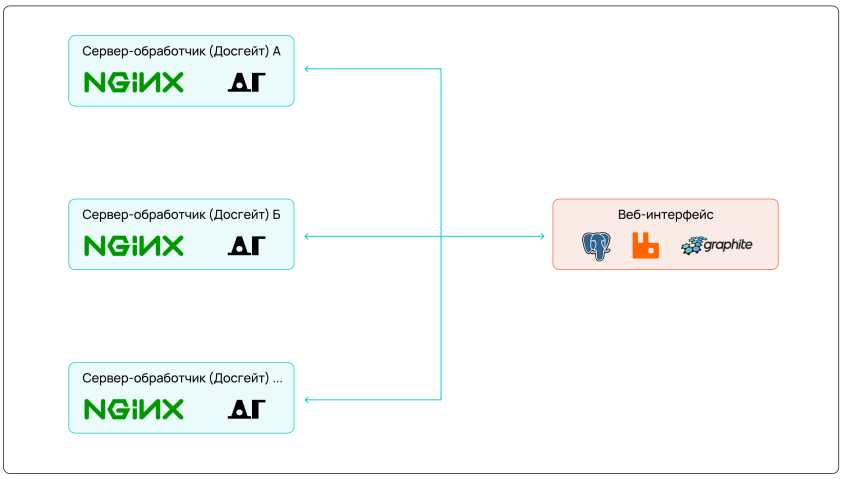
интерфейс и интеграцию с внешними системами мониторинга и хранения данных.

Серверы-обработчики DosGate выполняют фильтрацию входящего трафика и защиту от DDoS-атак. Каждый обработчик работает независимо, обеспечивая отказоустойчивость и возможность горизонтального масштабирования.

Все обработчики передают данные в единый веб-интерфейс, который выполняет роль централизованной точки управления и мониторинга. В качестве базовых технологий используются PostgreSQL для хранения данных, RabbitMQ для управления потоками сообщений и Graphite для сбора и визуализации метрик.

Кластер позволяет добавлять новые серверы-обработчики без перезапуска системы, что обеспечивает масштабируемость. Балансировка нагрузки между обработчиками позволяет распределять входящий трафик. Централизованное хранилище и брокер сообщений обеспечивают согласованность данных и их доступность в реальном времени.

Внешнее хранилище и веб-интерфейс управления



Архитектура кластера строится на основе распределённой обработки данных с балансировкой нагрузки и централизованным управлением. Основными компонентами являются серверы-обработчики, веб-интерфейс и внешнее хранилище.

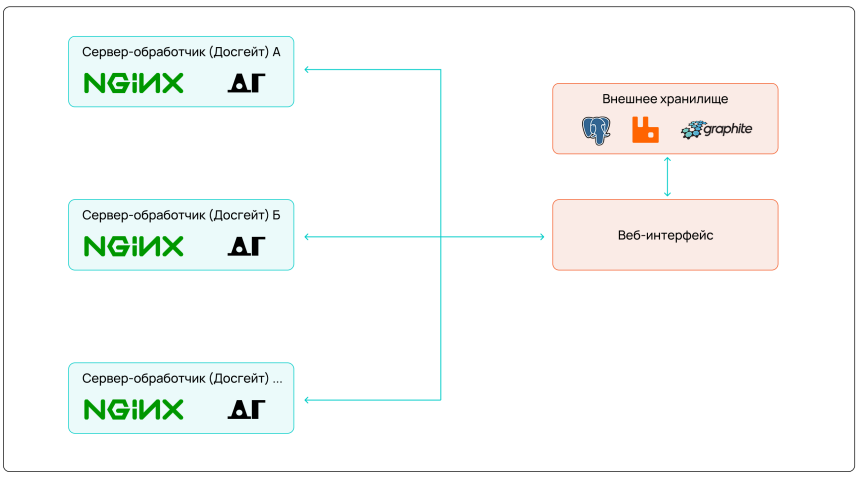
Серверы-обработчики DosGate выполняют фильтрацию входящего трафика и защиту от DDoS-атак. Они функционируют независимо друг от друга, что позволяет динамически увеличивать их количество для масштабирования системы.

Веб-интерфейс выполняет роль централизованной точки управления, обрабатывая запросы и предоставляя доступ к данным. В его основе используются PostgreSQL для хранения информации, RabbitMQ для организации очередей сообщений и Graphite для мониторинга.

Ключевой особенностью данной архитектуры является использование внешнего хранилища для долговременного хранения данных. Веб-интерфейс взаимодействует с этим хранилищем, обеспечивая быстрый доступ к информации и её обработку.

Инструкция по установке с внешним веб-интерфейсом управления

Разнесенные внешнее хранилище и веб-интерфейс управления



Архитектура кластера расширяет возможности предыдущих решений, добавляя внешний уровень хранения данных и его интеграцию с веб-интерфейсом.

Как и в предыдущих архитектурах, серверы-обработчики DosGate выполняют фильтрацию входящего трафика и защиту от DDoS-атак. Они работают независимо и могут масштабироваться по мере роста нагрузки.

Веб-интерфейс выполняет обработку пользовательских запросов, работая в связке с внешним хранилищем.

Отличительной чертой данной архитектуры является разделение веб-интерфейса и внешнего хранилища, что повышает отказоустойчивость и снижает нагрузку на систему. Веб-интерфейс взаимодействует с хранилищем по запросу, обеспечивая эффективное управление данными.

Внешнее хранилище позволяет сохранять большие объёмы информации и распределять нагрузку между различными компонентами системы. В случае выхода из строя одного из узлов система продолжает функционировать, переключаясь на резервные ресурсы.

Таким образом, архитектура кластера обеспечивает высокую надёжность, масштабируемость и отказоустойчивость, поддерживая эффективное взаимодействие между обработчиками, веб-интерфейсом и хранилищем.

Интеграция в сетевую инфраструктуру

Есть всего 4 способа интеграции в сетевую инфраструктуру

- In-line
- Off-line (вручную или автоматизированно)
- Cloud (IP-Transit)
- Hybrid

Local

Локальная интеграция представляет собой установку ПО на серверное оборудование Клиента, либо развёртывание программно-аппаратного комплекса (ПО + аппаратной платформы).

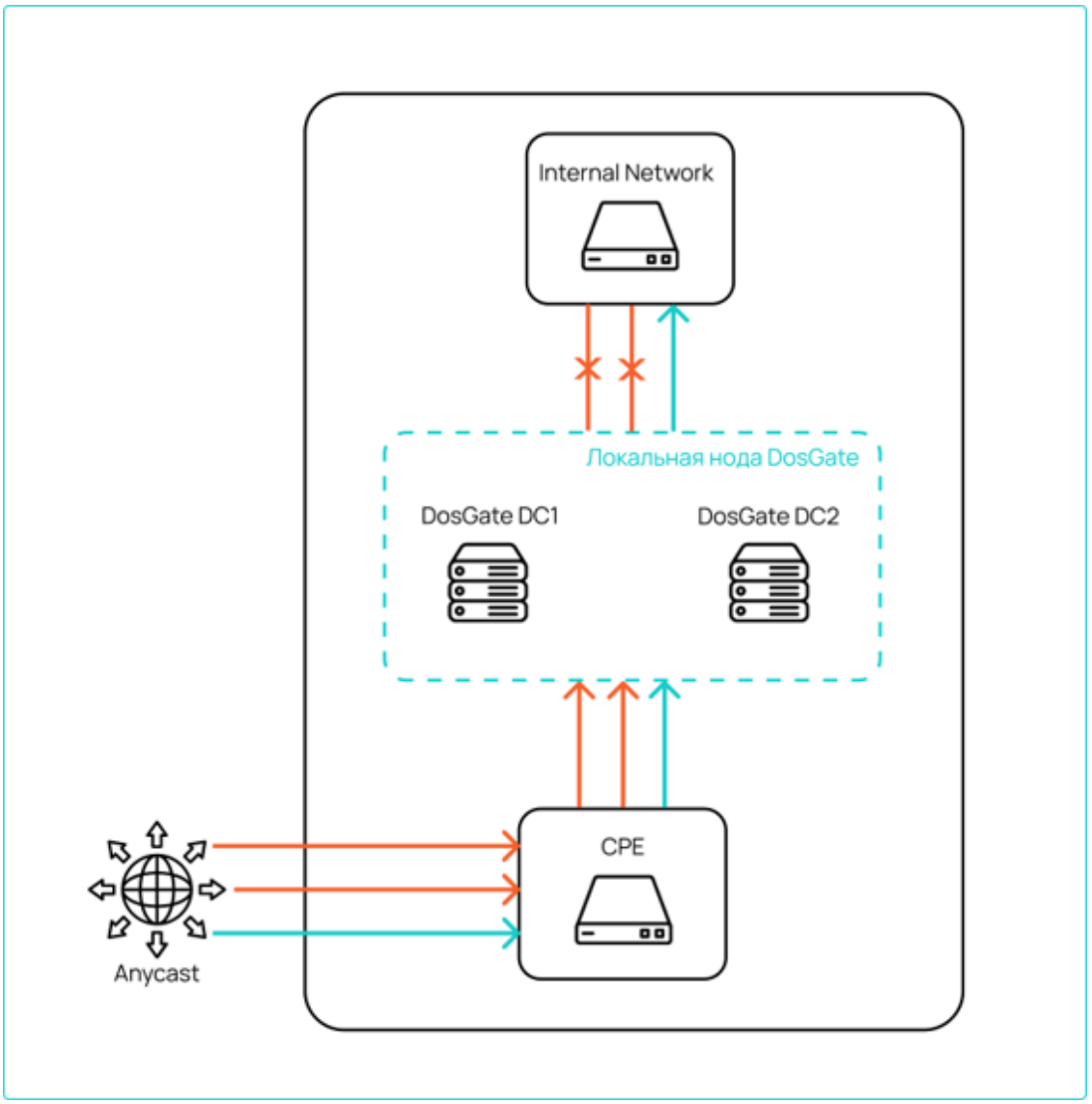
При этом, как ПО, так и ПАК могут управляться и поддерживаться силами службы технической поддержки Servicepipe (managed on-prem), при этом контроль за актуальностью ПО, создание правил (Anti-DDoS, firewall, DNAT, SNAT, rate-limit etc), мониторинг состояния сети, взаимодействие с инженерной командой заказчика - предоставляются в рамках сервиса.

Существует и “классический” подход, при котором Клиент берёт на себя управление и эксплуатацию решения, при этом получая необходимую помощь от Serviceepipe в рамках договора о технической поддержки.

In-line

Установка Inline ("в разрыв") подразумевает, что трафик постоянно маршрутизируется через ПО DoSGate. Трафик приходит на один сетевой интерфейс и возвращает его с другого.

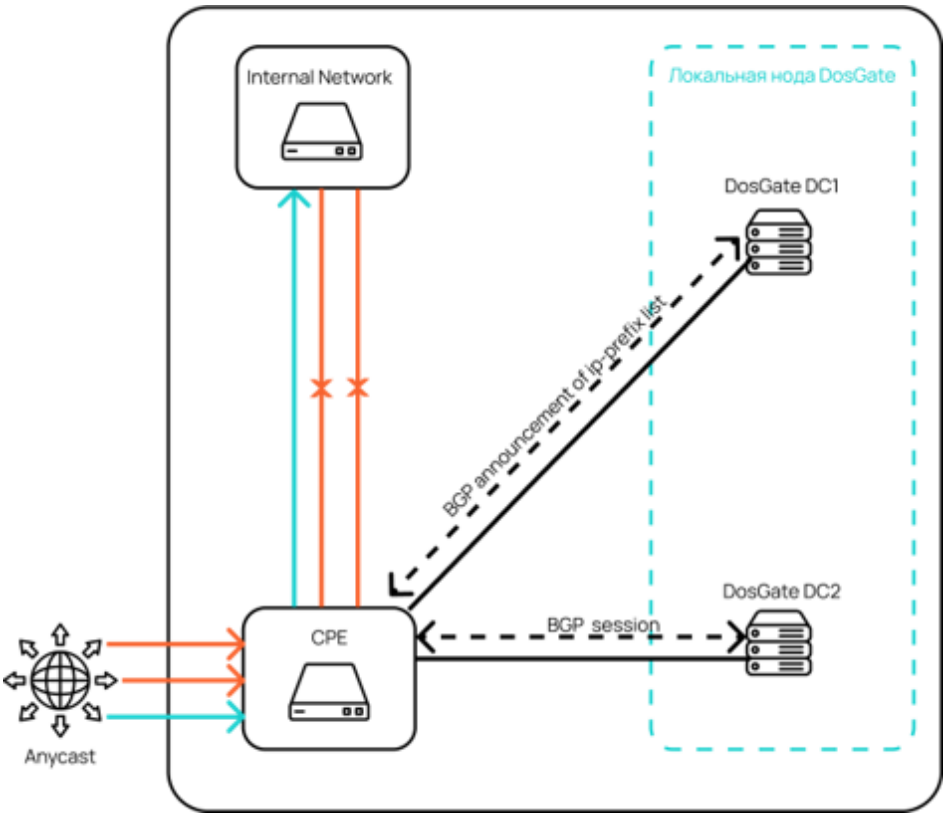
Поддерживается L2 multicast, ARP, LACP, LAG



Out-line

Установка out-line (или VLAN swap) подразумевает, что DoSGate может принимать и возвращать трафик в рамках одного интерфейса, например, принимая трафик с одним VLAN tag и возвращая с другим.

Досгейт держит BGP-соединение с роутерами и может как сам анонсировать от себя IP-адреса, используя bird, так и в него может приходить анонс от автоматизированной системы (например, анализатора)

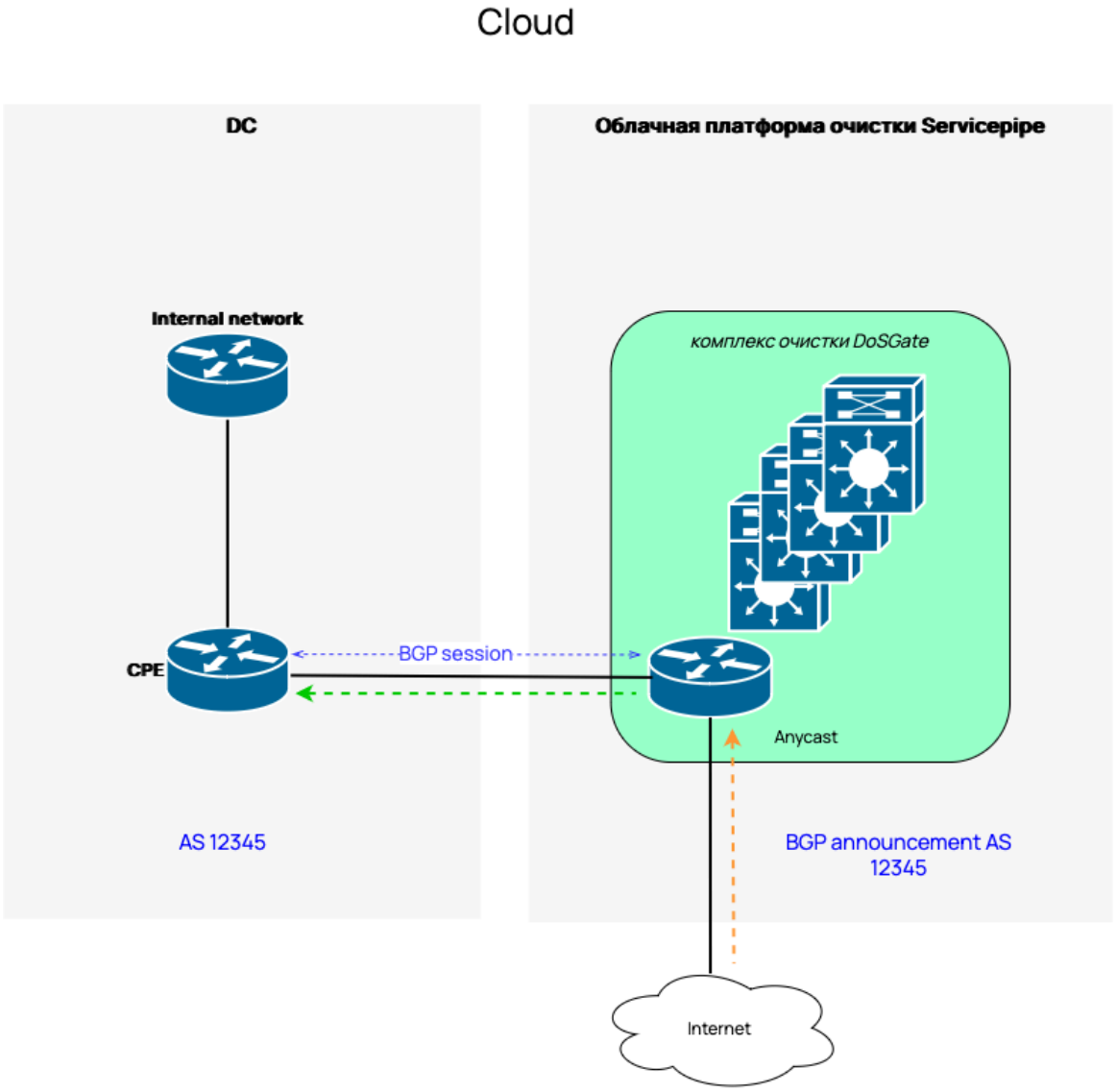


Cloud (IP-Transit)

Облачная интеграция подразумевает, что ноды фильтрации DoSGate располагаются в инфраструктуре Servicepipe в географически распределенных центрах очистки. Трафик идёт через DoSGate постоянно (Inline), или по запросу (outline) (автоматизированному от средств аналитики (анализатора), или ручному

В обоих случаях наша сетевая инфраструктура (`AS201706`) становится BGP-upstream для инфраструктуры Клиента, через неё маршрутизируется часть или весь входящий трафик.

Уровень SLA рассчитывается индивидуально



Shared Anti-DDoS + Stateless Firewall

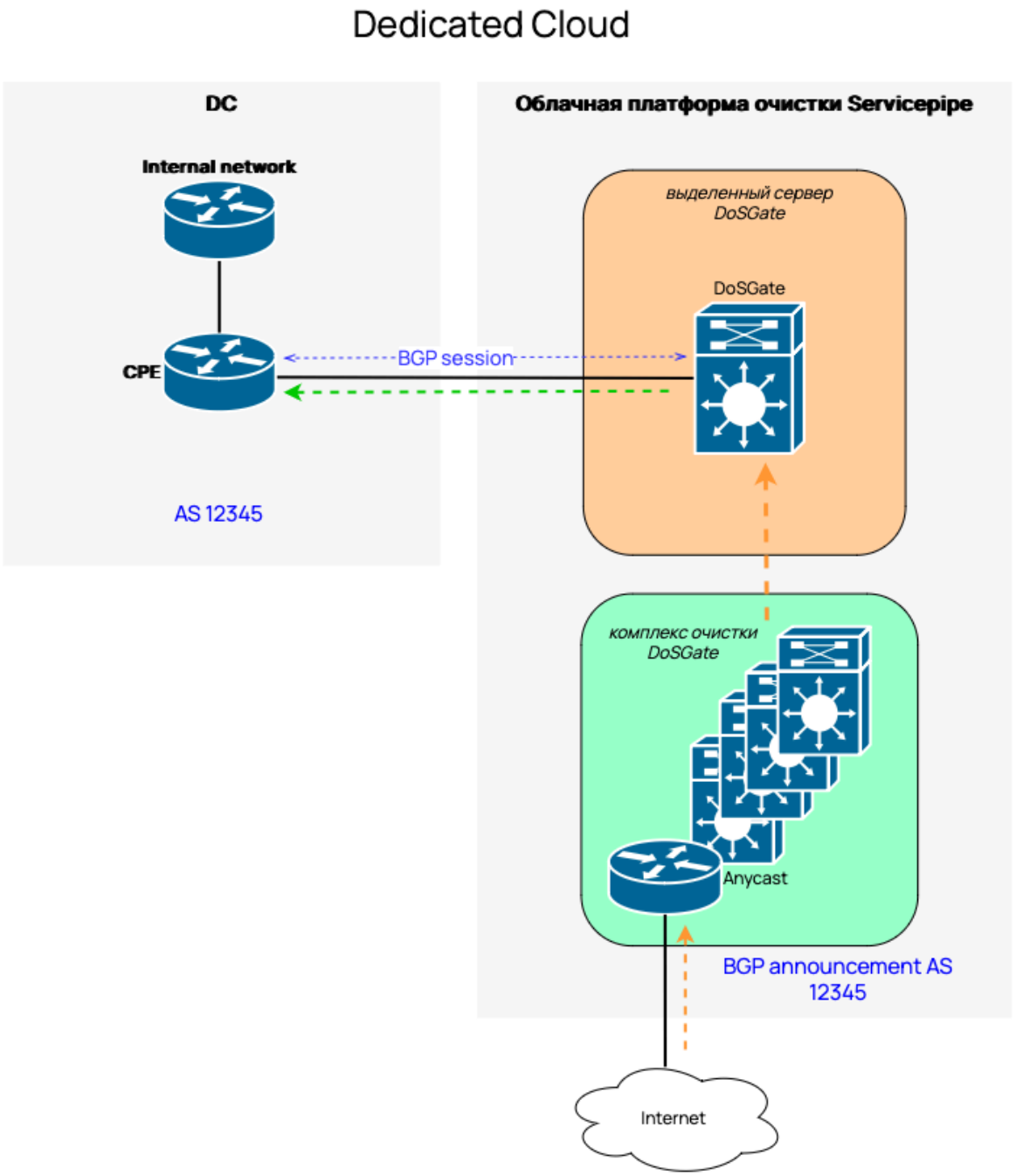
В случае подключения к "общему" аппаратному кластеру возможна организация только Stateless Fiewall и Anti-DDoS

В shared-решении конфигурацией сетевых правил занимается наша инженерная смена (24/7/365). Предоставляется личный кабинет с статистикой. Поддержка осуществляется по телефонной связи, электронной почте, в Telegram

Dedicated DoSGate

В случае подключения выделенного DoSGate кластера в нашей сетевой инфраструктуре, подразумевается что трафик сначала проходит через наши общие кластеры очистки, попадает на выделенный клиентский кластер, и после передается в сетевую инфраструктуру клиента.

Клиент имеет полноценный доступ к выделенному под него кластеру DoSGate в нашей инфраструктуре и может выполнять любые с ним операции, как будто он установлен в самой сети клиента



Cloud Signaling

Сигнализация позволяет сообщать какие IP-маски должны быть направлены через центр очистки DoSGate Cloud

Сигнализация может применяться в разных случаях. Например, когда локальное решение перегружено и требуется помощь облачного центра очистки

Досгейт поддерживает сигнализацию от самого себя (установленного локально) и сторонних решений

Список протестированных поддерживаемых вендоров

- БИФИТ Митигатор BGP Cloud Signaling

Hybrid

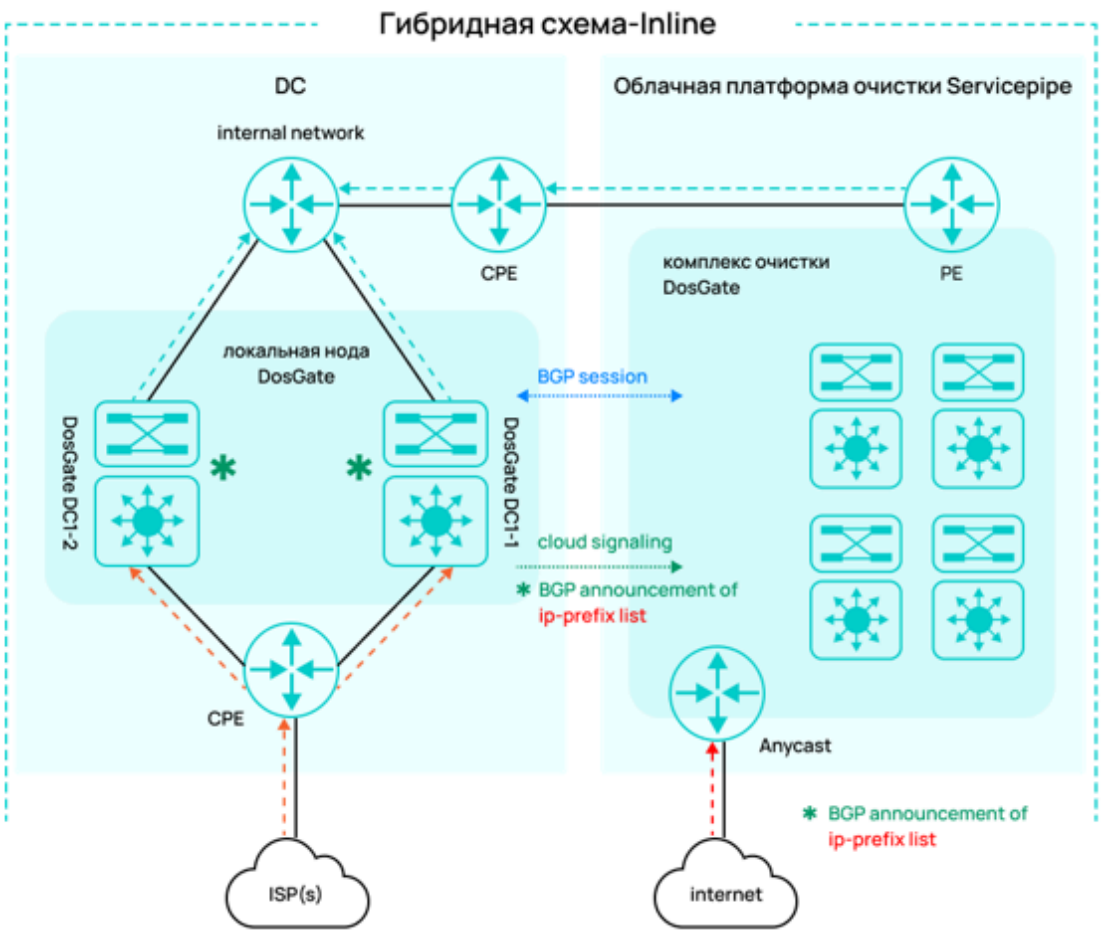
Гибридная схема инсталляции подразумевает комбинацию локального DoSGate (Onprem In-line или Onprem Out-line) и облачного (Cloud In-line или Cloud Out-line)

Облачный и локальный DoSGate могут синхронизировать списки правил (включая префикс-сеты) в реальном времени

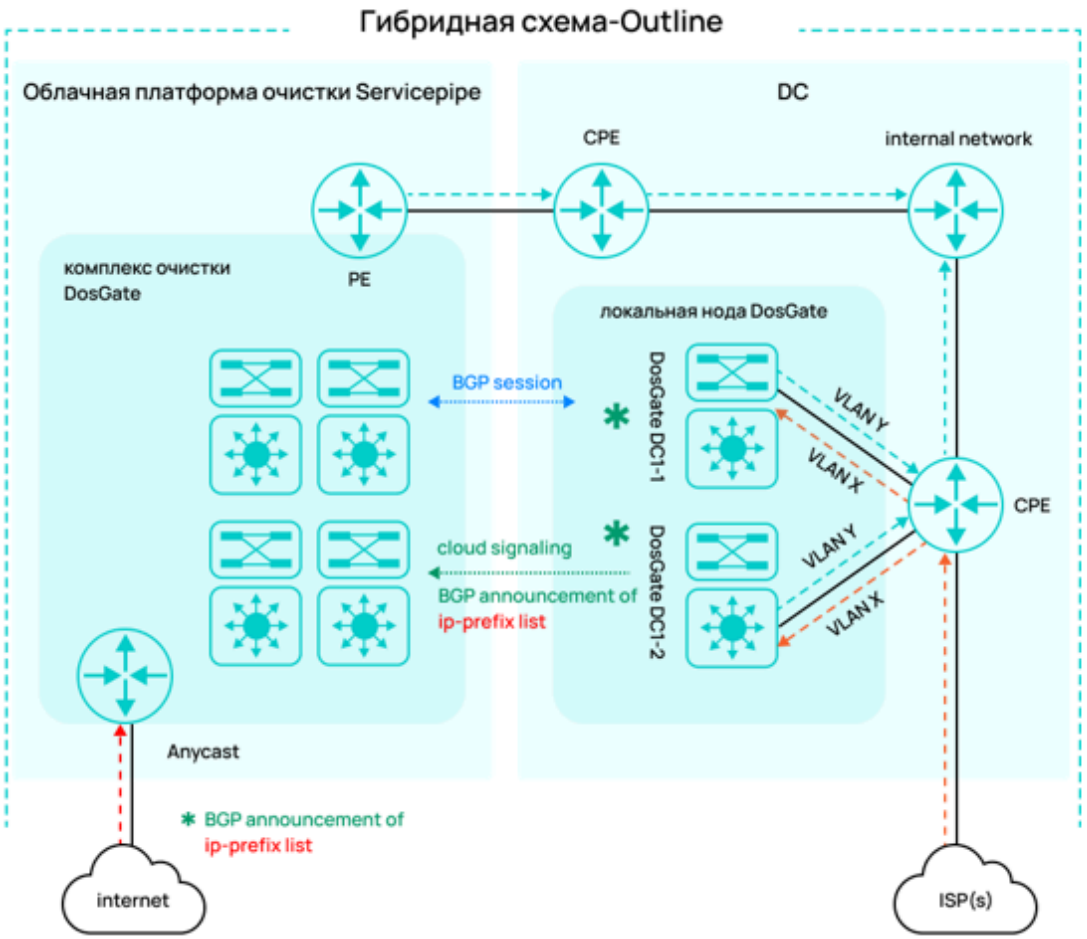
Облачный DoSGate активируется только при получении автоматизированного или ручного сообщения от локального

Гибридная схема работает как с Shared так и с Dedicated облачным DoSGate.

Hybrid In-line



Hybrid Out-line


Гибридная схема-Outline
Облачная платформа очистки Servicepipe
DC
CPE
internal network
PE
комплекс очистки DosGate
локальная нода DosGate
BGP session
DosGate DC1-1
VLAN Y
VLAN X
CPE
cloud signaling
BGP announcement of ip-prefix list
DosGate DC1-2
VLAN Y
VLAN X
Anycast
* BGP announcement of ip-prefix list
internet
ISP(s)

Рекомендованные технические характеристики

В этом разделе приведены аппаратные требования и производительность платформ. Аппаратные требования определяются спецификой выбранной платформы.

Технические возможности платформы

Платформа	BPS ACL	PPS ACL	XDP IPv4/IPv6 Map (pps)	Rate Function (pps)	TCP-авторизация (pps)
DG1-VM	1 Gbps	1.48 Mpps	1.48 Mpps	1.48 Mpps	1.48 Mpps
DG2-VM	2 Gbps	2.97 Mpps	2.97 Mpps	2.97 Mpps	2.97 Mpps
DG5-VM	5 Gbps	7.4 Mpps	7.4 Mpps	7.4 Mpps	7.4 Mpps
DG10	10 Gbps	14.8 Mpps	14.8 Mpps	14.8 Mpps	14.8 Mpps
DG20	20 Gbps	29.7 Mpps	29.7 Mpps	29.7 Mpps	29.7 Mpps
DG40	40 Gbps	59 Mpps	59 Mpps	59 Mpps	40 Mpps
DG100	100 Gbps	100 Mpps	100 Mpps	70 Mpps	50 Mpps

Таблица характеристик платформ

Платформа	Процессор	Оперативная память	Жесткий диск	Сетевая карта	Интерфейсы	БП
DG1-VM	4 ядра Intel Xeon Gold 5433N	8 GB	20 GB SSD (x2)	2x1G	2x1G	В зависимости от VM
DG2-VM	6 ядер Intel Xeon Gold 5433N	12 GB	40 GB SSD (x2)	3x1G	3x1G	В зависимости от VM
DG5-VM	10 ядер Intel Xeon Gold 5433N	16 GB	80 GB SSD (x2)	2x10G	2x10G	В зависимости от VM
DG10	Intel Xeon Gold 5433N	64 GB	240 GB SSD (x2)	Intel X520-DA2 (2x10G)	2x10G + 1x10G	2 шт

Платформа	Процессор	Оперативная память	Жесткий диск	Сетевая карта	Интерфейсы	БП
					management	
DG20	Intel Xeon Gold 6442Y	128 GB	240 GB SSD (x2)	Intel X520-DA2 (2x10G) x2	4x10G + 1x10G management	2 шт
DG40	Intel Xeon Gold 6548N	256 GB	240 GB SSD (x2)	MCX621102AN-ADAT (2x25G)	2x25G + 1x10G management	2 шт
DG100	AMD EPYC 9554	256 GB	240 GB SSD (x2)	MCX516A-CCAT (2x100G)	2x100G + 1x10G management	2 шт

Примечание:

Представленные в таблице спецификации соответствуют минимальным требованиям. Если установка указанных компонентов невозможна, обратитесь к вендору для подбора альтернативного решения

Поддерживаемые сетевые драйверы (NIC)

- mlx4
- mlx5
- i40e
- ixgbe
- ixgbevf
- nfp
- bnxt
- thunder
- dpaa2
- qede
- tun
- veth
- virtio_net
- netsec

Внимание!
Если ваш сетевой драйвер не поддерживается, DosGate будет запущен в режиме xdp_generic. Этот режим не гарантирует максимальной производительности и не рекомендуется для использования на скоростях выше 10G на платформу.

Рекомендованные операционные системы

DosGate совместим с любой операционной системой, при условии использования Linux Kernel версии 5.1 или выше.

В приведённом ниже списке указаны операционные системы, полностью совместимые с DosGate и прошедшие тщательное тестирование:

- Ubuntu 22.04
- Alma Linux 9
- Альт 8 СП

Список обновляется.

База вредоносных сигнатур

DosGate ведет собственную обновляющуюся базу вредоносных сигнатур которая поддерживается внутренней командой аналитики ServicePipe и обновляется каждый час. База вредоносных сигнатур применяется на решении в автоматическом или полу-автоматическом режиме

Содержимое Базы Данных

- Настроенные профили и контрмеры (пресеты)
- Вредоносные TLS-отпечатки
- IPv4/IPv6-адреса участвующие в ДДоС-атаках
- IPv4/IPv6-адреса участвующие в вредоносной автоматизации (парсинг, взлом)

Доставка обновлений

- API
- Через веб-интерфейс DosGate
- JSON-файлы
- Через приватный репозиторий

Подключение базы вредоносных сигнатур

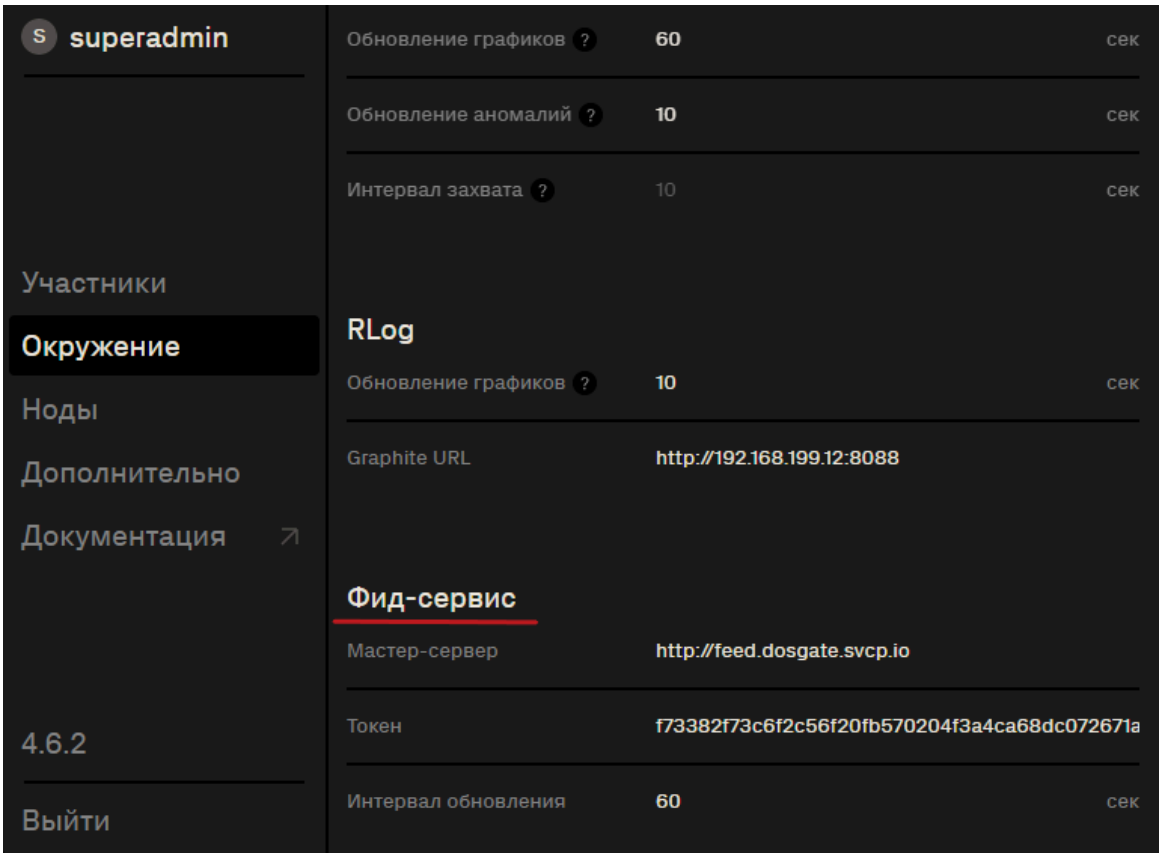
- База вредоносных сигнатур распространяет компоненты-пресеты (готовые легитимные и вредоносные сигнатуры) для защиты сетевых сегметов и сервисов, а также вредоносные IP-списки. Она подключается и настраивается к веб-интерфейсу Spider через настройки окружения

- Содержимое базы вредоносных сигнатур уникально для каждого заказчика
- База вредоносных сигнатур поддерживается в Spider с версии 3.9.7

Шаг 1

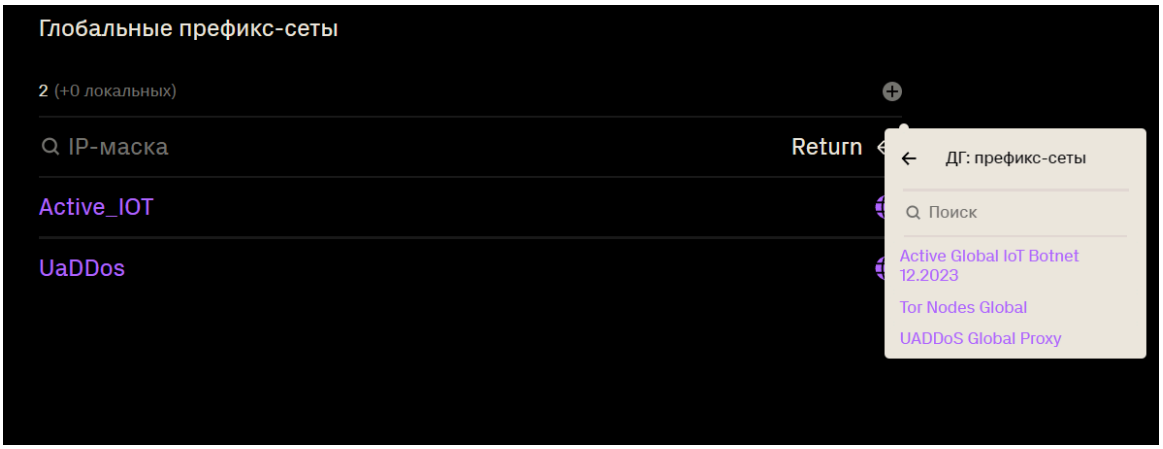
Получите от вендора ссылку на мастер-сервер базы вредоносных сигнатур и ключ

Шаг 2



Укажите ссылку и ключ в настройках окружения Spider. Также, укажите интервал обновления в секундах

Шаг 3



Компоненты-пресеты сразу появятся в вкладке пресетов. IP-списки нужно будет создать в глобальных префикс-сетах. После создания IP-списки будут обновляться сразу в уже созданном префикс-сете и создавать их повторно не потребуется

Все синхронизируемые с базой вредоносных сигнатур сущности помечаются фиолетовым цветом. Их нельзя изменить, но можно дублировать для дальнейшего изменения

Автоматическая установка DG на Ubuntu 22.04: локальная инсталляция

1. Подготовка операционной системы

1.1 Настройка сетевых интерфейсов

Внести необходимые изменения в сетевые интерфейсы в соответствии с текущей сетевой архитектурой компании. При Outline-инсталляции обязательно настроить VLAN'ы.

Для Inline-инсталляции необходимо использовать минимум два физических порта для передачи данных и один порт для управления (mgmt).

Для Outline-инсталляции требуется минимум один физический порт для передачи данных и один порт для управления.

При настройке интерфейсов *ifupdown* учесть следующее:

- Удалить конфигурации линейных интерфейсов из профиля *netplan*, отредактировав файл **/etc/netplan/00-installer-config.yaml**. Конфигурации, относящиеся к mgmt-интерфейсам, допускается оставить без изменений.
- Добавить DNS-сервер в настройку *systemd-resolved*, отредактировав файл **/etc/systemd/resolved.conf**.

В случае недоступности NTP-серверов в связи с политиками безопасности возможно добавить собственный NTP-сервер отредактировав файл **/etc/systemd/timesyncd.conf**.

Примечание
При использовании сетевых карт Intel с драйвером ixgbe рекомендуется ограничить кол-во потоков до 24:

```
ethtool -L eth1 combined 24
```

- https://www.spinics.net/lists/netdev/msg439438.html

При использовании сетевых карт Mellanox, в настройках аппаратных интерфейсов, на которых будет работать DosGate, рекомендуется указать настройку `tune_xdp = 1`. Необходимо открыть для редактирования файл **/etc/network/interfaces**. Вставить следующую строку:

```
tune_xdp = 1
```

1.2 Перезагрузка сервера

Перезагрузить сервер, выполнив команду:

```
sudo reboot
```

2. Установка DosGate с помощью скрипта

2.1 Выполнение скрипта установки DosGate

Скрипт выполняет подключение репозитория Servicepipe, установку DosGate в выбранной конфигурации и первоначальное конфигурирование системы.

Для запуска необходимо выполнить команду:

```
curl -o "./setup-dg.sh" "https://public-
repo.svcp.io/setup_script/setup-dg.sh" && \
```

```
    sudo chmod +x "./setup-dg.sh" && \
    ./setup-dg.sh
```

Перед началом установки выполняется автоматическая проверка системных требований. При обнаружении несоответствия минимально необходимым параметрам отобразится предупреждение:

```
=== Проверка системных требований ===
Количество ядер CPU: 12
Оперативная память: 4 ГБ
Внимание: объем оперативной памяти (4 ГБ) меньше минимального (8 ГБ)
Продолжить установку? (y/n):
```

2.2 Подключение репозитория

После запуска скрипта выполняется проверка наличия репозитория Servicepipe:

```
=== Проверка наличия подключенного репозитория https://public-repo.svcp.io/ ===
Репозиторий https://public-repo.svcp.io/ не подключен.
Выполнить подключение? (y/n): y
```

Для подключения требуется ввести учетные данные (логин и пароль) к репозиторию. Эти учетные данные предоставляются индивидуально для каждого заказчика. Получить их возможно запросив у вендора (Servicepipe или партнёра).

2.3 Выбор конфигурации DosGate для установки

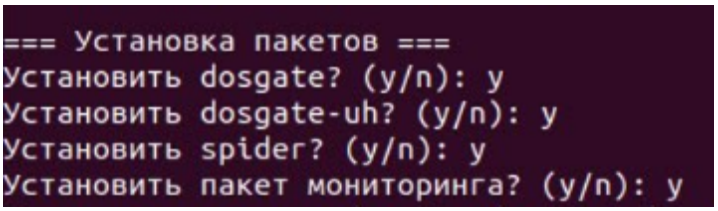
После подключения репозитория скрипт предложит выбрать конфигурацию DosGate.

Установка DosGate включает четыре метапакета:

Метапакет	Компоненты
dosgate Основные компоненты DosGate	• collectd • nginx • sp-spider-broker • libdt1 • libaevent1 • dosgate

Метапакет	Компоненты
dosgate-uh Сессионная защита	• libxskexp • dosgate-uh
spider Компоненты веб-интерфейса	• nodejs (= 18.18.2-1nodesource1) • libpq-dev • postgresql (= 14+238) • rabbitmq-server (= 3.13.6-1) • sp-spider-broker • sp-spider
dosgate-monitoring Компоненты мониторинга	• clickhouse-server (= 23.10.5.20-servicepipe-20250331.151941.UTC) • clickhouse-client (= 23.10.5.20) • carbon-clickhouse • graphite-clickhouse • carbonapi

Укажите необходимый вариант и подтвердите установку.

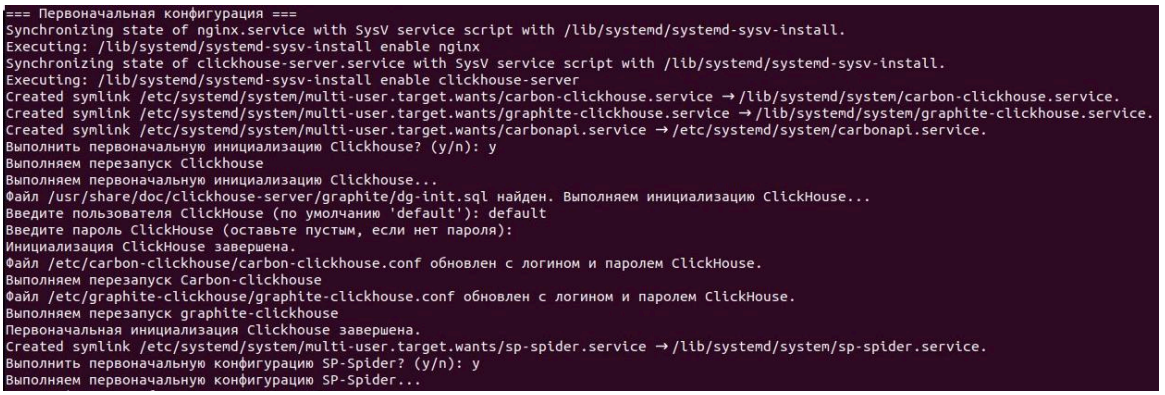


> ***Внимание:***
> В процессе установки, в зависимости от выбранной конфигурации, может потребоваться указать учетные данные (логины и пароли) для доступа к базам данных и брокерам сообщений. Эти данные необходимо сохранить, так как они используются при последующем конфигурировании системы.

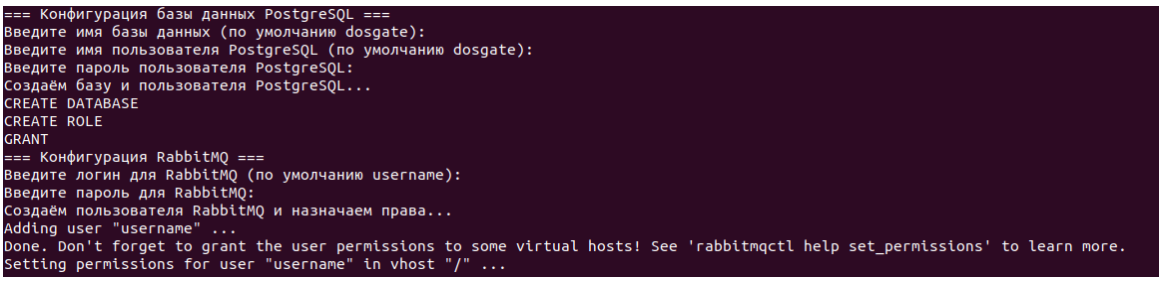
2.4 Первичная настройка системы

В зависимости от выбранной конфигурации выполняется начальная настройка установленных компонентов.

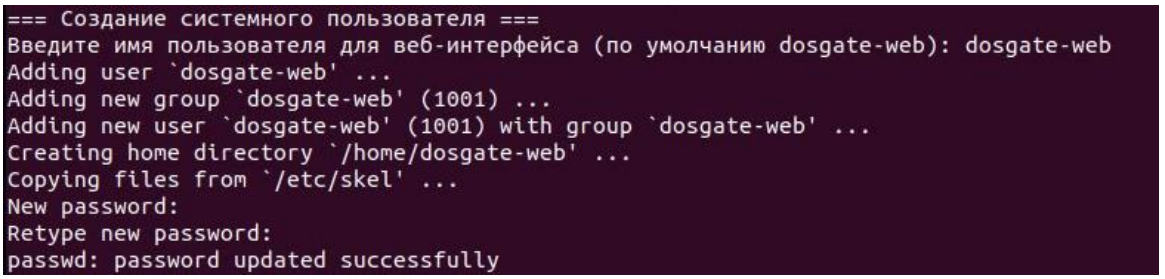
Так, при установке пакета Spider и пакета Monitoring скрипт предложит инициализировать ClickHouse с созданием базы данных, задать параметры в конфигурационных файлах .env для SP-Spider и SP-Spider-Broker.



Затем, выполняется создание базы данных и пользователя PostgreSQL, а также настройка учётной записи RabbitMQ с назначением пароля и прав доступа.



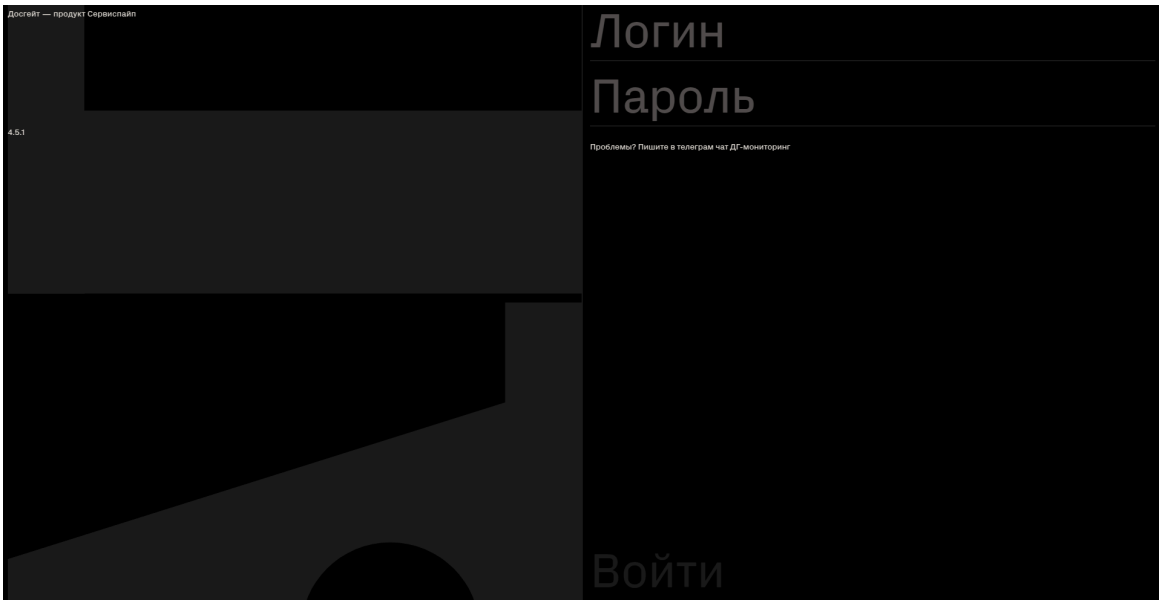
Затем выполняется создание системного пользователя для веб-интерфейса.



3. Первый вход в систему

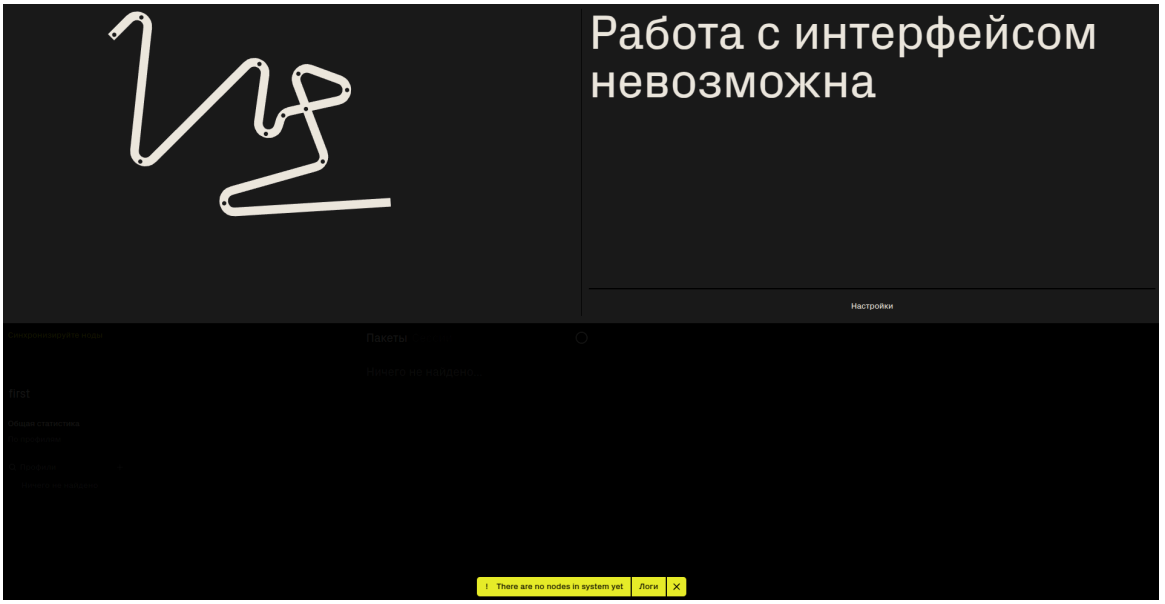
Для входа в Веб-интерфейс DosGate следует ввести в адресной строке браузера IP-адрес сервера и порт по шаблону: `ip:3333`.

Появится окно авторизации (см. рисунок ниже). В окне авторизации следует указать следующие логин и пароль по умолчанию: ***superadmin/superadmin***

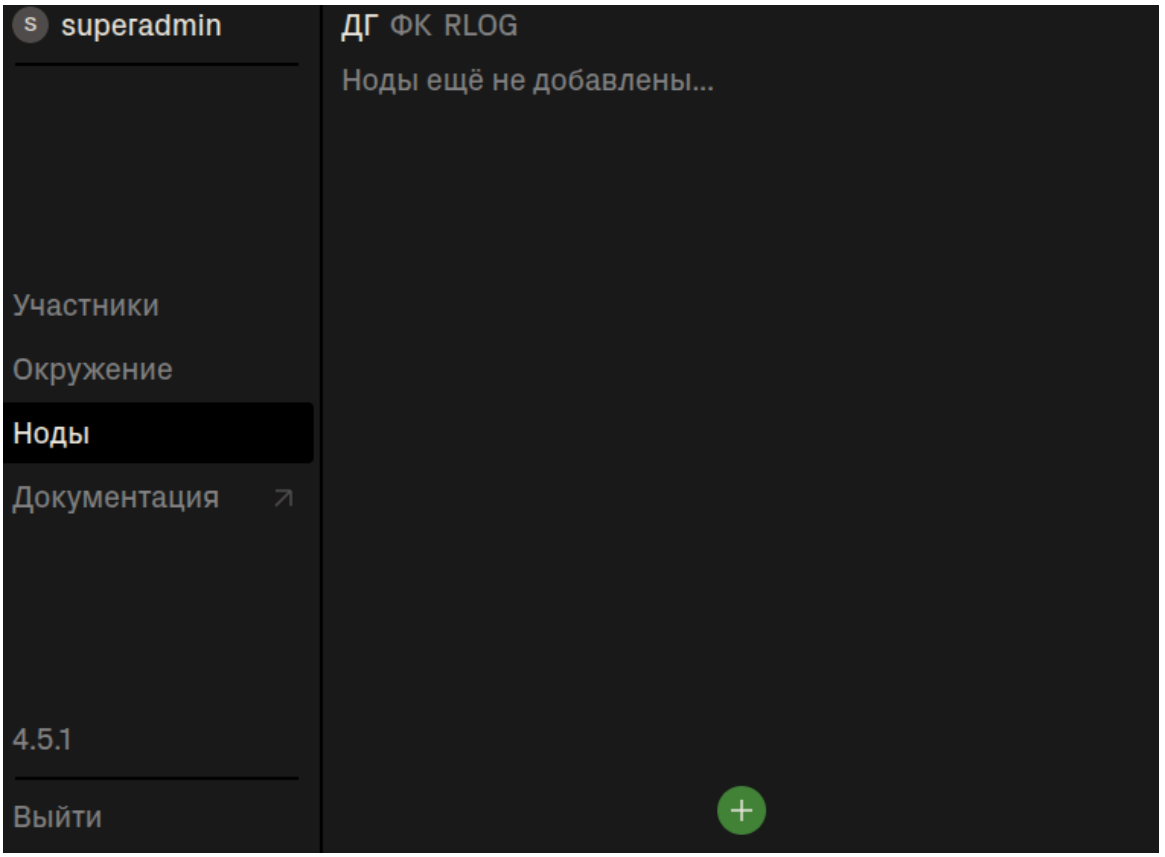


Окно авторизации при входе в систему

После авторизации появится уведомление **Работа с интерфейсом невозможна**. Это связано с тем, что в данный момент нет настроенной ноды.

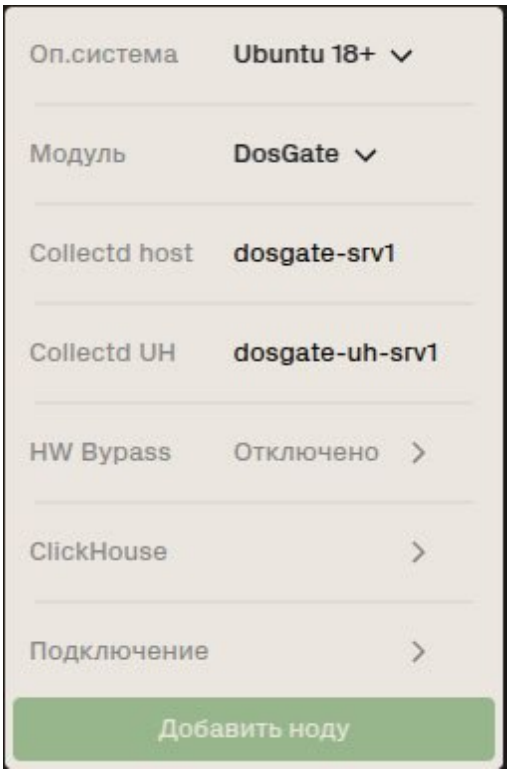


Нажать кнопнку **Настройки**. Откроется окно настроек.

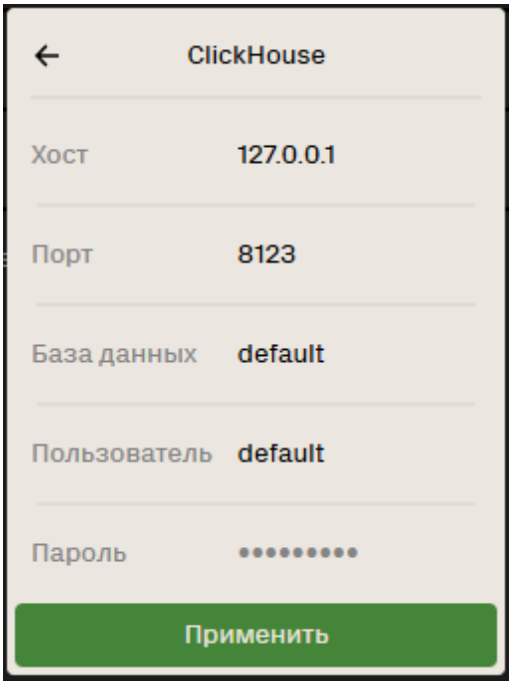


В меню **Ноды** нажать на зелёную иконку с плюсом. В открывшемся окне указать:

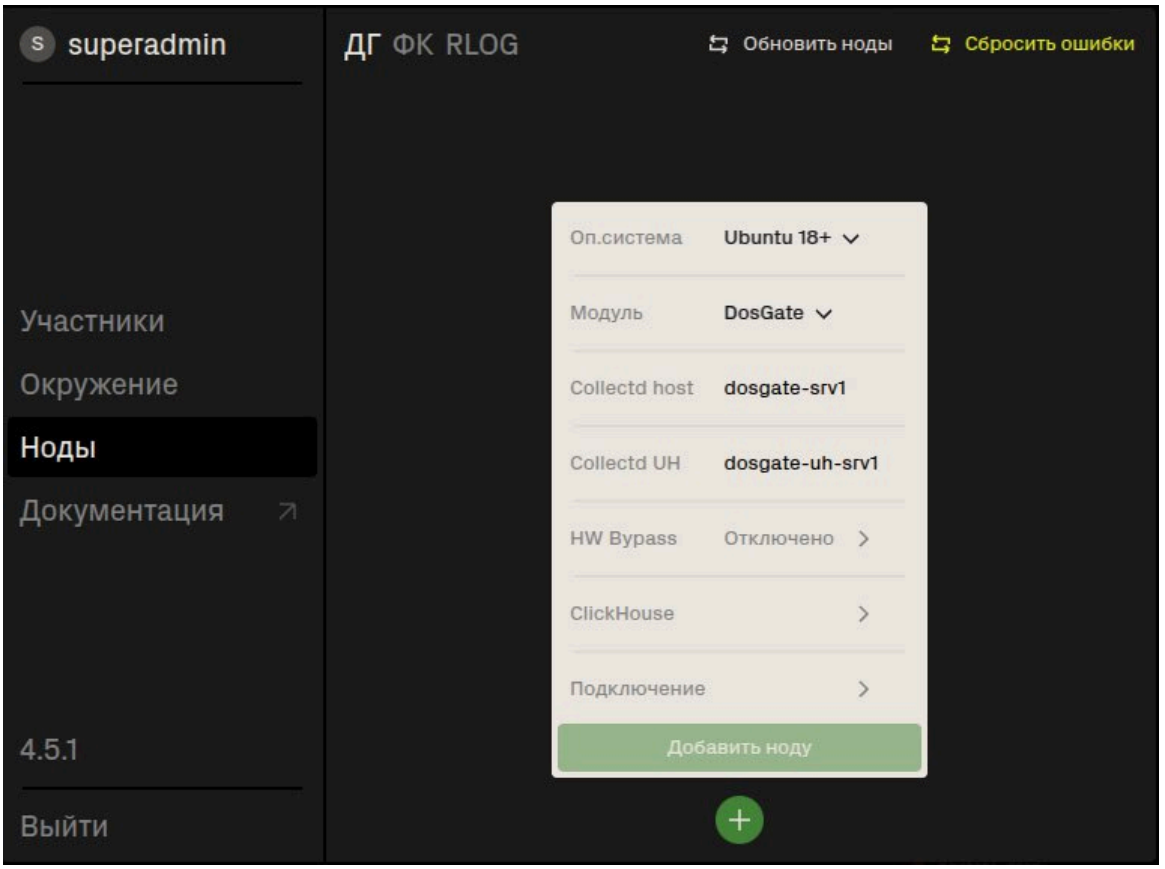
- **Collectd host** — значение должно соответствовать параметру `hostname`, указанному в конфигурационном файле *dosgate.conf* в блоке `collectd`. По умолчанию используется *dosgate-srv1*.
- **Collectd UH** — укажите имя узла, по умолчанию — *dosgate-uh-srv1*.



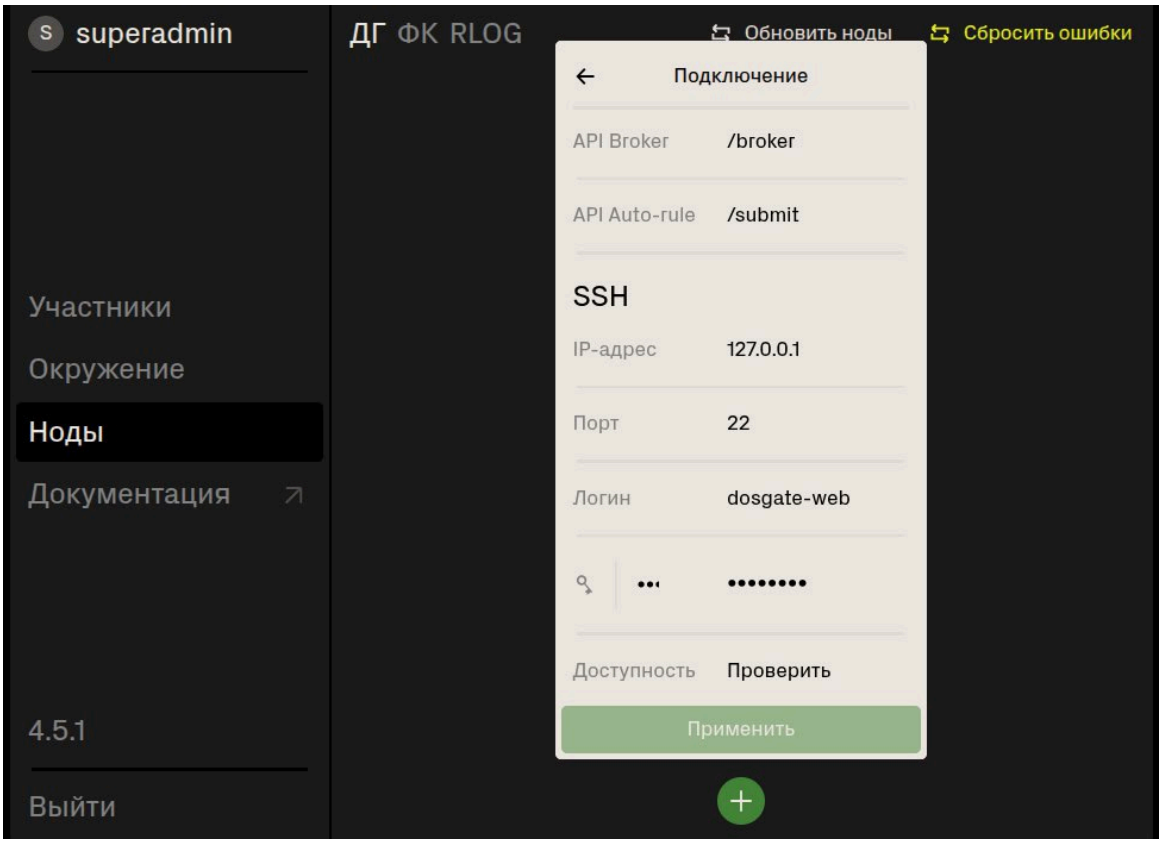
Перейти в настройки **ClickHouse** и указать параметры подключения. Пример настроек для подключения к ClickHouse, установленному на локальной ноде:



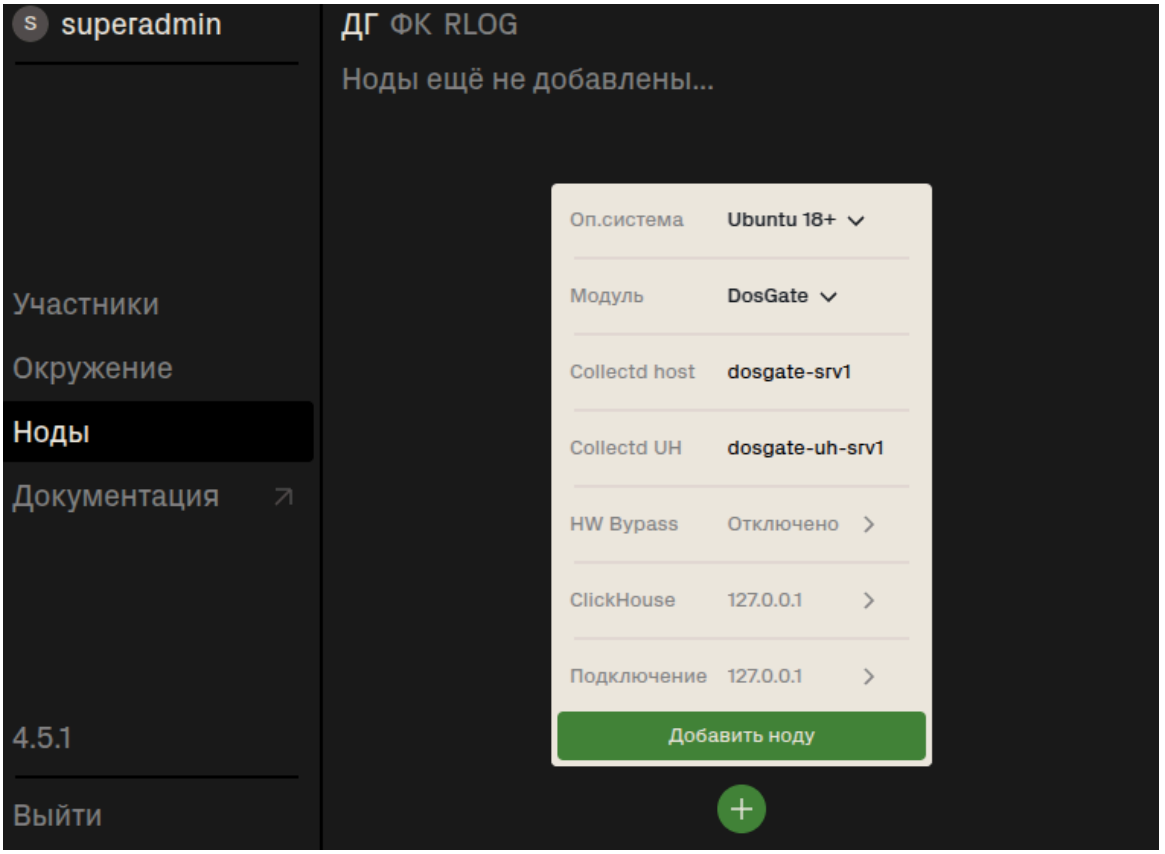
Нажать на кнопку **Применить**. Перейти в раздел **Подключение**.



В открывшемся окне указать SSH-данные для подключения к установленной ноде Dosgate (IP-адрес, логин, пароль). Нажать на кнопку **Проверить**, чтобы проверить подключение. Если данные введены правильно и нода доступна, статус изменится на **Доступна**. После этого нажать кнопку **Применить**. Пример заполненных настроек приведён ниже:

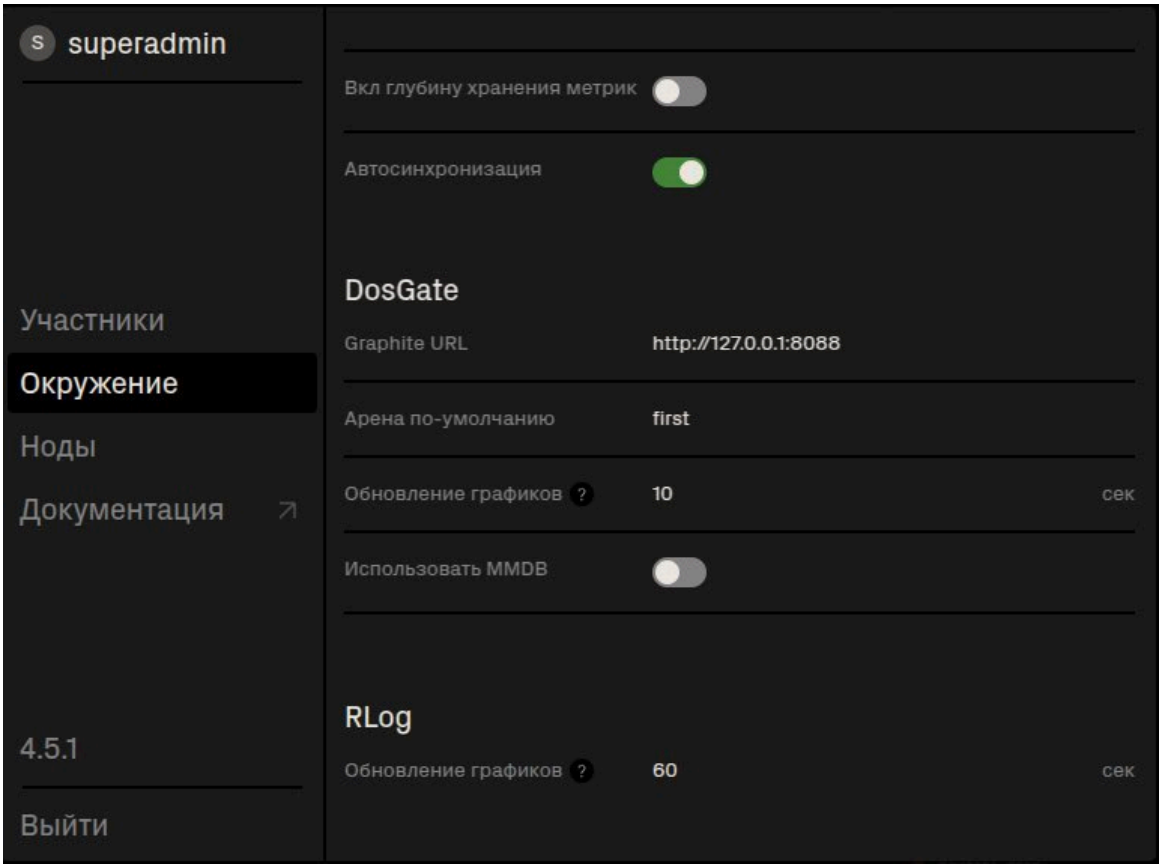


В открывшемся окне нажать **Добавить ноду**.

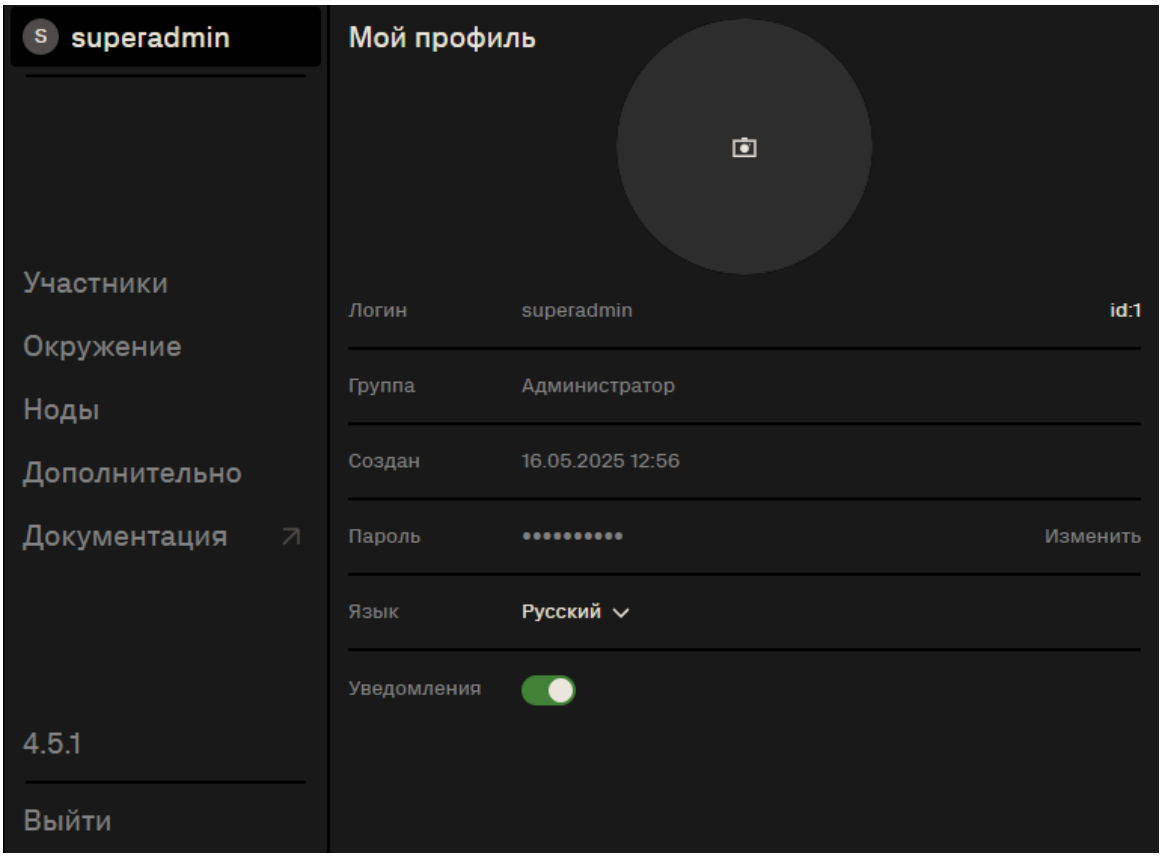


Для отображения графиков и статистики необходимо указать ссылку на Graphite. Перейдите в раздел **Окружение**. В разделе DosGate указать "Graphite URL" и "Арена по-умолчанию". Название арены должно соответствовать значению, указанному в конфигурационном файле dosgate.conf для всех нод кластера.

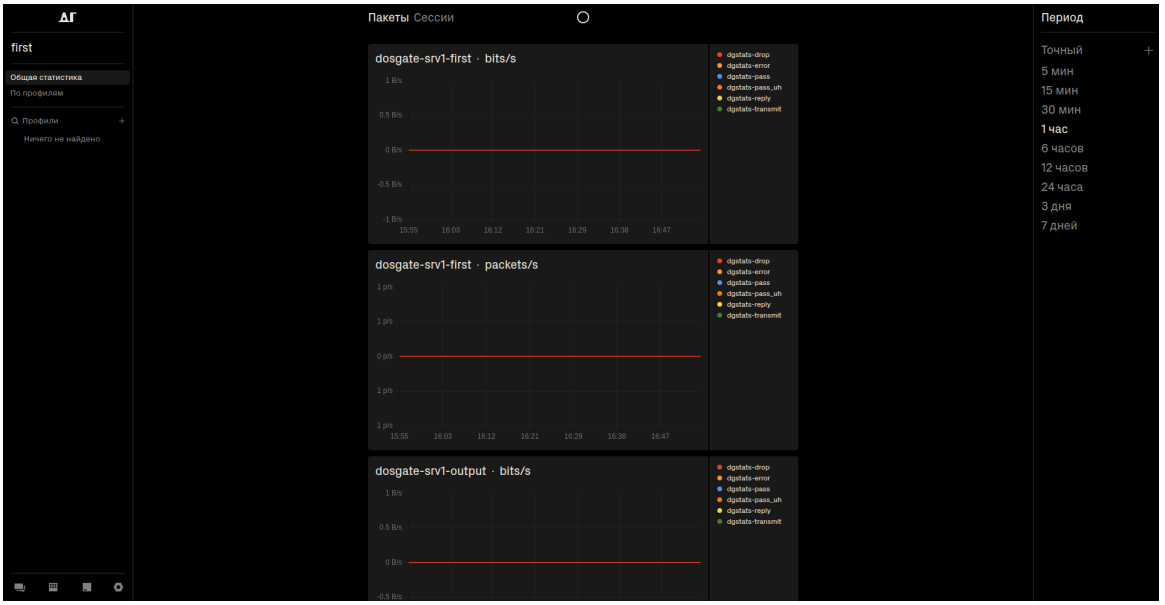
Пример настроек:



Нажать на свой профиль в левом верхнем углу экрана, чтобы открыть настройки профиля. Установить новый пароль.



Выполнить обновление страницы. Веб-интерфейс готов к использованию.



4. Настройка конфигурации DosGate

Все параметры работы Dosgate задаются в едином конфигурационном файле `dosgate.conf`. Конфигурационный файл находится по пути **/etc/dosgate.conf**. Его настройка обязательна перед первым запуском программного обеспечения. Для доступа к командам управления производится аутентификация по SSH.

Конфигурационный файл написан в формате YAML и содержит следующие блоки:

- socket_conf
- arena_conf
- collectd

Подробнее о каждом блоке описано в следующих разделах.

При конфигурировании файла dosgate.conf следует использовать только пробелы; табуляция недопустима.
Для валидации корректности синтаксиса YAML, допустимо использовать сайт https://www.yamllint.com.

4.1 Блок *socket_conf*

Блок *socket_conf* сразу после установки имеет значения по умолчанию. Он настроен для использования и работы с CLI.

Пример конфигурации:

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10
```

```yaml
  - url: /run/dosgate/crlf.socket
    user: nginx:nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10
```

Описание блока

URL

> URL для сокетов имеет формат `family://address`, где:

> *family* — тип сокета, который может принимать следующие значения:

- unix — UNIX-сокет, используемый на файловой системе сервера. В качестве адреса указывается полный путь к сокету.
- tcp — TCP-сокет. Адрес указывается в формате `host:port` или `:port`. Если указан только порт (`:port`), сокет будет прослушивать все доступные адреса (`0.0.0.0` или `::`).

> ***Определение типа сокета по строке адреса***

> Если `family` не указано в URL, тип сокета определяется автоматически по формату строки адреса:

- Если строка начинается с `/`, предполагается, что это UNIX-сокет (family = unix).
- Если строка содержит символ `:`, предполагается, что это TCP-сокет (family = tcp).

User

> Имя пользователя для UNIX-сокетов. Если указанный пользователь отсутствует, сокет будет использовать учетную запись пользователя, от имени которого выполняется процесс (по умолчанию root).

Group

> Группа для UNIX-сокетов. Если указанная группа отсутствует, используется первичная группа пользователя, под которым выполняется процесс (по умолчанию root).

Mode

> Режим доступа для UNIX-сокетов, задается в формате, аналогичном команде `chmod`.

ACL

> Список контроля доступа (Access Control List). Перечисляются через запятую разрешенные target (например: `profile`, `router`, `arena`, `mark`, `pset`), значение `any` - разрешает доступ ко всем частям системы.

Type

> Тип протокола/диалекта для сокета:
>
> - FCGI - FastCGI протокол, полный диалект
> - SCGI - SCGI протокол, полный диалект
> - CRLF - raw протокол, полный диалект
> - CLI - raw протокол, диалект CLI

> RAW - протокол, при котором запрос заканчивается либо последовательностью CRLF, либо закрытием сокета в сторону сервера. Ответ также завершается CRLF или окончательным закрытием сокета.

> ***Особенность для CLI:***

> Для отправки запросов через CLI должен быть настроен хотя бы один сокет с типом CLI, с family UNIX и адресом **/run/dosgate/cli.socket**

Timeout

> Общий лимит времени, в течение которого сокет ожидает завершения операции. Указывается в секундах. При отсутствии установленного таймаута сокет продолжает ожидание завершения операций или остается в состоянии бездействия без ограничения по времени.

- idle - время, в течение которого сокет может оставаться бездействующим (неактивным) перед тем, как будет разорвано соединение или предприняты другие действия.
- send - время, отведенное на отправку данных через сокет. Если данные не удается отправить в течение указанного времени, операция будет прервана.

4.2 Блок *arena_conf*

Основной блок конфигурации DosGate. Данный блок не имеет значений по умолчанию и требует обязательной настройки.

Пример конфигурации:

```
arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
        tx:
          name: ens1f0
          mac: 00:cc:34:4a:88:30
          mode: swap
          vid: 63
      - rx:
          name: ens3f0
          mode: vlan
          vid: 54
        tx:
          name: ens3f0
```

```
          mac: 00:cc:34:4a:88:30
          mode: swap
          vid: 55
      - rx:
          name: ens3f0
          mode: vlan
          vid: 58
        tx:
          name: ens3f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 59
```

Описание блока:

Arenas - Набор сетевых интерфейсов и настроек обработки и возврата трафика.

Name - Уникальное имя арены.

Id - Уникальный Id арены (обязателен с 3.2.2-5).

Name (nets) - Имя сетевого интерфейса, как показывает ip link. Обязательное поле.

MAC - MAC-адрес. Может быть записан в одном из следующих форматов:

`XX:XX:XX:XX:XX:XX` или `XX-XX-XX-XX-XX-XX` или `XXXX.XXXX.XXXX`

Где `X` - шестнадцатеричная цифра.

VID - VLAN id. Число от 0 до 4095, где 0 означает отсутствие тега.

Protocol - Протокол VLAN. Либо hex-число в формате 0x0000, либо мнемоническое значение:

Тэг	Значение
802.1q, 8021q, q	0x8100
802.1ad, 8021ad, ad	0x88A8
802.1ah, 8021ah, ah	0x88E7
q-in-q, qq, qinq	0x9100
q-in-q1, qq2, qinq2	0x9200

Тэг	Значение
q-in-q3, qq3, qinq3	0x9300

RX block - Описывает способ обработки входящего трафика. Должен присутствовать всегда.

```
      - rx:
          name: ens5
          inline: true
          mode: transparent
          tx-policy: lacp
```

Если в блоке указан MAC-адрес, то обрабатывается только трафик с этим destination address.

`inline` - Интерфейс работает в inline-режиме, то есть он невидим для других хостов в сети. ARP-запросы, широковещательные запросы, STP/GVRP/etc не передаются в ОС. Если опция не указана, то интерфейс пересылает этот трафик в ОС.

`mode` - Режим обработки входящего трафика:

- `vlan` - обрабатывается только трафик в указанном VLAN, остальной пропускается в ОС. Если VID = 0 или не указан, обрабатывается только нетегированный трафик.
- `transparent` - обрабатывается трафик во всех VLAN + нетегированный. Используется по умолчанию.

`swap` - Указывает, нужно ли менять MAC-адреса во фрейме при отправке.

> Если указано `false` или `0`, то адреса не меняются. Если указано `true`, `1` или значение не указано , то адреса меняются.

`tx-policy` - управляет обработкой следующих классов трафика:

- `lacp` — медленный протокол LACP.
- `llm` — IEEE802.1 Link-local multicast, предназначенная для 01:80:C2:00:00:x.
- `multicast` - Любой L2 multicast, кроме link-local.
- `unknown` - unhandled ethertypes.

Например, если параметр LACP отсутствует, то LACP будет передан в ОС DosGate, а не в TX-интерфейс.

TX block - Описывает политику обработки трафика, который должен быть переслан в соответствии с окончанием обработки правилами или срабатывании действия ACCEPT. Если не указан, то копируется из блока RX, а отсутствующие в нём параметры принимают значения по умолчанию.

```
      - tx:
          name: ens4
          mac: fa:16:3e:56:32:6a
          swap: false
```

Если в блоке указан MAC-адрес, то трафик пересылается на него. В противном случае он отправляется на тот адрес, с которого был получен

`Mode` - Режим обработки исходящего трафика:

> - `swap` - меняется последний в стеке тег VLAN, или добавляется если трафик нетегированный. Если VID отсутствует, то пакет не меняется, если равен 0, то верхний тег снимается при наличии. Используется по умолчанию.
> - `push` - новый тег добавляется безусловно, даже если последний был точно таким же. Если VID = 0 или отсутствует, то ничего не добавляется.

`cos` - Класс сервиса в тегированных пакетах. Число от 0 до 7.

Reply block - Описывает политику обработки трафика, который должен быть переслан в соответствии с правилами, которые генерируют собственный трафик в ответ на входящий пакет.

```
        tx:
          name: ens5
          swap: false
        reply:
          name: ens4
          swap: true
```

- Если `reply` не указан, то автоматически копируется из *TX block*. Формат полностью соответствует формату *TX block*.

4.3 Блок *collectd*

```
collectd:
  hostname: dosgate-srv1
  period: 10
```

- `hostname` - имя хоста, который будет использоваться для именования метрик. Если вы устанавливаете DosGate в кластере, название должно быть уникально для каждой платформы. Именно под этим именем будут отображаться графики по серверам в общей статистике. Также с этим именем записываются метрики относительно сервера.
- `period` - частота записи метрик в collectd.

4.4 Примеры конфигурационного dosgate.conf файла

Ниже приведены примеры конфигурационных файлов **dosgate.conf**:

Пример outline инсталяции с VLAN swap и возвратом трафика в том-же интерфейсе

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nginx:nginx
    mode: 0660
    acl: any
```

```
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
        tx:
          name: ens1f0
          mac: 00:aa:12:45:87:99
          mode: swap
          vid: 63

collectd:
  hostname: dosgate-srv1
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DosGate

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
```

```
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp4s0f0np0
          inline: true
          mode: transparent
        tx:
          name: enp4s0f1np1
          swap: false
        reply:
          name: enp4s0f0np0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
```

```
          name: enp4s0f1np1
          inline: true
          mode: transparent
        tx:
          name: enp4s0f0np0
          swap: false

collectd:
  hostname: dosgate-srv1
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DoSGate с LACP

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
```

```
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp136s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f1
          swap: false
        reply:
          name: enp136s0f0
          swap: true
      - rx:
          name: enp138s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f1
          swap: false
        reply:
          name: enp138s0f0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
          name: enp136s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f0
          swap: false
      - rx:
          name: enp138s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f0
          swap: false

collectd:
```

```
  hostname: dosgate-srv1
  period: 10
```

5. Настройка конфигурации сессионной защиты

Все параметры работы сессионной защиты задаются в едином конфигурационном файле `dosgate-uh.conf`.

Для редактирования конфигурационного файла выполнить команду:

```
sudo nano /etc/dosgate-uh.conf
```

5.1 Глобальная конфигурация

Глобальные параметры определяют политику обработки сетевого трафика:

```
global:
  traffic-policy:
    good: accept   # Разрешение корректного трафика
    bad: drop      # Отклонение подозрительного трафика
    violate: drop  # Отклонение нарушающего трафика
```

5.2 Конфигурация сетевых устройств

Для эффективного управления очередями приема и передачи пакетов необходимо настроить параметры сетевых интерфейсов:

```
net:
  ens224:
    rx:
      queues:
        count: 8  # Количество очередей приема
        len: 512  # Длина каждой очереди
  ens256:
    tx:
      queues:
```

```
        count: 8  # Количество очередей приема
        len: 512  # Длина каждой очереди
```

5.3 Настройки захвата трафика

Функция захвата трафика позволяет записывать сетевые пакеты в файлы для последующего анализа:

```
capture:
  path: /var/cache/dosgate-uh/capture      # Директория для
сохранения
  filename: cap_${DEV}_${ID}_${NUM}.pcap   # Шаблон имен файлов
  age: 3600                                # Максимальное время
хранения файла (в секундах)
  count: 10                                # Максимальное
количество файлов
  size: 10M                                # Максимальный размер
файла
```

5.4 Конфигурация сбора и экспорта статистики

Статистика помогает отслеживать состояние системы в реальном времени и экспортировать данные в систему мониторинга:

```
stats:
  period: 10                              # Период сбора статистики
(в секундах)
  push:
    type: collectd                        # Метод передачи данных
    plugin: unixsock                      # Используемый плагин
    target: /var/run/collectd-unixsock    # Целевой сокет
    stats: all                            # Объем передаваемых
данных
    hostname: dosgate-uh-srv1                # Идентификатор хоста
    queue-len: 0                          # Длина очереди отправки
    period:
      collect: 5                          # Интервал сбора данных
(в секундах)
      send: 10                            # Интервал отправки
данных (в секундах)
```

5.5 Настройка отслеживания подключений

Параметры контроля соединений позволяют задавать ограничения и определять политику обработки трафика:

```
conntrack:
  limit: 10000000       # Максимальное количество отслеживаемых
соединений
  reclaim:
    soft: 80            # Порог мягкого освобождения соединений (в
% от лимита)
    hard: 95            # Порог жесткого освобождения соединений
(в % от лимита)
```

5.6 Путь к каталогу с реестром профиля приложения

По умолчанию: **/var/lib/dosgate-uh/profiles**

```
application:
  registry: /var/lib/dosgate-uh/profiles
  monitor-fs: true
```

5.7 Настройка экспорта фреймов

Обеспечение работы функции экспорта фреймов, которая выполняется в рамках действия dosgate action `-j EXPORT`:

```
frame-export:
  enabled: true         # Включение функции экспорта фреймов
  export-objects: all   # Экспорт всех объектов
```

5.8 Пример конфигурационного файла *dosgate-uh.conf*

Ниже приведен пример конфигурационного файла **dosgate-uh.conf**:

```
global:
  threads: 8
  thread-policy: pooled
  cpus:
    irq: 0-7
    thread: 0-7
```

```
  traffic-policy:
    good: accept
    bad: drop
    violate: drop
  trace: exp

net:
  eth0:
    rx:
      queues:
        count: 8
        len: 512
    tx:
      queues:
        count: 8
        len: 512
  eth1:
    rx:
      queues:
        count: 8
        len: 512
    tx:
      queues:
        count: 8
        len: 512

capture:
  path: /var/cache/dosgate-uh/capture
  filename: cap_${DEV}_${ID}_${NUM}.pcap
  age: 10
  count: 1
  size: 100M

stats:
  period: 10
  push:
    type: collectd
    plugin: unixsock
    target: /var/run/collectd-unixsock
    stats: all
    hostname: dosgate-uh-srv1
    queue-len: 0
    period:
      collect: 5
      send: 10

conntrack:
  limit: 100000
  reclaim:
    soft: 80
    hard: 95
```

```
application:
  registry: /var/lib/dosgate-uh/profiles
  monitor-fs: true
```

Установка DG на Ubuntu 22.04: локальная инсталляция

Инструкция по установке с внешним веб-интерфейсом управления

1. Подготовка операционной системы

Актуальные версии элементов ПАК
DosGate (ядро): `3.9.2-1`
DosGate-UH: `1.5.3-2`
Библиотека libdt1: `1.2.7-4`
Библиотека libaevent1: `0.2.1-4`
Библиотека libxskexp: `0.0.2-1`
SP-Spider (веб-интерфейс): `4.7-1`
SP-Spider-Broker (брокер сообщений): `1.0.24`

1.1 Установка обновлений ОС

Для обновления ОС Ubuntu необходимо выполнить следующие команды:

```
sudo apt update
```

```
sudo apt upgrade
```

1.2 Подключение репозитория Servicepipe

Подключить репозиторий Servicepipe возможно двумя способами: через скрипт или вручную. Для подключения к репозиторию потребуются логин и пароль. Эти учетные данные предоставляются индивидуально для каждого заказчика. Получить их возможно запросив у вендора (Servicepipe или партнёра).

Подключение с помощью скрипта

Выполнить скрипт для автоматической настройки репозитория:

```
curl -o "./setup-repo.sh" "https://public-
repo.svcp.io/setup_script/setup-repo.sh" && \
    sudo chmod +x "./setup-repo.sh" && \
    sudo ./setup-repo.sh
```

При запуске скрипта потребуется ввести логин и пароль. После ввода учетных данных скрипт выполнит все необходимые действия автоматически. В случае некорректной работы скрипта рекомендуется использовать метод ручной настройки репозитория.

Подключение вручную

Добавить ключ:

```
sudo wget --http-user=[ваш логин] --http-password=[ваш пароль] -O
- https://public-repo.svcp.io/keyFile | \
            sudo gpg --dearmor -o
/etc/apt/keyrings/servicepipe.gpg
```

Добавить репозиторий:

```
echo "deb [arch=amd64 signed-by=/etc/apt/keyrings/servicepipe.gpg]
https://public-repo.svcp.io/ubuntu/ xenial contrib" >
/etc/apt/sources.list.d/servicepipe.list
```

Добавить авторизационные данные:

```
echo 'machine public-repo.svcp.io login [ЛОГИН] password [ПАРОЛЬ]'
> /etc/apt/auth.conf
```

Проверить доступность репозитория:

```
sudo apt update
```

1.3 Настройка сетевых интерфейсов

Внести необходимые изменения в сетевые интерфейсы в соответствии с текущей сетевой архитектурой компании. При Outline-инсталляции обязательно настроить VLAN'ы.

Для Inline-инсталляции необходимо использовать минимум два физических порта для передачи данных и один порт для управления.

Для Outline-инсталляции требуется минимум один физический порт для передачи данных и один порт для управления (mgmt).

При настройке интерфейсов *ifupdown* учесть следующее:

- Удалить конфигурации линейных интерфейсов из профиля *netplan*, отредактировав файл **/etc/netplan/00-installer-config.yaml**. Конфигурации, относящиеся к mgmt-интерфейсам, допускается оставить без изменений.
- Добавить DNS-сервер в настройку *systemd-resolved*, отредактировав файл **/etc/systemd/resolved.conf**.

В случае недоступности NTP-серверов в связи с политиками безопасности возможно добавить собственный NTP-сервер отредактировав файл **/etc/systemd/timesyncd.conf**.

Примечание
При использовании сетевых карт Intel с драйвером ixgbe рекомендуется ограничить кол-во потоков до 24:

```
ethtool -L eth1 combined 24
```

- https://www.spinics.net/lists/netdev/msg439438.html

При использовании сетевых карт Mellanox, в настройках аппаратных интерфейсов, на которых будет работать DosGate, рекомендуется указать настройку `tune_xdp = 1`. Необходимо открыть для редактирования файл **/etc/network/interfaces**. Вставить следующую строку:

```
tune_xdp = 1
```

1.4 Перезагрузка сервера

Перезагрузить сервер, выполнив команду:

```
sudo reboot
```

2. Установка компонентов DosGate

2.1 Состав метапакетов

Для установки DosGate в различной конфигурации доступны шесть метапакетов:

Метапакет	Компоненты
dosgate-only Основные компоненты	• dosgate • libdt1 • libaevent1 • collectd • nginx • sp-spider-broker
dosgate-dosgate-uh Основные компоненты и сессионная защита	• метапакет dosgate-only • dosgate-uh • libxskexp
spider-only Веб-интерфейс	• nodejs • libpq-dev • postgresql • rabbitmq-server • sp-spider-broker • sp-spider
dosgate-spider Основные компоненты и веб-интерфейс	• метапакет dosgate-only • метапакет spider-only
dosgate-dosgate-uh-spider Основные компоненты, сессионная защита и веб-интерфейс	• метапакет dosgate-dosgate-uh • метапакет spider-only
dosgate-monitoring Компоненты мониторинга	• clickhouse-server • clickhouse-client • carbon-clickhouse • graphite-clickhouse • carbonapi

Примечание
Пакет **dosgate-monitoring** можно не устанавливать, если система мониторинга развернута на отдельном сервере.

2.2 Установка компонентов

Для установки DosGate, веб-интерфейса и компонентов мониторинга следует выполнить следующую команду:

```
sudo NEEDRESTART_MODE=a apt-get install -y \
    dosgate-spider \
    dosgate-monitoring
```

2.3 Настройка конфигурации

Все параметры работы Dosgate задаются в едином конфигурационном файле `dosgate.conf`. Конфигурационный файл находится по пути **/etc/dosgate.conf**. Его настройка обязательна перед первым запуском программного обеспечения.

- Для доступа к командам управления производится аутентификация по SSH.
- Все функции ПО используются за счет взаимодействия с командой: `dgctl`

Конфигурационный файл написан в формате YAML и содержит следующие блоки:

- socket_conf
- arena_conf
- collectd

Подробнее о каждом блоке описано в следующих разделах.

При конфигурировании файла dosgate.conf следует использовать только пробелы; табуляция недопустима.
Для валидации корректности синтаксиса YAML, допустимо использовать сайт https://www.yamllint.com.

2.3.1 Блок *socket_conf*

Блок *socket_conf* сразу после установки имеет значения по умолчанию. Он настроен для использования и работы с CLI.

Пример конфигурации:

```yaml
sockets:
  - url: /run/dosgate/api.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10
```

Описание блока

URL

> URL для сокетов имеет формат `family://address`, где:

> *family* — тип сокета, который может принимать следующие значения:

- unix — UNIX-сокет, используемый на файловой системе сервера. В качестве адреса указывается полный путь к сокету.
- tcp — TCP-сокет. Адрес указывается в формате `host:port` или `:port`. Если указан только порт (`:port`), сокет будет прослушивать все доступные адреса (`0.0.0.0` или `::`).

> ***Определение типа сокета по строке адреса***

> Если `family` не указано в URL, тип сокета определяется автоматически по формату строки адреса:

- Если строка начинается с `/`, предполагается, что это UNIX-сокет (family = unix).
- Если строка содержит символ `:`, предполагается, что это TCP-сокет (family = tcp).

User

> Имя пользователя для UNIX-сокетов. Если указанный пользователь отсутствует, сокет будет использовать учетную запись пользователя, от имени которого выполняется процесс (по умолчанию root).

Group

> Группа для UNIX-сокетов. Если указанная группа отсутствует, используется первичная группа пользователя, под которым выполняется процесс (по умолчанию root).

Mode

> Режим доступа для UNIX-сокетов, задается в формате, аналогичном команде `chmod`.

ACL

> Список контроля доступа (Access Control List). Перечисляются через запятую разрешенные target (например: `profile`, `router`, `arena`, `mark`, `pset`), значение `any` - разрешает доступ ко всем частям системы.

Type

> Тип протокола/диалекта для сокета:
>
> - FCGI - FastCGI протокол, полный диалект
> - SCGI - SCGI протокол, полный диалект
> - CRLF - raw протокол, полный диалект
> - CLI - raw протокол, диалект CLI

> RAW - протокол, при котором запрос заканчивается либо последовательностью CRLF, либо закрытием сокета в сторону сервера. Ответ также завершается CRLF или окончательным закрытием сокета.

> ***Особенность для CLI:***

> Для отправки запросов через CLI должен быть настроен хотя бы один сокет с типом CLI, с family UNIX и адресом **/run/dosgate/cli.socket**

Timeout

> Общий лимит времени, в течение которого сокет ожидает завершения операции. Указывается в секундах. При отсутствии установленного таймаута сокет продолжает ожидание завершения операций или остается в состоянии бездействия без ограничения по времени.

- idle - время, в течение которого сокет может оставаться бездействующим (неактивным) перед тем, как будет разорвано соединение или предприняты другие действия.
- send - время, отведенное на отправку данных через сокет. Если данные не удается отправить в течение указанного времени, операция будет прервана.

2.3.2 Блок *arena_conf*

Основной блок конфигурации DosGate. Данный блок не имеет значений по умолчанию и требует обязательной настройки.

Пример конфигурации:

```
arenas:
  - name: first
    id: 1
```

```
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
        tx:
          name: ens1f0
          mac: 00:cc:34:4a:88:30
          mode: swap
          vid: 63
      - rx:
          name: ens3f0
          mode: vlan
          vid: 54
        tx:
          name: ens3f0
          mac: 00:cc:34:4a:88:30
          mode: swap
          vid: 55
      - rx:
          name: ens3f0
          mode: vlan
          vid: 58
        tx:
          name: ens3f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 59
```

Описание блока:

Arenas - Набор сетевых интерфейсов и настроек обработки и возврата трафика.

Name - Уникальное имя арены.

Id - Уникальный Id арены (обязателен с 3.2.2-5).

Name (nets) - Имя сетевого интерфейса, как показывает ip link. Обязательное поле.

MAC - MAC-адрес. Может быть записан в одном из следующих форматов:

`XX:XX:XX:XX:XX:XX` или `XX-XX-XX-XX-XX-XX` или `XXXX.XXXX.XXXX`

Где `X` - шестнадцатеричная цифра.

VID - VLAN id. Число от 0 до 4095, где 0 означает отсутствие тега.

Protocol - Протокол VLAN. Либо hex-число в формате 0x0000, либо мнемоническое значение:

Тэг	Значение
802.1q, 8021q, q	0x8100
802.1ad, 8021ad, ad	0x88A8
802.1ah, 8021ah, ah	0x88E7
q-in-q, qq, qinq	0x9100
q-in-q1, qq2, qinq2	0x9200
q-in-q3, qq3, qinq3	0x9300

RX block - Описывает способ обработки входящего трафика. Должен присутствовать всегда.

```
    - rx:
        name: ens5
        inline: true
        mode: transparent
        tx-policy: lacp
```

Если в блоке указан MAC-адрес, то обрабатывается только трафик с этим destination address.

`inline` - Интерфейс работает в inline-режиме, то есть он невидим для других хостов в сети. ARP-запросы, широковещательные запросы, STP/GVRP/etc не передаются в ОС. Если опция не указана, то интерфейс пересылает этот трафик в ОС.

`mode` - Режим обработки входящего трафика:

> - `vlan` - обрабатывается только трафик в указанном VLAN, остальной пропускается в ОС. Если VID = 0 или не указан, обрабатывается только нетегированный трафик.
> - `transparent` - обрабатывается трафик во всех VLAN + нетегированный. Используется по умолчанию.

`swap` - Указывает, нужно ли менять MAC-адреса во фрейме при отправке.

> Если указано `false` или `0`, то адреса не меняются. Если указано `true`, `1` или значение не указано , то адреса меняются.

`tx-policy` - управляет обработкой следующих классов трафика:

> - `lacp` — медленный протокол LACP.
> - `llm` — IEEE802.1 Link-local multicast, предназначенная для 01:80:C2:00:00:x.
> - `multicast` - Любой L2 multicast, кроме link-local.
> - `unknown` - unhandled ethertypes.

Например, если параметр LACP отсутствует, то LACP будет передан в ОС DosGate, а не в TX-интерфейс.

TX block - Описывает политику обработки трафика, который должен быть переслан в соответствии с окончанием обработки правилами или срабатывании действия ACCEPT. Если не указан, то копируется из блока RX, а отсутствующие в нём параметры принимают значения по умолчанию.

```
      - tx:
          name: ens4
```

```
          mac: fa:16:3e:56:32:6a
          swap: false
```

Если в блоке указан MAC-адрес, то трафик пересылается на него. В противном случае он отправляется на тот адрес, с которого был получен

`Mode` - Режим обработки исходящего трафика:

> - `swap` - меняется последний в стеке тег VLAN, или добавляется если трафик нетегированный. Если VID отсутствует, то пакет не меняется, если равен 0, то верхний тег снимается при наличии. Используется по умолчанию.
> - `push` - новый тег добавляется безусловно, даже если последний был точно таким же. Если VID = 0 или отсутствует, то ничего не добавляется.

`cos` - Класс сервиса в тегированных пакетах. Число от 0 до 7.

Reply block - Описывает политику обработки трафика, который должен быть переслан в соответствии с правилами, которые генерируют собственный трафик в ответ на входящий пакет.

```
        tx:
          name: ens5
          swap: false
        reply:
          name: ens4
          swap: true
```

- Если `reply` не указан, то автоматически копируется из *TX block*. Формат полностью соответствует формату *TX block*.

2.3.3 Блок *collectd*

```
collectd:
  hostname: dosgate-srv1
  period: 10
```

- `hostname` - имя хоста, который будет использоваться для именования метрик. Если вы устанавливаете DosGate в кластере, название должно быть уникально для каждой платформы. Именно под этим именем будут отображаться графики по серверам в общей статистике. Также с этим именем записываются метрики относительно сервера.
- `period` - частота записи метрик в collectd.

2.3.4 Примеры конфигурационного файла dosgate.conf

Пример outline инсталяции с VLAN swap и возвратом трафика в том-же интерфейсе

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: ![Alt text](/media/dosgate/image.png)
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nginx:nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
```

```
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
collectd:
  hostname: dosgate-srv1
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DosGate

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
```

```
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp4s0f0np0
          inline: true
          mode: transparent
        tx:
          name: enp4s0f1np1
          swap: false
        reply:
          name: enp4s0f0np0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
          name: enp4s0f1np1
          inline: true
          mode: transparent
        tx:
          name: enp4s0f0np0
          swap: false

collectd:
  hostname: dosgate-srv1
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DoSGate с LACP

```yaml
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp136s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f1
          swap: false
```

```
        reply:
          name: enp136s0f0
          swap: true
      - rx:
          name: enp138s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f1
          swap: false
        reply:
          name: enp138s0f0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
          name: enp136s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f0
          swap: false
      - rx:
          name: enp138s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f0
          swap: false

collectd:
  hostname: dosgate-srv1
  period: 10
```

2.3.5 Установка и настройка BIRD для Outline-схемы

Для Outline инсталляции трафик на очистку управляется по BGP демоном *bird*. Рекомендуемая версия *bird* 1.6.8; на более новых релизах настройки аналогичны, но синтаксис может отличаться.

Установить *bird*:

```
sudo apt install bird
```

Далее необходимо подготовить конфигурацию *bird*.

Очистить основной конфиг:

```
sudo cat /dev/null > /etc/bird/bird.conf
```

Создать файл для статических маршрутов:

```
sudo touch /etc/bird/routes.conf
```

Создать каталог для логов:

```
sudo mkdir /var/log/bird
```

Создать файл лога:

```
sudo touch /var/log/bird/bird.log
```

Назначить владельца каталога логов:

```
sudo chown -R  bird:bird /var/log/bird
```

Открыть конфиг для редактирования:

```
sudo nano /etc/bird/bird.conf
```

Пример концигурационного файла **/etc/bird/bird.conf**:

```
timeformat base     iso long;
timeformat log      iso long;
timeformat protocol iso long;
timeformat route    iso long;

log "/var/log/bird/bird.log" all;
log stderr all;

router id 10.10.10.2;                   # IPv4-адрес, с которого
```

```
BIRD устанавливает BGP-соседство
table dosgate;

protocol kernel {
        scan time 60;
        import none;
        export all;
}

protocol device {
        scan time 60;
}

protocol static nexthop {
        table dosgate;
        include "/etc/bird/routes.conf";  # Файл со статическими
маршрутами
}

# Конфигурация нейбора

protocol bgp dosgate_1 {
        table dosgate;
        export none;
        import all;
        local as 65000; # Dosgate local AS
        neighbor 10.0.10.2 as 11111; # BGP Neighbor IP & ASN
}
```

Перезагрузить *bird*

```
sudo service bird restart
```

Проверить статус сервиса:

```
sudo service bird status
```

Проверить общий статус BGP-протоколов (активные сессии должны быть Established):

```
sudo birdc show protocols
```

Проверить состояние конкретной BGP-сессии (замените dosgate_1 на имя вашей сессии):

```
sudo birdc show protocols dosgate_1
```

Посмотреть, какие маршруты экспортируются этому соседу:

```
sudo birdc show route export dosgate_1
```

Редактирование статических маршрутов для перенаправления трафика в DosGate выполняется в файле **/etc/bird/routes.conf**. Формат записи:

```
route 192.168.0.0/25 blackhole;
route 192.168.0.155/32 blackhole;
```

Изменения применяются командой:

```
sudo birdc c
```

2.4 Однократный запуск DosGate

Однократный запуск DosGate выполняется с целью проверки корректности заполнения конфигурационного файла и отсутствия ошибок. Выполнить следующую команду:

```
sudo dosgate -o -l err
```

где:

- `o` — режим однократного запуска (one-shot mode);
- `l err` — параметр, задающий уровень логирования.

Описание уровней логирования:

Уровень	Описание
debug	Отладочная информация. Подробные сведения о действиях процесса, включая системные и библиотечные вызовы.
info	Стандартная информация о работе процесса. Сообщает, например, об открытии файлов без деталей о внутренних вызовах.

Уровень	Описание
warn	Предупреждения о нарушениях нормальной работы процесса без его остановки.
err	Ошибки, приводящие к нарушению нормальной работы объекта.
crit	Критические ситуации, угрожающие стабильности системы.

Детали запуска рекомендуется просмотреть в логах сервиса:

```
sudo systemctl status dosgate
```

2.5 Логирование работы сервисов dosgate и dosgate-uh

Сервисы *dosgate* и *dosgate-uh* осуществляют логирование работы системы в зависимости от выбранного режима. Логирование ведется в *service log* и доступно для просмотра с использованием команд:

```
sudo journalctl -xefu dosgate
```

```
sudo journalctl -xefu dosgate-uh
```

Поддерживаются три режима логирования:

debug – детализированное логирование, фиксируются практически все действия системы, включая обработку каждого сетевого пакета.
error – запись только сообщений об ошибках.
crit – запись только критических ошибок.

Содержание логов зависит от выбранного режима. Для минимизации нагрузки на систему рекомендуется использовать режим **crit** и контролировать состояние сервиса.

2.6 Настройка ротации логов

Открыть файл **/etc/systemd/journald.conf**:

```
sudo nano /etc/systemd/journald.conf
```

Раскомментировать и задать параметры:

```
SystemMaxUse=500M
RuntimeMaxUse=200M
MaxRetentionSec=1day
```

Перезапустить службу:

```
sudo systemctl restart systemd-journald
```

Открыть файл **/etc/logrotate.d/rsyslog**:

```
sudo nano /etc/logrotate.d/rsyslog
```

Рекомендуемая конфигурация:

```
/var/log/syslog
/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
        rotate 2
        size 500M
        missingok
        notifempty
        compress
        delaycompress
        sharedscripts
        postrotate
                /usr/lib/rsyslog/rsyslog-rotate
        endscript
}
```

Открыть файл **/etc/clickhouse-server/config.xml**:

```
sudo nano /etc/clickhouse-server/config.xml
```

Установить уровень логирования *information*

```
<level>information</level>
```

Перезапустить службу:

```
sudo systemctl restart clickhouse-server
```

3. Настройка инструментов визуализации

Процесс включает два этапа:

1. Установка и конфигурация collectd для сбора аналитики и метрик.

Collectd — это системный демон, предназначенный для сбора метрик производительности и ресурсов. Collectd может собирать и агрегировать данные в реальном времени, отправляя их в систему мониторинга для дальнейшего анализа и визуализации.

DosGate предоставляет метрики по всей системе, охватывая различные уровни обработки трафика:

- **Статистика по аренам** – включает направление обработки трафика внутри сетевых интерфейсов и всех профилей, размещенных в арене.
- **Статистика по профилям** – собирается для каждого профиля, расположенного в пределах арен.
- **Статистика по меткам** – формируется для каждой метки статистики, добавленной через действие `-j STATS` до терминального действия (например, `-j DROP`). Метки статистики позволяют детализировать причины сброса или пропуска определенных типов сетевых пакетов.

Передаваемые значения метрик:

`drop` – объем сброшенного трафика.
`accept` (для профилей) / transmit (для арен) – объем пропущенного трафика до конечного получателя.
`pass` – объем трафика, переданного в операционную систему.
`reply` – ответы DosGate на входящие пакеты вместо конечного получателя (например, в рамках TCP-авторизации).
`error` – объем трафика, сброшенного из-за несоответствия IP RFC или другим встроенным проверкам.

Каждая метрика передается в двух форматах:

- BPS (бит в секунду).
- PPS (пакетов в секунду).

2. Установка и настройка локального Graphite или интеграция внешнего Graphite с collectd.

После конфигурации collectd настраивается система визуализации. Варианты включают развертывание локального экземпляра Graphite для

хранения и отображения метрик или настройку collectd для передачи собранных данных на внешний сервер Graphite.

3.1 Установка collectd (при необходимости, если установка выполялась не из метапакета)

Установить collectd, используя команду:

```
sudo apt install collectd
```

3.1.1 Настройка collectd

Для настройки следует открыть файл **/etc/collectd/collectd.conf**.

Файл должен содержать только указанную информацию:

```
FQDNLookup true
TypesDB "/usr/share/collectd/types.db"

LoadPlugin logfile
LoadPlugin syslog

<Plugin logfile>
        LogLevel "info"
        File STDOUT
        Timestamp true
        PrintSeverity false
</Plugin>

<Plugin syslog>
        LogLevel info
</Plugin>

<Include "/etc/collectd/collectd.conf.d">
        Filter "*.conf"
</Include>
```

Далее, открыть файл **/etc/collectd/collectd.conf.d/dosgate.conf**. Файл должен содержать только указанную информацию:

```
LoadPlugin write_graphite
<Plugin write_graphite>
        <Node "localhost">
                Host "127.0.0.1" ## Заменяется на адрес внешнего
Graphite при необходимости
                Port "2003"
                Protocol "tcp"
        </Node>
</Plugin>

LoadPlugin unixsock
<Plugin unixsock>
        SocketFile "/var/run/collectd-unixsock"
        SocketPerms "0660"
        DeleteSocket false
</Plugin>

TypesDB "/etc/collectd/collectd.conf.d/dosgate-types.db"
```

Далее, открыть файл **/etc/collectd/collectd.conf.d/dosgate-types.db**. Файл должен содержать только указанную информацию:

```
dgstats         packets:COUNTER:0:U     bytes:COUNTER:0:U
```

3.1.2 Запуск collectd

Для запуска collectd необходимо выполнить следующие шаги:

Перезапустить службу, используя команду:

```
sudo systemctl restart collectd
```

Проверить, что всё запустилось корректно, используя команду:

```
sudo systemctl status collectd
```

Включить автозапуск службы:

```
sudo systemctl enable collectd
```

3.1.3 Добавление collectd в конфигурационный файл DosGate

> **Внимание!**
> Данный пункт 3.1.3 полностью дублирует 2.3.3. Допустимо его пропустить, если настройка блока collectd уже производилась в пункте 2.3.3.

Открыть конфигурационный файл **/etc/dosgate.conf**. Добавить в него следующую информацию:

```
collectd:
  hostname: dosgate-srv1
  period: 10
```

- При установке DosGate в кластере, необходимо убедиться, что его hostname является уникальным для платформы.

3.1.4 Внесение изменений в DosGate после настройки collectd

Перезагрузить службу DoSGate:

```
sudo systemctl restart dosgate
```

Проверить записи метрик, выполнив команду:

```
sudo systemctl status dosgate
```

Лог должен содержать сообщение:

```
[dg_collectd_sender.c:70, GLOB] Collectd send success
```

Необходимо изменить уровень логирования, поскольку текущая конфигурация генерирует избыточные и подробные логи, что приводит к перегрузке диска. Рекомендуется установить уровень логирования на crit, чтобы фиксировать только критически важные события.

Открыть конфигурационный файл `dosgate.service`, используя команду:

```
sudo nano /etc/systemd/system/dosgate.service
```

или

```
sudo nano /usr/lib/systemd/system/dosgate.service
```

Заменить строку `ExecStart=dosgate -f` на `ExecStart=dosgate -f -l crit`.

> **Примечание**
> Пути к systemd-юнитам могут отличаться в зависимости от системы и версии программного обеспечения. Перед редактированием или созданием юнита убедитесь, что нужный файл существует и найдено его точное расположение.
>
> Чтобы проверить это, выполните команду: `sudo systemctl status имя-юнита`

Применить изменения:

```
sudo systemctl daemon-reload
```

Запустить службу DosGate:

```
sudo systemctl start dosgate
```

Убедиться, что служба запустилась корректно, выполнив команду:

```
sudo systemctl status dosgate
```

Активировать автозагрузку сервиса DosGate:

```
systemctl enable dosgate
```

3.1.5 Формат хранения данных в Graphite

DosGate имеет следующую вложенность при хранении данных в Graphite:

`hostname.arena|profile.stats.bytes|packets`

hostname - Задается в конфигурационном файле dosgate.conf в блоке collectd.

arena - Задается в конфигурационном файле dosgate.conf, в блоке arenas, атрибут `name`.

profile - Профиль защиты,задаваемый системным администратором при настройке DoSGate.

stats - Это действия, происходящие с трафиком, которые отображают его состояние и обработку. Возможные действия:

`drop` - Трафик сброшен как результат правила `-j DROP`.

`accept` - Трафик принят и отправлен согласно настройкам dosgate.conf, без сброса.

`pass` - Трафик передан операционной системе как результат правила `-j PASS`.

`reply` - DosGate отвечает на пакет вместо конечного получателя. Это применяется при TCP авторизации для проверки IP-спуфинга, когда DosGate отправляет пакет с флагом RST или с некорректным значением последовательности (Sequence) для верификации отправителя.

`error` - Пакет не обработан из-за несоответствия стандартам IP RFC или потому, что DosGate не смог его корректно разобрать (например, пакет поврежден).

`-j STATS name` - сбор статистики по указанной метке. Это настраивается администратором при создании правила и позволяет отслеживать статистику конкретного правила. Например, правило: `-m protocol udp -j STATS udp_packets`, `-j DROP` будет сбрасывать все пакеты UDP и собирать статистику по этим пакетам и их объему.

bytes - Статистика объема данных в байтах. Для перевода в биты умножьте значение на 8.

packets - Статистика количества переданных пакетов.

3.2 Настройка связки clickhouse - carbon-clickhouse - graphite-clickhouse - carbonapi

3.2.1 Настройка Clickhouse

Clickhouse — это высокопроизводительная аналитическая колоночная СУБД, используемая для хранения, обработки и анализа больших объёмов данных в реальном времени. В рамках работы DosGate, *clickhouse* предназначен для хранения метрик.

1. Запустить службу *clickhouse-server* и проверить её состояние на наличие ошибок:

```
sudo systemctl start clickhouse-server && systemctl status clickhouse-server
```

2. Необходимо создать следующие таблицы в Clickhouse:

- *graphite* — метрики;
- *graphite_index* — индексы метрик.
- *graphite_tagged* — теги graphite.

> **Примечание**
> Если при установке *clickhouse* был установлен пароль для пользователя, использовать соответствующую команду с параметром `--password`. Если пароль не задавался, выполнять команду без этого параметра.

Clickhouse без пароля:

```
clickhouse-client --multiline --multiquery < /usr/share/doc/clickhouse-server/graphite/dg-init.sql
```

Clickhouse с паролем:

```
clickhouse-client --multiline --multiquery --password=[пароль
clickhouse] < /usr/share/doc/clickhouse-server/graphite/dg-
init.sql
```

3. Проверить, что все необходимые таблицы созданы:

Clickhouse без пароля:

```
clickhouse-client --query="SHOW TABLES" | wc -l
```

Clickhouse с паролем:

```
clickhouse-client --query="SHOW TABLES" --password=[пароль
clickhouse] | wc -l
```

4. Открыть файл конфигурации для настройки уровня логирования:

```
sudo nano /etc/clickhouse-server/config.xml
```

5. Установить уровень логирования *information*:

```
<level>information</level>
```

6. Перезапустить службу:

```
sudo systemctl restart clickhouse-server
```

3.2.2 Настройка Carbon-clickhouse (только если для Clickhouse задан пароль)

1. Если при установке *clickhouse* был установлен пароль для пользователя, необходимо отредактировать конфигурационный файл:

```
sudo nano /etc/carbon-clickhouse/carbon-clickhouse.conf
```

В секциях `[upload.graphite]` и `[upload.graphite_index]` указать параметры подключения в формате:

```
default:[пароль clickhouse]@localhost:8123
```

вместо стандартного `localhost:8123`.

2. Включить автозапуск сервиса и проверить его состояние:

```
sudo systemctl enable --now carbon-clickhouse && systemctl status carbon-clickhouse
```

3.2.3 Настройка Graphite-clickhouse (только если для Clickhouse задан пароль)

1. Если при установке *clickhouse* был установлен пароль для пользователя, необходимо отредактировать конфигурационный файл:

```
sudo nano /etc/graphite-clickhouse/graphite-clickhouse.conf
```

В секции `[clickhouse]` указать параметры подключения в формате:

```
default:[пароль clickhouse]@localhost:8123
```

вместо стандартного `localhost:8123`.

2. Включить автозапуск сервиса и проверить его состояние:

```
sudo systemctl enable --now graphite-clickhouse && systemctl status graphite-clickhouse
```

3.2.4 Настройка Carbonapi

Carbonapi — это сервис для обработки и агрегации запросов к временным рядам метрик, получаемых из хранилища Clickhouse и других совместимых back-end систем. Carbonapi реализует совместимый с Graphite API, обеспечивая быстрый доступ к данным метрик и поддержку различных функций агрегации.

Включить автозапуск службы *carbonapi* и проверить её состояние:

```
sudo systemctl enable --now carbonapi && systemctl status
carbonapi
```

4. Установка веб-интерфейса

4.1 Архитектурные особенности

Веб-интерфейс SP-Spider предназначен для упрощения и автоматизации управления кластером DosGate, обеспечивая операторам удобный доступ к настройкам системы через визуальный интерфейс. С его помощью можно вводить новые правила, редактировать существующие, применять заранее настроенные пресеты, а также отслеживать состояние кластера и статистику работы в режиме реального времени.

Веб-интерфейс SP-Spider и ноды DosGate могут быть развернуты в различных архитектурных конфигурациях в зависимости от требований заказчика. Интерфейс поддерживает аппаратное резервирование и кластеризацию, обеспечивая работу в режиме active-active для повышения доступности и отказоустойчивости. Подробное описание различных архитектур доступно в разделе Архитектуры инсталляций.

Компоненты системы
Для работы веб-интерфейса используются следующие компоненты:

- **SP-Spider** — это веб-интерфейс, предназначенный для управления и настройки программного обеспечения DosGate.
- **SP-Spider-Broker** - выступает в роли брокера синхронизации для DosGate.
- **Node.js**: Среда выполнения для веб-интерфейса, обеспечивающая его основную функциональность.
- **PostgreSQL**: Реляционная база данных для хранения конфигурационных данных и правил.
- **RabbitMQ**: Брокер сообщений, обеспечивающий синхронизацию и обработку очередей сообщений.

4.2 Инструкция по установке и настройке компонентов

4.2.1 Установка обновления операционной системы

Выполнить команду для обновления списка пакетов:

```
sudo apt-get update
```

Обновить установленные пакеты:

```
sudo apt-get upgrade
```

4.2.2 Установка Node.js

Выполнить команду для установки NodeJS:

```
sudo apt install nodejs=18.18.2-1nodesource1
```

4.2.3 Установка PostgreSQL

Установить PostgreSQL и библиотеку для работы с ней:

```
sudo apt install -y libpq-dev postgresql
```

4.2.4 Настройка PostgreSQL

Открыть файл конфигурации для редактирования:

```
sudo nano /etc/postgresql/14/main/pg_hba.conf
```

Убедиться, что файл содержит запись:

```
host    all             all             127.0.0.1/32
scram-sha-256
```

Проверить наличие записи командой:

```
cat /etc/postgresql/14/main/pg_hba.conf | grep "host    all
all             127.0.0.1/32            scram-sha-256"
```

Создать базу данных и пользователя:

```
sudo -u postgres psql
```

Выполнить команды в консоли PostgreSQL:

```
CREATE DATABASE dosgate;
```

```
CREATE USER dosgate WITH ENCRYPTED PASSWORD 'password';
```

```
GRANT ALL PRIVILEGES ON DATABASE dosgate TO dosgate;
```

```
\q
```

4.2.5 Установка RabbitMQ

Создать скрипт установки:

```
sudo nano quickrabbitmq.sh
```

Вставить в скрипт следующий код:

```
#!/bin/sh

sudo apt-get install curl gnupg apt-transport-https -y

## Team RabbitMQ's main signing key
curl -1sLf "https://keys.openpgp.org/vks/v1/by-
fingerprint/0A9AF2115F4687BD29803A206B73A36E6026DFCA" | sudo gpg -
```

```
-dearmor | sudo tee /usr/share/keyrings/com.rabbitmq.team.gpg >
/dev/null
## Community mirror of Cloudsmith: modern Erlang repository
curl -1sLf https://ppa1.novemberain.com/gpg.E495BB49CC4BBE5B.key |
sudo gpg --dearmor | sudo tee
/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg > /dev/null
## Community mirror of Cloudsmith: RabbitMQ repository
curl -1sLf https://ppa1.novemberain.com/gpg.9F4587F226208342.key |
sudo gpg --dearmor | sudo tee
/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg > /dev/null

## Add apt repositories maintained by Team RabbitMQ
sudo tee /etc/apt/sources.list.d/rabbitmq.list <<EOF
## Provides modern Erlang/OTP releases
##
deb [signed-by=/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-erlang/deb/ubuntu
jammy main
deb-src [signed-
by=/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-erlang/deb/ubuntu
jammy main

## Provides RabbitMQ
##
deb [signed-by=/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-server/deb/ubuntu
jammy main
deb-src [signed-
by=/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-server/deb/ubuntu
jammy main
EOF

## Update package indices
sudo apt-get update -y

## Install Erlang packages
sudo apt-get install -y erlang-base \
                        erlang-asn1 erlang-crypto erlang-eldap
erlang-ftp erlang-inets \
                        erlang-mnesia erlang-os-mon erlang-
parsetools erlang-public-key \
                        erlang-runtime-tools erlang-snmp erlang-
ssl \
                        erlang-syntax-tools erlang-tftp erlang-
tools erlang-xmerl

## Install rabbitmq-server and its dependencies
sudo apt-get install rabbitmq-server -y --fix-missing
```

Сохранить и закрыть файл. Запустить скрипт для установки RabbitMQ:

```
sudo bash quickrabbitmq.sh
```

4.2.6 Настроика RabbitMQ

Создать пользователя RabbitMQ:

```
sudo rabbitmqctl add_user "username" "password"
```

Назначить права доступа пользователю:

```
sudo rabbitmqctl set_permissions -p "/" "username" ".*" ".*" ".*"
```

4.3 Инструкция по подготовке системы DosGate

4.3.1 Увеличить значение TimeoutStartSec (необязательно)

Если конфигурация содержит более 25 профилей, необходимо увеличить тайм-аут для запуска сервиса DosGate. Необходимо открыть файл конфигурации сервиса:

```
sudo nano /lib/systemd/system/dosgate.service
```

Установить значение `TimeoutStartSec=600`:

```
[Unit]
Description=Dosgate anti-ddos controller
After=network.target
ConditionPathExists=/etc/dosgate.conf

[Service]
Type=notify
ExecStart=dosgate -f -l crit
RuntimeDirectory=dosgate
StateDirectory=dosgate
```

```
TimeoutStartSec=600

[Install]
WantedBy=multi-user.target
```

Сохранить изменения и закрыть файл.

4.3.2 Настроить конфигурационный файл dosgate.conf

Проверить, что в файле **/etc/dosgate.conf** настроен параметр FAPI.socket для взаимодействия веб-интерфейса:

```
- url: /run/dosgate/fapi.socket
  user: www-data
  group: www-data
  mode: 0660
  acl: any
  type: FCGI
  timeout:
 send: 120
 idle: 120
```

4.3.3 Добавление сервиса проверки прав FAPI.socket

Установить права для FAPI-сокета:

```
chmod 660 /run/dosgate/fapi.socket
```

Перезапустить службу DosGate, выполнив команду:

```
sudo service dosgate restart
```

Создать новый сервис:

```
sudo nano /etc/systemd/system/fix_fapi.service
```

Вставить следующую конфигурацию в созданный файл:

```
[Unit]
Description=Run fix fapi-socket at startup after all systemd
services
After=default.target

[Service]
Type=simple
RemainAfterExit=yes
ExecStart=chmod 660 /run/dosgate/fapi.socket
TimeoutStartSec=0

[Install]
WantedBy=default.target
```

Сохранить файл, активировать и запустить сервис:

```
systemctl enable --now /etc/systemd/system/fix_fapi.service
```

4.3.4 Заведение SSH-пользователя

Для синхронизации и дополнительных проверок, веб-интерфейс соединяется по SSH с каждой системой-dosgate

Убедитесь что на каждой системе-dosgate есть настроенный SSH-пользователь с доступом к `sudo`.

Создать нового пользователя:

```
sudo adduser dosgate-web
```

Добавить пользователя в группу sudo:

```
sudo usermod -aG sudo dosgate-web
```

Убедиться, что авторизация по SSH через пароль разрешена для этого пользователя.

4.3.5 Настроика NGINX

Если Graphite установлен через Docker, важно учитывать некоторые особенности настройки портов и конфигурации.

По умолчанию, Graphite, запущенный через Docker, работает на порту 8080 и не задействует основной сервер nginx. Однако, если на платформе имеются другие конфигурации nginx, которые используют порты 80 или 443, это может привести к конфликтам.

Если Graphite запущен на той же аппаратной платформе, необходимо убедиться, что порты 80 и 443 свободны или не используются другими сервисами. Чтобы проверить текущую конфигурацию Graphite, выполнить следующие шаги:

Откройть файл конфигурации nginx для Graphite, используя команду:

```
sudo nano /etc/nginx/sites-available/graphite
```

Если установлен 80 или 443 порт, изменить на 8080 :

```
listen 8080 default_server;
listen [::]:8080 default_server;
```

Примечание
Если в системе используется Grafana, обновите настройки источника данных.

Обновить систему, используя команды:

```
sudo apt update
```

```
sudo apt upgrade
```

Установить NGINX:

```
sudo apt install nginx=1.28.0-1~jammy-servicepipe-
20250819.143131.UTC
```

Удалить стандартную конфигурацию NGINX:

```
sudo rm /etc/nginx/sites-available/default /etc/nginx/sites-
enabled/default
```

Создать файл конфигурации для FAPI:

```
sudo nano /etc/nginx/sites-available/fapi.conf
```

Вставить следующую конфигурацию:

```
server {
  listen 80 default_server;
  listen [::]:80 default_server;

  server_name REPLACE_ON_DOMAIN_OR_IP;
  root /var/www/html;
  index index.php;

  location /fapi {
    include fastcgi_params;
    fastcgi_pass  unix:/run/dosgate/fapi.socket;
  }

  location /broker {
    rewrite ^/broker(.*)$ $1 break;
    proxy_pass http://localhost:3335;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_cache_bypass $http_upgrade;
  }
}
```

Примечание
Заменить `server_name REPLACE_ON_DOMAIN_OR_IP` на домен или IP-адрес!

Создать ссылку:

```
sudo ln -s /etc/nginx/sites-available/fapi.conf /etc/nginx/sites-
```

```
enabled
```

Перезапустить NGINX:

```
sudo systemctl restart nginx
```

4.3.6 Настройка сети

Убедитесь, что веб-интерфейс имеет связанность до каждой системы-dosgate.

4.4 Инструкция по установке веб-интерфейса и брокера синхронизации

Установить пакеты веб-интерфейса и брокера синхронизации:

```
sudo apt install sp-spider sp-spider-broker
```

4.4.1 Настройка веб-интерфейса

В зависимости от условий установки необходимо обновить авторизационные данные, порты базы данных и другие параметры в .env-файле. Сначала выполняется настройка веб-интерфейса, затем — брокера.

Открыть для редактирования файл **/opt/sp-spider/.env**:

```
sudo nano /opt/sp-spider/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
NODE_ENV=production

VITE_APP_PORT=3333                              # Порт веб-
интерфейса
HTTP_TIMEOUT=10000                              # Таймаут HTTP-
запросов, мс
IS_PRIMARY=true                                 # Определяет,
```

```
является ли интерфейс основным, независимо от наличия
резервирования

APP_SECRET=salt_salt_salt                          # Секретный ключ
для хэширования паролей. Не меняйте после первого запуска

# Параметры подключения к PostgreSQL
DB_HOST="localhost"                                # Адрес сервера
PostgreSQL
DB_PORT="5432"                                     # Порт PostgreSQL
DB_USER="YOUR_DB_USER"                             # Имя пользователя
PostgreSQL
DB_DATABASE="YOUR_DB_NAME"                         # Имя базы данных
PostgreSQL
DB_PASSWORD="YOUR_DB_PASSWORD"                     # Пароль
пользователя PostgreSQL

# Параметры RabbitMQ для синхронизации и брокера
RMQ_ENABLE="true"                                  # Включает
RabbitMQ
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"      # URL подключения
к RabbitMQ с учётными данными
RMQ_RECONNECT_INTERVAL="5000"                      # Интервал
переподключения к RabbitMQ, мс

# Параметры аутентификации через LDAP
LDAP_ENABLED=true                                  # Включает
интеграцию с LDAP
LDAP_URL="ldap://ldap.example.local:389"           # Адрес LDAP-
сервера
LDAP_DN="dc=company,dc=local"                      # Базовый DN
каталога
LDAP_GROUP_CN="users"                              # CN группы
пользователей
LDAP_SERVICE_ACCOUNT_DN="uid=user1,ou=people,dc=company,dc=local"
# DN сервисной учётной записи
LDAP_SERVICE_ACCOUNT_PASSWORD="YOUR_LDAP_PASSWORD"
# Пароль сервисной учётной записи

# Параметры подключения по LDAPS
LDAP_CERT=""                                       # Путь к CA-
сертификату при использовании LDAPS

# Параметры аутентификации через TACACS
TAC_ENABLED=true                                   # Включает
интеграцию с TACACS
TAC_HOST="YOUR_TACACS_HOST"                        # Адрес TACACS
сервера
TAC_PORT="49"                                      # Порт TACACS
TAC_SECRET="your_secret_key"                       # Секретный ключ
TACACS
```

```
TAC_GROUP_NAME="group_admin,group_operator"      # Группы доступа
TAC_SERVICE_NAME="spider"                        # Имя сервиса

# Параметры подключения к ClickHouse
CLICKHOUSE_USER=default                          # Пользователь
ClickHouse
CLICKHOUSE_PASSWORD=password                     # Пароль
ClickHouse
CLICKHOUSE_DB=default                            # База данных
ClickHouse
CLICKHOUSE_HOST=127.0.0.1                        # Адрес ClickHouse
CLICKHOUSE_PORT=8123                             # Порт ClickHouse
```

Примечание

Использовать AMQPs при необходимости.

Если требуется поддержка TLS замените

```
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"
```

на

```
 RMQ_URL="amqps://USER:PASSWORD@localhost:5672"
```

4.4.2 Настройка брокера

Открыть для редактирования файл **/opt/sp-spider-broker/.env**:

```
sudo nano /opt/sp-spider-broker/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
APP_PORT=3335 # Порт, на котором запустится сервис

# Ключ из .env веб-интерфейса
APP_SECRET="YOUR_APP_SECRET"                                  #
Секретный ключ приложения

# Параметры от PostgreSQL из .env веб-интерфейса
```

```
DB_HOST="localhost"                                    #
Адрес сервера PostgreSQL
DB_PORT="5432"                                         # Порт
PostgreSQL
DB_USER="YOUR_DB_USER"                                 # Имя
пользователя PostgreSQL
DB_DATABASE="YOUR_DB_NAME"                             # Имя
базы данных PostgreSQL
DB_PASSWORD="YOUR_DB_PASSWORD"                         #
Пароль пользователя PostgreSQL

# Параметры RabbitMQ из .env веб-интерфейса
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"          # URL
подключения к RabbitMQ
RMQ_RECONNECT_INTERVAL="5000"                          #
Интервал переподключения к RabbitMQ, мс

# Путь к папке с политиками DosGate UH.
POLICY_PATH="/var/lib/dosgate-uh/profiles/"            #
Обязательно в конце ставить "/"

# Путь к конфигурации обработчика оффендеров DosGate UH
OFFENDERS_CONF_PATH="/opt/sp-spider-
broker/offenders/offenders.conf"

# Путь к объектам защиты FlowCollector.
FC_MO_PATH="/opt/spfc/etc/mo/"                         #
Обязательно в конце ставить "/"

# Путь к симлинкам на объекты защиты FlowCollector.
FC_MO_SYMLINK_PATH="/opt/spfc/etc/mo.enabled/"         #
Обязательно в конце ставить "/"

# Путь к объектам обучения Treshold Learner.
FC_LEARNER_PATH="/opt/spfc/etc/learner/"               #
Обязательно в конце ставить "/"

# Путь к симлинкам на объекты обучения Treshold Learner.
FC_LEARNER_SYMLINK_PATH="/opt/spfc/etc/learner.enabled/"    #
Обязательно в конце ставить "/"

# Путь к конфигурации анализатора FlowCollector.
FC_ANALYZER_CONF_PATH="/opt/spfc/etc/analyzer.yaml"

# Путь к бинарному файлу анализатора
FC_ANALYZER_BINARY_PATH="/opt/spfc/bin/analyzer"

# Путь к конфигурации DosGate UH
DGUH_CONF="/etc/dosgate-uh.conf"

# Путь к снэпшотам дампов DosGate UH
```

```
DGUH_SNAPSHOTS="/var/cache/dosgate-uh-snapshots"

# Параметры GeoIP
MMDB_PATH="/etc/dosgate/GeoLite2-Country.mmdb"                #
Путь к mmdb-файлу
MMDB_DEFAULT_PATH="/usr/share/dosgate/GeoLite2-Country.mmdb" #
Путь к дефолтному mmdb файлу

# Параметры Rlog
RLOG_RULES_PATH="/var/lib/rlog/rules/"                        #
Путь к правилам обработки syslog
RLOG_DUMP_PATH= "/var/lib/rlog/dumps/"                        #
Путь к дампам Rlog
RLOG_URL= "http://127.0.0.1:3003"                             # URL
сервиса Rlog

# Параметры BGP
GOBGP_GRPC_SERVER="GOBGP_HOST:PORT"                           #
Адрес gRPC-сервера GoBGP

# Путь к файлу со списками правил FlowSpec
FLOWSPEC_CONF_PATH="/opt/spfc/etc/"


# Параметры синхронизации
UPDATE_CONFIG_INTERVAL_SECONDS=10                             #
Интервал обновления конфигурации, с
SPIDER_URL="http://SPIDER_HOST:3333"                          # URL
интерфейса Spider

# Параметры подключения к ClickHouse
CLICKHOUSE_USER=default                                       #
Пользователь ClickHouse
CLICKHOUSE_PASSWORD=password                                  #
Пароль ClickHouse
CLICKHOUSE_DB=default                                         #
База данных ClickHouse
CLICKHOUSE_HOST=127.0.0.1                                     #
Адрес ClickHouse
CLICKHOUSE_PORT=8123                                          #
Порт ClickHouse
```

4.4.3 Создание сервиса

Для веб-интерфейса:

Отредактировать файл **/usr/lib/systemd/system/sp-spider.service**:

```
sudo nano /usr/lib/systemd/system/sp-spider.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider

[Service]
ExecStart=/usr/bin/node /opt/sp-spider/server/main.js
WorkingDirectory=/opt/sp-spider
Restart=always

[Install]
WantedBy=multi-user.target
```

Для брокера:

Отредактировать файл **/usr/lib/systemd/system/sp-spider-broker.service**:

```
sudo nano /usr/lib/systemd/system/sp-spider-broker.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider Broker

[Service]
ExecStart=/opt/sp-spider-broker/sp-spider-broker
WorkingDirectory=/opt/sp-spider-broker
Restart=always

[Install]
WantedBy=multi-user.target
```

Активировать и запустить сервисы:

```
sudo systemctl enable --now sp-spider sp-spider-broker
```

Проверить статус всех компонентов:

```
sudo systemctl status sp-spider
```

```
sudo systemctl status sp-spider-broker
```

```
sudo systemctl status rabbitmq-server
```

```
sudo systemctl status postgresql
```

```
sudo systemctl status nginx
```

4.4.4 Настройка веб-интерфейса с использованием протокола HTTPS

Сгенерировать самоподписанный сертификат, заменив значения CN и DNS на соответствующие окружению.

```
openssl req -x509 -out server.crt -keyout server.key \
  -newkey rsa:2048 -nodes -sha256 \
  -subj '/CN=DosGate Web-Interface' -extensions EXT -config <( \
   printf "[dn]\nCN=DosGate Web-
Interface\n[req]\ndistinguished_name =
dn\n[EXT]\nsubjectAltName=DNS:server.local\nkeyUsage=digitalSignatur
```

Сохранить сгенерированные файлы *server.crt* и *server.key* в директорию **/etc/certs/**.

Необходимо отредактировать конфигурацию NGINX.
При размещении DosGate и SP-Spider на одной платформе, необходимо скорректировать файл **/etc/nginx/sites-available/fapi.conf**, указав IP-адрес или доменное имя вместо `REPLACE_ON_DOMAIN_OR_IP`.

```
server {
  listen 80;
  server_name REPLACE_ON_DOMAIN_OR_IP localhost;

  location /fapi {
    include fastcgi_params;
    fastcgi_pass  unix:/run/dosgate/fapi.socket;
```

```
  }

  if ($request_uri !~ "/fapi") {
    return 301 https://$server_name$request_uri;
  }
}

server {
  listen 443 default ssl;

  ssl_certificate /etc/certs/server.crt;
  ssl_certificate_key /etc/certs/server.key;

  root /var/www/html;
  index index.php;

  location /broker {
    rewrite ^/broker(.*)$ $1 break;
    proxy_pass http://localhost:3335;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_cache_bypass $http_upgrade;
  }

  location / {
    proxy_pass http://localhost:3333;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  }
}
```

Для применения изменений необходимо перезапустить NGINX:

```
sudo systemctl restart nginx
```

Настроить UFW для ограничения доступа к порту 3333 только с локального интерфейса:

```
sudo ufw allow from 127.0.0.1
```

```
sudo ufw allow from ::1
```

```
sudo ufw deny 3333
```

```
sudo ufw allow in from any
```

```
sudo ufw enable
```

Запустить веб-интерфейс в браузере, перейдя по адресу https://`REPLACE_ON_DOMAIN_OR_IP`. По умолчанию соединение будет установлено через HTTPS.

При необходимости добавить сертификат в доверенные на устройствах конечных пользователей.

4.4.5 Логирование работы сервисов sp-spider

При использовании веб-интерфейса доступен сервис *sp-spider*, который ведет логи взаимодействия с нодами DosGate.

Функции логирования в *sp-spider*:

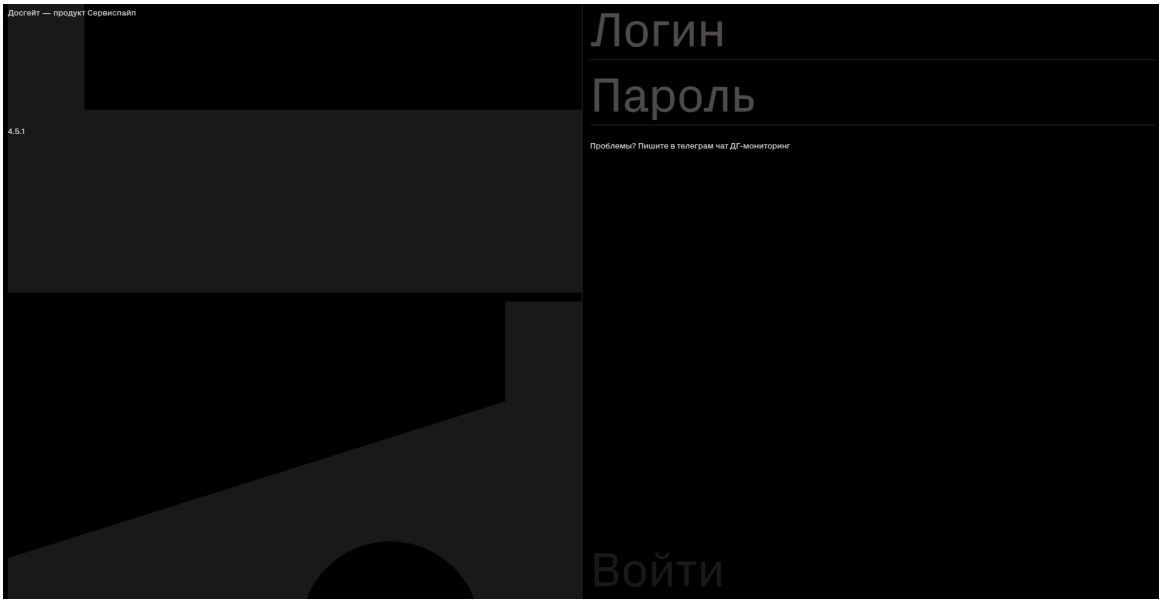
- Фиксация событий, связанных с подключением к DosGate.
- Отображение ошибок DosGate в реальном времени при успешном соединении.
- Помощь в диагностике. Например, при некорректном формировании правил, которые DosGate не принимает.

5. Первый вход в систему

Для входа в Веб-интерфейс DosGate следует ввести в адресной строке браузера IP-адрес и порт по шаблону: `ip:port`. Указать порт, указанный

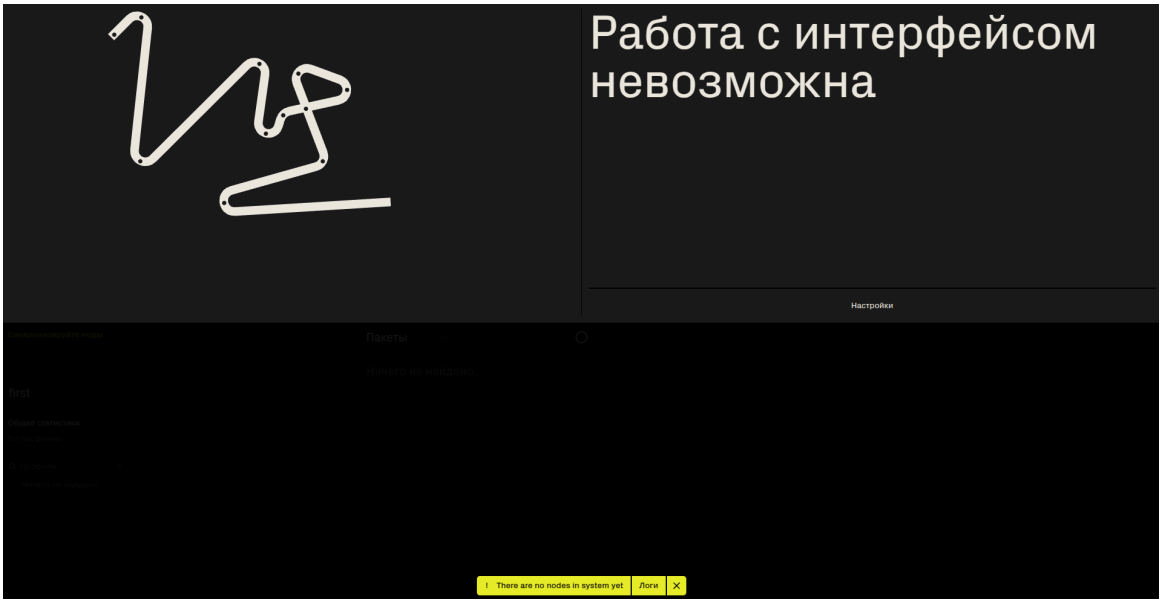
в переменной `VITE_APP_PORT` файла **/opt/sp-spider/.env** в разделе 4.4.1 Настройка веб-интерфейса

Появится окно авторизации (см. рисунок ниже). В окне авторизации следует указать следующие логин и пароль по умолчанию: ***superadmin/superadmin***

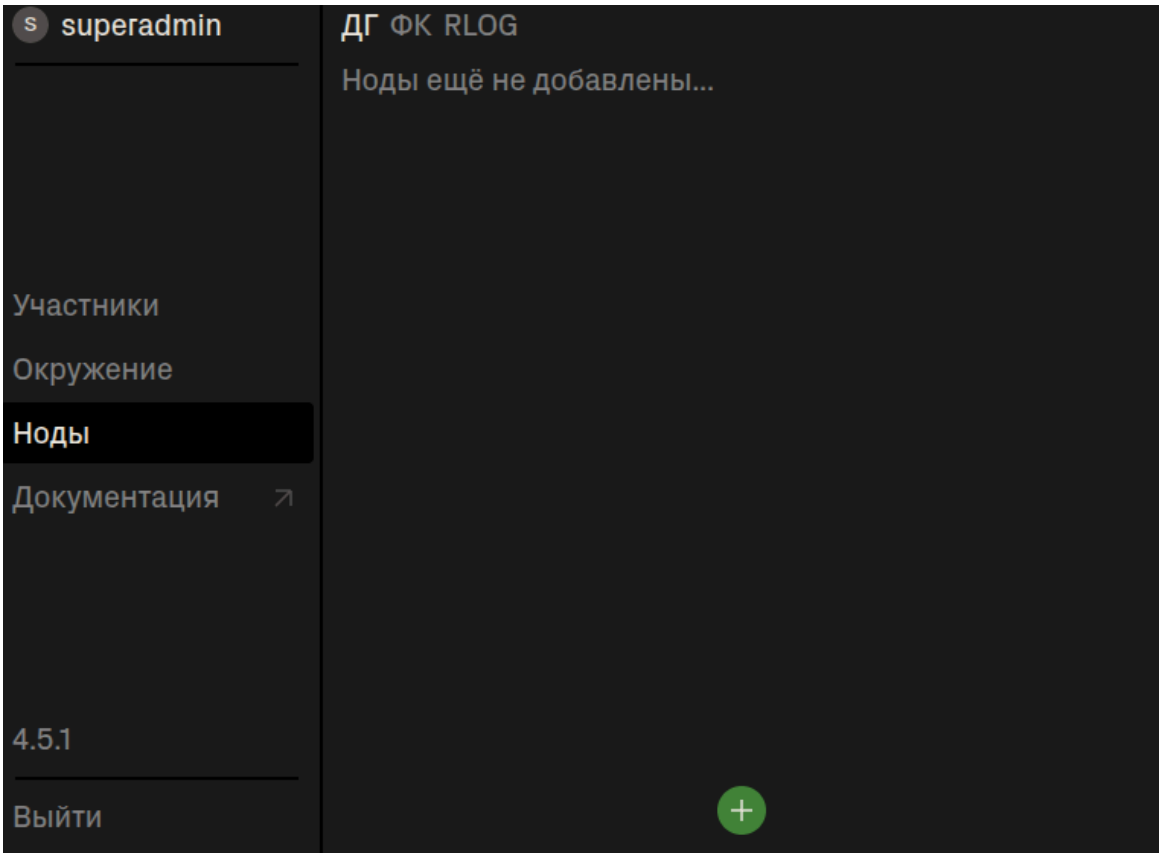


Окно авторизации при входе в систему

После авторизации появится уведомление **Работа с интерфейсом невозможна**. Это связано с тем, что в данный момент нет настроенной ноды.

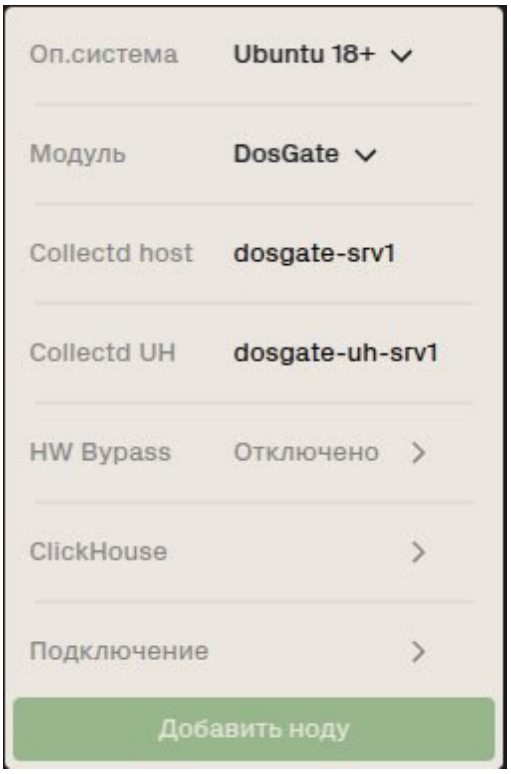


Нажать кнопнку **Настройки**. Откроется окно настроек.

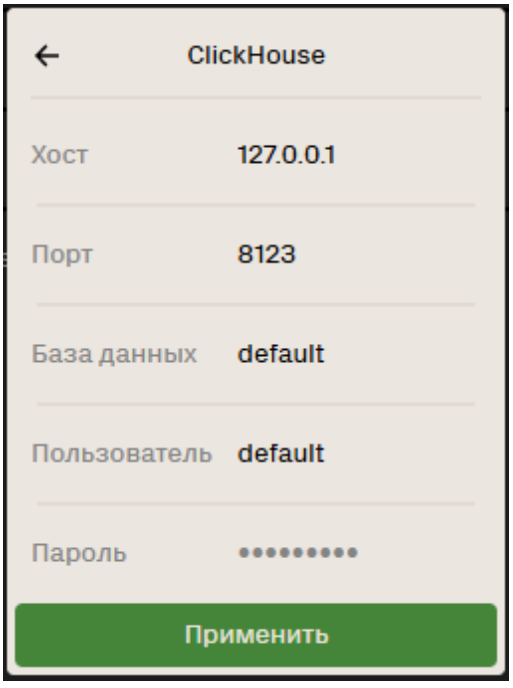


В меню **Ноды** нажать на зелёную иконку с плюсом. В открывшемся окне указать:

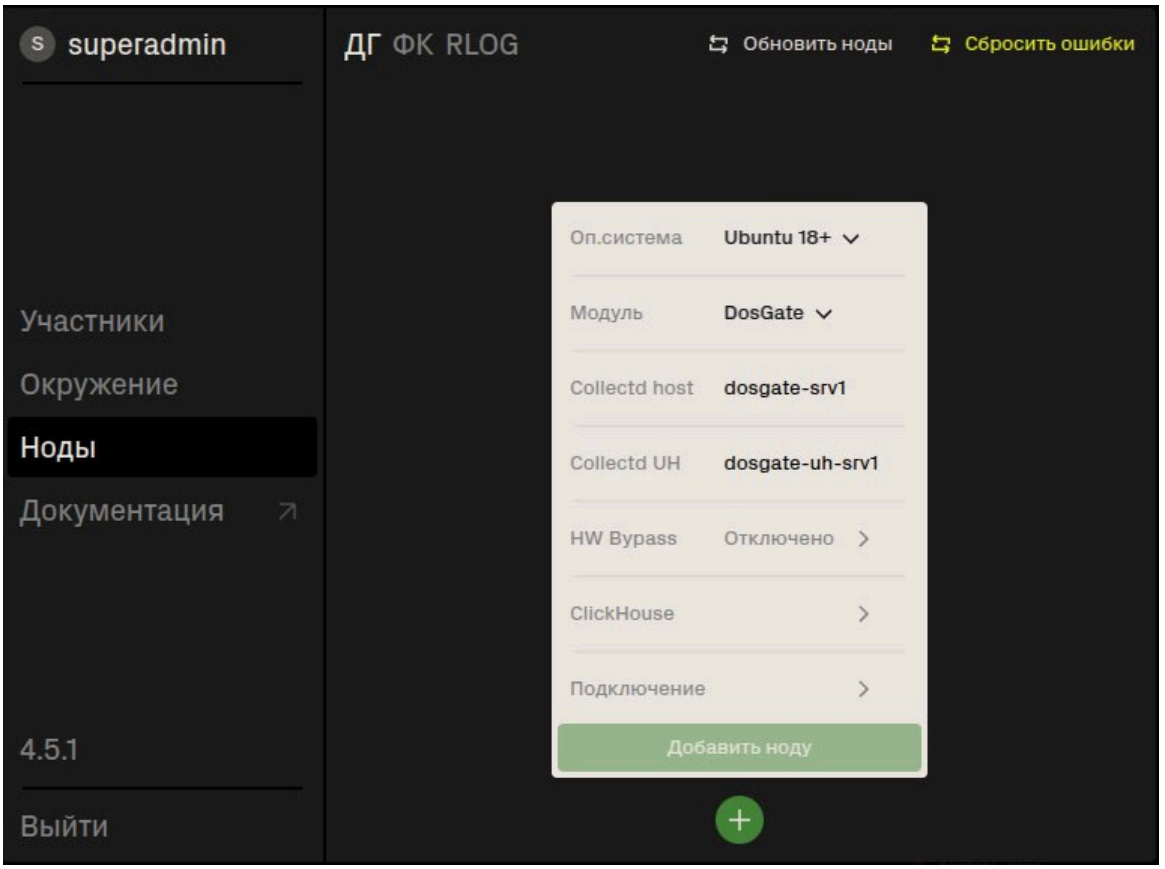
- **Collectd host** — значение должно соответствовать параметру `hostname`, указанному в конфигурационном файле *dosgate.conf* в блоке `collectd`. По умолчанию используется *dosgate-srv1*.
- **Collectd UH** — укажите имя узла, по умолчанию — *dosgate-uh-srv1*.



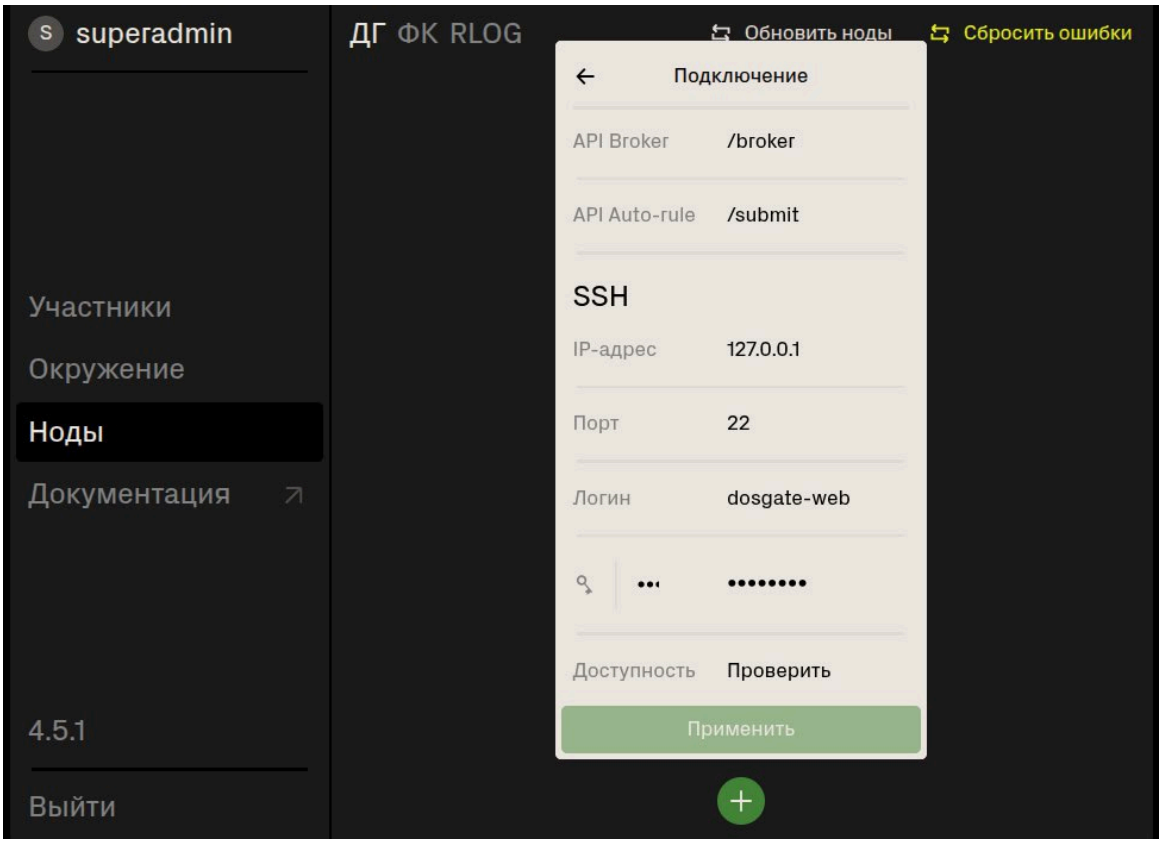
Перейти в настройки **ClickHouse** и указать параметры подключения. Пример настроек для подключения к ClickHouse, установленному на локальной ноде:



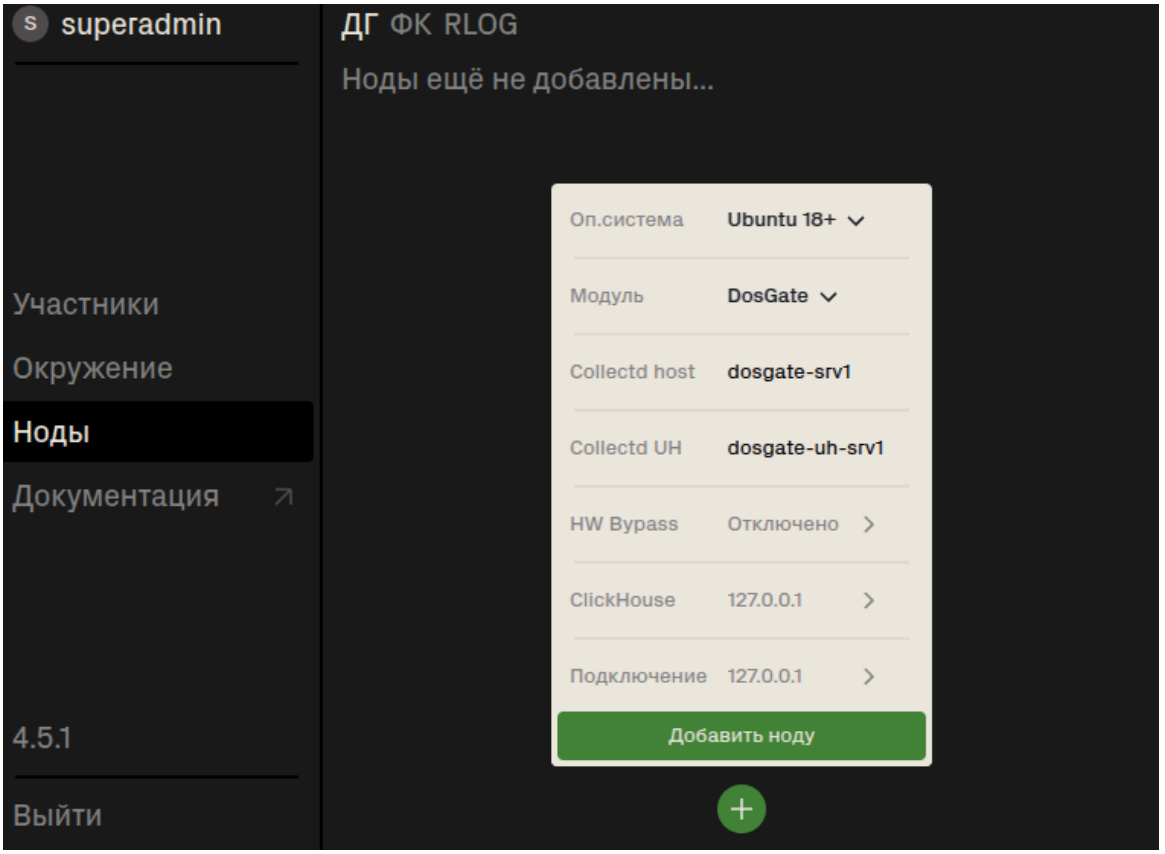
Нажать на кнопку **Применить**. Перейти в раздел **Подключение**.



В открывшемся окне указать SSH-данные для подключения к установленной ноде Dosgate (IP-адрес, логин, пароль). Нажать на кнопку **Проверить**, чтобы проверить подключение. Если данные введены правильно и нода доступна, статус изменится на **Доступна**. После этого нажать кнопку **Применить**. Пример заполненных настроек приведён ниже:

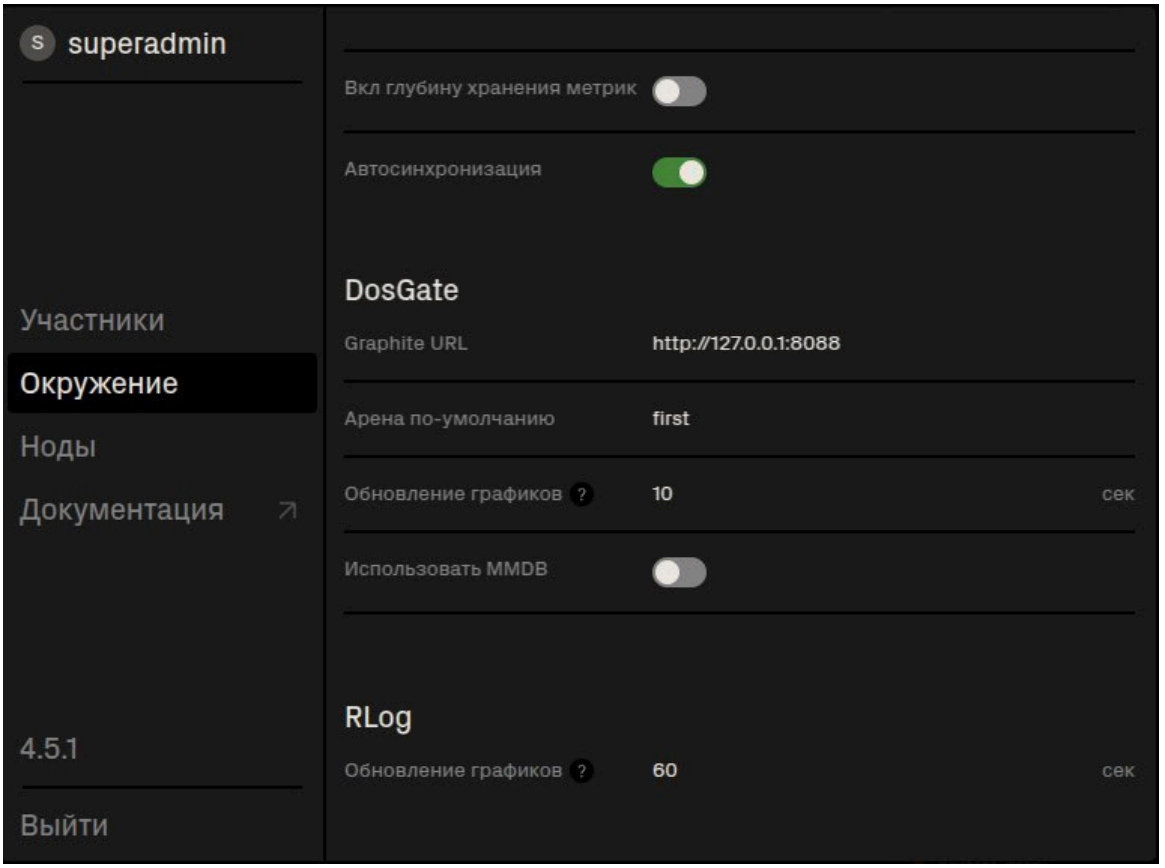


В открывшемся окне нажать **Добавить ноду**.

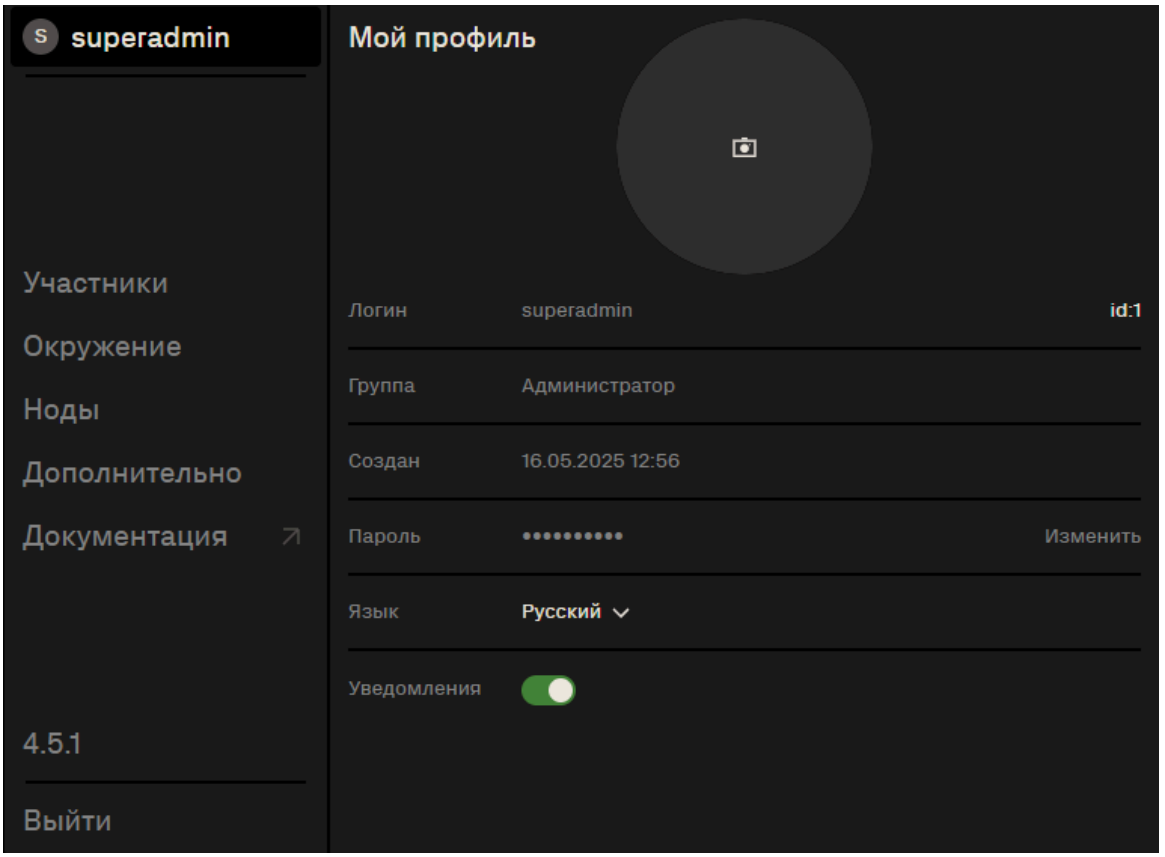


Для отображения графиков и статистики необходимо указать ссылку на Graphite. Перейдите в раздел **Окружение**. В разделе DosGate указать "Graphite URL" и "Арена по-умолчанию". Название арены должно соответствовать значению, указанному в конфигурационном файле dosgate.conf для всех нод кластера.

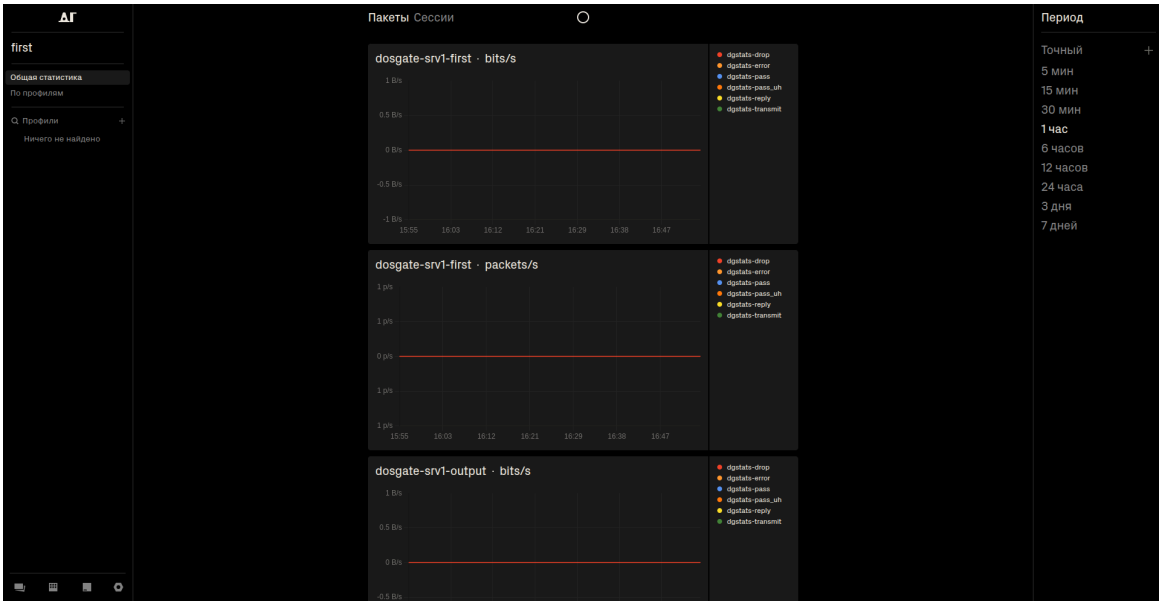
Пример настроек:



Нажать на свой профиль в левом верхнем углу экрана, чтобы открыть настройки профиля. Установить новый пароль.



Выполнить обновление страницы. Веб-интерфейс готов к использованию.



Установка ПО DosGate на Альт 8 СП

1. Подготовка операционной системы

1.1 Отключение репозитория CD-ROM

Удалить репозитории CD-ROM, выполнив команду:

```
apt-repo rm all
```

1.2 Подключение репозитория Servicepipe и официального репозитория Альт СП 8

Установить скрипт настройки репозитория, используя команду:

```
curl -o "./setup-repo.sh" "https://public-
repo.svcp.io/setup_script/setup-repo.sh" && \
    chmod +x "./setup-repo.sh" && \
    ./setup-repo.sh
```

Открыть файл с репозиториями для редактирования:

```
vi /etc/apt/sources.list.d/altsp.list
```

Удалить символы комментария (#) перед следующими строками:

```
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux
c10f/branch/x86_64 classic gostcrypto
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux
c10f/branch/noarch classic
```

1.3 Установка необходимых пакетов для работы ПО DosGate

Установить необходимые пакеты, выполнив команду:

```
apt-get install -y clang14.0 libjson-c5 libmaxminddb libnl3
libnuma libssl1.1 libyaml2 libsysfs libbpf=0.5.0-alt1 libbpf-
devel=0.5.0-alt1
```

1.4 Установка clang 14 в качестве версии по умолчанию

Создать конфигурационный файл для установки версии clang по умолчанию:

```
echo "/usr/bin/clang          /usr/bin/clang-14       100" >
/etc/alternatives/packages.d/clang
```

Проверить и обновить альтернативы:

```
alternatives-validate && alternatives-update
```

Проверить, что используется версия clang 14:

```
clang --version
```

2. Установка Dosgate

2.1 Установка пакетов Dosgate

Установить необходимые библиотеки и пакеты DosGate выполнив команду:

```
apt-get install -y libdt1=1.2.2-1-alt1 libaevent1=0.2.0.1-alt1
dosgate=3.7.4.1-alt1
```

2.1 Настройка конфигурации

Все параметры работы Dosgate задаются в едином конфигурационном файле `dosgate.conf`. Конфигурационный файл находится по пути **/etc/dosgate.conf**. Его настройка обязательна перед первым запуском программного обеспечения.

- Для доступа к командам управления производится аутентификация по SSH.
- Все функции ПО используются за счет взаимодействия с командой: `dgctl`

Конфигурационный файл написан в формате YAML и содержит следующие блоки:

- socket_conf
- arena_conf
- collectd

Подробнее о каждом блоке описано в следующих разделах.

При конфигурировании файла dosgate.conf следует использовать только пробелы; табуляция недопустима. При заполнении конфигурационного файла dosgate.conf, для валидации корректности синтаксиса YAML, допустимо использовать сайт https://www.yamllint.com.

2.1.1 Блок *socket_conf*

Блок *socket_conf* сразу после установки имеет значения по умолчанию. Он настроен для использования и работы с CLI.

Пример конфигурации:

```
sockets:
  - url: /run/dosgate/api.socket
    user: nowhere
    group: www-data
    mode: 0660
```

```
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10
```

Описание блока

URL

> URL для сокетов имеет формат `family://address`, где:

> *family* — тип сокета, который может принимать следующие значения:

- unix — UNIX-сокет, используемый на файловой системе сервера. В качестве адреса указывается полный путь к сокету.
- tcp — TCP-сокет. Адрес указывается в формате `host:port` или `:port`. Если указан только порт (`:port`), сокет будет прослушивать все доступные адреса (`0.0.0.0` или `::`).

> ***Определение типа сокета по строке адреса***

> Если `family` не указано в URL, тип сокета определяется автоматически по формату строки адреса:
>
> - Если строка начинается с `/`, предполагается, что это UNIX-сокет (family = unix).
> - Если строка содержит символ `:`, предполагается, что это TCP-сокет (family = tcp).

User

> Имя пользователя для UNIX-сокетов. Если указанный пользователь отсутствует, сокет будет использовать учетную запись пользователя, от имени которого выполняется процесс (по умолчанию root).

Group

> Группа для UNIX-сокетов. Если указанная группа отсутствует, используется первичная группа пользователя, под которым выполняется процесс (по умолчанию root).

Mode

> Режим доступа для UNIX-сокетов, задается в формате, аналогичном команде `chmod`.

ACL

> Список контроля доступа (Access Control List). Перечисляются через запятую разрешенные target (например: `profile`, `router`, `arena`, `mark`, `pset`), значение `any` - разрешает доступ ко всем частям системы.

Type

> Тип протокола/диалекта для сокета:
>
> - FCGI - FastCGI протокол, полный диалект
> - SCGI - SCGI протокол, полный диалект
> - CRLF - raw протокол, полный диалект
> - CLI - raw протокол, диалект CLI

> RAW - протокол, при котором запрос заканчивается либо последовательностью CRLF, либо закрытием сокета в сторону сервера.

> Ответ также завершается CRLF или окончательным закрытием сокета.

> ***Особенность для CLI:***

> Для отправки запросов через CLI должен быть настроен хотя бы один сокет с типом CLI, с family UNIX и адресом **/run/dosgate/cli.socket**

Timeout

> Общий лимит времени, в течение которого сокет ожидает завершения операции. Указывается в секундах. При отсутствии установленного таймаута сокет продолжает ожидание завершения операций или остается в состоянии бездействия без ограничения по времени.

- idle - время, в течение которого сокет может оставаться бездействующим (неактивным) перед тем, как будет разорвано соединение или предприняты другие действия.
- send - время, отведенное на отправку данных через сокет. Если данные не удается отправить в течение указанного времени, операция будет прервана.

2.1.2 Блок *arena_conf*

Основной блок конфигурации DosGate. Данный блок не имеет значений по умолчанию и требует обязательной настройки.

Пример конфигурации:

```
arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
```

```
      tx:
        name: ens1f0
        mac: 00:cc:34:4a:88:30
        mode: swap
        vid: 63
    - rx:
        name: ens3f0
        mode: vlan
        vid: 54
      tx:
        name: ens3f0
        mac: 00:cc:34:4a:88:30
        mode: swap
        vid: 55
    - rx:
        name: ens3f0
        mode: vlan
        vid: 58
      tx:
        name: ens3f0
        mac: 00:cc:34:47:a8:44
        mode: swap
        vid: 59
```

Описание блока:

Arenas - Набор сетевых интерфейсов и настроек обработки и возврата трафика.

Name - Уникальное имя арены.

Id - Уникальный Id арены (обязателен с 3.2.2-5).

Name (nets) - Имя сетевого интерфейса, как показывает ip link. Обязательное поле.

MAC - MAC-адрес. Может быть записан в одном из следующих форматов:

`XX:XX:XX:XX:XX:XX` или `XX-XX-XX-XX-XX-XX` или `XXXX.XXXX.XXXX`

Где `X` - шестнадцатеричная цифра.

VID - VLAN id. Число от 0 до 4095, где 0 означает отсутствие тега.

Protocol - Протокол VLAN. Либо hex-число в формате 0x0000, либо мнемоническое значение:

Тэг	Значение
802.1q, 8021q, q	0x8100
802.1ad, 8021ad, ad	0x88A8
802.1ah, 8021ah, ah	0x88E7
q-in-q, qq, qinq	0x9100
q-in-q1, qq2, qinq2	0x9200
q-in-q3, qq3, qinq3	0x9300

RX block - Описывает способ обработки входящего трафика. Должен присутствовать всегда.

```
      - rx:
          name: ens5
          inline: true
          mode: transparent
          tx-policy: lacp
```

Если в блоке указан MAC-адрес, то обрабатывается только трафик с этим destination address.

`inline` - Интерфейс работает в inline-режиме, то есть он невидим для других хостов в сети. ARP-запросы, широковещательные запросы, STP/GVRP/etc не передаются в ОС. Если опция не указана, то интерфейс пересылает этот трафик в ОС.

`mode` - Режим обработки входящего трафика:

- `vlan` - обрабатывается только трафик в указанном VLAN, остальной пропускается в ОС. Если VID = 0 или не указан, обрабатывается только нетегированный трафик.
- `transparent` - обрабатывается трафик во всех VLAN + нетегированный. Используется по умолчанию.

`swap` - Указывает, нужно ли менять MAC-адреса во фрейме при отправке.

> Если указано `false` или `0`, то адреса не меняются. Если указано `true`, `1` или значение не указано , то адреса меняются.

`tx-policy` - управляет обработкой следующих классов трафика:

- `lacp` — медленный протокол LACP.
- `llm` — IEEE802.1 Link-local multicast, предназначенная для 01:80:C2:00:00:x.
- `multicast` - Любой L2 multicast, кроме link-local.
- `unknown` - unhandled ethertypes.

Например, если параметр LACP отсутствует, то LACP будет передан в ОС DosGate, а не в TX-интерфейс.

TX block - Описывает политику обработки трафика, который должен быть переслан в соответствии с окончанием обработки правилами или срабатывании действия ACCEPT. Если не указан, то копируется из блока RX, а отсутствующие в нём параметры принимают значения по умолчанию.

```
    - tx:
        name: ens4
        mac: fa:16:3e:56:32:6a
        swap: false
```

Если в блоке указан MAC-адрес, то трафик пересылается на него. В противном случае он отправляется на тот адрес, с которого был получен

`Mode` - Режим обработки исходящего трафика:

- `swap` - меняется последний в стеке тег VLAN, или добавляется если трафик нетегированный. Если VID отсутствует, то пакет не меняется, если равен 0, то верхний тег снимается при наличии. Используется по умолчанию.

> - `push` - новый тег добавляется безусловно, даже если последний был точно таким же. Если VID = 0 или отсутствует, то ничего не добавляется.

`cos` - Класс сервиса в тегированных пакетах. Число от 0 до 7.

Reply block - Описывает политику обработки трафика, который должен быть переслан в соответствии с правилами, которые генерируют собственный трафик в ответ на входящий пакет.

```
        tx:
          name: ens5
          swap: false
        reply:
          name: ens4
          swap: true
```

- Если `reply` не указан, то автоматически копируется из *TX block*. Формат полностью соответствует формату *TX block*.

2.1.3 Блок *collectd*

```
collectd:
  hostname: dosgate
  period: 10
```

- `hostname` - имя хоста, который будет использоваться для именования метрик. Если вы устанавливаете DosGate в кластере, название должно быть уникально для каждой платформы. Именно под этим именем будут отображаться графики по серверам в общей статистике. Также с этим именем записываются метрики относительно сервера.
- `period` - частота записи метрик в collectd.

2.1.4 Примеры конфигурационного файла dosgate.conf

Пример outline инсталяции с VLAN swap и возвратом трафика в том-же интерфейсе

```
sockets:
  - url: /run/dosgate/api.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
```

```
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
collectd:
  hostname: dosgate
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DosGate

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
```

```
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp4s0f0np0
          inline: true
          mode: transparent
        tx:
          name: enp4s0f1np1
          swap: false
        reply:
          name: enp4s0f0np0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
          name: enp4s0f1np1
          inline: true
          mode: transparent
        tx:
          name: enp4s0f0np0
          swap: false

collectd:
  hostname: dosgate
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DoSGate с LACP

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
```

```
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp136s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f1
          swap: false
        reply:
          name: enp136s0f0
          swap: true
      - rx:
          name: enp138s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f1
          swap: false
        reply:
          name: enp138s0f0
          swap: true
  - name: output
    id: 2
```

```
    nets:
      - rx:
          name: enp136s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f0
          swap: false
      - rx:
          name: enp138s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f0
          swap: false

collectd:
  hostname: dosgate
  period: 10
```

2.2 Однократный запуск DosGate

Однократный запуск DosGate выполняется с целью проверки корректности заполнения конфигурационного файла и отсутствия ошибок. Выполнить следующую команду:

```
dosgate -o -l err
```

где:

- `o` — режим однократного запуска (one-shot mode);
- `l err` — параметр, задающий уровень логирования.

Описание уровней логирования:

Уровень	Описание
debug	Отладочная информация. Подробные сведения о действиях процесса, включая системные и библиотечные вызовы.
info	Стандартная информация о работе процесса. Сообщает, например, об открытии файлов без деталей о внутренних вызовах.

Уровень	Описание
warn	Предупреждения о нарушениях нормальной работы процесса без его остановки.
err	Ошибки, приводящие к нарушению нормальной работы объекта.
crit	Критические ситуации, угрожающие стабильности системы.

2.3 Логирование работы сервисов dosgate и dosgate-uh

Сервисы *dosgate* и *dosgate-uh* осуществляют логирование работы системы в зависимости от выбранного режима. Логирование ведется в *service log* и доступно для просмотра с использованием команд:

```
sudo journalctl -xefu dosgate
```

```
sudo journalctl -xefu dosgate-uh
```

Поддерживаются три режима логирования:

debug – детализированное логирование, фиксируются практически все действия системы, включая обработку каждого сетевого пакета.
error – запись только сообщений об ошибках.
crit – запись только критических ошибок.

Содержание логов зависит от выбранного режима. Для минимизации нагрузки на систему рекомендуется использовать режим **crit** и контролировать состояние сервиса.

2.4 Настройка ротации логов

Открыть файл **/etc/systemd/journald.conf**:

```
sudo vi /etc/systemd/journald.conf
```

Раскомментировать и задать параметры:

```
SystemMaxUse=500M
RuntimeMaxUse=200M
MaxRetentionSec=1day
```

Перезапустить службу:

```
sudo systemctl restart systemd-journald
```

Открыть файл **/etc/logrotate.d/rsyslog**:

```
sudo vi /etc/logrotate.d/rsyslog
```

Рекомендуемая конфигурация:

```
/var/log/syslog
/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
        rotate 2
        size 500M
        missingok
        notifempty
        compress
        delaycompress
        sharedscripts
        postrotate
                /usr/lib/rsyslog/rsyslog-rotate
        endscript
}
```

Открыть файл **/etc/mongod.conf**:

```
sudo vi /etc/mongod.conf
```

Установить уровень логирования *0*:

```
systemLog:
  verbosity: 0       # Уровень логирования (0-5)
```

Перезапустить службу:

```
sudo systemctl restart mongod
```

Открыть файл **/etc/clickhouse-server/config.xml**:

```
sudo vi /etc/clickhouse-server/config.xml
```

Установить уровень логирования *information*

```
<level>information</level>
```

Перезапустить службу:

```
sudo systemctl restart clickhouse-server
```

3. Настройка инструментов визуализации

Процесс включает два этапа:

1 - Установка и конфигурация collectd для сбора аналитики и метрик.

> Collectd — это системный демон, предназначенный для сбора метрик производительности и ресурсов. Collectd может собирать и агрегировать данные в реальном времени, отправляя их в систему мониторинга для дальнейшего анализа и визуализации.

> Collectd настраивается для сбора показатели арены: BPS (бит в секунду), PPS (пакетов в секунду), в рамках метрик DosGate: `ACCEPT`, `PASS`, `DROP`, `ERROR`, `PASS_UH`, `REPLY`, а также в рамках меток статистики при использовании команды `-j STATS`.

2 - Установка и настройка локального Graphite или интеграция внешнего Graphite с collectd.

> После конфигурации collectd настраивается система визуализации. Варианты включают развертывание локального экземпляра Graphite для хранения и отображения метрик или настройку collectd для передачи собранных данных на внешний сервер Graphite.

3.1 Установка collectd

Установить collectd, используя команду:

```
apt-get install -y collectd=5.12.0-alt1
```

3.1.1 Настройка collectd

Для настройки следует открыть файл **/etc/collectd.conf**. Файл должен содержать только указанную информацию:

```
FQDNLookup true
TypesDB "/usr/share/collectd/types.db"

LoadPlugin logfile
LoadPlugin syslog

<Plugin logfile>
        LogLevel "info"
        File STDOUT
        Timestamp true
        PrintSeverity false
</Plugin>

<Plugin syslog>
        LogLevel info
</Plugin>

<Include "/etc/collectd.d">
```

```
        Filter "*.conf"
</Include>
```

Затем, создайть директорию **/etc/collectd.d**:

```
mkdir /etc/collectd.d
```

Открыть файл **/etc/collectd.d/dosgate.conf**. Файл должен содержать только указанную информацию:

```
LoadPlugin write_graphite
<Plugin write_graphite>
        <Node "localhost">
                Host "127.0.0.1" ## Заменяется на адрес внешнего
Graphite при необходимости
                Port "2003"
                Protocol "tcp"
        </Node>
</Plugin>

LoadPlugin unixsock
<Plugin unixsock>
        SocketFile "/var/run/collectd-unixsock"
        SocketPerms "0660"
        DeleteSocket false
</Plugin>

TypesDB "/etc/collectd.d/dosgate-types.db"
```

Открыть для редактирования файл **/etc/collectd.d/dosgate-types.db**. Файл должен содержать только указанную информацию:

```
dgstats         packets:COUNTER:0:U     bytes:COUNTER:0:U
```

3.1.2 Запуск collectd

Для запуска collectd необходимо выполнить следующие шаги:

Перезапустить службу, используя команду:

```
systemctl restart collectd
```

Проверить, что всё запустилось корректно, используя команду:

```
systemctl status collectd
```

Включить автозапуск службы:

```
systemctl enable collectd
```

3.1.3 Добавление collectd в конфигурационный файл DosGate

> **Внимание!**
> Данный пункт 3.1.3 полностью дублирует 2.1.3. Допустимо его пропустить, если настройка блока collectd уже производилась в пункте 2.1.3.

Открыть конфигурационный файл **/etc/dosgate.conf**. Добавить в него следующую информацию:

```
collectd:
  hostname: dosgate # Если вы устанавливаете DosGate в кластере, название должно быть уникально для платформы
  period: 10
```

- При установке DosGate в кластере, необходимо убедиться, что его hostname является уникальным для платформы.

3.1.4 Внесение изменений в DosGate после настройки collectd

Перезагрузить службу DoSGate:

```
sudo systemctl restart dosgate
```

Проверить записи метрик, выполнив команду:

```
sudo systemctl status dosgate
```

Лог должен содержать сообщение:

```
[dg_collectd_sender.c:70, GLOB] Collectd send success
```

Необходимо изменить уровень логирования, поскольку текущая конфигурация генерирует избыточные и подробные логи, что приводит к перегрузке диска. Рекомендуется установить уровень логирования на crit, чтобы фиксировать только критически важные события.

Открыть конфигурационный файл `dosgate.service`, используя команду:

```
sed -i 's/dosgate -f/dosgate -f -l crit/'
/lib/systemd/system/dosgate.service
```

Заменить строку `ExecStart=dosgate -f` на `ExecStart=dosgate -f -l crit`.

Примечание
Пути к systemd-юнитам могут отличаться в зависимости от системы и версии программного обеспечения. Перед редактированием или созданием юнита убедитесь, что нужный файл существует и найдено его точное расположение.

Чтобы проверить это, выполните команду: `sudo systemctl status имя-юнита`

Применить изменения:

```
systemctl daemon-reload
```

Запустить службу DosGate:

```
systemctl start dosgate
```

Убедиться, что служба запустилась корректно, выполнив команду:

```
systemctl status dosgate
```

Активировать автозагрузку сервиса DosGate:

```
systemctl enable dosgate
```

3.2 Установка Graphite

Установка Graphite на Альт СП 8 не была протестирована! Рекомендуется выполнять установку на отдельном сервере с операционной системой Ubuntu.

Далее приведена иструкция для установки на операционную систему Ubuntu

3.2.1 Установка Docker

Docker — это платформа, которая помогает запускать приложения в изолированных средах, называемых контейнерами. Эти контейнеры содержат всё необходимое для работы приложения, что делает его проще в установке и запуске на разных компьютерах.

Добавить ключ GPG для Docker:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg
--dearmor -o /etc/apt/keyrings/docker.gpg
```

Изменить права доступа к ключу:

```
sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

Добавить официальный репозиторий Docker в список источников APT:

```
echo \
  "deb [arch="$(dpkg --print-architecture)" signed-
by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
```

```
  "$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Обновить список пакетов и установить Docker с помощью следующих команд:

```
sudo apt update
```

```
sudo apt install docker-ce docker-ce-cli containerd.io
```

Добавить пользователя в группу Docker:

```
sudo usermod -aG docker $USER
```

Убедиться, что Docker установлен и работает, запустив следующую команду:

```
docker version
```

Проверить, что служба Docker запущена, с помощью команды:

```
sudo systemctl status docker
```

3.2.2 Установка контейнера Graphite

Создать директории, которые будут использоваться контейнером Graphite для хранения данных, логов, конфигурации и настроек:

```
sudo mkdir -p /data/graphite/{data,logs,conf,statsd_config}
```

3.2.3 Добавление Graphite в systemd

Отредактируйте файл службы graphite-docker.service:

```
sudo vi /etc/systemd/system/graphite-docker.service
```

Вставьте следующее содержимое в файл:

```
[Unit]
Description=Graphite Docker Container
Documentation=https://github.com/graphite-project/docker-graphite-
statsd
After=docker.service
Requires=docker.service

[Service]
Type=simple
TimeoutStartSec=0
Restart=on-failure
RestartSec=30s
ExecStartPre=-/usr/bin/docker kill graphite
ExecStartPre=-/usr/bin/docker rm graphite
ExecStartPre=/usr/bin/docker pull graphiteapp/graphite-statsd
ExecStart=/usr/bin/docker run \
            --name graphite \
            --restart=always \
            -p 8080:80 \
            -p 2003-2004:2003-2004 \
            -p 2023-2024:2023-2024 \
            -p 8125:8125/udp \
            -p 8126:8126 \
            -v /data/graphite/data:/opt/graphite/storage \
            -v /data/graphite/conf:/opt/graphite/conf \
            -v /data/graphite/statsd_config:/opt/statsd/config \
            -v /data/graphite/logs:/var/log \
            graphiteapp/graphite-statsd

SyslogIdentifier=graphite
ExecStop=/usr/bin/docker stop graphite

[Install]
WantedBy=multi-user.target
```

3.2.4 Запуск Graphite

Обновить конфигурацию systemd:

```
sudo systemctl daemon-reload
```

Активировать службу для автозапуска:

```
sudo systemctl enable graphite-docker
```

Запуск службы Graphite:

```
sudo systemctl start graphite-docker.service
```

Проверить статус службы, с помощью команды:

```
sudo systemctl status graphite-docker.service
```

3.2.5 Настройка Graphite

Необходимо установить диапазон хранения Graphite в 10 секунд вместо 1 минуты (стандартное значение после установки) для более точной статистики.

Откройте файл `storage-schemas.conf` для редактирования:

```
sudo vi /data/graphite/conf/storage-schemas.conf
```

Добавить следующую конфигурацию в начало файла перед другими записями:

```
[default]
pattern = .*
retentions = 10s:14d,60s:365d
```

Сохраните изменения и закройте файл.

3.2.6 Перезапуск и очистка данных

Остановить службу Graphite перед удалением старых данных:

```
sudo systemctl stop graphite-docker
```

Удалить старые данные из папки dosgate:

```
sudo rm -rf /data/graphite/data/whisper/dosgate
```

Перезапустить службы Graphite:

```
sudo systemctl start graphite-docker
```

3.2.7 Формат хранения данных в Graphite

DosGate имеет следующую вложенность при хранении данных в Graphite:

`hostname.arena|profile.stats.bytes|packets`

hostname - Задается в конфигурационном файле dosgate.conf в блоке collectd.

arena - Задается в конфигурационном файле dosgate.conf, в блоке arenas, атрибут `name`.

profile - Профиль защиты,задаваемый системным администратором при настройке DoSGate.

stats - Это действия, происходящие с трафиком, которые отображают его состояние и обработку. Возможные действия:

`drop` - Трафик сброшен как результат правила `-j DROP`.

`accept` - Трафик принят и отправлен согласно настройкам dosgate.conf, без сброса.

`pass` - Трафик передан операционной системе как результат правила `-j PASS`.

`reply` - DosGate отвечает на пакет вместо конечного получателя. Это применяется при TCP авторизации для проверки IP-спуфинга, когда DosGate отправляет пакет с флагом RST или с некорректным значением последовательности (Sequence) для верификации отправителя.

`error` - Пакет не обработан из-за несоответствия стандартам IP RFC или потому, что DosGate не смог его корректно разобрать (например, пакет поврежден).

`-j STATS name` - сбор статистики по указанной метке. Это настраивается администратором при создании правила и позволяет отслеживать статистику конкретного правила. Например, правило: `-m protocol udp -j STATS udp_packets`, `-j DROP` будет сбрасывать все пакеты UDP и собирать статистику по этим пакетам и их объему.

bytes - Статистика объема данных в байтах. Для перевода в биты умножьте значение на 8.

packets - Статистика количества переданных пакетов.

4. Установка и настройка веб-интерфейса

4.1 Архитектурные особенности

Веб-интерфейс SP-Spider предназначен для упрощения и автоматизации управления кластером DosGate, обеспечивая операторам удобный доступ к настройкам системы через визуальный интерфейс. С его помощью можно вводить новые правила, редактировать существующие, применять заранее настроенные пресеты, а также отслеживать состояние кластера и статистику работы в режиме реального времени.

Веб-интерфейс SP-Spider и ноды DosGate могут быть развернуты в различных архитектурных конфигурациях в зависимости от требований заказчика. Интерфейс поддерживает аппаратное резервирование и кластеризацию, обеспечивая работу в режиме active-active для повышения доступности и отказоустойчивости. Подробное описание различных архитектур доступно в разделе Архитектуры инсталляций.

Компоненты системы
Для работы веб-интерфейса используются следующие компоненты:

- **SP-Spider** — это веб-интерфейс, предназначенный для управления и настройки программного обеспечения DosGate.
- **SP-Spider-Broker** - выступает в роли брокера синхронизации для DosGate.

- **Node.js**: Среда выполнения для веб-интерфейса, обеспечивающая его основную функциональность.
- **PostgreSQL**: Реляционная база данных для хранения конфигурационных данных и правил.
- **RabbitMQ**: Брокер сообщений, обеспечивающий синхронизацию и обработку очередей сообщений.

4.2 Инструкция по установке и настройке компонентов

4.2.1 Установка обновления операционной системы

Выполнить команду для обновления списка пакетов:

```
apt-get update
```

4.2.2 Установка Node.js

Выполнить команду для установки NodeJS:

```
apt-get install -y node
```

4.2.3 Установка PostgreSQL

Установить PostgreSQL и библиотеку для работы с ней:

```
apt-get install -y libpq5-devel postgresql14-server postgresql14-
contrib
```

Инициализировать системные базы данных:

```
/etc/init.d/postgresql initdb
```

- Этот шаг создаёт начальные каталоги данных и системные таблицы.

Перезагрузить и добавить сервис PostgreSQL в автозагрузку:

```
systemctl enable --now postgresql
```

4.2.4 Настройка PostgreSQL

Открыть файл конфигурации для редактирования:

```
/var/lib/pgsql/data/pg_hba.conf
```

Убедиться, что файл содержит запись:

```
host    all             all             127.0.0.1/32
scram-sha-256
```

Проверить наличие записи командой:

```
cat /var/lib/pgsql/data/pg_hba.conf | grep "host    all
all             127.0.0.1/32            scram-sha-256"
```

Создать базу данных и пользователя:

```
psql -U postgres
```

Выполнить команды в консоли PostgreSQL:

```
CREATE DATABASE dosgate;
```

```
CREATE USER dosgate WITH ENCRYPTED PASSWORD 'password';
```

```
GRANT ALL PRIVILEGES ON DATABASE dosgate TO dosgate;
```

```
\q
```

4.2.5 Установка RabbitMQ

Установить сервер RabbitMQ:

```
apt-get install rabbitmq-server
```

Перезагрузить и добавить сервис RabbitMQ в автозагрузку:

```
systemctl enable --now rabbitmq.service
```

4.2.6 Настроика RabbitMQ

Создать пользователя RabbitMQ:

```
rabbitmqctl add_user "username" "password"
```

Назначить права доступа пользователю:

```
rabbitmqctl set_permissions -p "/" "username" ".*" ".*" ".*"
```

4.3 Инструкция по подготовке системы DosGate

4.3.1 Настроить конфигурационный файл dosgate.conf

Проверить, что в файле **/etc/dosgate.conf** настроен параметр FAPI.socket для взаимодействия веб-интерфейса:

```
- url: /run/dosgate/fapi.socket
  user: www-data
  group: www-data
  mode: 0660
  acl: any
  type: FCGI
  timeout:
 send: 120
 idle: 120
```

4.3.2 Добавление сервиса проверки прав FAPI.socket

Установить права для FAPI-сокета:

```
chmod 660 /run/dosgate/fapi.socket
```

Перезапустить службу DosGate, выполнив команду:

```
systemctl restart dosgate
```

Создать новый сервис:

```
sudo vi /etc/systemd/system/fix_fapi.service
```

Вставить следующую конфигурацию в созданный файл:

```
[Unit]
Description=Run fix fapi-socket at startup after all systemd
services
After=default.target

[Service]
Type=simple
RemainAfterExit=yes
ExecStart=chmod 660 /run/dosgate/fapi.socket
TimeoutStartSec=0

[Install]
WantedBy=default.target
```

Сохранить файл, активировать и запустить сервис:

```
systemctl enable --now /etc/systemd/system/fix_fapi.service
```

4.3.3 Заведение SSH-пользователя

Для синхронизации и дополнительных проверок, веб-интерфейс соединяется по SSH с каждой системой-dosgate

Убедитесь что на каждой системе-dosgate есть настроенный SSH-пользователь с доступом к `sudo`.

Создать нового пользователя:

```
adduser dosgate-web && usermod -aG wheel dosgate-web
```

Убедиться, что авторизация по SSH через пароль разрешена для этого пользователя.

4.3.4 Настроика NGINX

Если Graphite установлен через Docker, важно учитывать некоторые особенности настройки портов и конфигурации.

По умолчанию, Graphite, запущенный через Docker, работает на порту 8080 и не задействует основной сервер nginx. Однако, если на платформе имеются другие конфигурации nginx, которые используют порты 80 или 443, это может привести к конфликтам.

Если Graphite запущен на той же аппаратной платформе, необходимо убедиться, что порты 80 и 443 свободны или не используются другими сервисами. Чтобы проверить текущую конфигурацию Graphite, выполнить следующие шаги:

Открыть файл конфигурации nginx для Graphite, используя команду:

```
 vi /etc/nginx/sites-available.d/graphite
```

Если установлен 80 или 443 порт, изменить на 8080 :

```
listen 8080 default_server;
listen [::]:8080 default_server;
```

> **Примечание**
> Если в системе используется Grafana, обновите настройки источника данных.

Установить NGINX:

```
apt-get install nginx
```

Удалить стандартную конфигурацию NGINX:

```
rm -f /etc/nginx/sites-available.d/default.conf /etc/nginx/sites-enabled.d/default.conf
```

Создать файл конфигурации для FAPI:

```
vi /etc/nginx/sites-available.d/fapi.conf
```

Вставить следующую конфигурацию:

```
server {
  listen 80 default_server;
  listen [::]:80 default_server;

  server_name REPLACE_ON_DOMAIN_OR_IP;
  root /var/www/html;
  index index.php;

  location /fapi {
    include fastcgi_params;
    fastcgi_pass  unix:/run/dosgate/fapi.socket;
  }

  location /broker {
    rewrite ^/broker(.*)$ $1 break;
    proxy_pass http://localhost:3335;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_cache_bypass $http_upgrade;
  }
}
```

Примечание
Заменить `server_name REPLACE_ON_DOMAIN_OR_IP` на домен или IP-адрес!

Создать ссылку:

```
ln -s /etc/nginx/sites-available.d/fapi.conf /etc/nginx/sites-
enabled.d
```

Перезапустить NGINX:

```
systemctl restart nginx
```

4.3.6 Настройка сети

Убедитесь, что веб-интерфейс имеет связанность до каждой системы-dosgate.

4.4 Инструкция по установке веб-интерфейса и брокера синхронизации

Установить пакеты веб-интерфейса и брокера синхронизации:

```
apt-get install sp-spider=4.4-alt1 sp-spider-broker=1.0.16-alt1
```

4.4.1 Настройка веб-интерфейса

В зависимости от условий установки необходимо обновить авторизационные данные, порты базы данных и другие параметры в .env-файле. Сначала выполняется настройка веб-интерфейса, затем — брокера.

Открыть для редактирования файл **/opt/sp-spider/.env**:

```
sudo vi /opt/sp-spider/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
NODE_ENV=production

VITE_APP_PORT=3333                                  # Порт веб-
интерфейса
```

```
HTTP_TIMEOUT=10000                                  # Таймаут HTTP-
запросов, мс
IS_PRIMARY=true                                     # Определяет,
является ли интерфейс основным, независимо от наличия
резервирования

APP_SECRET=salt_salt_salt                           # Секретный ключ
для хэширования паролей. Не меняйте после первого запуска

# Параметры подключения к PostgreSQL
DB_HOST="localhost"                                 # Адрес сервера
PostgreSQL
DB_PORT="5432"                                      # Порт PostgreSQL
DB_USER="YOUR_DB_USER"                              # Имя пользователя
PostgreSQL
DB_DATABASE="YOUR_DB_NAME"                          # Имя базы данных
PostgreSQL
DB_PASSWORD="YOUR_DB_PASSWORD"                      # Пароль
пользователя PostgreSQL

# Параметры RabbitMQ для синхронизации и брокера
RMQ_ENABLE="true"                                   # Включает
RabbitMQ
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"       # URL подключения
к RabbitMQ с учётными данными
RMQ_RECONNECT_INTERVAL="5000"                       # Интервал
переподключения к RabbitMQ, мс

# Параметры аутентификации через LDAP
LDAP_ENABLED=true                                   # Включает
интеграцию с LDAP
LDAP_URL="ldap://ldap.example.local:389"            # Адрес LDAP-
сервера
LDAP_DN="dc=company,dc=local"                       # Базовый DN
каталога
LDAP_GROUP_CN="users"                               # CN группы
пользователей
LDAP_SERVICE_ACCOUNT_DN="uid=user1,ou=people,dc=company,dc=local"
# DN сервисной учётной записи
LDAP_SERVICE_ACCOUNT_PASSWORD="YOUR_LDAP_PASSWORD"
# Пароль сервисной учётной записи

# Параметры подключения по LDAPS
LDAP_CERT=""                                        # Путь к CA-
сертификату при использовании LDAPS

# Параметры аутентификации через TACACS
TAC_ENABLED=true                                    # Включает
интеграцию с TACACS
TAC_HOST="YOUR_TACACS_HOST"                         # Адрес TACACS
сервера
```

```
TAC_PORT="49"                                    # Порт TACACS
TAC_SECRET="your_secret_key"                     # Секретный ключ
TACACS
TAC_GROUP_NAME="group_admin,group_operator"      # Группы доступа
TAC_SERVICE_NAME="spider"                        # Имя сервиса

# Параметры подключения к ClickHouse
CLICKHOUSE_USER=default                          # Пользователь
ClickHouse
CLICKHOUSE_PASSWORD=password                     # Пароль
ClickHouse
CLICKHOUSE_DB=default                            # База данных
ClickHouse
CLICKHOUSE_HOST=127.0.0.1                        # Адрес ClickHouse
CLICKHOUSE_PORT=8123                             # Порт ClickHouse
```

Примечание

Использовать AMQPs при необходимости.

Если требуется поддержка TLS замените

```
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"
```

на

```
 RMQ_URL="amqps://USER:PASSWORD@localhost:5672"
```

4.4.2 Настройка брокера

Открыть для редактирования файл **/opt/sp-spider-broker/.env**:

```
 vi /opt/sp-spider-broker/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
APP_PORT=3335 # Порт, на котором запустится сервис

# Ключ из .env веб-интерфейса
APP_SECRET="YOUR_APP_SECRET"                                  #
```

```
Секретный ключ приложения

# Параметры от PostgreSQL из .env веб-интерфейса
DB_HOST="localhost"                                    #
Адрес сервера PostgreSQL
DB_PORT="5432"                                         # Порт
PostgreSQL
DB_USER="YOUR_DB_USER"                                 # Имя
пользователя PostgreSQL
DB_DATABASE="YOUR_DB_NAME"                             # Имя
базы данных PostgreSQL
DB_PASSWORD="YOUR_DB_PASSWORD"                         #
Пароль пользователя PostgreSQL

# Параметры RabbitMQ из .env веб-интерфейса
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"          # URL
подключения к RabbitMQ
RMQ_RECONNECT_INTERVAL="5000"                          #
Интервал переподключения к RabbitMQ, мс

# Путь к папке с политиками DosGate UH.
POLICY_PATH="/var/lib/dosgate-uh/profiles/"            #
Обязательно в конце ставить "/"

# Путь к конфигурации обработчика оффендеров DosGate UH
OFFENDERS_CONF_PATH="/opt/sp-spider-
broker/offenders/offenders.conf"

# Путь к объектам защиты FlowCollector.
FC_MO_PATH="/opt/spfc/etc/mo/"                         #
Обязательно в конце ставить "/"

# Путь к симлинкам на объекты защиты FlowCollector.
FC_MO_SYMLINK_PATH="/opt/spfc/etc/mo.enabled/"         #
Обязательно в конце ставить "/"

# Путь к объектам обучения Treshold Learner.
FC_LEARNER_PATH="/opt/spfc/etc/learner/"               #
Обязательно в конце ставить "/"

# Путь к симлинкам на объекты обучения Treshold Learner.
FC_LEARNER_SYMLINK_PATH="/opt/spfc/etc/learner.enabled/"    #
Обязательно в конце ставить "/"

# Путь к конфигурации анализатора FlowCollector.
FC_ANALYZER_CONF_PATH="/opt/spfc/etc/analyzer.yaml"

# Путь к бинарному файлу анализатора
FC_ANALYZER_BINARY_PATH="/opt/spfc/bin/analyzer"

# Путь к конфигурации DosGate UH
```

```
DGUH_CONF="/etc/dosgate-uh.conf"

# Путь к снэпшотам дампов DosGate UH
DGUH_SNAPSHOTS="/var/cache/dosgate-uh-snapshots"

# Параметры GeoIP
MMDB_PATH="/etc/dosgate/GeoLite2-Country.mmdb"                # Путь к mmdb-файлу
MMDB_DEFAULT_PATH="/usr/share/dosgate/GeoLite2-Country.mmdb" # Путь к дефолтному mmdb файлу

# Параметры Rlog
RLOG_RULES_PATH="/var/lib/rlog/rules/"                        # Путь к правилам обработки syslog
RLOG_DUMP_PATH= "/var/lib/rlog/dumps/"                        # Путь к дампам Rlog
RLOG_URL= "http://127.0.0.1:3003"                             # URL сервиса Rlog

# Параметры BGP
GOBGP_GRPC_SERVER="GOBGP_HOST:PORT"                           # Адрес gRPC-сервера GoBGP

# Путь к файлу со списками правил FlowSpec
FLOWSPEC_CONF_PATH="/opt/spfc/etc/"


# Параметры синхронизации
UPDATE_CONFIG_INTERVAL_SECONDS=10                             # Интервал обновления конфигурации, с
SPIDER_URL="http://SPIDER_HOST:3333"                          # URL интерфейса Spider

# Параметры подключения к ClickHouse
CLICKHOUSE_USER=default                                       # Пользователь ClickHouse
CLICKHOUSE_PASSWORD=password                                  # Пароль ClickHouse
CLICKHOUSE_DB=default                                         # База данных ClickHouse
CLICKHOUSE_HOST=127.0.0.1                                     # Адрес ClickHouse
CLICKHOUSE_PORT=8123                                          # Порт ClickHouse
```

4.4.3 Создание сервиса

Для веб-интерфейса:

Отредактировать файл **/usr/lib/systemd/system/sp-spider.service**:

```
vi /usr/lib/systemd/system/sp-spider.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider

[Service]
ExecStart=/usr/bin/node /opt/sp-spider/server/main.js
WorkingDirectory=/opt/sp-spider
Restart=always

[Install]
WantedBy=multi-user.target
```

Для брокера:

Отредактировать файл **/usr/lib/systemd/system/sp-spider-broker.service**:

```
vi /usr/lib/systemd/system/sp-spider-broker.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider Broker

[Service]
ExecStart=/opt/sp-spider-broker/sp-spider-broker
WorkingDirectory=/opt/sp-spider-broker
Restart=always

[Install]
WantedBy=multi-user.target
```

Активировать и запустить сервисы:

```
systemctl enable --now sp-spider sp-spider-broker
```

Проверить статус всех компонентов:

```
systemctl status sp-spider
```

```
systemctl status sp-spider-broker
```

```
systemctl status rabbitmq-server
```

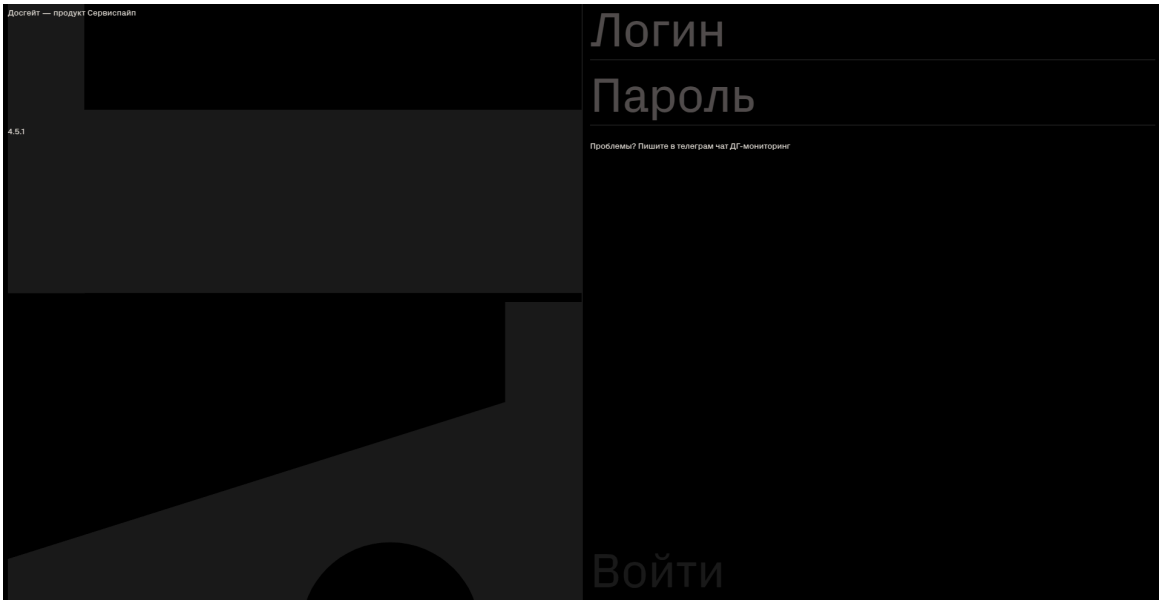
```
systemctl status postgresql
```

```
systemctl status nginx
```

5. Первый вход в систему

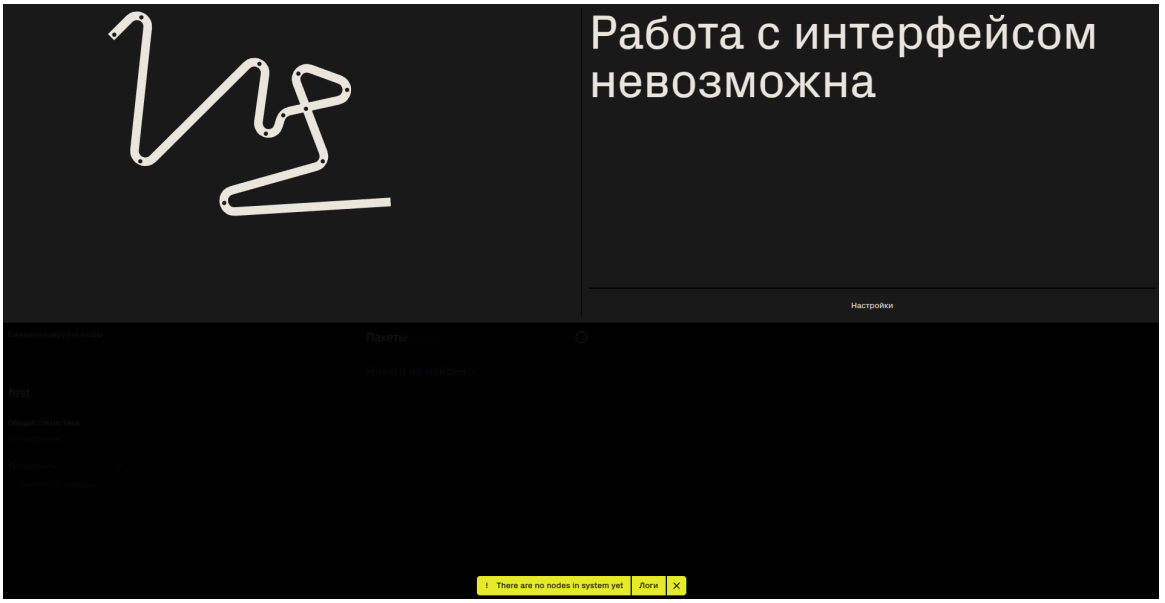
Для входа в Веб-интерфейс DosGate следует ввести в адресной строке браузера IP-адрес и порт по шаблону: `ip:port`. Указать порт, указанный в переменной `VITE_APP_PORT` файла **/opt/sp-spider/.env** в разделе 4.4.1 Настройка веб-интерфейса

Появится окно авторизации (см. рисунок ниже). В окне авторизации следует указать следующие логин и пароль по умолчанию: ***superadmin/superadmin***

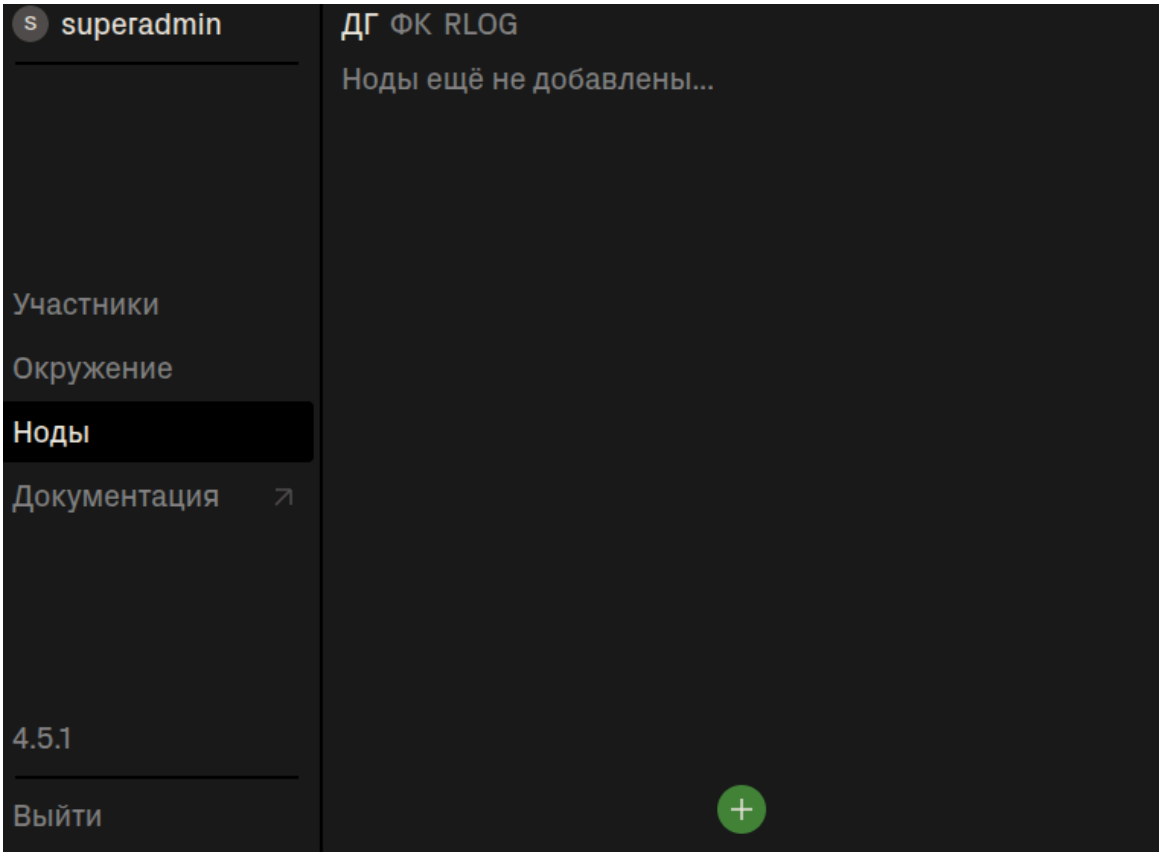


Окно авторизации при входе в систему

После авторизации появится уведомление "Работа с интерфейсом невозможна" (см. рисунок ниже). Это связано с тем, что в данный момент нет настроенной ноды.

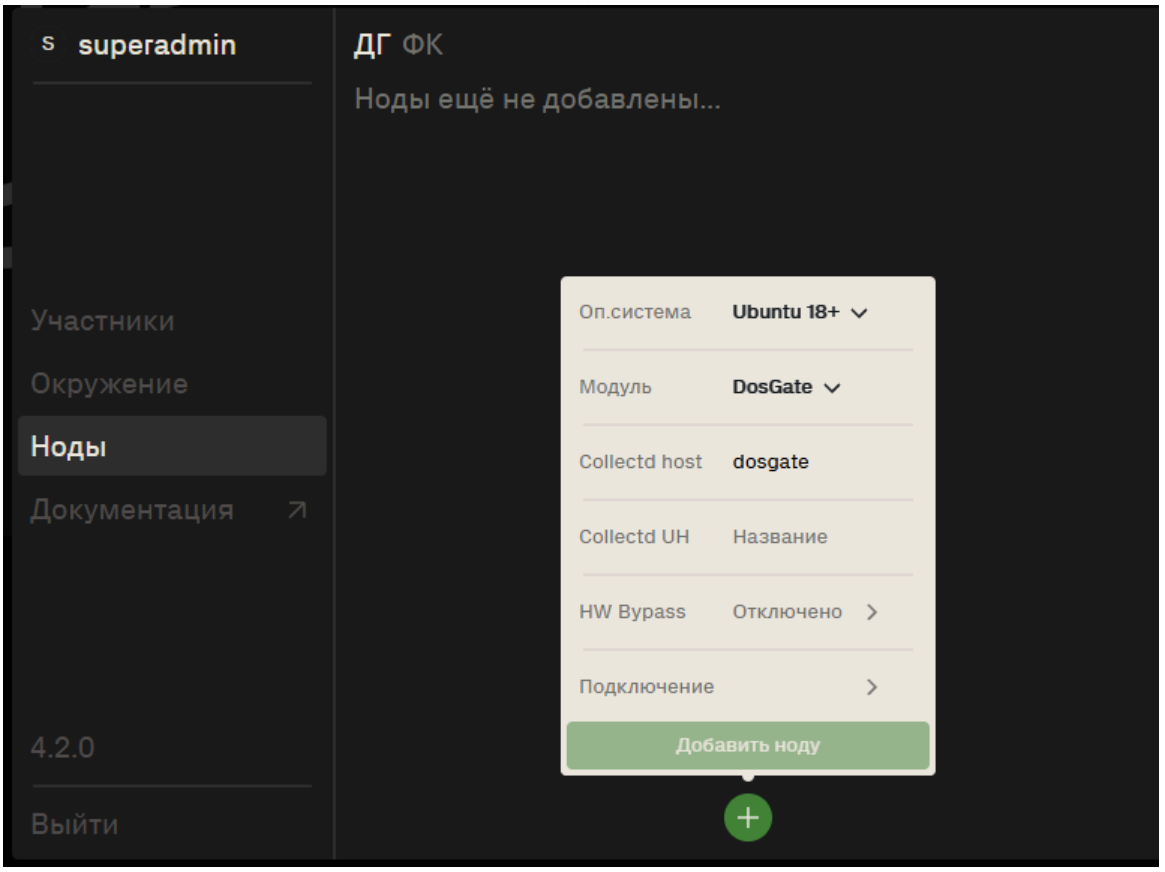


Нажать кнопнку "Настройки". Откроется окно настроек (см. рисунок ниже).

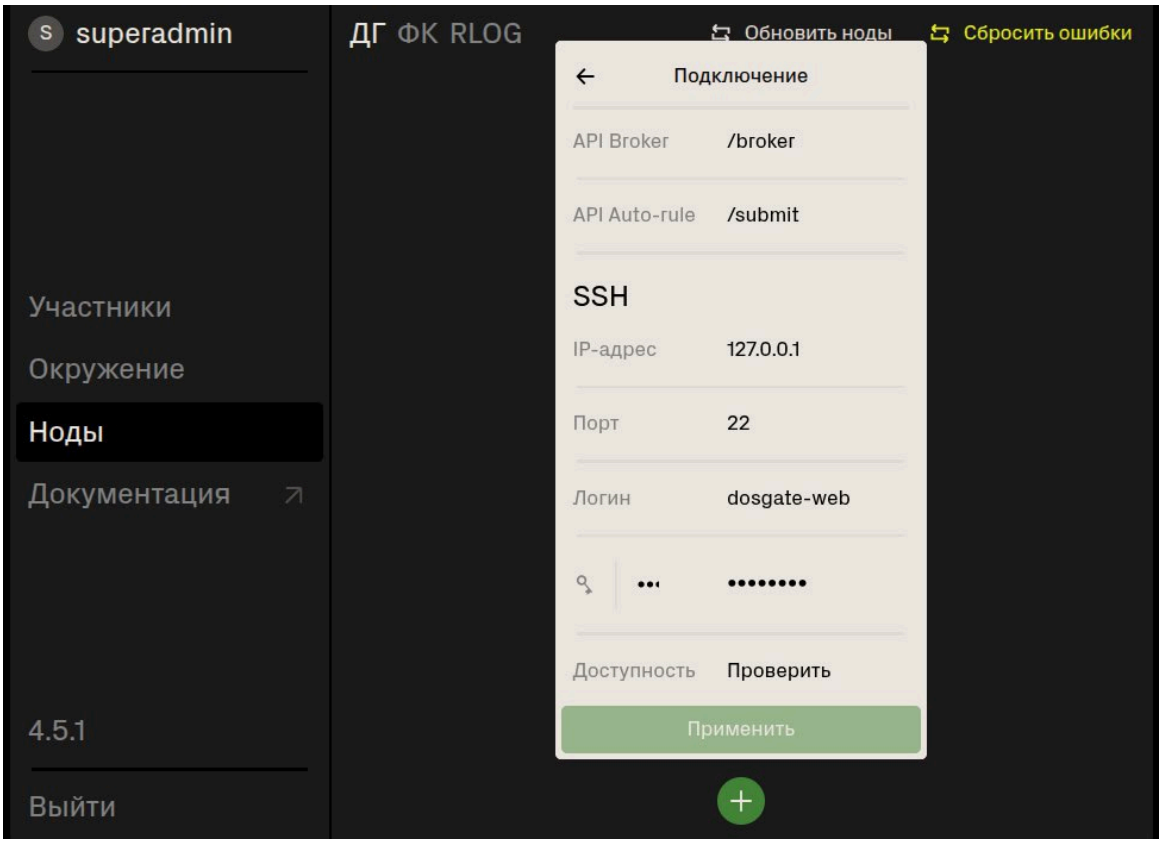


Выбрать меню "Ноды" - нажать на кнопку добавления новой ноды. В открывшимя окне необходимо заполнить "Collectd host". Необходимо

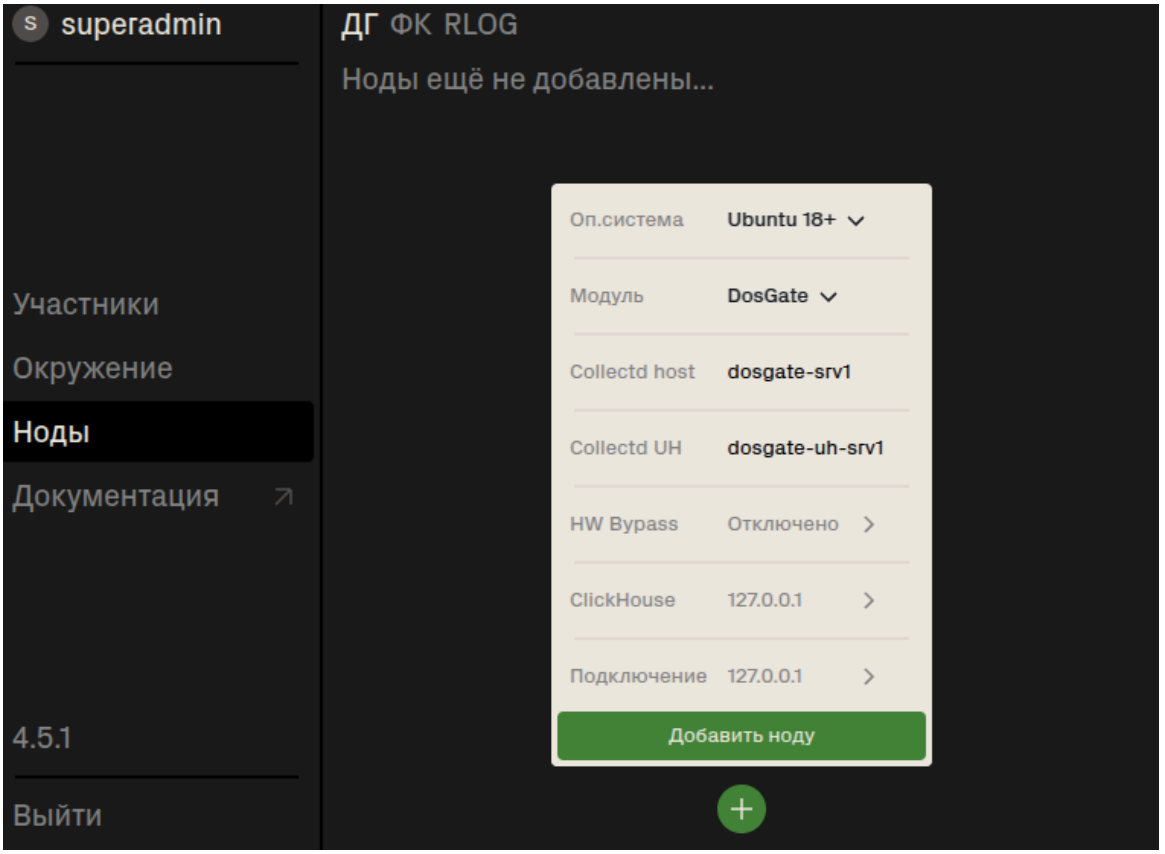
использовать hostname, который прописан в конфигурационном файле dosgate.conf в блоке *collectd*. Нажать на кнопку "Подключение".



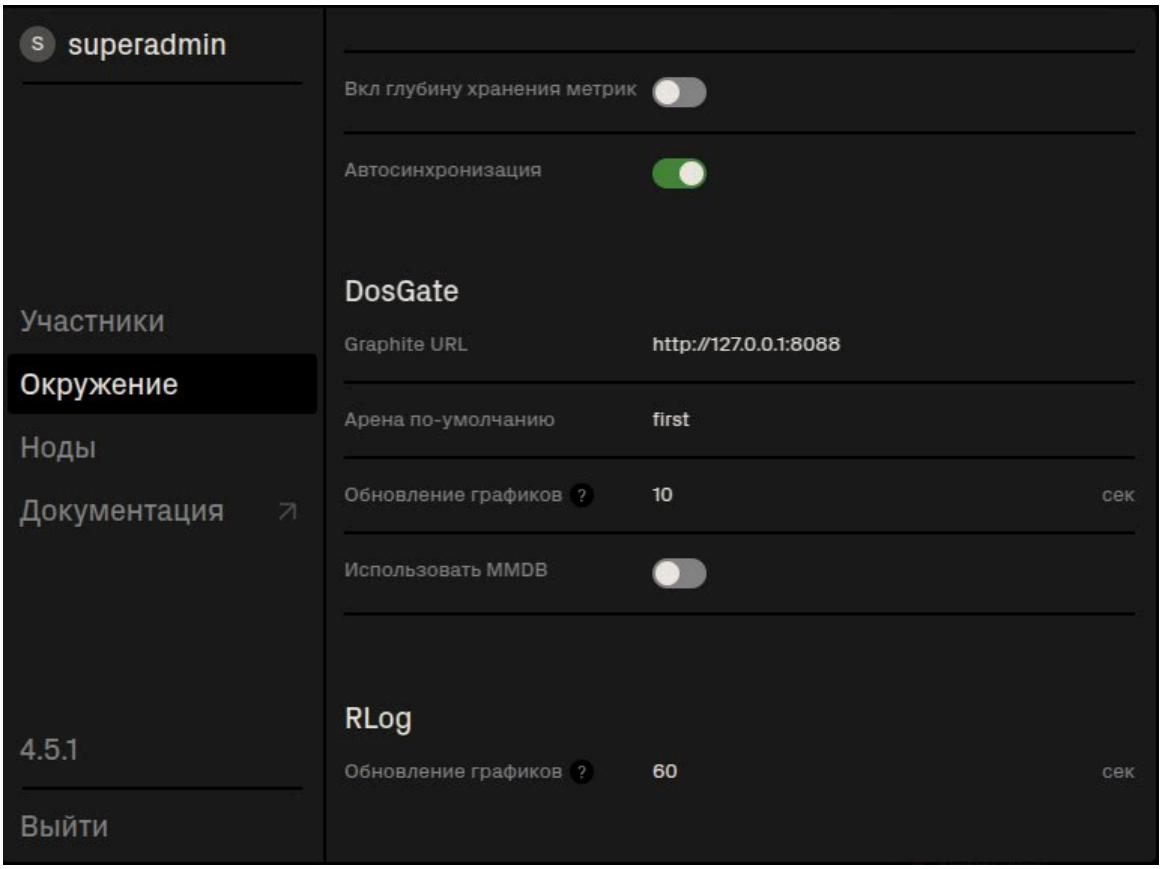
В открывшемся окне указать SSH-данные для подключения к установленной ноде Dosgate (IP-адрес, логин, пароль). Нажать на кнопку "Проверить", чтобы проверить подключение. Если данные введены правильно и нода доступна, статус изменится на "Доступна". После этого нажать кнопку "Применить".



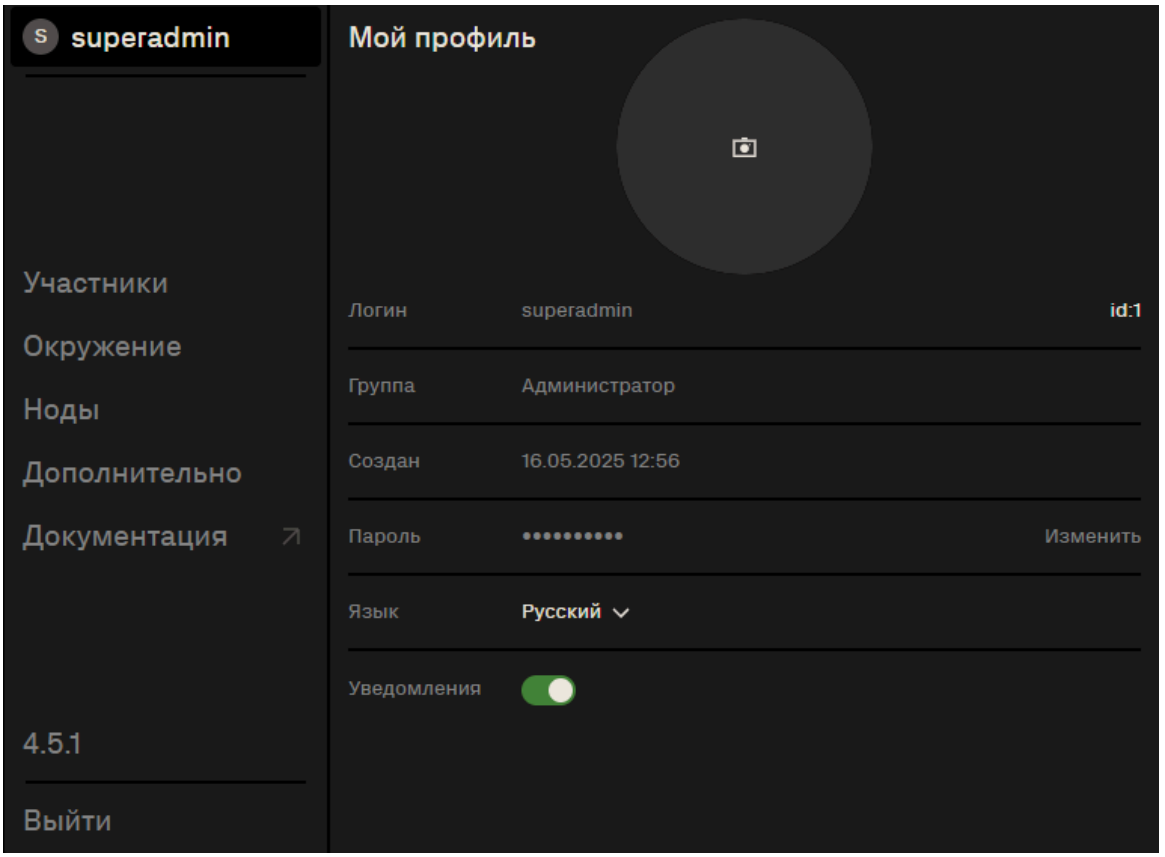
В открывшемся окне нажать "Добавить ноду".



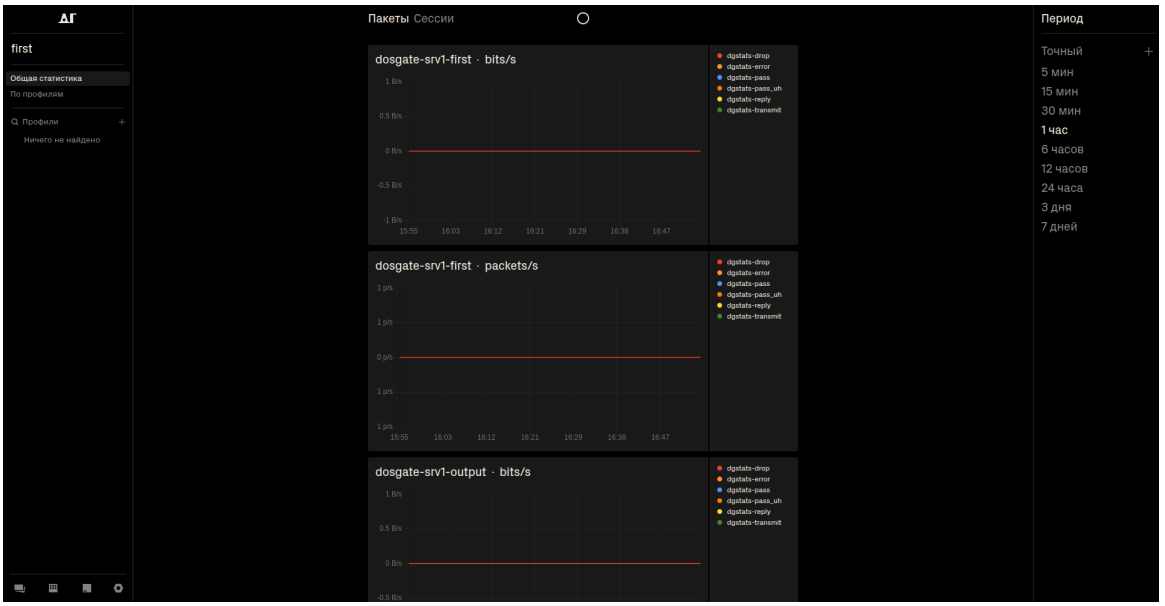
Для отображения графиков и статистики необходимо указать ссылку на Graphite. Перейдите в раздел "Окружение". В разделе DosGate указать "Graphite URL" и "Арена по-умолчанию". Название арены должно соответствовать значению, указанному в конфигурационном файле dosgate.conf для всех нод кластера.



Нажать на свой профиль в левом верхнем углу экрана, чтобы открыть настройки профиля. Установить новый пароль.



Веб-интерфейс готов к использованию.



Установка ПО DosGate на РЕД ОС 7.3

1. Подготовка операционной системы

1.1 Установка обновлений ОС

Для обновления РЕД ОС необходимо выполнить следующие команды:

```
sudo dnf update
```

```
sudo dnf upgrade
```

1.2 Подключение репозитория Servicepipe

Подключить репозиторий Servicepipe возможно двумя способами: через скрипт или вручную. Для подключения к репозиторию потребуются логин и пароль. Эти учетные данные предоставляются индивидуально для каждого заказчика. Получить их возможно запросив у вендора (Servicepipe или партнёра).

Подключение с помощью скрипта

Выполнить скрипт для автоматической настройки репозитория:

```
curl -o "./setup-repo.sh" "https://public-
repo.svcp.io/setup_script/setup-repo.sh" && \
    sudo chmod +x "./setup-repo.sh" && \
    sudo ./setup-repo.sh
```

При запуске скрипта потребуется ввести логин и пароль. После ввода учетных данных скрипт выполнит все необходимые действия

автоматически. В случае некорректной работы скрипта рекомендуется использовать метод ручной настройки репозитория.

1.3 Настройка сетевых интерфейсов

Внести необходимые изменения в сетевые интерфейсы в соответствии с текущей сетевой архитектурой компании. При Outline-инсталляции обязательно настроить VLAN'ы.

Для Inline-инсталляции необходимо использовать минимум два физических порта для передачи данных и один порт для управления.

Для Outline-инсталляции требуется минимум один физический порт для передачи данных и один порт для управления (mgmt).

Примечание
При использовании сетевых карт Intel с драйвером ixgbe рекомендуется ограничить кол-во потоков до 24:

```
ethtool -L eth1 combined 24
```

- https://www.spinics.net/lists/netdev/msg439438.html

При использовании сетевых карт Mellanox, в настройках аппаратных интерфейсов, на которых будет работать DosGate, рекомендуется указать настройку `tune_xdp = 1`. Необходимо открыть для редактирования файл **/etc/network/interfaces**. Вставить следующую строку:

```
tune_xdp = 1
```

1.4 Перезагрузка сервера

Перезагрузить сервер, выполнив команду:

```
sudo reboot
```

2. Установка DosGate

Для установки DosGate следует выполнить следующие действия:

- Установить необходимые библиотеки, выполнив команду:

```
sudo dnf update && sudo dnf install -y clang glibc glibc-
devel.i686 libbpf-0.5.0-1.el8 libbpf-0.5.0-1.el8 libbpf-devel-
0.5.0-1.el8.x86_64
```

- Установить DosGate, выполнив команду:

```
sudo dnf install -y libdt-1.2.0.1-1.el7 libaevent-0.1.1.3-1.el7
dosgate-3.2.3.1-1.el7
```

2.1 Настройка конфигурации

Все параметры работы Dosgate задаются в едином конфигурационном файле `dosgate.conf`. Конфигурационный файл находится по пути **/etc/dosgate.conf**. Его настройка обязательна перед первым запуском программного обеспечения.

- Для доступа к командам управления производится аутентификация по SSH.
- Все функции ПО используются за счет взаимодействия с командой: `dgctl`

Конфигурационный файл написан в формате YAML и содержит следующие блоки:

- socket_conf
- arena_conf
- collectd

Подробнее о каждом блоке описано в следующих разделах.

При конфигурировании файла dosgate.conf следует использовать только пробелы; табуляция недопустима. При заполнении конфигурационного файла dosgate.conf, для валидации корректности синтаксиса YAML, допустимо использовать сайт https://www.yamllint.com.

2.1.1 Блок *socket_conf*

Блок *socket_conf* сразу после установки имеет значения по умолчанию. Он настроен для использования и работы с CLI.

Пример конфигурации:

```yaml
sockets:
  - url: /run/dosgate/api.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10
```

Описание блока

URL

> URL для сокетов имеет формат `family://address`, где:

> *family* — тип сокета, который может принимать следующие значения:

- unix — UNIX-сокет, используемый на файловой системе сервера. В качестве адреса указывается полный путь к сокету.
- tcp — TCP-сокет. Адрес указывается в формате `host:port` или `:port`. Если указан только порт (`:port`), сокет будет прослушивать все доступные адреса (`0.0.0.0` или `::`).

> ***Определение типа сокета по строке адреса***

> Если `family` не указано в URL, тип сокета определяется автоматически по формату строки адреса:

- Если строка начинается с `/`, предполагается, что это UNIX-сокет (family = unix).
- Если строка содержит символ `:`, предполагается, что это TCP-сокет (family = tcp).

User

> Имя пользователя для UNIX-сокетов. Если указанный пользователь отсутствует, сокет будет использовать учетную запись пользователя, от имени которого выполняется процесс (по умолчанию root).

Group

> Группа для UNIX-сокетов. Если указанная группа отсутствует, используется первичная группа пользователя, под которым выполняется процесс (по умолчанию root).

Mode

> Режим доступа для UNIX-сокетов, задается в формате, аналогичном команде `chmod`.

ACL

> Список контроля доступа (Access Control List). Перечисляются через запятую разрешенные target (например: `profile`, `router`, `arena`, `mark`, `pset`), значение `any` - разрешает доступ ко всем частям системы.

Type

> Тип протокола/диалекта для сокета:
>
> - FCGI - FastCGI протокол, полный диалект
> - SCGI - SCGI протокол, полный диалект
> - CRLF - raw протокол, полный диалект
> - CLI - raw протокол, диалект CLI

> RAW - протокол, при котором запрос заканчивается либо последовательностью CRLF, либо закрытием сокета в сторону сервера. Ответ также завершается CRLF или окончательным закрытием сокета.

> ***Особенность для CLI:***

> Для отправки запросов через CLI должен быть настроен хотя бы один сокет с типом CLI, с family UNIX и адресом **/run/dosgate/cli.socket**

Timeout

> Общий лимит времени, в течение которого сокет ожидает завершения операции. Указывается в секундах. При отсутствии установленного таймаута сокет продолжает ожидание завершения операций или остается в состоянии бездействия без ограничения по времени.

- idle - время, в течение которого сокет может оставаться бездействующим (неактивным) перед тем, как будет разорвано соединение или предприняты другие действия.
- send - время, отведенное на отправку данных через сокет. Если данные не удается отправить в течение указанного времени, операция будет прервана.

2.1.2 Блок *arena_conf*

Основной блок конфигурации DosGate. Данный блок не имеет значений по умолчанию и требует обязательной настройки.

Пример конфигурации:

```
arenas:
  - name: first
    id: 1
```

```
    nets:
      - rx:
          name: ens1f0
          mode: vlan
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
        tx:
          name: ens1f0
          mac: 00:cc:34:4a:88:30
          mode: swap
          vid: 63
      - rx:
          name: ens3f0
          mode: vlan
          vid: 54
        tx:
          name: ens3f0
          mac: 00:cc:34:4a:88:30
          mode: swap
          vid: 55
      - rx:
          name: ens3f0
          mode: vlan
          vid: 58
        tx:
          name: ens3f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 59
```

Описание блока:

Arenas - Набор сетевых интерфейсов и настроек обработки и возврата трафика.

Name - Уникальное имя арены.

Id - Уникальный Id арены (обязателен с 3.2.2-5).

Name (nets) - Имя сетевого интерфейса, как показывает ip link. Обязательное поле.

MAC - MAC-адрес. Может быть записан в одном из следующих форматов:

`XX:XX:XX:XX:XX:XX` или `XX-XX-XX-XX-XX-XX` или `XXXX.XXXX.XXXX`

Где `X` - шестнадцатеричная цифра.

VID - VLAN id. Число от 0 до 4095, где 0 означает отсутствие тега.

Protocol - Протокол VLAN. Либо hex-число в формате 0x0000, либо мнемоническое значение:

Тэг	Значение
802.1q, 8021q, q	0x8100
802.1ad, 8021ad, ad	0x88A8
802.1ah, 8021ah, ah	0x88E7
q-in-q, qq, qinq	0x9100
q-in-q1, qq2, qinq2	0x9200
q-in-q3, qq3, qinq3	0x9300

RX block - Описывает способ обработки входящего трафика. Должен присутствовать всегда.

```
      - rx:
          name: ens5
          inline: true
          mode: transparent
          tx-policy: lacp
```

Если в блоке указан MAC-адрес, то обрабатывается только трафик с этим destination address.

`inline` - Интерфейс работает в inline-режиме, то есть он невидим для других хостов в сети. ARP-запросы, широковещательные запросы, STP/GVRP/etc не передаются в ОС. Если опция не указана, то интерфейс пересылает этот трафик в ОС.

`mode` - Режим обработки входящего трафика:

- `vlan` - обрабатывается только трафик в указанном VLAN, остальной пропускается в ОС. Если VID = 0 или не указан, обрабатывается только нетегированный трафик.
- `transparent` - обрабатывается трафик во всех VLAN + нетегированный. Используется по умолчанию.

`swap` - Указывает, нужно ли менять MAC-адреса во фрейме при отправке.

> Если указано `false` или `0`, то адреса не меняются. Если указано `true`, `1` или значение не указано , то адреса меняются.

`tx-policy` - управляет обработкой следующих классов трафика:

- `lacp` — медленный протокол LACP.
- `llm` — IEEE802.1 Link-local multicast, предназначенная для 01:80:C2:00:00:x.
- `multicast` - Любой L2 multicast, кроме link-local.
- `unknown` - unhandled ethertypes.

Например, если параметр LACP отсутствует, то LACP будет передан в ОС DosGate, а не в TX-интерфейс.

TX block - Описывает политику обработки трафика, который должен быть переслан в соответствии с окончанием обработки правилами или срабатывании действия ACCEPT. Если не указан, то копируется из блока RX, а отсутствующие в нём параметры принимают значения по умолчанию.

```
      - tx:
          name: ens4
          mac: fa:16:3e:56:32:6a
          swap: false
```

Если в блоке указан MAC-адрес, то трафик пересылается на него. В противном случае он отправляется на тот адрес, с которого был получен

`Mode` - Режим обработки исходящего трафика:

> - `swap` - меняется последний в стеке тег VLAN, или добавляется если трафик нетегированный. Если VID отсутствует, то пакет не меняется, если равен 0, то верхний тег снимается при наличии. Используется по умолчанию.
> - `push` - новый тег добавляется безусловно, даже если последний был точно таким же. Если VID = 0 или отсутствует, то ничего не добавляется.

`cos` - Класс сервиса в тегированных пакетах. Число от 0 до 7.

Reply block - Описывает политику обработки трафика, который должен быть переслан в соответствии с правилами, которые генерируют собственный трафик в ответ на входящий пакет.

```
        tx:
          name: ens5
          swap: false
        reply:
          name: ens4
          swap: true
```

- Если `reply` не указан, то автоматически копируется из *TX block*. Формат полностью соответствует формату *TX block*.

2.1.3 Блок *collectd*

```
collectd:
  hostname: dosgate
  period: 10
```

- `hostname` - имя хоста, который будет использоваться для именования метрик. Если вы устанавливаете DosGate в кластере, название должно быть уникально для каждой платформы. Именно под этим именем будут отображаться графики по серверам в общей статистике. Также с этим именем записываются метрики относительно сервера.
- `period` - частота записи метрик в collectd.

2.1.4 Примеры конфигурационного файла dosgate.conf

Пример outline инсталяции с VLAN swap и возвратом трафика в том-же интерфейсе

```
sockets:
  - url: /run/dosgate/api.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: root:dosgate
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: ens1f0
          mode: vlan
```

```
          vid: 50
        tx:
          name: ens1f0
          mac: 00:cc:34:47:a8:44
          mode: swap
          vid: 51
      - rx:
          name: ens1f0
          mode: vlan
          vid: 62
collectd:
  hostname: dosgate
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DosGate

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
```

```
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp4s0f0np0
          inline: true
          mode: transparent
        tx:
          name: enp4s0f1np1
          swap: false
        reply:
          name: enp4s0f0np0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
          name: enp4s0f1np1
          inline: true
          mode: transparent
        tx:
          name: enp4s0f0np0
          swap: false

collectd:
  hostname: dosgate
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DoSGate с LACP

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
```

```
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 120
      idle: 120

  - url: /run/dosgate/crlf.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CRLF
    timeout:
      idle: 10
      send: 10

  - url: /run/dosgate/cli.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: CLI
    timeout:
      idle: 10
      send: 10

arenas:
  - name: first
    id: 1
    nets:
      - rx:
          name: enp136s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f1
          swap: false
        reply:
          name: enp136s0f0
          swap: true
      - rx:
          name: enp138s0f0
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f1
          swap: false
        reply:
```

```
          name: enp138s0f0
          swap: true
  - name: output
    id: 2
    nets:
      - rx:
          name: enp136s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp136s0f0
          swap: false
      - rx:
          name: enp138s0f1
          mode: transparent
          inline: true
          tx-policy: lacp
        tx:
          name: enp138s0f0
          swap: false

collectd:
  hostname: dosgate
  period: 10
```

2.2 Однократный запуск DosGate

Однократный запуск DosGate выполняется с целью проверки корректности заполнения конфигурационного файла и отсутствия ошибок. Выполнить следующую команду:

```
dosgate -o -l err
```

где:

- `o` — режим однократного запуска (one-shot mode);
- `l err` — параметр, задающий уровень логирования.

Описание уровней логирования:

Уровень	Описание
debug	Отладочная информация. Подробные сведения о действиях процесса, включая системные и библиотечные вызовы.

Уровень	Описание
info	Стандартная информация о работе процесса. Сообщает, например, об открытии файлов без деталей о внутренних вызовах.
warn	Предупреждения о нарушениях нормальной работы процесса без его остановки.
err	Ошибки, приводящие к нарушению нормальной работы объекта.
crit	Критические ситуации, угрожающие стабильности системы.

2.3 Логирование работы сервисов dosgate и dosgate-uh

Сервисы *dosgate* и *dosgate-uh* осуществляют логирование работы системы в зависимости от выбранного режима. Логирование ведется в *service log* и доступно для просмотра с использованием команд:

```
sudo journalctl -xefu dosgate
```

```
sudo journalctl -xefu dosgate-uh
```

Поддерживаются три режима логирования:

debug – детализированное логирование, фиксируются практически все действия системы, включая обработку каждого сетевого пакета.
error – запись только сообщений об ошибках.
crit – запись только критических ошибок.

Содержание логов зависит от выбранного режима. Для минимизации нагрузки на систему рекомендуется использовать режим **crit** и контролировать состояние сервиса.

2.4 Настройка ротации логов

Открыть файл **/etc/systemd/journald.conf**:

```
sudo nano /etc/systemd/journald.conf
```

Раскомментировать и задать параметры:

```
SystemMaxUse=500M
RuntimeMaxUse=200M
MaxRetentionSec=1day
```

Перезапустить службу:

```
sudo systemctl restart systemd-journald
```

Открыть файл **/etc/logrotate.d/rsyslog**:

```
sudo nano /etc/logrotate.d/rsyslog
```

Рекомендуемая конфигурация:

```
/var/log/syslog
/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
        rotate 2
        size 500M
        missingok
        notifempty
        compress
        delaycompress
        sharedscripts
        postrotate
                /usr/lib/rsyslog/rsyslog-rotate
        endscript
}
```

Открыть файл **/etc/mongod.conf**:

```
sudo nano /etc/mongod.conf
```

Установить уровень логирования *0*:

```
systemLog:
  verbosity: 0       # Уровень логирования (0-5)
```

Перезапустить службу:

```
sudo systemctl restart mongod
```

Открыть файл **/etc/clickhouse-server/config.xml**:

```
sudo nano /etc/clickhouse-server/config.xml
```

Установить уровень логирования *information*

```
<level>information</level>
```

Перезапустить службу:

```
sudo systemctl restart clickhouse-server
```

3. Настройка инструментов визуализации

Процесс включает два этапа:

1 - Установка и конфигурация collectd для сбора аналитики и метрик.

> Collectd — это системный демон, предназначенный для сбора метрик производительности и ресурсов. Collectd может собирать и агрегировать данные в реальном времени, отправляя их в систему мониторинга для дальнейшего анализа и визуализации.

> Collectd настраивается для сбора показатели арены: BPS (бит в секунду), PPS (пакетов в секунду), в рамках метрик DosGate: `ACCEPT`, `PASS`, `DROP`, `ERROR`, `PASS_UH`, `REPLY`, а также в рамках меток статистики при использовании команды `-j STATS`.

2 - Установка и настройка локального Graphite или интеграция внешнего Graphite с collectd.

> После конфигурации collectd настраивается система визуализации. Варианты включают развертывание локального экземпляра Graphite для хранения и отображения метрик или настройку collectd для передачи собранных данных на внешний сервер Graphite.

3.1 Установка collectd

Установить collectd, используя команду:

```
dnf install -y collectd-5.12.0-1.el7
```

3.1.1 Настройка collectd

Для настройки следует открыть файл **/etc/collectd.conf**. Файл должен содержать только указанную информацию:

```
FQDNLookup true
TypesDB "/usr/share/collectd/types.db"

LoadPlugin logfile
LoadPlugin syslog

<Plugin logfile>
        LogLevel "info"
        File STDOUT
        Timestamp true
        PrintSeverity false
</Plugin>

<Plugin syslog>
        LogLevel info
</Plugin>

<Include "/etc/collectd.d">
        Filter "*.conf"
</Include>
```

Далее, открыть файл **/etc/collectd.d/dosgate.conf**. Файл должен содержать только указанную информацию:

```
LoadPlugin write_graphite
<Plugin write_graphite>
        <Node "localhost">
                Host "127.0.0.1" ## Заменяется на адрес внешнего
Graphite при необходимости
                Port "2003"
                Protocol "tcp"
        </Node>
</Plugin>

LoadPlugin unixsock
<Plugin unixsock>
        SocketFile "/var/run/collectd-unixsock"
        SocketPerms "0660"
        DeleteSocket false
```

```
</Plugin>

TypesDB "/etc/collectd.d/dosgate-types.db"
```

Далее, открыть файл **/etc/collectd.d/dosgate-types.db**. Файл должен содержать только указанную информацию:

```
dgstats         packets:COUNTER:0:U     bytes:COUNTER:0:U
```

3.1.2 Запуск collectd

Для запуска collectd необходимо выполнить следующие шаги:

Перезапустить службу, используя команду:

```
sudo systemctl restart collectd
```

Проверить, что всё запустилось корректно, используя команду:

```
sudo systemctl status collectd
```

Включить автозапуск службы:

```
sudo systemctl enable collectd
```

3.1.3 Добавление collectd в конфигурационный файл DosGate

> **Внимание!**
> Данный пункт 3.1.3 полностью дублирует 2.1.3. Допустимо его пропустить, если настройка блока collectd уже производилась в пункте 2.1.3.

Открыть конфигурационный файл **/etc/dosgate.conf**. Добавить в него следующую информацию:

```
collectd:
  hostname: dosgate
```

```
  period: 10
```

- При установке DosGate в кластере, необходимо убедиться, что его hostname является уникальным для платформы.

3.1.4 Внесение изменений в DosGate после настройки collectd

Перезагрузить службу DoSGate:

```
sudo systemctl restart dosgate
```

Проверить записи метрик, выполнив команду:

```
sudo systemctl status dosgate
```

Лог должен содержать сообщение:

```
[dg_collectd_sender.c:70, GLOB] Collectd send success
```

Необходимо изменить уровень логирования, поскольку текущая конфигурация генерирует избыточные и подробные логи, что приводит к перегрузке диска. Рекомендуется установить уровень логирования на crit, чтобы фиксировать только критически важные события.

Открыть конфигурационный файл `dosgate.service`, используя команду:

```
sed -i 's/dosgate -f/dosgate -f -l crit/'
/usr/lib/systemd/system/dosgate.service
```

Заменить строку `ExecStart=dosgate -f` на `ExecStart=dosgate -f -l crit`.

Примечание
Пути к systemd-юнитам могут отличаться в зависимости от системы и версии программного обеспечения. Перед редактированием или созданием юнита убедитесь, что нужный файл существует и найдено его точное расположение.

Чтобы проверить это, выполните команду: `sudo systemctl status имя-юнита`

Применить измненения:

```
sudo systemctl daemon-reload
```

Запустить службу DosGate:

```
sudo systemctl start dosgate
```

Убедиться, что служба запустилась корректно, выполнив команду:

```
sudo systemctl status dosgate
```

Активировать автозагрузку сервиса DosGate:

```
systemctl enable dosgate
```

3.2 Установка Graphite

Установка Graphite на РЕД ОС не была протестирована! Рекомендуется выполнять установку на отдельном сервере с операционной системой Ubuntu.

Далее приведена иструкция для установки на операционную систему Ubuntu

3.2.1 Установка Docker

Docker — это платформа, которая помогает запускать приложения в изолированных средах, называемых контейнерами. Эти контейнеры содержат всё необходимое для работы приложения, что делает его проще в установке и запуске на разных компьютерах.

Добавить ключ GPG для Docker:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg
--dearmor -o /etc/apt/keyrings/docker.gpg
```

Изменить права доступа к ключу:

```
sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

Добавить официальный репозиторий Docker в список источников APT:

```
echo \
  "deb [arch="$(dpkg --print-architecture)" signed-
by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
  "$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Обновить список пакетов и установить Docker с помощью следующих команд:

```
sudo apt update
```

```
sudo apt install docker-ce docker-ce-cli containerd.io
```

Добавить пользователя в группу Docker:

```
sudo usermod -aG docker $USER
```

Убедиться, что Docker установлен и работает, запустив следующую команду:

```
docker version
```

Проверить, что служба Docker запущена, с помощью команды:

```
sudo systemctl status docker
```

3.2.2 Установка контейнера Graphite

Создать директории, которые будут использоваться контейнером Graphite для хранения данных, логов, конфигурации и настроек:

```
sudo mkdir -p /data/graphite/{data,logs,conf,statsd_config}
```

3.2.3 Добавление Graphite в systemd

Отредактируйте файл службы graphite-docker.service:

```
sudo nano /etc/systemd/system/graphite-docker.service
```

Вставьте следующее содержимое в файл:

```
[Unit]
Description=Graphite Docker Container
Documentation=https://github.com/graphite-project/docker-graphite-
statsd
After=docker.service
Requires=docker.service

[Service]
Type=simple
TimeoutStartSec=0
Restart=on-failure
RestartSec=30s
ExecStartPre=-/usr/bin/docker kill graphite
ExecStartPre=-/usr/bin/docker rm graphite
ExecStartPre=/usr/bin/docker pull graphiteapp/graphite-statsd
ExecStart=/usr/bin/docker run \
            --name graphite \
            --restart=always \
            -p 8080:80 \
            -p 2003-2004:2003-2004 \
            -p 2023-2024:2023-2024 \
            -p 8125:8125/udp \
            -p 8126:8126 \
            -v /data/graphite/data:/opt/graphite/storage \
            -v /data/graphite/conf:/opt/graphite/conf \
```

```
            -v /data/graphite/statsd_config:/opt/statsd/config \
            -v /data/graphite/logs:/var/log \
            graphiteapp/graphite-statsd

SyslogIdentifier=graphite
ExecStop=/usr/bin/docker stop graphite

[Install]
WantedBy=multi-user.target
```

3.2.4 Запуск Graphite

Обновить конфигурацию systemd:

```
sudo systemctl daemon-reload
```

Активировать службу для автозапуска:

```
sudo systemctl enable graphite-docker
```

Запуск службы Graphite:

```
sudo systemctl start graphite-docker.service
```

Проверить статус службы, с помощью команды:

```
sudo systemctl status graphite-docker.service
```

3.2.5 Настройка Graphite

Необходимо установить диапазон хранения Graphite в 10 секунд вместо 1 минуты (стандартное значение после установки) для более точной статистики.

Откройте файл `storage-schemas.conf` для редактирования:

```
sudo nano /data/graphite/conf/storage-schemas.conf
```

Добавить следующую конфигурацию в начало файла перед другими записями:

```
[default]
pattern = .*
retentions = 10s:14d,60s:365d
```

Сохраните изменения и закройте файл.

3.2.6 Перезапуск и очистка данных

Остановить службу Graphite перед удалением старых данных:

```
sudo systemctl stop graphite-docker
```

Удалить старые данные из папки dosgate:

```
sudo rm -rf /data/graphite/data/whisper/dosgate
```

Перезапустить службы Graphite:

```
sudo systemctl start graphite-docker
```

3.2.7 Формат хранения данных в Graphite

DosGate имеет следующую вложенность при хранении данных в Graphite:

`hostname.arena|profile.stats.bytes|packets`

hostname - Задается в конфигурационном файле dosgate.conf в блоке collectd.

arena - Задается в конфигурационном файле dosgate.conf, в блоке arenas, атрибут `name`.

profile - Профиль защиты,задаваемый системным администратором при настройке DoSGate.

stats - Это действия, происходящие с трафиком, которые отображают его состояние и обработку. Возможные действия:

`drop` - Трафик сброшен как результат правила `-j DROP`.

`accept` - Трафик принят и отправлен согласно настройкам dosgate.conf, без сброса.

`pass` - Трафик передан операционной системе как результат правила `-j PASS`.

`reply` - DosGate отвечает на пакет вместо конечного получателя. Это применяется при TCP авторизации для проверки IP-спуфинга, когда DosGate отправляет пакет с флагом RST или с некорректным значением последовательности (Sequence) для верификации отправителя.

`error` - Пакет не обработан из-за несоответствия стандартам IP RFC или потому, что DosGate не смог его корректно разобрать (например, пакет поврежден).

`-j STATS name` - сбор статистики по указанной метке. Это настраивается администратором при создании правила и позволяет отслеживать статистику конкретного правила. Например, правило: `-m protocol udp -j STATS udp_packets`, `-j DROP` будет сбрасывать все пакеты UDP и собирать статистику по этим пакетам и их объему.

bytes - Статистика объема данных в байтах. Для перевода в биты умножьте значение на 8.

packets - Статистика количества переданных пакетов.

4. Установка веб-интерфейса

Установка веб-интерфейса на РЕД ОС не поддерживается! Рекомендуется выполнять установку на отдельном сервере с операционной системой Ubuntu или Альт 8 СП.

Инструкция по установке веб-интерфейса на Альт 8 СП

Далее приведена иструкция для установки на операционную систему Ubuntu

4.1 Архитектурные особенности

Веб-интерфейс SP-Spider предназначен для упрощения и автоматизации управления кластером DosGate, обеспечивая операторам удобный доступ к настройкам системы через визуальный интерфейс. С его помощью можно вводить новые правила, редактировать существующие, применять заранее настроенные пресеты, а также отслеживать состояние кластера и статистику работы в режиме реального времени.

Веб-интерфейс SP-Spider и ноды DosGate могут быть развернуты в различных архитектурных конфигурациях в зависимости от требований заказчика. Интерфейс поддерживает аппаратное резервирование и кластеризацию, обеспечивая работу в режиме active-active для повышения доступности и отказоустойчивости. Подробное описание различных архитектур доступно в разделе Архитектуры инсталляций.

Компоненты системы
Для работы веб-интерфейса используются следующие компоненты:

- **SP-Spider** — это веб-интерфейс, предназначенный для управления и настройки программного обеспечения DosGate.
- **SP-Spider-Broker** - выступает в роли брокера синхронизации для DosGate.
- **Node.js**: Среда выполнения для веб-интерфейса, обеспечивающая его основную функциональность.
- **PostgreSQL**: Реляционная база данных для хранения конфигурационных данных и правил.
- **RabbitMQ**: Брокер сообщений, обеспечивающий синхронизацию и обработку очередей сообщений.

4.2 Инструкция по установке и настройке компонентов

4.2.1 Установка обновления операционной системы

Выполнить команду для обновления списка пакетов:

```
sudo apt-get update
```

Обновить установленные пакеты:

```
sudo apt-get upgrade
```

4.2.2 Установка Node.js

Выполнить команду для установки NodeJS:

```
sudo apt install nodejs=18.18.2-1nodesource1
```

4.2.3 Установка PostgreSQL

Установить PostgreSQL и библиотеку для работы с ней:

```
sudo apt install -y libpq-dev postgresql
```

4.2.4 Настройка PostgreSQL

Открыть файл конфигурации для редактирования:

```
sudo nano /etc/postgresql/14/main/pg_hba.conf
```

Убедиться, что файл содержит запись:

```
host    all             all             127.0.0.1/32
scram-sha-256
```

Проверить наличие записи командой:

```
cat /etc/postgresql/14/main/pg_hba.conf | grep "host    all
all             127.0.0.1/32            scram-sha-256"
```

Создать базу данных и пользователя:

```
sudo -u postgres psql
```

Выполнить команды в консоли PostgreSQL:

```
CREATE DATABASE dosgate;
```

```
CREATE USER dosgate WITH ENCRYPTED PASSWORD 'password';
```

```
GRANT ALL PRIVILEGES ON DATABASE dosgate TO dosgate;
```

```
\q
```

4.2.5 Установка RabbitMQ

Создать скрипт установки:

```
sudo nano quickrabbitmq.sh
```

Вставить в скрипт следующий код:

```
#!/bin/sh

sudo apt-get install curl gnupg apt-transport-https -y

## Team RabbitMQ's main signing key
curl -1sLf "https://keys.openpgp.org/vks/v1/by-
fingerprint/0A9AF2115F4687BD29803A206B73A36E6026DFCA" | sudo gpg -
-dearmor | sudo tee /usr/share/keyrings/com.rabbitmq.team.gpg >
/dev/null
## Community mirror of Cloudsmith: modern Erlang repository
curl -1sLf https://ppa1.novemberain.com/gpg.E495BB49CC4BBE5B.key |
sudo gpg --dearmor | sudo tee
/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg > /dev/null
## Community mirror of Cloudsmith: RabbitMQ repository
```

```
curl -1sLf https://ppa1.novemberain.com/gpg.9F4587F226208342.key |
sudo gpg --dearmor | sudo tee
/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg > /dev/null

## Add apt repositories maintained by Team RabbitMQ
sudo tee /etc/apt/sources.list.d/rabbitmq.list <<EOF
## Provides modern Erlang/OTP releases
##
deb [signed-by=/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-erlang/deb/ubuntu
jammy main
deb-src [signed-
by=/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-erlang/deb/ubuntu
jammy main

## Provides RabbitMQ
##
deb [signed-by=/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-server/deb/ubuntu
jammy main
deb-src [signed-
by=/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-server/deb/ubuntu
jammy main
EOF

## Update package indices
sudo apt-get update -y

## Install Erlang packages
sudo apt-get install -y erlang-base \
                        erlang-asn1 erlang-crypto erlang-eldap
erlang-ftp erlang-inets \
                        erlang-mnesia erlang-os-mon erlang-
parsetools erlang-public-key \
                        erlang-runtime-tools erlang-snmp erlang-
ssl \
                        erlang-syntax-tools erlang-tftp erlang-
tools erlang-xmerl

## Install rabbitmq-server and its dependencies
sudo apt-get install rabbitmq-server -y --fix-missing
```

Сохранить и закрыть файл. Запустить скрипт для установки RabbitMQ:

```
sudo bash quickrabbitmq.sh
```

4.2.6 Настроика RabbitMQ

Создать пользователя RabbitMQ:

```
sudo rabbitmqctl add_user "username" "password"
```

Назначить права доступа пользователю:

```
sudo rabbitmqctl set_permissions -p "/" "username" ".*" ".*" ".*"
```

4.3 Инструкция по подготовке системы DosGate

4.3.1 Увеличить значение TimeoutStartSec (необязательно)

Если конфигурация содержит более 25 профилей, необходимо увеличить тайм-аут для запуска сервиса DosGate. Необходимо открыть файл конфигурации сервиса:

```
sudo nano /lib/systemd/system/dosgate.service
```

Установить значение `TimeoutStartSec=600`:

```
[Unit]
Description=Dosgate anti-ddos controller
After=network.target
ConditionPathExists=/etc/dosgate.conf

[Service]
Type=notify
ExecStart=dosgate -f -l crit
RuntimeDirectory=dosgate
StateDirectory=dosgate
TimeoutStartSec=600

[Install]
WantedBy=multi-user.target
```

Сохранить изменения и закрыть файл.

4.3.2 Настроить конфигурационный файл dosgate.conf

Проверить, что в файле **/etc/dosgate.conf** настроен параметр FAPI.socket для взаимодействия веб-интерфейса:

```
- url: /run/dosgate/fapi.socket
  user: www-data
  group: www-data
  mode: 0660
  acl: any
  type: FCGI
  timeout:
 send: 120
 idle: 120
```

4.3.3 Добавление сервиса проверки прав FAPI.socket

Установить права для FAPI-сокета:

```
chmod 660 /run/dosgate/fapi.socket
```

Перезапустить службу DosGate, выполнив команду:

```
sudo service dosgate restart
```

Создать новый сервис:

```
sudo nano /etc/systemd/system/fix_fapi.service
```

Вставить следующую конфигурацию в созданный файл:

```
[Unit]
Description=Run fix fapi-socket at startup after all systemd
services
After=default.target
```

```
[Service]
Type=simple
RemainAfterExit=yes
ExecStart=chmod 660 /run/dosgate/fapi.socket
TimeoutStartSec=0

[Install]
WantedBy=default.target
```

Сохранить файл, активировать и запустить сервис:

```
systemctl enable --now /etc/systemd/system/fix_fapi.service
```

4.3.4 Заведение SSH-пользователя

Для синхронизации и дополнительных проверок, веб-интерфейс соединяется по SSH с каждой системой-dosgate

Убедитесь что на каждой системе-dosgate есть настроенный SSH-пользователь с доступом к `sudo`.

Создать нового пользователя:

```
sudo adduser dosgate-web
```

Добавить пользователя в группу sudo:

```
sudo usermod -aG sudo dosgate-web
```

Убедиться, что авторизация по SSH через пароль разрешена для этого пользователя.

4.3.5 Настроика NGINX

Если Graphite установлен через Docker, важно учитывать некоторые особенности настройки портов и конфигурации.

По умолчанию, Graphite, запущенный через Docker, работает на порту 8080 и не задействует основной сервер nginx. Однако, если на платформе имеются другие конфигурации nginx, которые используют порты 80 или 443, это может привести к конфликтам.

Если Graphite запущен на той же аппаратной платформе, необходимо убедиться, что порты 80 и 443 свободны или не используются другими сервисами. Чтобы проверить текущую конфигурацию Graphite, выполнить следующие шаги:

Открыть файл конфигурации nginx для Graphite, используя команду:

```
sudo nano /etc/nginx/sites-available/graphite
```

Если установлен 80 или 443 порт, изменить на 8080 :

```
listen 8080 default_server;
listen [::]:8080 default_server;
```

Примечание
Если в системе используется Grafana, обновите настройки источника данных.

Обновить систему, используя команды:

```
sudo apt update
```

```
sudo apt upgrade
```

Установить NGINX:

```
sudo apt install nginx=1.26.2-1~jammy-servicepipe-
20241111.162950.UTC
```

Удалить стандартную конфигурацию NGINX:

```
sudo rm /etc/nginx/sites-available/default /etc/nginx/sites-
enabled/default
```

Создать файл конфигурации для FAPI:

```
sudo nano /etc/nginx/sites-available/fapi.conf
```

Вставить следующую конфигурацию:

```
server {
  listen 80 default_server;
  listen [::]:80 default_server;

  server_name REPLACE_ON_DOMAIN_OR_IP;
  root /var/www/html;
  index index.php;

  location /fapi {
    include fastcgi_params;
    fastcgi_pass  unix:/run/dosgate/fapi.socket;
  }

  location /broker {
    rewrite ^/broker(.*)$ $1 break;
    proxy_pass http://localhost:3335;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_cache_bypass $http_upgrade;
  }
}
```

Примечание
Заменить `server_name REPLACE_ON_DOMAIN_OR_IP` на домен или IP-адрес!

Создать ссылку:

```
sudo ln -s /etc/nginx/sites-available/fapi.conf /etc/nginx/sites-enabled
```

Перезапустить NGINX:

```
sudo systemctl restart nginx
```

4.3.6 Настройка сети

Убедитесь, что веб-интерфейс имеет связанность до каждой системы-dosgate.

4.4 Инструкция по установке веб-интерфейса и брокера синхронизации

Установить пакеты веб-интерфейса и брокера синхронизации:

```
sudo apt install sp-spider sp-spider-broker
```

4.4.1 Настройка веб-интерфейса

В зависимости от условий установки необходимо обновить авторизационные данные, порты базы данных и другие параметры в .env-файле. Сначала выполняется настройка веб-интерфейса, затем — брокера.

Открыть для редактирования файл **/opt/sp-spider/.env**:

```
sudo nano /opt/sp-spider/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
NODE_ENV=production

VITE_APP_PORT=3333                              # Порт веб-интерфейса
HTTP_TIMEOUT=10000                              # Таймаут HTTP-запросов, мс
IS_PRIMARY=true                                 # Определяет, является ли интерфейс основным, независимо от наличия резервирования

APP_SECRET=salt_salt_salt                       # Секретный ключ для хэширования паролей. Не меняйте после первого запуска
```

```
# Параметры подключения к PostgreSQL
DB_HOST="localhost"                                 # Адрес сервера
PostgreSQL
DB_PORT="5432"                                      # Порт PostgreSQL
DB_USER="YOUR_DB_USER"                              # Имя пользователя
PostgreSQL
DB_DATABASE="YOUR_DB_NAME"                          # Имя базы данных
PostgreSQL
DB_PASSWORD="YOUR_DB_PASSWORD"                      # Пароль
пользователя PostgreSQL

# Параметры RabbitMQ для синхронизации и брокера
RMQ_ENABLE="true"                                   # Включает
RabbitMQ
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"       # URL подключения
к RabbitMQ с учётными данными
RMQ_RECONNECT_INTERVAL="5000"                       # Интервал
переподключения к RabbitMQ, мс

# Параметры аутентификации через LDAP
LDAP_ENABLED=true                                   # Включает
интеграцию с LDAP
LDAP_URL="ldap://ldap.example.local:389"            # Адрес LDAP-
сервера
LDAP_DN="dc=company,dc=local"                       # Базовый DN
каталога
LDAP_GROUP_CN="users"                               # CN группы
пользователей
LDAP_SERVICE_ACCOUNT_DN="uid=user1,ou=people,dc=company,dc=local"
# DN сервисной учётной записи
LDAP_SERVICE_ACCOUNT_PASSWORD="YOUR_LDAP_PASSWORD"
# Пароль сервисной учётной записи

# Параметры подключения по LDAPS
LDAP_CERT=""                                        # Путь к CA-
сертификату при использовании LDAPS

# Параметры аутентификации через TACACS
TAC_ENABLED=true                                    # Включает
интеграцию с TACACS
TAC_HOST="YOUR_TACACS_HOST"                         # Адрес TACACS
сервера
TAC_PORT="49"                                       # Порт TACACS
TAC_SECRET="your_secret_key"                        # Секретный ключ
TACACS
TAC_GROUP_NAME="group_admin,group_operator"         # Группы доступа
TAC_SERVICE_NAME="spider"                           # Имя сервиса

# Параметры подключения к ClickHouse
CLICKHOUSE_USER=default                             # Пользователь
```

```
ClickHouse
CLICKHOUSE_PASSWORD=password                    # Пароль
ClickHouse
CLICKHOUSE_DB=default                           # База данных
ClickHouse
CLICKHOUSE_HOST=127.0.0.1                       # Адрес ClickHouse
CLICKHOUSE_PORT=8123                            # Порт ClickHouse
```

Примечание

Использовать AMQPs при необходимости.

Если требуется поддержка TLS замените

```
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"
```

на

```
 RMQ_URL="amqps://USER:PASSWORD@localhost:5672"
```

4.4.2 Настройка брокера

Открыть для редактирования файл **/opt/sp-spider-broker/.env**:

```
sudo nano /opt/sp-spider-broker/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
APP_PORT=3335 # Порт, на котором запустится сервис

# Ключ из .env веб-интерфейса
APP_SECRET="YOUR_APP_SECRET"                    #
Секретный ключ приложения

# Параметры от PostgreSQL из .env веб-интерфейса
DB_HOST="localhost"                             #
Адрес сервера PostgreSQL
DB_PORT="5432"                                  # Порт
PostgreSQL
DB_USER="YOUR_DB_USER"                          # Имя
```

```
пользователя PostgreSQL
DB_DATABASE="YOUR_DB_NAME"                                  # Имя
базы данных PostgreSQL
DB_PASSWORD="YOUR_DB_PASSWORD"                              #
Пароль пользователя PostgreSQL

# Параметры RabbitMQ из .env веб-интерфейса
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"               # URL
подключения к RabbitMQ
RMQ_RECONNECT_INTERVAL="5000"                               #
Интервал переподключения к RabbitMQ, мс

# Путь к папке с политиками DosGate UH.
POLICY_PATH="/var/lib/dosgate-uh/profiles/"                 #
Обязательно в конце ставить "/"

# Путь к конфигурации обработчика оффендеров DosGate UH
OFFENDERS_CONF_PATH="/opt/sp-spider-
broker/offenders/offenders.conf"

# Путь к объектам защиты FlowCollector.
FC_MO_PATH="/opt/spfc/etc/mo/"                              #
Обязательно в конце ставить "/"

# Путь к симлинкам на объекты защиты FlowCollector.
FC_MO_SYMLINK_PATH="/opt/spfc/etc/mo.enabled/"              #
Обязательно в конце ставить "/"

# Путь к объектам обучения Treshold Learner.
FC_LEARNER_PATH="/opt/spfc/etc/learner/"                    #
Обязательно в конце ставить "/"

# Путь к симлинкам на объекты обучения Treshold Learner.
FC_LEARNER_SYMLINK_PATH="/opt/spfc/etc/learner.enabled/"    #
Обязательно в конце ставить "/"

# Путь к конфигурации анализатора FlowCollector.
FC_ANALYZER_CONF_PATH="/opt/spfc/etc/analyzer.yaml"

# Путь к бинарному файлу анализатора
FC_ANALYZER_BINARY_PATH="/opt/spfc/bin/analyzer"

# Путь к конфигурации DosGate UH
DGUH_CONF="/etc/dosgate-uh.conf"

# Путь к снэпшотам дампов DosGate UH
DGUH_SNAPSHOTS="/var/cache/dosgate-uh-snapshots"

# Параметры GeoIP
MMDB_PATH="/etc/dosgate/GeoLite2-Country.mmdb"               #
Путь к mmdb-файлу
```

```
MMDB_DEFAULT_PATH="/usr/share/dosgate/GeoLite2-Country.mmdb" #
Путь к дефолтному mmdb файлу

# Параметры Rlog
RLOG_RULES_PATH="/var/lib/rlog/rules/"                        #
Путь к правилам обработки syslog
RLOG_DUMP_PATH= "/var/lib/rlog/dumps/"                        #
Путь к дампам Rlog
RLOG_URL= "http://127.0.0.1:3003"                             # URL
сервиса Rlog

# Параметры BGP
GOBGP_GRPC_SERVER="GOBGP_HOST:PORT"                           #
Адрес gRPC-сервера GoBGP

# Путь к файлу со списками правил FlowSpec
FLOWSPEC_CONF_PATH="/opt/spfc/etc/"


# Параметры синхронизации
UPDATE_CONFIG_INTERVAL_SECONDS=10                             #
Интервал обновления конфигурации, с
SPIDER_URL="http://SPIDER_HOST:3333"                          # URL
интерфейса Spider

# Параметры подключения к ClickHouse
CLICKHOUSE_USER=default                                       #
Пользователь ClickHouse
CLICKHOUSE_PASSWORD=password                                  #
Пароль ClickHouse
CLICKHOUSE_DB=default                                         #
База данных ClickHouse
CLICKHOUSE_HOST=127.0.0.1                                     #
Адрес ClickHouse
CLICKHOUSE_PORT=8123                                          #
Порт ClickHouse
```

4.4.3 Создание сервиса

Для веб-интерфейса:

Отредактировать файл **/usr/lib/systemd/system/sp-spider.service**:

```
sudo nano /usr/lib/systemd/system/sp-spider.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider

[Service]
ExecStart=/usr/bin/node /opt/sp-spider/server/main.js
WorkingDirectory=/opt/sp-spider
Restart=always

[Install]
WantedBy=multi-user.target
```

Для брокера:

Отредактировать файл **/usr/lib/systemd/system/sp-spider-broker.service**:

```
sudo nano /usr/lib/systemd/system/sp-spider-broker.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider Broker

[Service]
ExecStart=/opt/sp-spider-broker/sp-spider-broker
WorkingDirectory=/opt/sp-spider-broker
Restart=always

[Install]
WantedBy=multi-user.target
```

Активировать и запустить сервисы:

```
sudo systemctl enable --now sp-spider sp-spider-broker
```

Проверить статус всех компонентов:

```
sudo systemctl status sp-spider
```

```
sudo systemctl status sp-spider-broker
```

```
sudo systemctl status rabbitmq-server
```

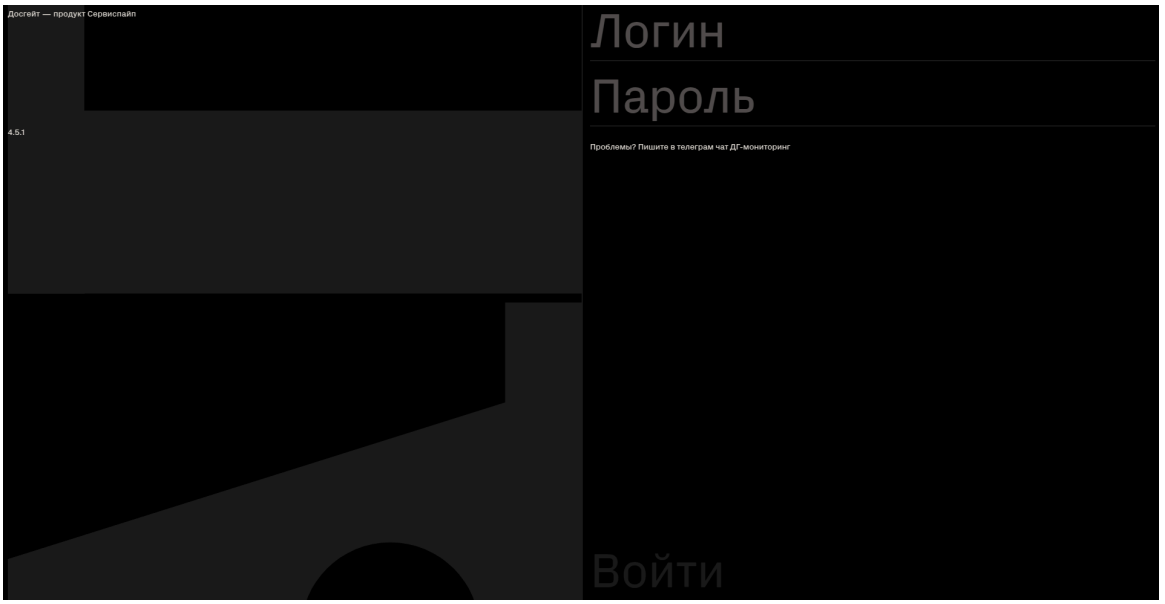
```
sudo systemctl status postgresql
```

```
sudo systemctl status nginx
```

5. Первый вход в систему

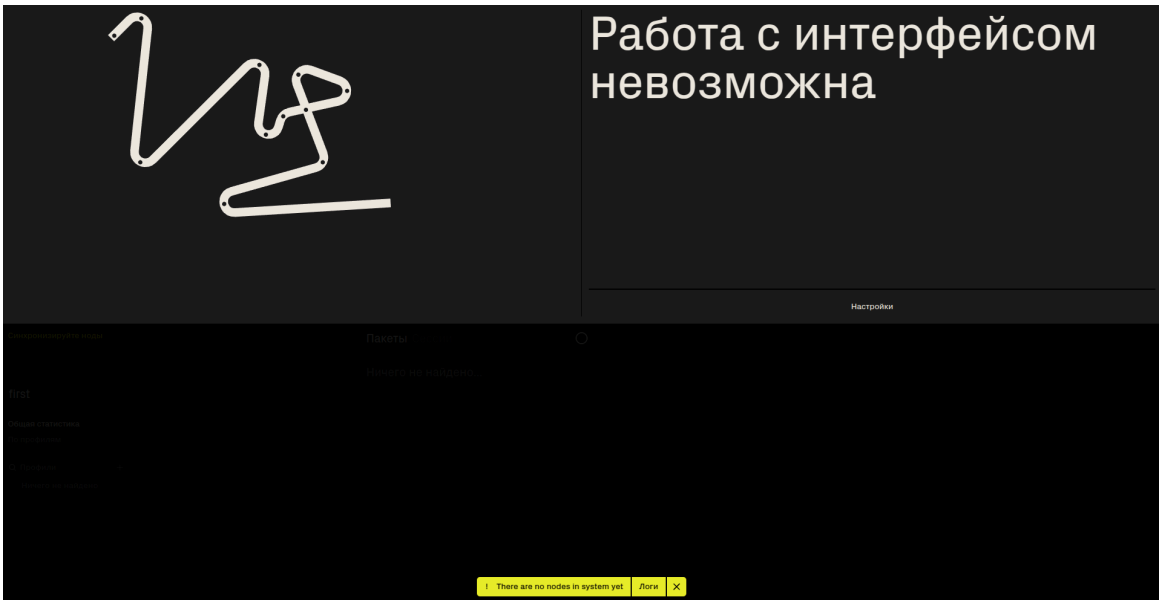
Для входа в Веб-интерфейс DosGate следует ввести в адресной строке браузера IP-адрес и порт по шаблону: `ip:port`. Указать порт, указанный в переменной `VITE_APP_PORT` файла **/opt/sp-spider/.env** в разделе 4.4.1 Настройка веб-интерфейса

Появится окно авторизации (см. рисунок ниже). В окне авторизации следует указать следующие логин и пароль по умолчанию: ***superadmin/superadmin***

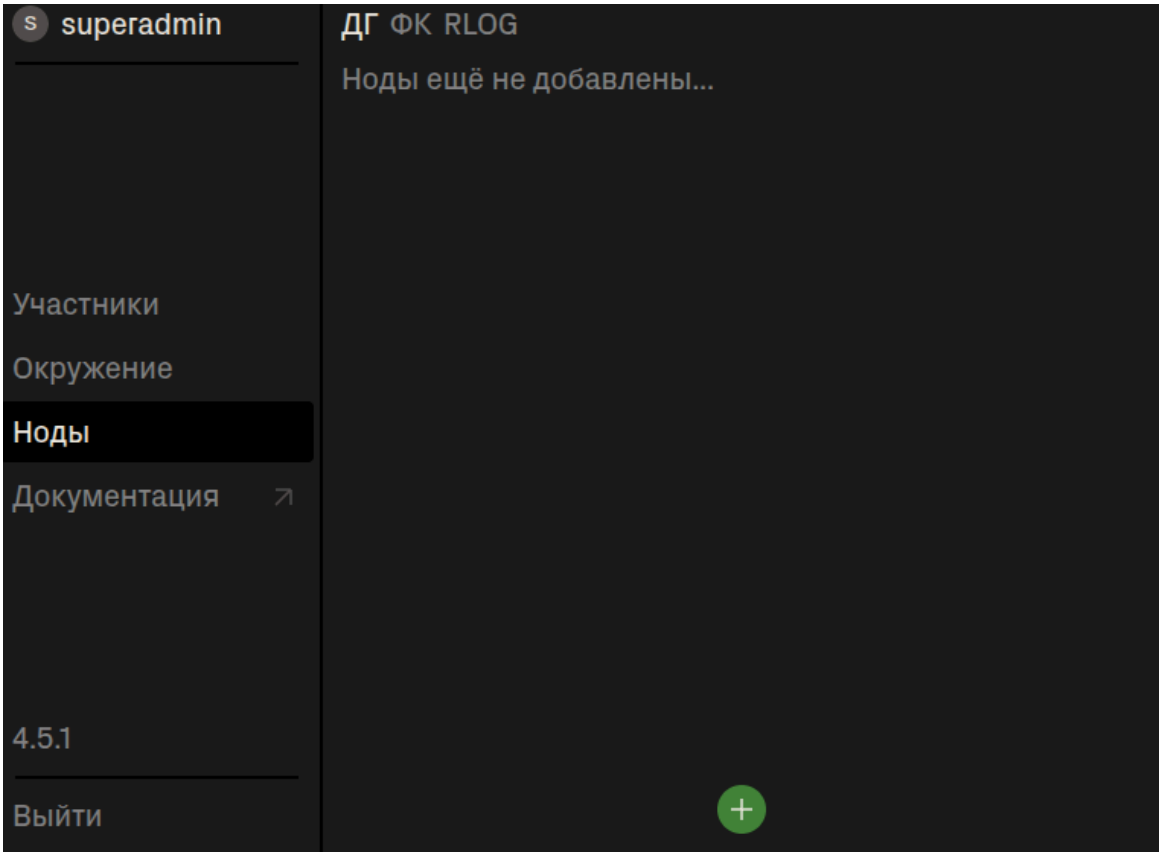


Окно авторизации при входе в систему

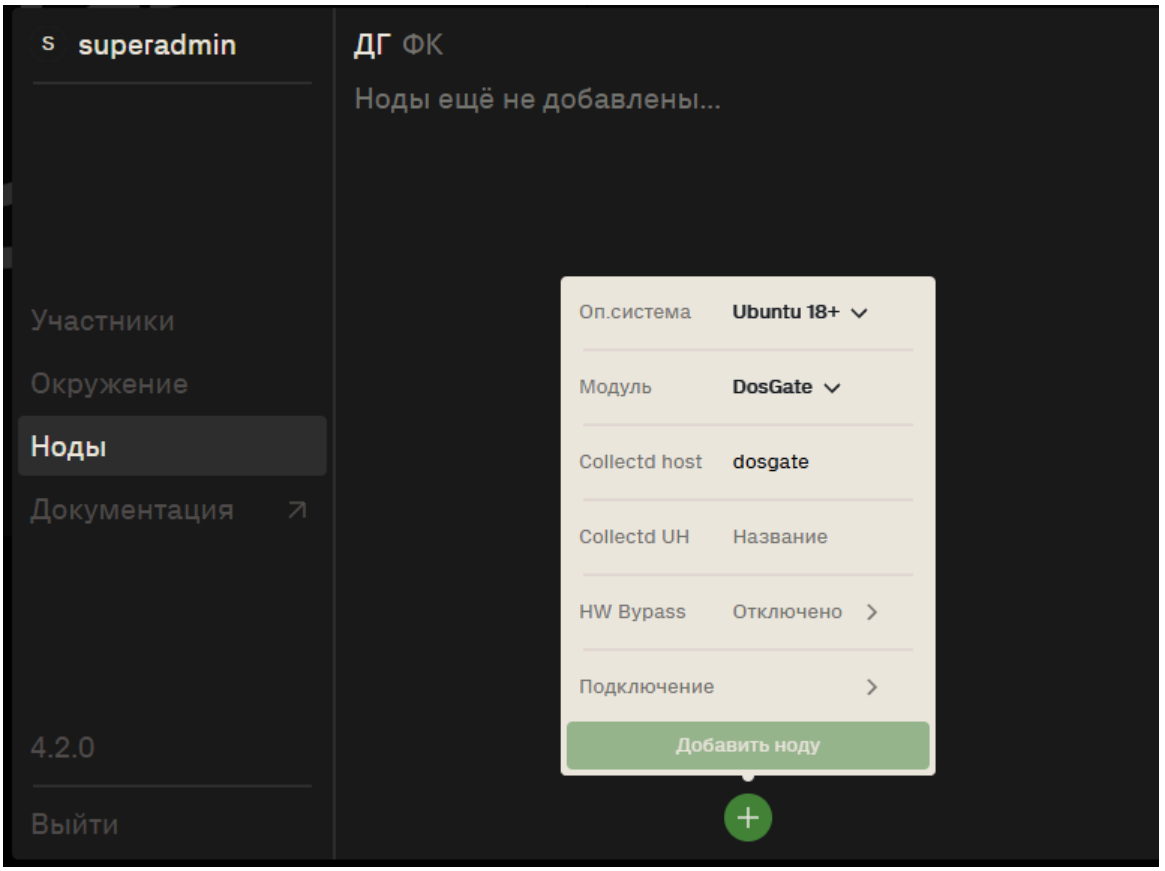
После авторизации появится уведомление "Работа с интерфейсом невозможна" (см. рисунок ниже). Это связано с тем, что в данный момент нет настроенной ноды.



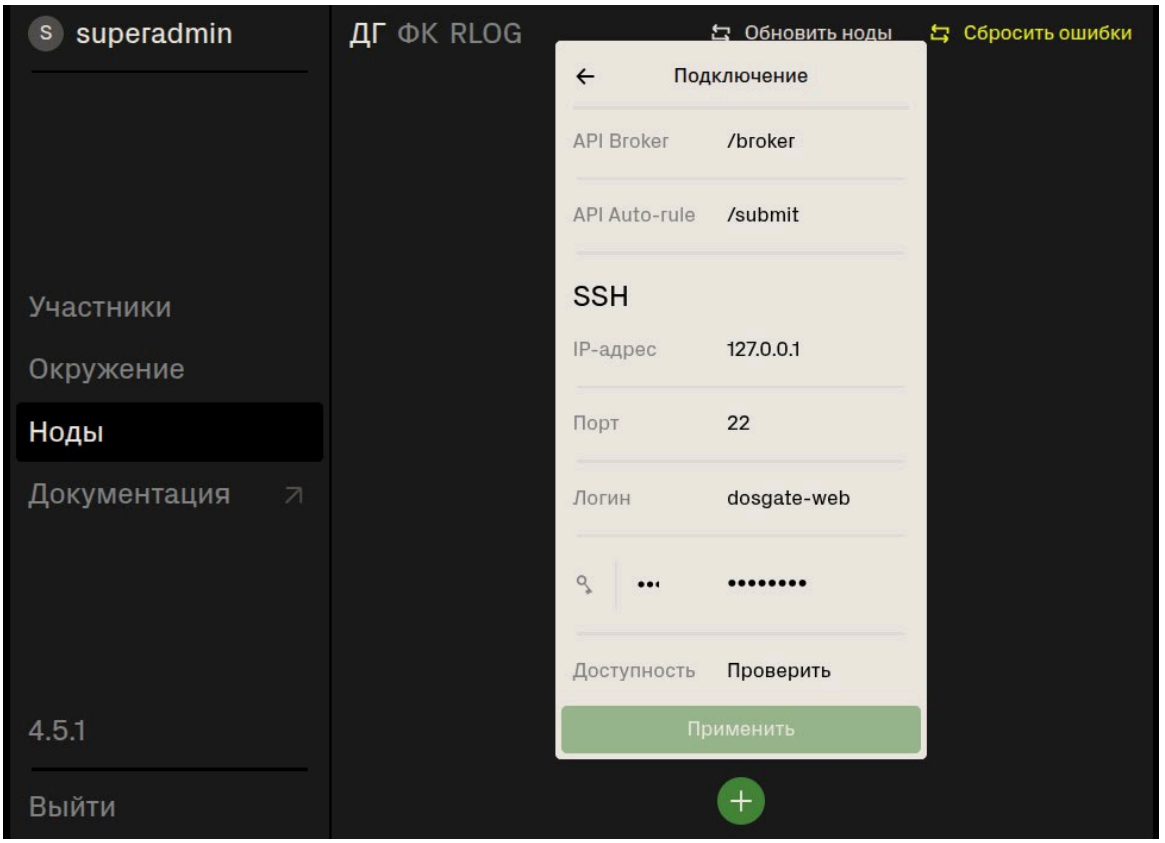
Нажать кнопнку "Настройки". Откроется окно настроек (см. рисунок ниже).



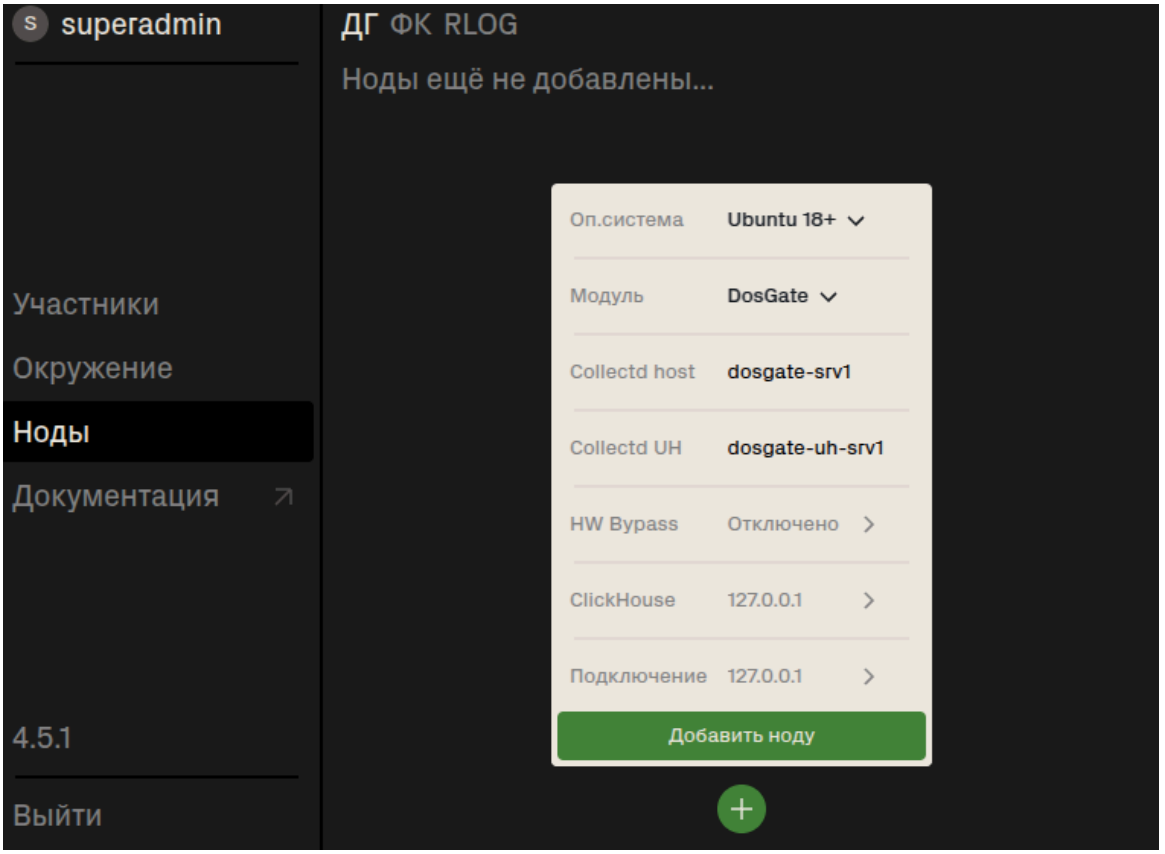
Выбрать меню "Ноды" - нажать на кнопку добавления новой ноды. В открывшимя окне необходимо заполнить "Collectd host". Необходимо использовать hostname, который прописан в конфигурационном файле dosgate.conf в блоке *collectd*. Нажать на кнопку "Подключение".



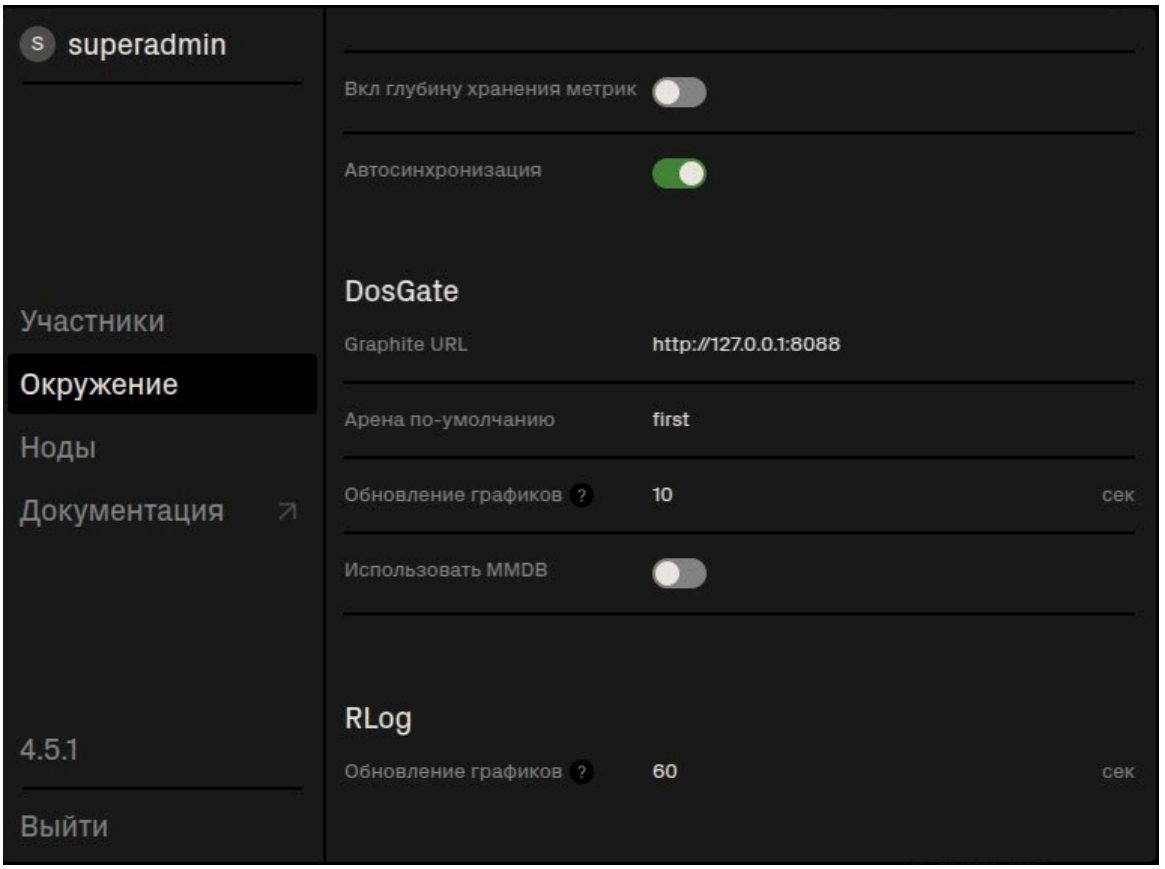
В открывшемся окне указать SSH-данные для подключения к установленной ноде Dosgate (IP-адрес, логин, пароль). Нажать на кнопку "Проверить", чтобы проверить подключение. Если данные введены правильно и нода доступна, статус изменится на "Доступна". После этого нажать кнопку "Применить".



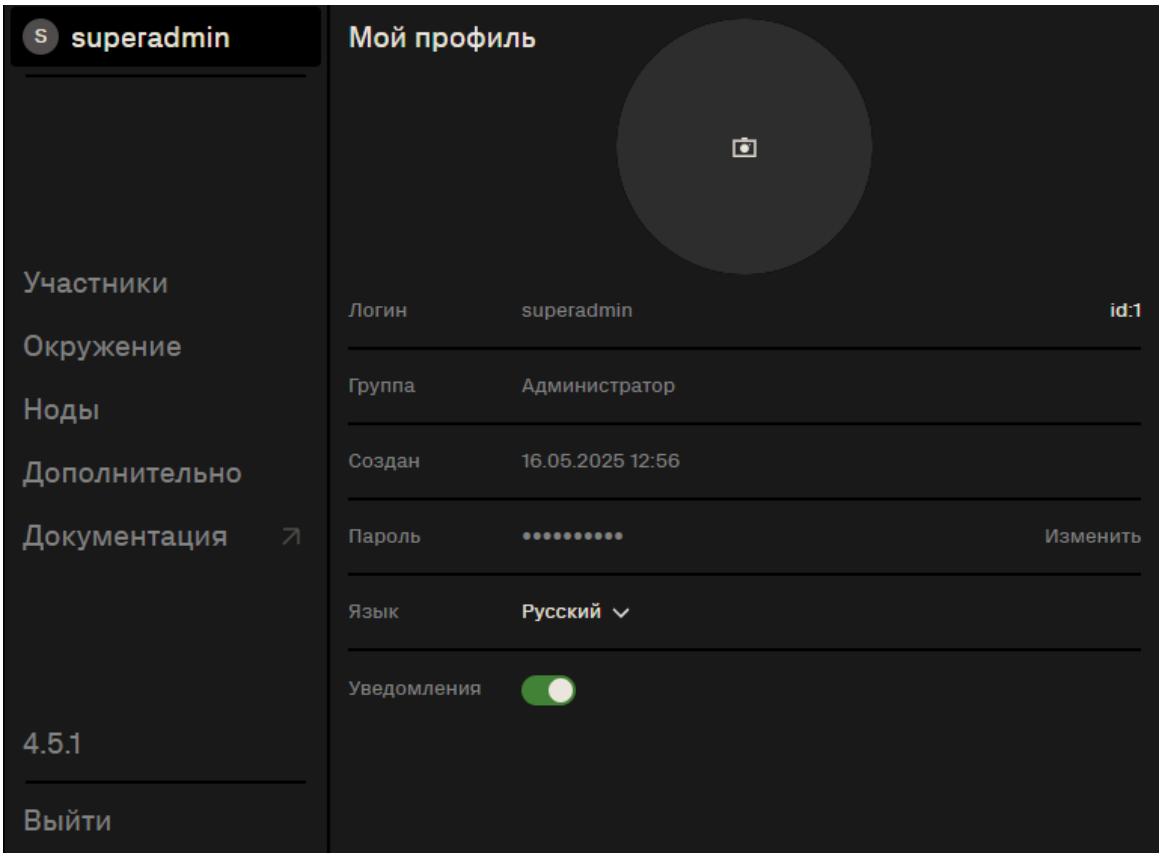
В открывшемся окне нажать "Добавить ноду".



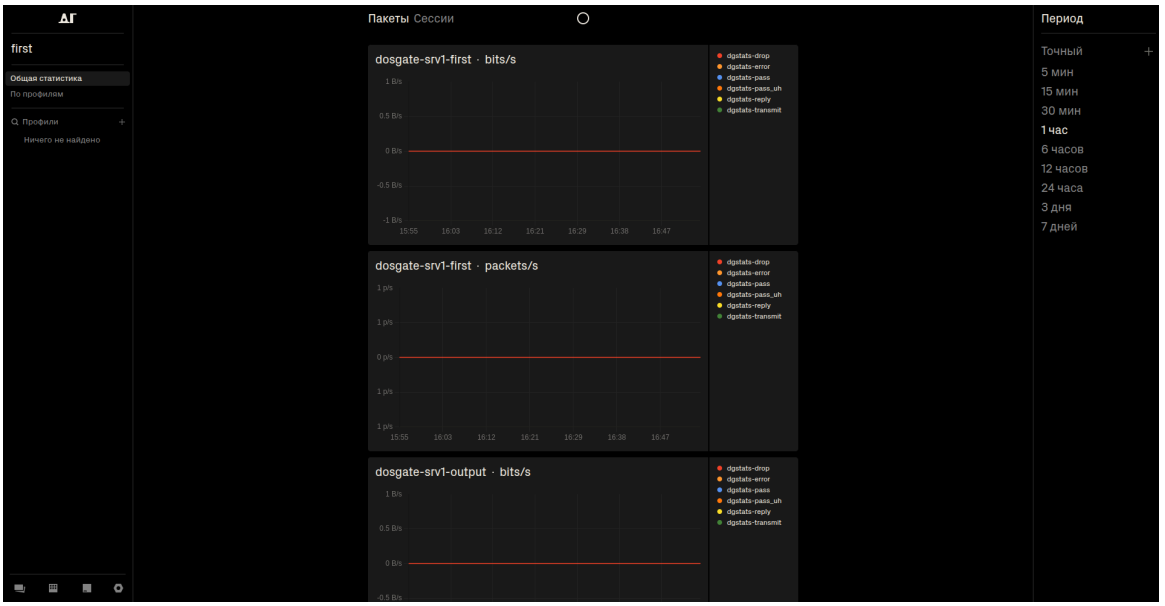
Для отображения графиков и статистики необходимо указать ссылку на Graphite. Перейдите в раздел "Окружение". В разделе DosGate указать "Graphite URL" и "Арена по-умолчанию". Название арены должно соответствовать значению, указанному в конфигурационном файле dosgate.conf для всех нод кластера.



Нажать на свой профиль в левом верхнем углу экрана, чтобы открыть настройки профиля. Установить новый пароль.



Веб-интерфейс готов к использованию.



Оптимизация производительности платформы

Скрипт оптимизации сетевой карты

Для улучшения производительности сетевых карт важно настроить их параметры таким образом, чтобы они могли работать с максимальной пропускной способностью и минимальными задержками. Включение агрессивной компрессии (CQE) и отключение расслабленного порядка PCI-операций помогает ускорить передачу данных и оптимизировать взаимодействие с памятью. Включение DevX увеличивает пропускную способность и снижает задержки.

Для оптимизации работы сетевой карты запустить следующий скрипт:

```
#!/bin/sh

# Enable aggressive CQE Zipping.
cqe_compression=1

# Disable relaxed ordering for PCI operations.
pci_wr_ordering=0

# Enable DevX.
uctx_en=1


devs=$(ls -d /sys/class/net/*/device/infiniband_verbs/uverbs* |
cut -d / -f 5)

for dev in $devs; do
    pci_addr=$(grep PCI_SLOT_NAME
/sys/class/net/$dev/device/uevent | tail -c +15)

    echo Device: $dev $pci_addr

    mstconfig -y -d $pci_addr s \
        CQE_COMPRESSION=$cqe_compression \
        PCI_WR_ORDERING=$pci_wr_ordering \
```

```
        UCTX_EN=$uctx_en

    # Switch link type to Ethernet if supported
    mstconfig -y -d $pci_addr s LINK_TYPE_P1=2
    mstconfig -y -d $pci_addr s LINK_TYPE_P2=2
done
```

Режим pass-through для IOMMU

Для оптимальной работы виртуализированных систем важно обеспечить прямой доступ к аппаратным ресурсам для виртуальных машин. Это возможно при включении режима pass-through для IOMMU. Такой подход значительно повышает производительность, поскольку исключает вмешательство гипервизора, что позволяет виртуальным машинам работать с максимально возможной пропускной способностью и низкими задержками.

- Открыть файл **/etc/default/grub**
- Найти строку

```
GRUB_CMDLINE_LINUX=""
```

и заменить на:

```
GRUB_CMDLINE_LINUX="iommu=pt"
```

- Обновить параметры загрузчика с помощью команды:

```
update-grub
```

Скрипты оптимизации для сетевых карт Mellanox

Для повышения производительности сетевых карт Mellanox важно оптимизировать распределение прерываний и настроить привязку их к процессорным ядрам NUMA. Это помогает улучшить балансировку нагрузки, снизить задержки и обеспечить правильную работу системы при высокой нагрузке. Отключение службы irqbalance важно, чтобы

избежать возможных конфликтов в распределении прерываний. Этот процесс помогает обеспечить стабильную работу и высокую производительность при использовании сетевых карт Mellanox в высоконагруженных системах.

- Загрузить архив скриптов оптимизации Mellanox
- Определить номера процессорных ядер для NUMA с помощью команды:

```
lscpu | grep "NUMA node"
```

- Остановить и отключить автозапуск сервиса *irqbalance*:

```
systemctl stop irqbalance.service && systemctl disable
irqbalance.service
```

- Запустить загруженный скрипт *set_irq_affinity_cpulist.sh* с указанием нужных номеров ядер NUMA и названия интерфейса. В качестве параметров указать номера ядер нужной NUMA, а так же название интерфейса. Пример команды: `/set_irq_affinity_cpulist.sh 0-19,40-59 enp216s0f0np0`

Режим максимальной производительности для CPU

Применение режима performance позволяет процессорам работать на максимальной тактовой частоте, что особенно важно при выполнении ресурсоемких операций. Установка этого режима помогает избежать потери производительности из-за энергосберегающих функций процессора, гарантируя, что система будет работать на максимуме своих вычислительных возможностей.

- Проверить текущий режим работы процессора командой:

```
cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
```

- Проверить доступные режимы работы процессора:

```
cat
/sys/devices/system/cpu/cpu0/cpufreq/scaling_available_governors
```

- Если среди доступных режимов есть `performance`, применить его командой:

```
echo performance | tee
/sys/devices/system/cpu/cpu*/cpufreq/scaling_governor
```

Установка и настройка драйверов для сетевых карт Silicom Bypass

1. Сборка драйвера ixgbe (версия 5.19.6)

Рекомендованное ядро:

- `6.5` для Ubuntu
- `6.1.67-un-def` для Альт СП

Необходимые пакеты:

- `image` и `kernel-headers-modules` соответствующей версии.
- Компилятор `gcc`.

Установка компилятора:

```
apt-get install gcc
```

Загрузка исходных файлов:

```
wget --http-user=[ваш логин] --http-password=[ваш пароль]
https://public-repo.svcp.io/PxGxBP_VSD40f.zip
```

Сборка и установка драйвера для Ubuntu:

```
unzip PxGxBP_VSD40f.zip
```

```
cd PxGxBP_VSD40f/Linux/Network_Drivers/PE210GxBPi9/ixgbe-5.19.6/
```

```
tar -xzvf ixgbe-5.19.6ms7.2.tar.gz
```

```
cd ixgbe-5.19.6ms7.2/src/
```

```
uname -r
```

```
sudo make -C /lib/modules/$(uname -r)/build M=$(pwd) modules
```

```
sudo make install
```

```
modprobe ixgbe
```

Сборка и установка драйвера для Альт СП:

```
unzip PxGxBP_VSD40f.zip
```

```
cd PxGxBP_VSD40f/Linux/Network_Drivers/PE210GxBPi9/ixgbe-5.19.6/
```

```
tar -xzvf ixgbe-5.19.6ms7.2.tar.gz
```

```
cd ixgbe-5.19.6ms7.2/src/
```

```
make KSRC=/usr/src/linux-6.1.67-un-def-alt0.c10f.1
```

```
make KSRC=/usr/src/linux-6.1.67-un-def-alt0.c10f.1 install
```

```
modprobe ixgbe
```

Проверка загрузки драйвера и версии:

```
lsmod | grep ixgbe
```

```
modinfo ixgbe
```

2. Сборка bypass-драйвера

Сборка и установка для Ubuntu:

```
cd ~/PxGxBP_VSD40f/Linux/Bypass/Libs/Kernel/
```

```
tar -xzvf bypass-9.0.8.tar.gz
```

```
cd bypass-9.0.8/lib
```

```
uname -r
```

```
make -C /lib/modules/$(uname -r)/build M=$(pwd) modules
```

```
sudo make -C /lib/modules/$(uname -r)/build M=$(pwd)
modules_install
```

```
sudo depmod -a
```

```
sudo modprobe bypass
```

Сборка и установка для Альт СП:

```
cd ~/PxGxBP_VSD40f/Linux/Bypass/Libs/Kernel/
```

```
tar -xzvf bypass-9.0.8.tar.gz
```

```
cd bypass-9.0.8/lib
```

```
make KSRC=/usr/src/linux-6.1.67-un-def-alt0.c10f.1
```

```
make KSRC=/usr/src/linux-6.1.67-un-def-alt0.c10f.1 install
```

```
modprobe bypass
```

Проверка загрузки драйвера и версии:

```
lsmod | grep bypass
```

```
modinfo bypass
```

3. Сборка и проверка утилиты bp_ctl

Сборка утилиты Ubuntu:

```
cd ~/PxGxBP_VSD40f/Linux/Bypass/BP_Control/
```

```
tar -xzvf bp_ctl-5.2.0.49.tar.gz
```

```
cd bp_ctl-5.2.0.49/
```

```
uname -r
```

```
make -C /lib/modules/$(uname -r)/build M=$(pwd) install
```

```
bpctl_start
```

Сборка утилиты для Альт СП:

```
cd ~/PxGxBP_VSD40f/Linux/Bypass/BP_Control/
```

```
tar -xzvf bp_ctl-5.2.0.49.tar.gz
```

```
cd bp_ctl-5.2.0.49/
```

```
make KSRC=/usr/src/linux-6.1.67-un-def-alt0.c10f.1 install
```

```
bpctl_start
```

Проверка работы на интерфейсе:

```
bpctl_util enp94s0f0 get_bypass_pwoff
```

При выключенном bypass ожидается следующий вывод:

```
The interface is in the Bypass mode at power off state.
```

4. Настройка автоматического запуска bpctl

Если в системе уже установлен DosGate, важно, чтобы XDP от DosGate применялся после инициализации bypass-драйвера и запуска утилиты bpctl.

Для этого создаем systemd-сервис:

```
nano /etc/systemd/system/bpctl_autostart.service
```

Добавляем содержимое:

```
[Unit]
Description=Bypass Service
After=network.target

[Service]
Type=oneshot
ExecStartPre=/bin/bash -c 'CHECK_BPCTL=$(bpctl_util info); if echo
$CHECK_BPCTL | grep -q "Bypass-SD"; then echo "bpctl is already
running"; exit 1; fi'
ExecStart=/bin/bpctl_start
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

Активируем сервис:

```
sudo systemctl daemon-reload
```

```
systemctl enable --now bpctl_autostart
```

```
systemctl status bpctl_autostart
```

Перезагрузить сервер и убедиться, что интерфейсы не отключаются при совместной работе DosGate и bpctl.

Проверка успешного запуска bpctl:

```
bpctl_util
```

Если утилита запустилась корректно, она выведет список доступных команд.

Проверка работы XDP на интерфейсах:

```
ip link | grep xdp
```

Если xdp присутствует на интерфейсах — DosGate запущен и работает корректно.

Изменение максимального размера XDP map

XDP map — это таблица «ключ–значение», к которой обращаются BPF-программы. В качестве ключа могут использоваться IP-адрес источника, параметры соединения (l3_proto — IPv4 или IPv6, l4_proto — TCP или UDP, адреса и порты источника и назначения) или любые другие идентификаторы, по которым ядро должно быстро находить запись. Значение XDP map содержит служебные данные: счётчики пакетов или байт, временные метки, флаги состояния или другие параметры, которые используют правила DosGate.

XDP maps применяются для хранения IP-адресов и соединений, поддержки счётчиков, а также для TCP-авторизации — в этом случае таблица фиксирует текущий шаг и состояние отправителя, чтобы на каждом пакете понимать, на каком этапе проверки находится отправитель.

XDP maps являются частью жизненного цикла объектов BPF и размещаются в файловой системе **bpffs** по пути:

```
/sys/fs/bpf
```

Для DosGate используется отдельное поддерево:

```
/sys/fs/bpf/dosgate
```

В системе доступны два уровня XDP maps. Глобальные карты едины для всей системы и находятся по пути:

```
/sys/fs/bpf/dosgate/base/maps
```

Локальные карты относятся к конкретной арене и размещаются здесь:

```
/sys/fs/bpf/dosgate/contexts/<name>/maps
```

Доступные для изменения XDP map

Используйте команду `dosgate -m` чтобы вывести общий список XDP map доступных к изменению в CLI.

Список XDP map

```
Map "daemon_stats_map", owned by daemon
    Description: Daemon Statistics
    Pin as: daemon_stats_map
    Type percpu_array (6), flags 0x0 ()
    Key size 4b, value size 16b
    Default max entries 6
    Features: BTF-, L2-
    Tunables: max entries-

Map "daemon_xsk_map", owned by daemon
    Description: AF_XDP redirect to upper half
    Pin as: daemon_xsk_map
    Type xskmap (17), flags 0x0 ()
    Key size 4b, value size 4b
    Default max entries 1000000
    Features: BTF-, L2-
    Tunables: max entries-

Map "daemon_log_entry_map", owned by daemon
    Description: Logging export ring buffer
    Pin as: not pinned
    Type ringbuf (27), flags 0x0 ()
    Key size 0b, value size 0b
    Default max entries 1048576
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 512, max 67108864
    Suffix unit: 1024

Map "daemon_log_map", owned by daemon
    Description: Logging export ring buffer collection
    Pin as: daemon_log_map
    Type array_of_maps (12), flags 0x0 ()
    Key size 4b, value size 4b
    Default max entries 0, effective 4
    Features: BTF-, L2+
    Tunables: max entries-
```

```
    L2 map: daemon_log_entry_map

Map "daemon_flow_index_map", owned by daemon
    Description: Logging export flow collector index
    Pin as: daemon_flow_index_map
    Type percpu_array (6), flags 0x0 ()
    Key size 4b, value size 144b
    Default max entries 65536
    Features: BTF-, L2-
    Tunables: max entries-

Map "daemon_flow_cache_map", owned by daemon
    Description: Logginig export flow collector cache
    Pin as: daemon_flow_cache_map
    Type hash (1), flags 0x0 ()
    Key size 136b, value size 24b
    Default max entries 0, effective 262148
    Features: BTF-, L2-
    Tunables: max entries-

Map "interfaces_map", owned by daemon
    Description: Interfaces
    Pin as: interfaces_map
    Type devmap (14), flags 0x0 ()
    Key size 4b, value size 4b
    Default max entries 100
    Features: BTF-, L2-
    Tunables: max entries-

Map "geoip_map", owned by daemon
    Description: GeoIP database
    Pin as: geoip_map
    Type lpm_trie (11), flags 0x1 (BPF_F_NO_PREALLOC)
    Key size 32b, value size 8b
    Default max entries 10000000
    Features: BTF-, L2-
    Tunables: max entries-

Map "ctx_map", owned by daemon
    Description: Context
    Pin as: ctx_map
    Type percpu_array (6), flags 0x0 ()
    Key size 4b, value size 3336b
    Default max entries 1
    Features: BTF-, L2-
    Tunables: max entries-

Map "prog_map", owned by arena
    Description: Program
    Pin as: prog_map
    Type prog_array (3), flags 0x0 ()
```

```
    Key size 4b, value size 4b
    Default max entries 1100
    Features: BTF-, L2-
    Tunables: max entries-

Map "tree_ipv4_map", owned by arena
    Description: IPv4 Router
    Pin as: tree_ipv4_map
    Type lpm_trie (11), flags 0x1 (BPF_F_NO_PREALLOC)
    Key size 8b, value size 8b
    Default max entries 1000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "tree_ipv6_map", owned by arena
    Description: IPv6 Router
    Pin as: tree_ipv6_map
    Type lpm_trie (11), flags 0x1 (BPF_F_NO_PREALLOC)
    Key size 24b, value size 8b
    Default max entries 1000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "stats_map", owned by arena
    Description: Statistics
    Pin as: stats_map
    Type percpu_array (6), flags 0x0 ()
    Key size 4b, value size 16b
    Default max entries 256012
    Features: BTF-, L2-
    Tunables: max entries-

Map "lock_map", owned by arena
    Description: Locking
    Pin as: lock_map
    Type array (2), flags 0x0 ()
    Key size 4b, value size 4b
    Default max entries 1048576
    Features: BTF+, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "hmark_inet_map", owned by arena
    Description: Host Mark IPv4
    Pin as: hmark_inet_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
```

```
    Key size 22b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "hmark_inet6_map", owned by arena
    Description: Host Mark IPv6
    Pin as: hmark_inet6_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 34b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "sdhmark_inet_map", owned by arena
    Description: Source-Destination Host Mark IPv4
    Pin as: sdhmark_inet_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 26b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "sdhmark_inet6_map", owned by arena
    Description: Source-Destination Host Mark IPv6
    Pin as: sdhmark_inet6_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 50b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "dmark_inet_map", owned by arena
    Description: Destination Host Mark IPv4
    Pin as: dmark_inet_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 22b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000
```

```
Map "dmark_inet6_map", owned by arena
    Description: Destination Host Mark IPv6
    Pin as: dmark_inet6_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 34b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "connmark_map", owned by arena
    Description: Connection Mark IPv4 and IPv6
    Pin as: connmark_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 124b, value size 16b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "ratelimit_map", owned by arena
    Description: RateLimit IPv4 and IPv6
    Pin as: ratelimit_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 124b, value size 32b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "sample_map", owned by arena
    Description: Sampling IPv4 and IPv6
    Pin as: sample_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 124b, value size 8b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "tcpauth_map", owned by arena
    Description: TCP Authentication temporary data
    Pin as: tcpauth_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 34b, value size 48b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
```

```
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "prefixset_map", owned by arena
    Description: Prefixset storage
    Pin as: prefixset_map
    Type lpm_trie (11), flags 0x1 (BPF_F_NO_PREALLOC)
    Key size 32b, value size 8b
    Default max entries 10000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "rate_map", owned by arena
    Description: Rate estimation data
    Pin as: rate_map
    Type lru_hash (9), flags 0x2 (BPF_F_NO_COMMON_LRU)
    Key size 124b, value size 104b
    Default max entries 1000000, effective 2000000
    Features: BTF-, L2-
    Tunables: max entries+
    Max entries min 100, max 100000000
    Suffix unit: 1000

Map "pstats_map", owned by passthrough
    Description: Passthrough statistics
    Pin as: pstats_map
    Type percpu_array (6), flags 0x0 ()
    Key size 4b, value size 16b
    Default max entries 6
    Features: BTF-, L2-
    Tunables: max entries-
```

Настройка размера XDP map

Перед изменением конфигурации необходимо остановить работу сервиса:

```
sudo service dosgate stop
```

Очистить данные во всех XDP map командой:

```
dgadm --clear=sa -y
```

Для изменения размера конкретной XDP map выполнить следующие шаги:

Определите размер ключа (`Key size`) и значение (`Value size`) в байтах для требуемой XDP map.

Установите новый максимальный размер XDP map (например: 2 000 000 записей для TCP-авторизации).

Рассчитайте требуемый объем оперативной памяти по формуле:

Объем памяти = `Key size` * Новый размер XDP map

> **Примечание**
> Если у XDP map `Key size` и `Value size` равны 0b, используйте обозначения K (килобайты), M (мегабайты), G (гигабайты).

- Изменение размера локальной XDP map

Откройте файл **/etc/dosgate.conf** и добавьте параметр maps с новым значением:

```
arenas:
  - name: first
    id: 1
    maps:
      hmark_inet_map: 50000000
```

- Изменение размера глобальной XDP map

```
daemon:
  maps:
    daemon_log_entry_map: 1M

arenas:
  - name: first
    id: 1
```

Запуск сервиса DosGate:

```
service dosgate start
```

Убедитесь, что сервис работает корректно и ошибки отсутствуют:

```
service dosgate status
```

Установка и настройка сессионной защиты

Назначение

Сессионная защита — функция платформы DosGate, предназначенная для stateful-обработки сетевого трафика. Она позволяет анализировать соединения на уровне сессий, выявлять аномалии и применять защитные меры до передачи трафика в прикладные сервисы.

Сессионная защита использует базу вредоносных сигнатур для автоматического выявления и блокировки аномального трафика.

Функциональность

- Поддержка: TCP, UDP, SCTP, ICMP, ICMPv6.
- Принудительный разрыв соединений (active-close) без генерации исходящего трафика и без терминирования внутри системы.
- Анализ этапов установки соединения (Handshake).
- Обработка и фильтрация Client-Hello и Server-Hello.
- Контроль TLS SNI (Server Name Indication) и TLS ALPN (Application-Layer Protocol Negotiation).
- Проверка списка поддерживаемых шифров (Cipher List).
- Проверка и валидация контрольных сумм.
- Обнаружение и обработка IP-фрагментации с функцией дефрагментации.
- Поиск JA3 и JA4-отпечатков для анализа шифрованного трафика.
- Поиск TLS Cipher Suites для анализа безопасности и совместимости.

Установка и ввод в эксплуатацию

Внимание! Перед установкой и запуском рекомендуется снять весь продуктивный трафик с платформы.

Настройка конфигурации сессионной защиты

Редактирование конфигурационного файла

Для редактирования конфигурационного файла выполнить команду:

```
nano /etc/dosgate-uh.conf
```

Глобальная конфигурация

Задать глобальные параметры политики обработки сетевого трафика:

```
global:
  traffic-policy:
    good: accept   # Разрешение корректного трафика
    bad: drop      # Отклонение подозрительного трафика
    violate: drop  # Отклонение нарушающего трафика
```

Конфигурация сетевых устройств

Для эффективного управления очередями приема и передачи пакетов настроить параметры сетевых интерфейсов:

```
net:
  ens224:
    rx:
      queues:
        count: 8  # Количество очередей приема
        len: 512  # Длина каждой очереди
  ens256:
    tx:
      queues:
```

```
        count: 8  # Количество очередей приема
        len: 512  # Длина каждой очереди
```

Настройки захвата трафика

Функция захвата трафика позволяет записывать сетевые пакеты в файлы для последующего анализа:

```
capture:
  path: /var/cache/dosgate-uh/capture      # Директория для
сохранения
  filename: cap_${DEV}_${ID}_${NUM}.pcap   # Шаблон имен файлов
  age: 3600                                # Максимальное время
хранения файла (в секундах)
  count: 10                                # Максимальное
количество файлов
  size: 10M                                # Максимальный размер
файла
```

Конфигурация сбора и экспорта статистики

Статистика помогает отслеживать состояние системы в реальном времени и экспортировать данные в систему мониторинга:

```
stats:
  period: 10                              # Период сбора статистики
(в секундах)
  push:
    type: collectd                        # Метод передачи данных
    plugin: unixsock                      # Используемый плагин
    target: /var/run/collectd-unixsock    # Целевой сокет
    stats: all                            # Объем передаваемых
данных
    hostname: dosgate-uh01                # Идентификатор хоста
    queue-len: 0                          # Длина очереди отправки
    period:
      collect: 5                          # Интервал сбора данных
(в секундах)
      send: 10                            # Интервал отправки
данных (в секундах)
```

Настройка отслеживания подключений

Параметры контроля соединений позволяют задавать ограничения и определять политику обработки трафика:

```
conntrack:
  limit: 10000000       # Максимальное количество отслеживаемых
соединений
  reclaim:
    soft: 80            # Порог мягкого освобождения соединений (в
% от лимита)
    hard: 95            # Порог жесткого освобождения соединений
(в % от лимита)
```

Путь к каталогу с реестром профиля приложения

По умолчанию: **/var/lib/dosgate-uh/profiles**

```
application:
  registry: /var/lib/dosgate-uh/profiles
  monitor-fs: true
```

Настройка экспорта фреймов

Обеспечение работы функции экспорта фреймов, которая выполняется в рамках действия dosgate action `-j EXPORT`:

```
frame-export:
  enabled: true         # Включение функции экспорта фреймов
  export-objects: all   # Экспорт всех объектов
```

Установка пакета

```
sudo apt-get update
sudo apt-get install dosgate-uh=1.3.0-1
```

Обработка статистики в collectd

Collectd — служба сбора и передачи метрик. Для передачи статистики сессионной защиты необходимо описание типов метрик и перезапустить службу *collectd*.

Создать файл описания типов метрик **/etc/collectd/dosgate-uh-types.db**:

```
sudo touch /etc/collectd/dosgate-uh-types.db
```

Добавить в файл описания метрик следующие определения:

```
xsk_rx_frames frames:COUNTER:0:U
xsk_rx_bytes bytes:COUNTER:0:U
xsk_tx_frames frames:COUNTER:0:U
xsk_tx_bytes bytes:COUNTER:0:U
xsk_rx_drop drop:COUNTER:0:U
xsk_tx_error error:COUNTER:0:U
xsk_frame_alloc bytes:COUNTER:0:U
xsk_frame_alloc_error bytes:COUNTER:0:U
xsk_frame_free bytes:COUNTER:0:U
xsk_partial_writes bytes:COUNTER:0:U
xsk_full_reads bytes:COUNTER:0:U
xsk_opterr bytes:COUNTER:0:U
xsk_fill_frames frames:COUNTER:0:U
xsk_comp_frames frames:COUNTER:0:U
xsk_kick_tx bytes:COUNTER:0:U
xsk_rounds bytes:COUNTER:0:U
xsk_poll bytes:COUNTER:0:U
xsk_poll_nb bytes:COUNTER:0:U
xsk_rx_inv_desc bytes:COUNTER:0:U
xsk_tx_inv_desc bytes:COUNTER:0:U
xsk_rx_ring_full bytes:COUNTER:0:U
xsk_fill_ring_empty bytes:COUNTER:0:U
cap_frames frames:COUNTER:0:U
cap_bytes bytes:COUNTER:0:U
cap_rotates bytes:COUNTER:0:U
cap_errors bytes:COUNTER:0:U
proc_frames frames:COUNTER:0:U
proc_bytes bytes:COUNTER:0:U
proc_dg_error bytes:COUNTER:0:U
proc_frame_error bytes:COUNTER:0:U
proc_frame_verify_error bytes:COUNTER:0:U
proc_frame_mod_error bytes:COUNTER:0:U
proto_buf_alloc bytes:COUNTER:0:U
proto_buf_alloc_error bytes:COUNTER:0:U
proto_buf_destroy bytes:COUNTER:0:U
proto_map_alloc bytes:COUNTER:0:U
proto_map_alloc_error bytes:COUNTER:0:U
proto_map_destroy bytes:COUNTER:0:U
```

```
proto_stack_alloc bytes:COUNTER:0:U
proto_stack_alloc_error bytes:COUNTER:0:U
proto_stack_destroy bytes:COUNTER:0:U
tcp_open bytes:COUNTER:0:U
tcp_close bytes:COUNTER:0:U
tcp_seq_late bytes:COUNTER:0:U
tcp_seq_early bytes:COUNTER:0:U
tcp_large_syn bytes:COUNTER:0:U
tcp_invalid_checksum bytes:COUNTER:0:U
stream_block_alloc bytes:COUNTER:0:U
stream_block_alloc_error bytes:COUNTER:0:U
stream_block_free bytes:COUNTER:0:U
stream_shard_alloc bytes:COUNTER:0:U
stream_shard_alloc_error bytes:COUNTER:0:U
stream_shard_free bytes:COUNTER:0:U
ct_allocated bytes:COUNTER:0:U
ct_destroyed bytes:COUNTER:0:U
ct_alloc_error bytes:COUNTER:0:U
ct_reclaim_soft bytes:COUNTER:0:U
ct_reclaim_soft_scanned bytes:COUNTER:0:U
ct_reclaim_soft_reclaimed bytes:COUNTER:0:U
ct_reclaim_hard bytes:COUNTER:0:U
ct_reclaim_hard_scanned bytes:COUNTER:0:U
ct_reclaim_hard_reclaimed bytes:COUNTER:0:U
ct_collsisions bytes:COUNTER:0:U
ct_collision_reclaimed bytes:COUNTER:0:U
ct_collision_errors bytes:COUNTER:0:U
ct_overlimit bytes:COUNTER:0:U
ct_closed bytes:COUNTER:0:U
ct_timeout bytes:COUNTER:0:U
ct_frames_status_good bytes:COUNTER:0:U
ct_frames_status_bad bytes:COUNTER:0:U
ct_frames_status_violate bytes:COUNTER:0:U
ct_frames_error bytes:COUNTER:0:U
ct_frames_invalid bytes:COUNTER:0:U
tls_create bytes:COUNTER:0:U
tls_free bytes:COUNTER:0:U
tls_records bytes:COUNTER:0:U
tls_handshake bytes:COUNTER:0:U
tls_appdata bytes:COUNTER:0:U
tls_version_error bytes:COUNTER:0:U
tls_length_error bytes:COUNTER:0:U
tls_content_error bytes:COUNTER:0:U
tls_version_missmatch_error bytes:COUNTER:0:U
tls_system_error bytes:COUNTER:0:U
dtls_create bytes:COUNTER:0:U
dtls_free bytes:COUNTER:0:U
dtls_records bytes:COUNTER:0:U
dtls_handshake bytes:COUNTER:0:U
dtls_appdata bytes:COUNTER:0:U
dtls_tls12_cid bytes:COUNTER:0:U
```

```
dtls_tls13_uh bytes:COUNTER:0:U
dtls_version_error bytes:COUNTER:0:U
dtls_length_error bytes:COUNTER:0:U
dtls_content_error bytes:COUNTER:0:U
dtls_system_error bytes:COUNTER:0:U
dtls_epoch_error bytes:COUNTER:0:U
dtls_seq_error bytes:COUNTER:0:U
mem_pbuf_alloc bytes:COUNTER:0:U
mem_pbuf_alloc_error bytes:COUNTER:0:U
mem_pbuf_free bytes:COUNTER:0:U
mem_pbuf_data_alloc bytes:COUNTER:0:U
mem_pbuf_data_alloc_error bytes:COUNTER:0:U
mem_pbuf_data_free bytes:COUNTER:0:U
mem_seg_alloc bytes:COUNTER:0:U
mem_seg_alloc_error bytes:COUNTER:0:U
mem_seg_free bytes:COUNTER:0:U
mem_hash_alloc bytes:COUNTER:0:U
mem_hash_alloc_error bytes:COUNTER:0:U
mem_hash_free bytes:COUNTER:0:U
offenders_alloc bytes:COUNTER:0:U
offenders_alloc_error bytes:COUNTER:0:U
offenders_destroy bytes:COUNTER:0:U
offenders_first bytes:COUNTER:0:U
offenders_known bytes:COUNTER:0:U
offenders_error bytes:COUNTER:0:U
offenders_reg_error bytes:COUNTER:0:U
offenders_queued bytes:COUNTER:0:U
offenders_queue_overflow bytes:COUNTER:0:U
offenders_lost bytes:COUNTER:0:U
offenders_exported bytes:COUNTER:0:U
offenders_handler_miss bytes:COUNTER:0:U
offenders_handler_expired bytes:COUNTER:0:U
offenders_handler_send bytes:COUNTER:0:U
offenders_handler_send_error bytes:COUNTER:0:U
offenders_child_restart_request bytes:COUNTER:0:U
offenders_child_restart bytes:COUNTER:0:U
push_msg_alloc bytes:COUNTER:0:U
push_msg_alloc_error bytes:COUNTER:0:U
push_msg_free bytes:COUNTER:0:U
push_created bytes:COUNTER:0:U
push_create_error bytes:COUNTER:0:U
push_started bytes:COUNTER:0:U
push_socket_error bytes:COUNTER:0:U
push_config_error bytes:COUNTER:0:U
push_connect_start bytes:COUNTER:0:U
push_connect_error bytes:COUNTER:0:U
push_connect_timeout bytes:COUNTER:0:U
push_connect_success bytes:COUNTER:0:U
push_timeout bytes:COUNTER:0:U
push_send_error bytes:COUNTER:0:U
push_send_msgs bytes:COUNTER:0:U
```

```
push_enqueued bytes:COUNTER:0:U
push_enqueue_error bytes:COUNTER:0:U
push_rounds bytes:COUNTER:0:U
push_rounds_empty bytes:COUNTER:0:U
defrag_in bytes:COUNTER:0:U
defrag_valid bytes:COUNTER:0:U
defrag_dup bytes:COUNTER:0:U
defrag_invalid bytes:COUNTER:0:U
defrag_out bytes:COUNTER:0:U
defrag_reclaim_soft bytes:COUNTER:0:U
defrag_reclaim_hard bytes:COUNTER:0:U
defrag_scan_confirmed bytes:COUNTER:0:U
defrag_scan_new bytes:COUNTER:0:U
defrag_reclaim_new bytes:COUNTER:0:U
defrag_confirm_new bytes:COUNTER:0:U
defrag_full bytes:COUNTER:0:U
defrag_error bytes:COUNTER:0:U
defrag_frag_alloc bytes:COUNTER:0:U
defrag_frag_alloc_error bytes:COUNTER:0:U
defrag_frag_free bytes:COUNTER:0:U
defrag_entry_alloc bytes:COUNTER:0:U
defrag_entry_alloc_error bytes:COUNTER:0:U
defrag_entry_free bytes:COUNTER:0:U
defrag_key_error bytes:COUNTER:0:U
defrag_key_id_error bytes:COUNTER:0:U
```

Открыть конфигурационный файл службы *collectd*:

```
sudo nano /etc/collectd/collectd.conf
```

Добавить ссылку на файл с типами метрик:

```
TypesDB "/etc/collectd/dosgate-uh-types.db"
```

Перезапустить службу *collectd*, чтобы применить изменения:

```
sudo systemctl restart collectd
```

Запуск службы сессионной защиты

Сессионная защита реализуется службой *dosgate-uh*. Для управления службой выполните следующие команды:

Запустить службу:

```
sudo systemctl start dosgate-uh
```

Проверить статус службы:

```
sudo systemctl status dosgate-uh
```

Включить автозапуск службы:

```
sudo systemctl enable dosgate-uh
```

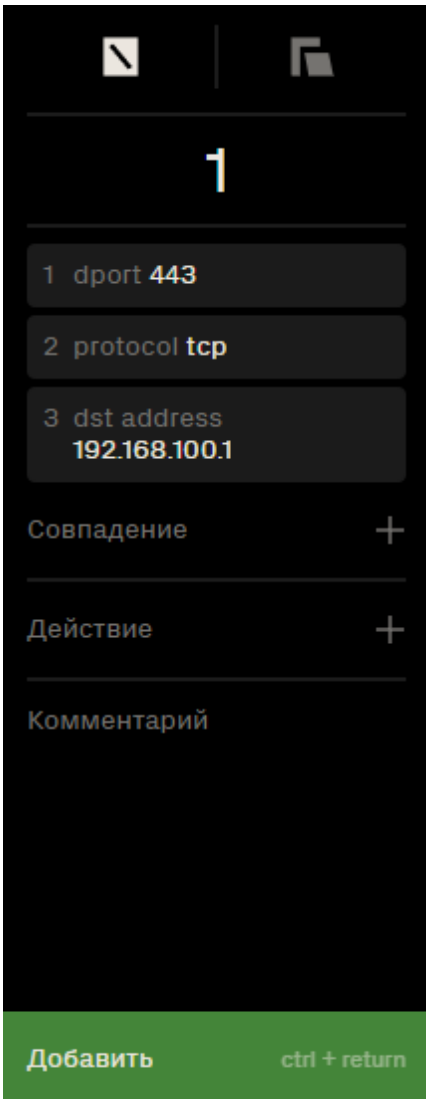
Направление трафика в сессионную защиту

Для передачи сетевого трафика на обработку в сессионную защиту необходимо создать правило фильтрации.

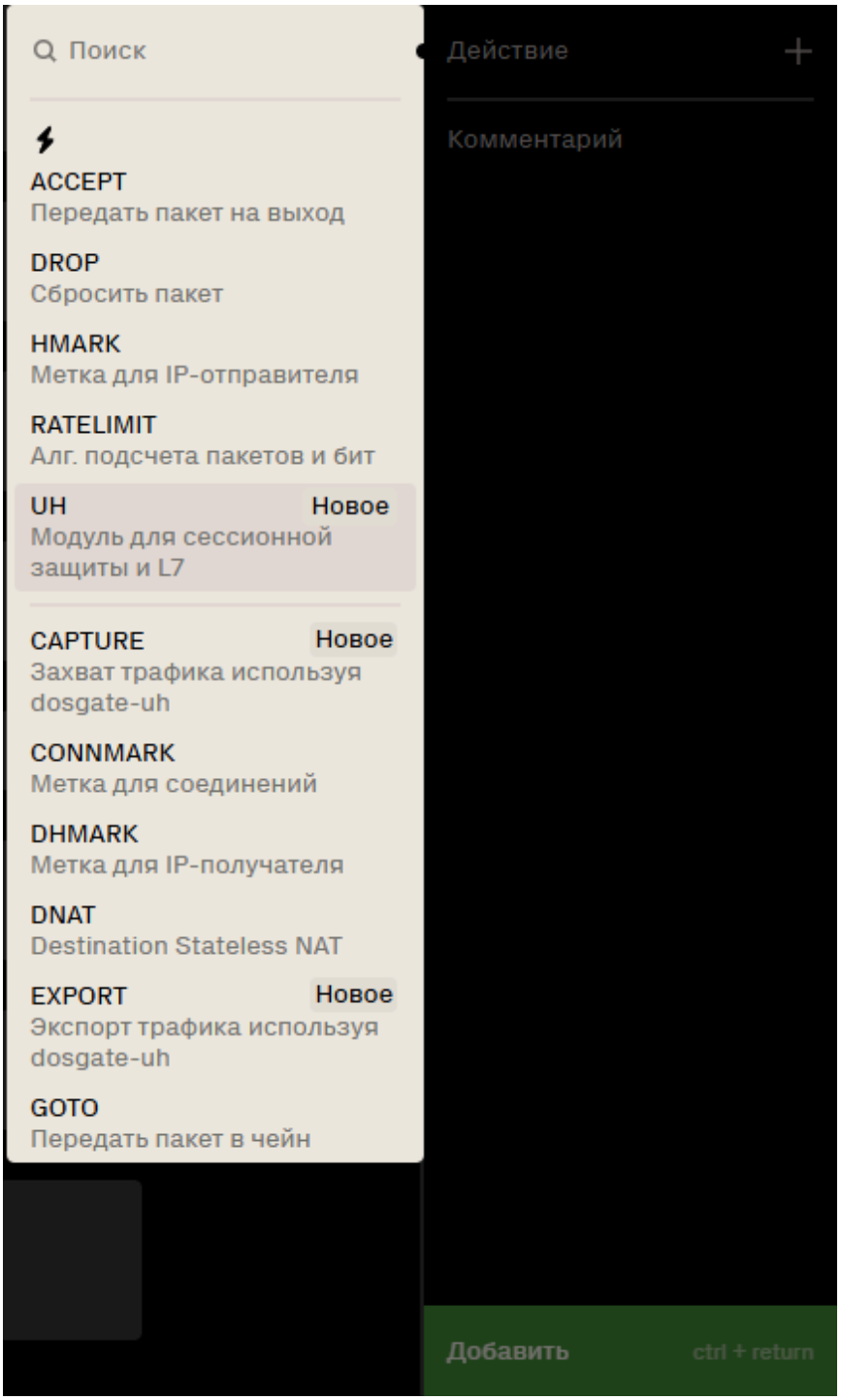
Настройка правила через веб-интерфейс

1. Открыть нужный профиль в DosGate.
2. Создать новое правило:

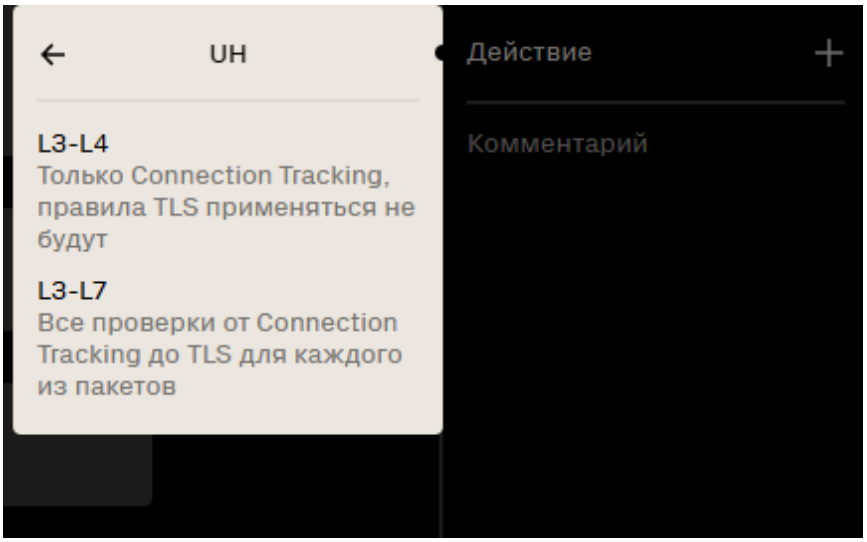
- В поле "Совпадение" указать условия, по которым будет фильтроваться трафик (например, IP-адреса, порты, протоколы):



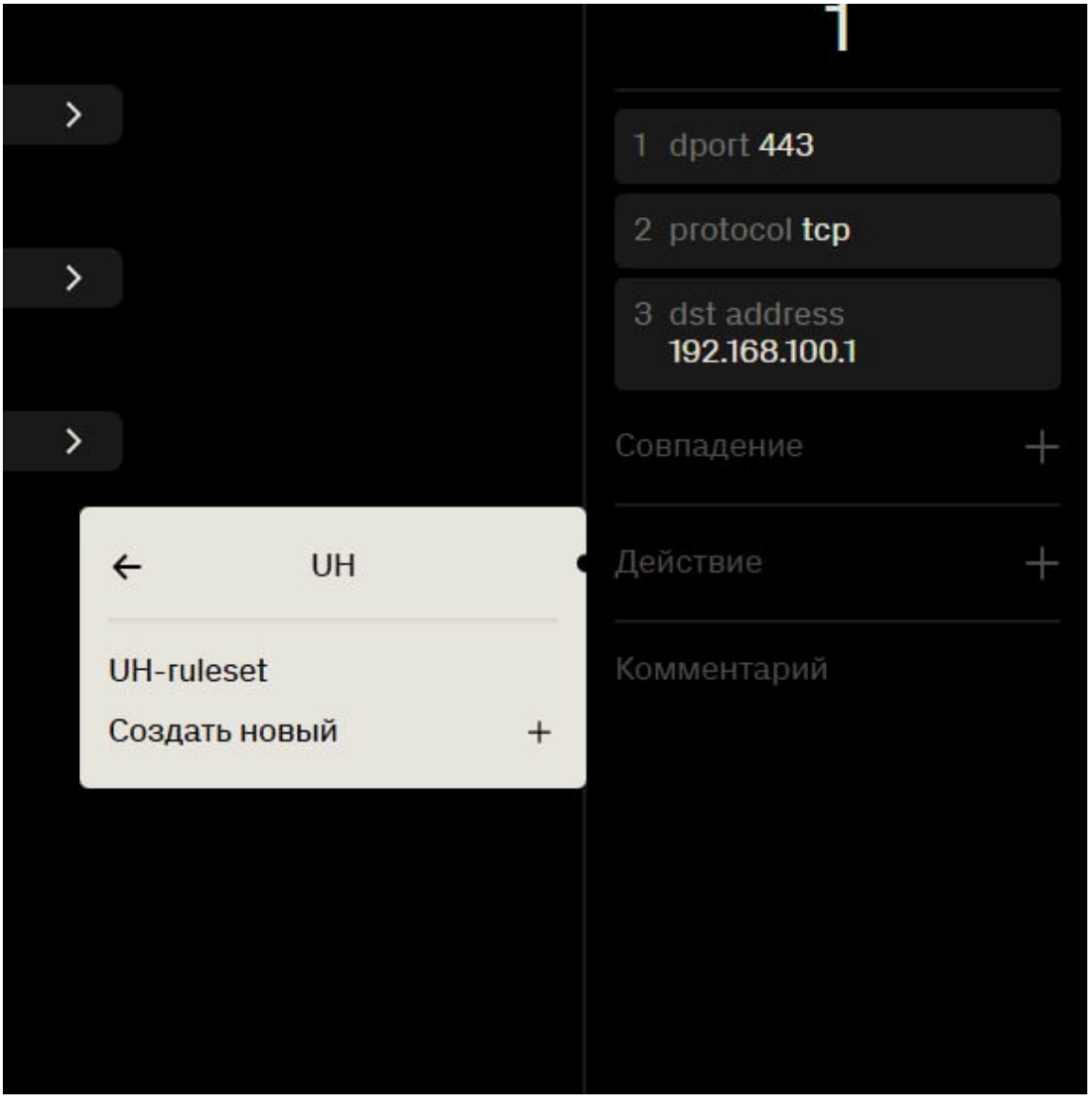
- В поле "Действие" выбрать "UH". Это действие направляет трафик на обработку в сессионную защиту.



- Выбрать вариант обработки трафика:



- Выбрать существующий UH или создать новый:



Примечание: подробнее о первичной настройке UH можно узнать в Руководстве пользователя

- При необходимости оставить комментарий к правилу и нажать зеленую кнопку **Добавить**.

Нажать **Применить**, чтобы правило вступило в силу. После этого трафик будет направляться в сессионную защиту.

Настройка правила через CLI

Для добавления правила выполнить следующую команду:

```
dgctl -u profile://<arena-name>/<profile-name> -c insert -- -m
protocol tcp -m dst 192.168.100.1 -m dport 443 -j PASS uh app tls
1
```

Параметры команды:

- `<arena-name>` — имя арены в соответствии с файлом конфигурации `/etc/dosgate.conf`
- `<profile-name>` — имя профиля, используемого для обработки трафика
- `-m protocol tcp` — *(опционально)* указание протокола. По умолчанию можно направлять весь трафик
- `-m dst 192.168.100.1` — *(опционально)* фильтрация по IP-адресу получателя
- `-m dport 443` — *(опционально)* фильтрация по целевому порту
- `-j PASS` — действие, разрешающее передачу трафика на обработку в сессионную защиту
- `uh app tls` — параметры, указывающие на применение профиля `tls` для обработки
- `1` - ID политики приложения в файле policy

При необходимости направить весь трафик без дополнительных условий, создать правило без параметров `-m`:

```
dgctl -u profile://<arena-name>/<profile-name> -c insert -- -j
PASS uh app tls 1
```

Диагностика и устранение проблем при запуске сессионной защиты

Работа службы сессионной защиты *dosgate-uh* зависит от сетевого драйвера и версии ядра операционной системы. При возникновении проблем рекомендуется выполнить предварительные диагностические шаги и проверки, описанные ниже.

Предварительные действия перед внесением изменений

Перед выполнением изменений рекомендуется выполнить следующие шаги, чтобы избежать сбоев в работе:

1. **Перенаправление продуктивного трафика**
   Перед внесением изменений убедиться, что трафик направляется в обход DosGate.
2. **Остановка служб**
   Полностью остановить работающие службы *dosgate* и *dosgate-uh*:

   ```
   sudo systemctl stop dosgate
   sudo systemctl stop dosgate-uh
   ```

3. **Отключение XDP-программ**
   Для всех задействованных интерфейсов отключить XDP-программы:

```
sudo ip link set dev <interface_name> xdp off
```

где `<interface_name>` — имя сетевого интерфейса.

Действия перед запуском после внесения изменений

После выполнения настроек очистить кэш и подготовить систему к запуску:

```
rm -rf /sys/fs/bpf/dosgate
```

```
dgadm --batch=uh -y
```

Отключение zero-copy для службы dosgate-uh

В случае возникновения проблем с обработкой трафика попробуйте отключить режим zero-copy в файле конфигурации **/etc/dosgate-uh.conf**:

```
net:
  enp59s0f0:
    nozc: 1
  tx:
    ....
```

При отключении zero-copy рекомендуется активировать функцию **Оффендеры**.
Она позволяет блокировать IP-адреса вредоносных ботов на уровне *dosgate*, снижая нагрузку на службу *dosgate-uh*, особенно при использовании ресурсоемких алгоритмов. Следует учитывать, что отключение zero-copy **снижает производительность службы dosgate-uh примерно в 2,1 раза.**

Перевод DosGate в generic-режим

Этот режим обладает сниженной производительностью, но может обеспечить корректную работу в средах, где использование XDP невозможно или нестабильно. Для изменения режима открыть конфигурационный файл **/etc/dosgate.conf** и задать параметр:

```
daemon:
    xdp-mode: generic
```

После изменения конфигурации перезапустить службу *dosgate*:

```
sudo systemctl restart dosgate
```

Связанные разделы

Сессионная защита

Установка модуля DosGate Autopilot

Ключевые требования

Для работы модуля **DosGate Autopilot** требуется:

1. Установленная и настроенная сессионная защита.
2. Версия веб-интерфейса **sp-spider** не ниже **4.4**.
3. Версия **sp-spider-broker** не ниже **1.0.16**.

Настройка сессионной защиты

Открыть для редактирования конфигурационный файл:

```
sudo nano /etc/dosgate-uh.conf
```

В конце конфигурационного файла активировать опцию *frame export*:

```
frame-export:
  enabled: true
  export-objects: all
```

Сохранить изменения и перезапустить службу:

```
sudo systemctl restart dosgate-uh
```

Установка Autopilot

Установить пакет:

```
sudo apt-get install auto-rule
```

Открыть для редактирования файл окружения:

```
sudo nano /opt/auto-rule/.env
```

Указать следующие параметры:

```
HOST=127.0.0.1                # IP-адрес, на котором будет слушать сервис
PORT=3336                     # Порт для входящих соединений
RESPONSE_IP=127.0.0.1         # IP-адрес sp-spider
RESPONSE_PORT=3333            # Порт sp-spider
BEARER_TOKEN=YOUR_TOKEN_HERE # API-токен из интерфейса sp-spider: Настройки → Окружение → API-токен
UNSECURE=true                 # Отключение проверки SSL-сертификата
DEBUG=false                   # Уровень логирования
LIC_KEY=                      # Лицензионный ключ, предоставленный вендором
MANUAL=true                   # Режим активации лицензии (только ручной)
```

Скопировать лицензионный файл с расширением .lic в директорию **/opt/auto-rule/**. Лицензионный файл предоставляется вендором.

Перезапустить службу:

```
sudo systemctl restart auto_rule.service
```

Убедиться в успешной инициализации службы и её запуске без ошибок:

```
sudo systemctl status auto_rule.service
```

При корректной инициализации отображается сообщение с датой окончания лицензии и адресом `ip:port`, на котором запущен сервис.

```
Started Auto Rule Server.
INFO - Лицензия действительна до: YYYY-MM-DD HH:MM:SS
INFO - Сервер запущен на 127.0.0.1:3336
```

Настройка nginx

Для корректной работы необходимо добавить директиву `location` в конфигурационный файл **nginx** для приема входящих запросов от **sp-spider**.

Открыть конфигурационный файл nginx:

```
sudo nano /etc/nginx/sites-available/dosgate.conf
```

Добавить в конфигурацию следующую директиву:

```
location /submit {
  proxy_pass http://localhost:3336/submit;
  proxy_http_version 1.1;
  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;
  proxy_set_header X-Forwarded-Proto $scheme;
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_cache_bypass $http_upgrade;
}
```

Перезапустить службу nginx:

```
sudo systemctl restart nginx
```

Убедиться в корректной работе службы:

```
sudo systemctl status nginx
```

После успешной установки, в интерфейсе становится доступна функция **Автогенерация правил**. Подробное описание функциональности и механизма работы доступно в разделе DosGate Autopilot

Установка модуля RLOG

Ключевые требования

Для работы модуля **RLOG** требуется:

1. **ClickHouse**. Используется в качестве хранилища для системных метрик, собираемых в процессе обработки логов.
2. **Carbon-clickhouse**. Служит для отправки метрик, формируемых модулем, в ClickHouse в формате Graphite.
3. **Веб-интерфейс Spider** версии **4.4** или выше
4. **Компонент Broker** версии **1.0.16** или выше
5. **TLS-сертификат и ключ**. Обязательны при использовании режима *tcptls* для обеспечения защищённого соединения.

Установка модуля

Установить пакет:

```
sudo apt-get install rlog
```

Открыть для редактирования файл окружения:

```
sudo nano /opt/rlog/.env
```

Указать следующие параметры:

```
## Основные параметры
PROTOCOL=tcp                          # Протокол (tcp|udp|tcptls)
HOST=0.0.0.0                          # Хост для приема сообщений
PORT=514                              # Порт приема сообщений
HTTP_PORT=3003                        # HTTP-порт веб-интерфейса
CERT_FILE=./cert/server.crt           # Путь к TLS-сертификату
KEY_FILE=./cert/server.key            # Путь к TLS-ключу
SPIDER_URL=http://localhost:3000      # URL интерфейса Spider
BROKER_URL=http://localhost:8081      # URL интерфейса Broker
```

```
APP_SECRET=YOUR_APP_SECRET              # Ключ приложения из
интерфейса .env
RULES_FOLDER=/var/lib/rlog/rules/       # Путь до правил обработки
syslog-сообщений ("/" обязателен)

## Параметры дампов
DUMP_FOLDER=./dumps/                    # Директория для хранения
дампов
DUMP_MAX_LOGS_IN_FILE=10000             # Максимальное число логов
в одном дамп-файле
DUMP_MAX_LOGS_BUFFER_SIZE=5000          # Размер буфера логов перед
сбросом в дамп

## Параметры метрик
HOSTNAME=rlog                           # Имя хоста в системе
метрик
METRICS_EXPORT_INTERVAL=1               # Интервал отправки метрик
(секунды)
METRICS_EXPORT_THRESHOLD=10             # Порог для отправки метрик
CLICKHOUSE_PORT=9000                    # Порт ClickHouse
CLICKHOUSE_HOST=10.25.78.48             # Хост ClickHouse
CLICKHOUSE_DATABASE=default             # Имя базы данных
CLICKHOUSE_USER=default                 # Пользователь ClickHouse
CLICKHOUSE_PASSWORD=                    # Пароль
CARBON_CLICKHOUSE_API=10.25.78.48:2003 # Адрес API carbon-
clickhouse

## Профилирование
PROFILING=false                         # Включение профилировщика
```

Для включения определения геолокации IP-адресов источников запросов требуется файл базы данных MaxMind в формате .mmdb. В файл окружения необходимо добавить следующую строку:

```
MMDB_PATH=./GeoLite2-Country.mmdb       # Путь к mmdb-файлу
```

Обновление на Ubuntu 22.04

При обновлении возможны перебои в обработке трафика. Рекомендуется перенаправить трафик с DosGate перед обновлением.

В случае неудачного обновления возможно восстановление предыдущей версии.

Инструкция по обновлению

1. Остановить маршрутизацию трафика через DosGate.

Например, при использовании BGP и bird выполнить команду:

```
sudo systemctl stop bird bird6
```

2. Остановить DosGate.

```
sudo systemctl stop dosgate
```

3. Сохранить текущее состояние.

```
tar czf dosgate-state.tar.gz /var/lib/dosgate
```

4. Подготовить систему к обновлению. Дополнительные параметры ключа dgadm предоставляет вендор при передаче обновления.

```
dgadm --batch=uh -y
```

5. Установить обновления.

Установить переданные вендором пакеты:

```
dpkg -i dosgate_<new_ver>_amd64.deb [additional packages if
```

```
required]
```

6. Обновить конфигурацию dosgate.service. Открыть для редактировани файл dosgate.service:

```
sudo nano /lib/systemd/system/dosgate.service
```

В строке:

```
ExecStart=dosgate -f
```

Заменить на:

```
ExecStart=dosgate -f -l crit
```

7. Запустить Dosgate в однократном режиме для проверки ошибок.

```
dosgate -o -l err
```

8. Запустить Dosgate.

```
sudo systemctl start dosgate
```

9. Проверить статус Dosgate.

```
sudo systemctl status dosgate
```

10. Восстановить маршрутизацию трафика через Dosgate.

Например, при использовании BGP и bird выполнить команду:

```
sudo systemctl start bird bird6
```

Если работа сервиса нарушена или изменилась конфигурация сервера, выполните следующие команды и перезапустите сервис:

```
rm -rf /sys/fs/bpf/dosgate
```

```
ip link set dev **интерфейс_dosgate** xdp off
```

Откат к предыдущей версии

1. Остановить маршрутизацию трафика через DosGate.

Например, при использовании BGP и bird выполнить команду:

```
sudo systemctl stop bird bird6
```

2. Остановить Dosgate.

```
sudo systemctl stop dosgate
```

3. Подготовить систему к откату.

```
dgadm --batch=uh -y
```

4. Установить предыдущую версию пакетов.

```
dpkg –force-all -i dosgate_<old_ver> [old versions of additional
packages if required]
```

5. Восстановить сохраненное состояние.

```
rm -rf /var/lib/dosgate
```

```
tar xzf dosgate-state.tar.gz -C /
```

6. Обновить конфигурацию dosgate.service. Открыть для редактировани файл dosgate.service:

```
sudo nano /lib/systemd/system/dosgate.service
```

В строке:

```
ExecStart=dosgate -f
```

Заменить на:

```
ExecStart=dosgate -f -l crit
```

7. Запустить DosGate в однократном режиме для проверки ошибок.

```
dosgate -o -l err
```

8. Запустить DosGate.

```
sudo systemctl start dosgate
```

9. Проверить статус DosGate.

```
sudo systemctl status dosgate
```

Обновление на Альт 8 СП

При обновлении возможны перебои в обработке трафика. Рекомендуется перенаправить трафик с DosGate перед обновлением.

В случае неудачного обновления возможно восстановление предыдущей версии.

Инструкция по обновлению

Все команды CLI в данной инструкции следует выполнять от имени суперпользователя, используя команду `su -c`, или `sudo` если он установлен и настроен.

1. Остановить маршрутизацию трафика через DosGate.

Например, при использовании BGP и bird выполнить команду:

```
systemctl stop bird bird6
```

2. Остановить DosGate.

```
systemctl stop dosgate
```

3. Сохранить текущее состояние.

```
dgadm --backup='dgbackup_$(date +"%FT%H%M")'
```

4. Подготовить систему к обновлению. Дополнительные параметры ключа dgadm предоставляет вендор при передаче обновления.

```
dgadm --batch=uh -y
```

```
ip link set dev **интерфейс_dosgate** xdp off
```

```
rm -rf /sys/fs/bpf/dosgate
```

5. Установить обновления.

Установить переданные вендором пакеты:

```
apt-get install dosgate=<version>
```

6. Обновить конфигурацию dosgate.service. Открыть для редактировани файл dosgate.service:

```
nano /usr/lib/systemd/system/dosgate.service
```

В строке:

```
ExecStart=dosgate -f
```

Заменить на:

```
ExecStart=dosgate -f -l crit
```

7. Запустить Dosgate в однократном режиме для проверки ошибок.

```
dosgate -o -l err
```

8. Запустить Dosgate.

```
systemctl start dosgate
```

9. Проверить статус Dosgate.

```
systemctl status dosgate
```

10. Восстановить маршрутизацию трафика через Dosgate.

Например, при использовании BGP и bird выполнить команду:

```
systemctl start bird bird6
```

Откат к предыдущей версии

1. Остановить маршрутизацию трафика через DosGate.

Например, при использовании BGP и bird выполнить команду:

```
systemctl stop bird bird6
```

2. Остановить Dosgate.

```
systemctl stop dosgate
```

3. Подготовить систему к откату.

```
dgadm --batch=uh -y
```

```
ip link set dev **интерфейс_dosgate** xdp off
```

```
rm -rf /sys/fs/bpf/dosgate
```

4. Установить предыдущую версию пакетов.

```
apt-get install dosgate=<old version>
```

5. Восстановить сохраненное состояние.

```
dgadm --restore=dgbackupname
```

6. Обновить конфигурацию dosgate.service. Открыть для редактировани файл dosgate.service:

```
nano /lib/systemd/system/dosgate.service
```

В строке:

```
ExecStart=dosgate -f
```

Заменить на:

```
ExecStart=dosgate -f -l crit
```

7. Запустить DosGate в однократном режиме для проверки ошибок.

```
dosgate -o -l err
```

8. Запустить DosGate.

```
systemctl start dosgate
```

9. Проверить статус DosGate.

```
systemctl status dosgate
```

Обновление на РЕД ОС 7.3

При обновлении возможны перебои в обработке трафика. Рекомендуется перенаправить трафик с DosGate перед обновлением.

В случае неудачного обновления возможно восстановление предыдущей версии.

Инструкция по обновлению

Все команды CLI в данной инструкции следует выполнять от имени суперпользователя, используя команду `su -c`, или `sudo` если он установлен и настроен.

1. Остановить маршрутизацию трафика через DosGate.

Например, при использовании BGP и bird выполнить команду:

```
systemctl stop bird bird6
```

2. Остановить DosGate.

```
systemctl stop dosgate
```

3. Сохранить текущее состояние.

```
dgadm --backup='dgbackup_$(date +"%FT%H%M")'
```

4. Подготовить систему к обновлению. Дополнительные параметры ключа dgadm предоставляет вендор при передаче обновления.

```
dgadm --batch=uh -y
```

```
ip link set dev **интерфейс_dosgate** xdp off
```

```
rm -rf /sys/fs/bpf/dosgate
```

5. Установить обновления.

Установить переданные вендором пакеты:

```
apt-get install dosgate=<version>
```

6. Обновить конфигурацию dosgate.service. Открыть для редактировани файл dosgate.service:

```
nano /usr/lib/systemd/system/dosgate.service
```

В строке:

```
ExecStart=dosgate -f
```

Заменить на:

```
ExecStart=dosgate -f -l crit
```

7. Запустить Dosgate в однократном режиме для проверки ошибок.

```
dosgate -o -l err
```

8. Запустить Dosgate.

```
systemctl start dosgate
```

9. Проверить статус Dosgate.

```
systemctl status dosgate
```

10. Восстановить маршрутизацию трафика через Dosgate.

Например, при использовании BGP и bird выполнить команду:

```
systemctl start bird bird6
```

Откат к предыдущей версии

1. Остановить маршрутизацию трафика через DosGate.

Например, при использовании BGP и bird выполнить команду:

```
systemctl stop bird bird6
```

2. Остановить Dosgate.

```
systemctl stop dosgate
```

3. Подготовить систему к откату.

```
dgadm --batch=uh -y
```

```
ip link set dev **интерфейс_dosgate** xdp off
```

```
rm -rf /sys/fs/bpf/dosgate
```

4. Установить предыдущую версию пакетов.

```
apt-get install dosgate=<old version>
```

5. Восстановить сохраненное состояние.

```
dgadm --restore=dgbackupname
```

6. Обновить конфигурацию dosgate.service. Открыть для редактировани файл dosgate.service:

```
nano /lib/systemd/system/dosgate.service
```

В строке:

```
ExecStart=dosgate -f
```

Заменить на:

```
ExecStart=dosgate -f -l crit
```

7. Запустить DosGate в однократном режиме для проверки ошибок.

```
dosgate -o -l err
```

8. Запустить DosGate.

```
systemctl start dosgate
```

9. Проверить статус DosGate.

```
systemctl status dosgate
```

Обновление веб-интерфейса

Обновление веб-интерфейса включает следующие компоненты:

- **SP-Spider** — это веб-интерфейс, предназначенный для управления и настройки программного обеспечения DosGate.
- **SP-Spider-Broker** — брокер синхронизации для DosGate.

Примечание
Установка веб-интерфейса на РЕД ОС не поддерживается! Рекомендуется выполнять установку на отдельном сервере с операционной системой Ubuntu или Альт 8 СП.

Обновление на Ubuntu

Обновление компонента SP-Spider

Создать резервную копию конфигурационного файла веб-интерфейса:

```
cp /opt/sp-spider/.env /opt/sp-spider/.env_bkp
```

Обновить список пакетов:

```
apt update
```

Установить новую версию:

```
apt install sp-spider=<version>
```

Отредактировать конфигурационный файл **/opt/sp-spider/.env** в соответствии с вашей конфигурацией. Используйте данные из ранее созданной резервной копии.

Перезапустить сервис:

```
systemctl restart sp-spider
```

Проверить состояние сервиса:

```
systemctl status sp-spider
```

Откат обновления компонента SP-Spider

Восстановить конфигурационный файл:

```
cp /opt/sp-spider/.env_bkp /opt/sp-spider/.env
```

Установить предыдущую версию пакета:

```
apt-get install sp-spider=<old_version>
```

Перезапустить сервис:

```
systemctl restart sp-spider
```

Проверить состояние сервиса:

```
systemctl status sp-spider
```

Обновление компонента SP-Spider-Broker

Создать резервную копию конфигурационного файла брокера синхронизации:

```
cp /opt/sp-spider-broker/.env /opt/sp-spider-broker/.env_bkp
```

Обновить список пакетов:

```
apt update
```

Установить новую версию пакета:

```
apt install sp-spider-broker=<version>
```

Отредактировать конфигурационный файл **/opt/sp-spider-broker/.env** в соответствии с вашей конфигурацией. Используйте данные из ранее созданной резервной копии.

Перезапустить сервис:

```
systemctl restart sp-spider-broker
```

Проверить состояние сервиса:

```
systemctl status sp-spider-broker
```

Откат обновления компонента SP-Spider-Broker

Восстановить конфигурационный файл:

```
cp /opt/sp-spider-broker/.env_bkp /opt/sp-spider-broker/.env
```

Установить предыдущую версию пакета:

```
apt-get install sp-spider-broker=<old_version>
```

Перезапустить сервис:

```
systemctl restart sp-spider-broker
```

Проверить состояние сервиса:

```
systemctl status sp-spider-broker
```

Обновление на Альт Linux

Обновление компонента SP-Spider

Создать резервную копию конфигурационного файла веб-интерфейса:

```
cp /opt/sp-spider/.env /opt/sp-spider/.env_bkp
```

Обновить список пакетов:

```
apt-cache update
```

Установить новую версию пакета:

```
apt-get install sp-spider=<version>
```

Отредактировать конфигурационный файл **/opt/sp-spider/.env** в соответствии с вашей конфигурацией. Используйте данные из ранее созданной резервной копии.

Перезапустить сервис:

```
systemctl restart sp-spider
```

Проверить состояние сервиса:

```
systemctl status sp-spider
```

Откат обновления компонента SP-Spider

Восстановить конфигурационный файл:

```
cp /opt/sp-spider/.env_bkp /opt/sp-spider/.env
```

Установить предыдущую версию пакета:

```
apt-get install sp-spider=<old_version>
```

Перезапустить сервис:

```
systemctl restart sp-spider
```

Проверить состояние сервиса:

```
systemctl status sp-spider
```

Обновление компонента SP-Spider-Broker

Создать резервную копию конфигурационного файла брокера синхронизации:

```
cp /opt/sp-spider-broker/.env /opt/sp-spider-broker/.env_bkp
```

Обновить список пакетов:

```
apt-cache update
```

Установить новую версию пакета:

```
apt-get install sp-spider-broker=<version>
```

Отредактировать конфигурационный файл **/opt/sp-spider-broker/.env** в соответствии с вашей конфигурацией. Используйте данные из ранее созданной резервной копии.

Перезапустить сервис:

```
systemctl restart sp-spider-broker
```

Проверить состояние сервиса:

```
systemctl status sp-spider-broker
```

Откат обновления компонента SP-Spider-Broker

Восстановить конфигурационный файл:

```
cp /opt/sp-spider-broker/.env_bkp /opt/sp-spider-broker/.env
```

Установить предыдущую версию пакета:

```
apt-get install sp-spider-broker=<old_version>
```

Перезапустить сервис:

```
systemctl restart sp-spider-broker
```

Проверить состояние сервиса:

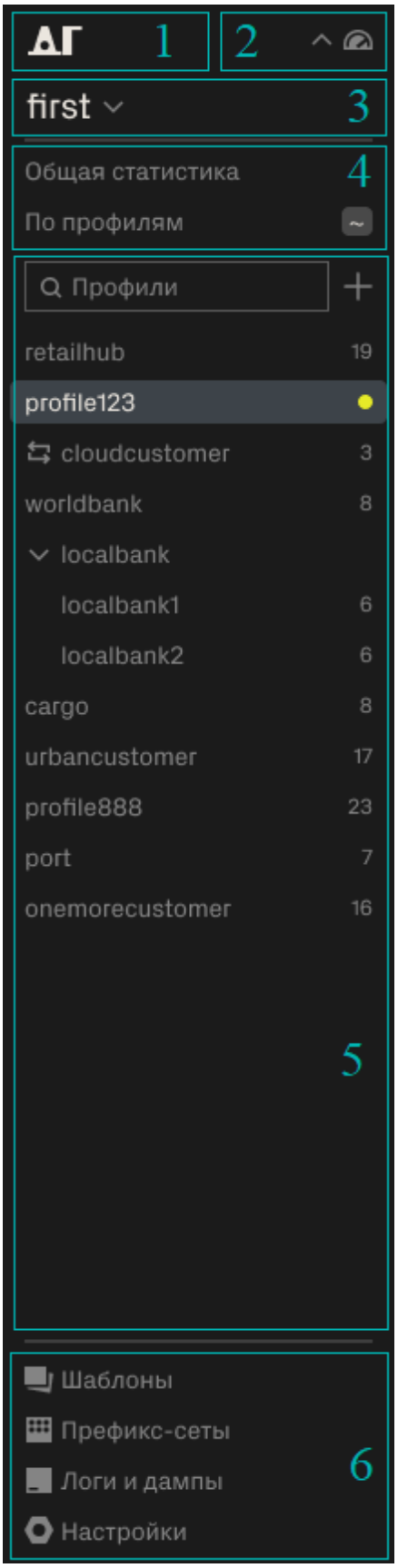
```
systemctl status sp-spider-broker
```

Интерфейс DosGate

В этом разделе содержится описание основных элементов пользовательского интерфейса.

Панель быстрого доступа

Панель быстрого доступа включает пять основных блоков:



1. **Переключение между продуктами** – позволяет выбрать доступный продукт SP (DosGate, FlowCollector).
2. **Мониторинг** - показывает текущую загрузку выбранного узла.
3. **Выбор арены** – предназначен для выбора рабочей арены.

4. **Статистика** – предоставляет доступ к общей статистике либо к статистическим данным по каждому профилю.
5. **Список профилей** – отображает перечень всех существующих профилей в системе.
6. **Панель управления** – содержит следующие функциональные элементы:

- Шаблоны

- Префикс-сеты

- Логи и дампы

- Настройки

Статистика

Раздел включает в себя два блока:

- **Общая статистика**
- **По профилям**

Общая статистика

"Общая статистика" отображает графики трафика для всех арен. Данные представлены в виде двух отдельных графиков для каждой арены, показывающих пропускную способность:

- В битах в секунду (bits/s).
- В пакетах в секунду (packets/s).

При переходе на вкладку **Сессии** отображается статистика по сессиям, обрабатываемым **Сессионной защитой DosGate**. Статистика предоставляется только по тем протоколам, которые были выбраны пользователем в настройках модуля.

Атрибуты трафика

По умолчанию на графиках присутствуют следующие атрибуты:

- **drop** — пакеты, отброшенные DosGate в соответствии с правилами.
- **error** — пакеты, не прошедшие проверку согласно IP RFC и также отброшенные.
- **pass** — трафик, переданный в пользовательское пространство ОС по действию **PASS**.
- **pass_uh** — трафик, отправленный в сессионную защиту для дополнительной проверки.
- **reply** — ответный трафик от DosGate в сторону отправителя в рамках механизма TCP-аутентификации.
- **transmit** — трафик, успешно прошедший фильтрацию и отправленный дальше.

При выборе каждого атрибута формируется отдельный график, отображающий динамику соответствующего трафика.

В правой части интерфейса расположен блок **"Период"**, позволяющий задать временной интервал, за который будут построены графики трафика.

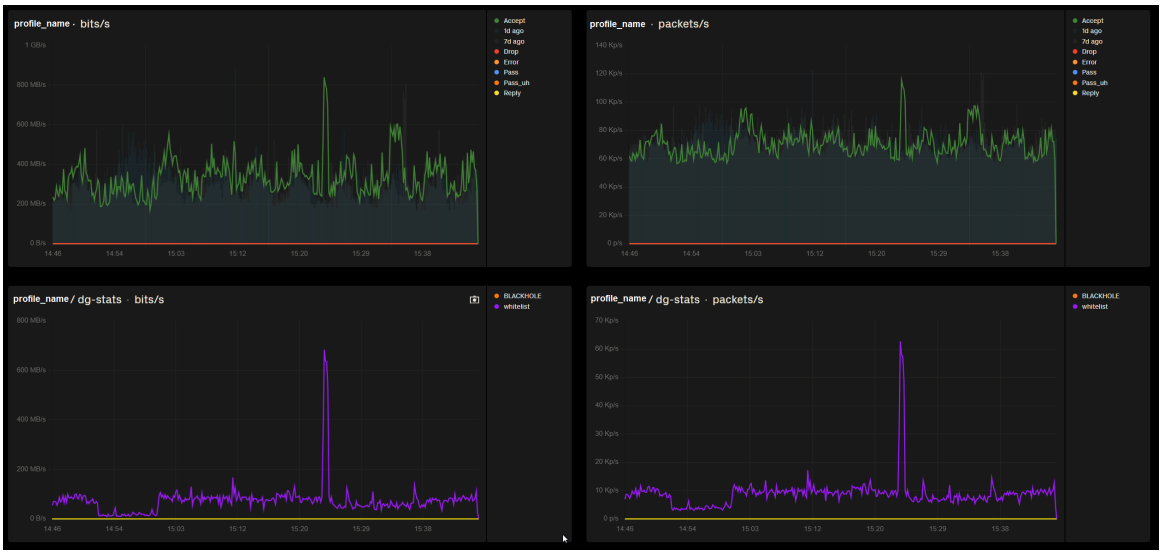
Точный — позволяет вручную задать диапазон дат и времени или выбрать промежуток от нескольких месяцев до одной минуты.

По профилям

Пункт меню "По профилям" предоставляет детализированную статистику для каждого профиля. Выбор профиля осуществляется через выпадающее меню. После выбора профиля отображаются следующие графики:

- **График общего трафика по профилю** представлен в двух форматах: packets/s и bits/s.
- **График трафика по правилу STATS** (profile_name/dg-stats) отображаются при наличии трафика, удовлетворяющего правилу **STATS**, и также представлены в форматах packets/s и bits/s.

Графики формируются исключительно при наличии соответствующего трафика в пределах заданных условий. Иными словами: если в правиле указано действие **STATS**, но трафик, подпадающий под это правило, отсутствует, график не будет отрисован.



Атрибуты трафика

На графике присутствуют следующие атрибуты:

- **Accept** — принятые пакеты, успешно прошедшие через систему.
- **1d ago** — скорость трафика один день назад.
- **7d ago** — скорость трафика семь дней назад.
- **Drop** — пакеты, отброшенные DosGate в соответствии с правилами.
- **Error** — ошибки при передаче или обработке пакетов.
- **Pass** — трафик, переданный в пользовательское пространство ОС по действию **PASS**.
- **Pass_uh** — трафик, отправленный в сессионную защиту для дополнительной проверки.
- **Reply** — ответный трафик от DosGate в сторону отправителя в рамках механизма TCP-аутентификации.

Панель управления

Шаблоны

Шаблон — это готовый набор настроек, который помогает быстрее создавать профили и правила.

Шаблоны делятся на два типа:

- **Профили** – используются только при создании профилей.
- **Контрмеры** – добавляются в профили для формирования правил.

Шаблоны, связанные с базой вредоносных сигнатур, отображаются **фиолетовым цветом** и обновляются автоматически при каждом обновлении базы.

Локальные шаблоны, отображаются **белым цветом** и обновляются только вручную. Шаблоны с несохранёнными изменениями выделяются **желтым цветом**.

Профили, созданные из шаблонов, обновляются автоматически, пока связь с шаблоном не разорвана или автообновление не отключено.

Связь с шаблоном можно разорвать вручную с помощью кнопки «Разорвать связь». После этого профиль перестаёт получать обновления шаблона.

Пользователь может экспортировать, импортировать и редактировать шаблоны через соответствующие функции интерфейса.

Добавление нового шаблона

Добавление шаблона

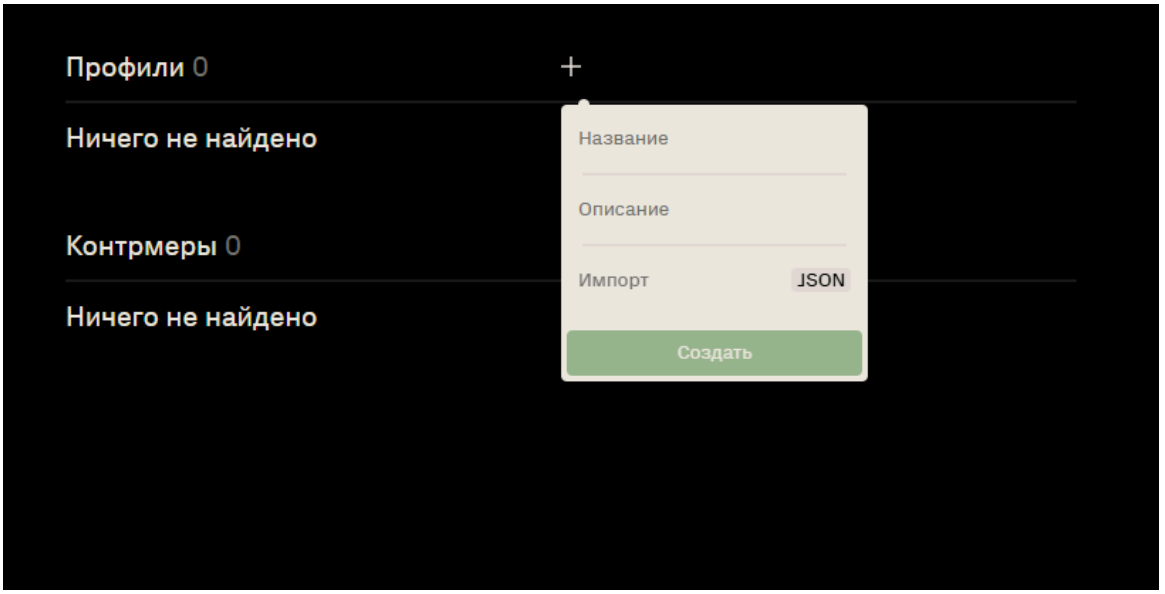
Чтобы создать шаблон, откройте раздел **Шаблоны**. В верхней части списка, рядом с заголовком **Профили**, нажать на значок серого плюса. Откроется окно для ввода параметров.

Укажите **Название**.

> **Примечание**
> Система не позволяет присваивать одинаковые названия профилям и контрмерам.

Добавьте **Описание**, указав назначение или параметры шаблона.

При наличии подготовленного JSON-файла загрузите его через кнопку **Импорт**.



Нажмите **Создать**. Новый шаблон появится в списке и будет доступен для редактирования.

Добавление контрмеры

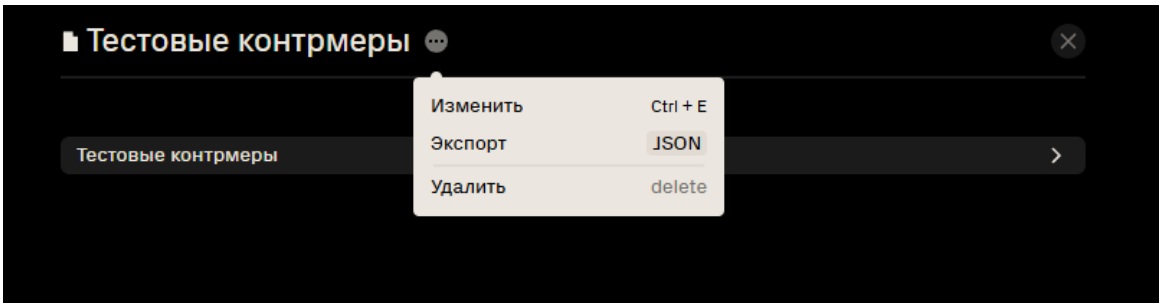
Добавление контрмер осуществляется аналогично добавлению профилей.

Редактирование шаблона

При открытии шаблона отображается интерфейс создания правил. Подробную информацию об этом процессе см. в разделе "Создать правило".

Экспорт шаблона

Чтобы экспортировать шаблон, выберите его в списке. В открывшемся меню редактирования нажмите на значок трёх точек для вызова дополнительных действий. Веберите **Экспорт**, шаблон сохранится в виде JSON-файла.



Префикс-сет

Префикс-сет — это набор IP-адресов, который используют в правилах для формирования белых и чёрных списков.

Префикс-сеты делятся на:

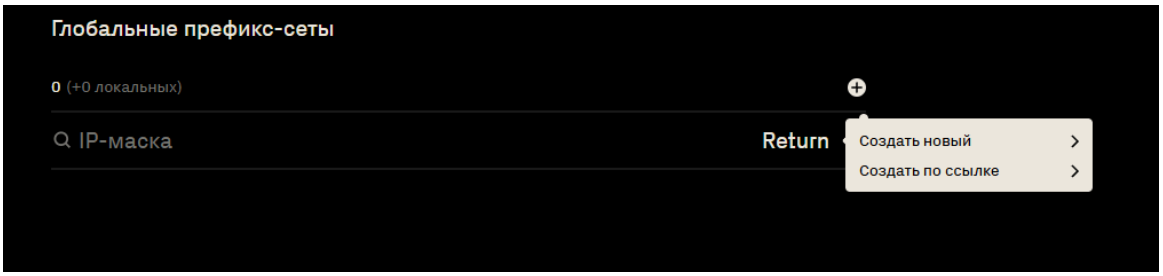
- **Глобальные** – распространяются на всю арену и используются во всех профилях.
- **Локальные** – применяются только в рамках конкретного профиля.

Добавление префикс-сета

Для создания нового префикс-сета выполните следующие шаги:

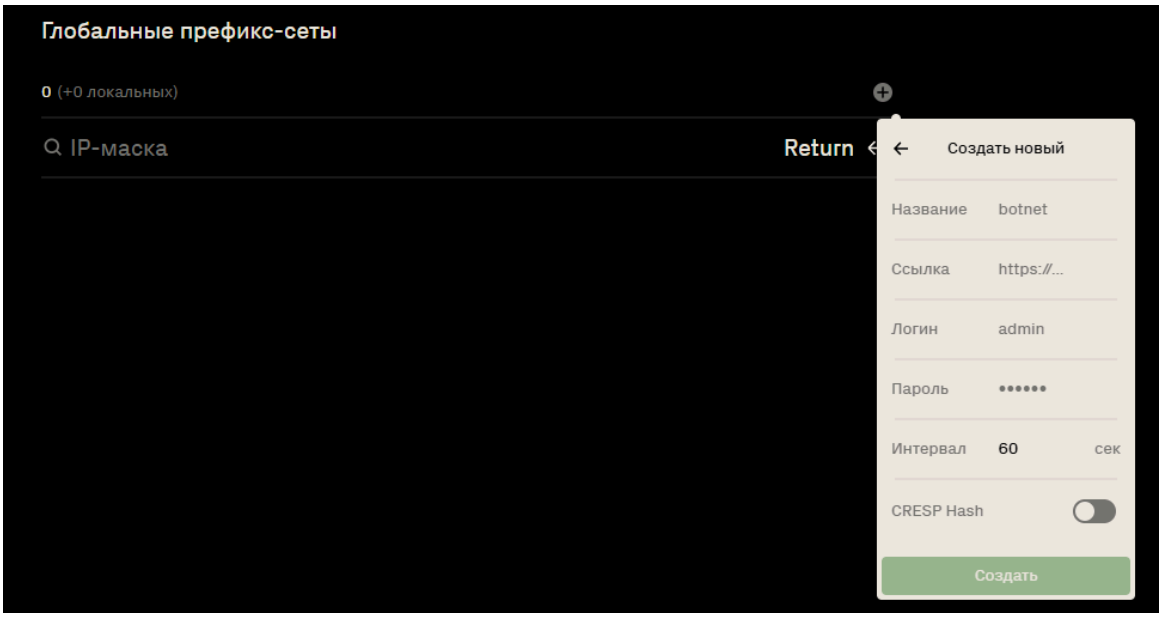
- Для создания глобального префикс-сета: Перейдите в раздел **Глобальные префикс-сеты**.
- Для создания локального префикс-сета: Перейдите в раздел **Профиль → Префикс-сеты**.

В верхней части списка нажать значок плюса. В ниспадающем меню выбрать один из вариантов создания префикс-сета.



- **Создать новый**
  Указать имя создаваемого префикс-сета.
- **Создать по ссылке**

Префикс-сет может быть создан путем загрузки данных из внешнего источника по ссылке. Это позволяет автоматически обновлять записи в префикс-сете, используя актуальные данные, предоставленные по HTTP/HTTPS.



Для добавления префикс-сета по ссылке необходимо заполнить следующие поля:

Название – задать имя префикс-сета (например, whitelist).
Ссылка – указать URL-адрес источника списка (http/https).
Логин – ввести логин для аутентификации на удаленном ресурсе (если требуется).
Пароль – указать пароль для аутентификации (если требуется).
Интервал – задать периодичность обновления списка в секундах (например, 60).
CRESP Hash – включить обработку хешированного формата списка (используется в инсталяциях с модулем Антибот).

Нажать **Создать** для сохранения префикс-сета.

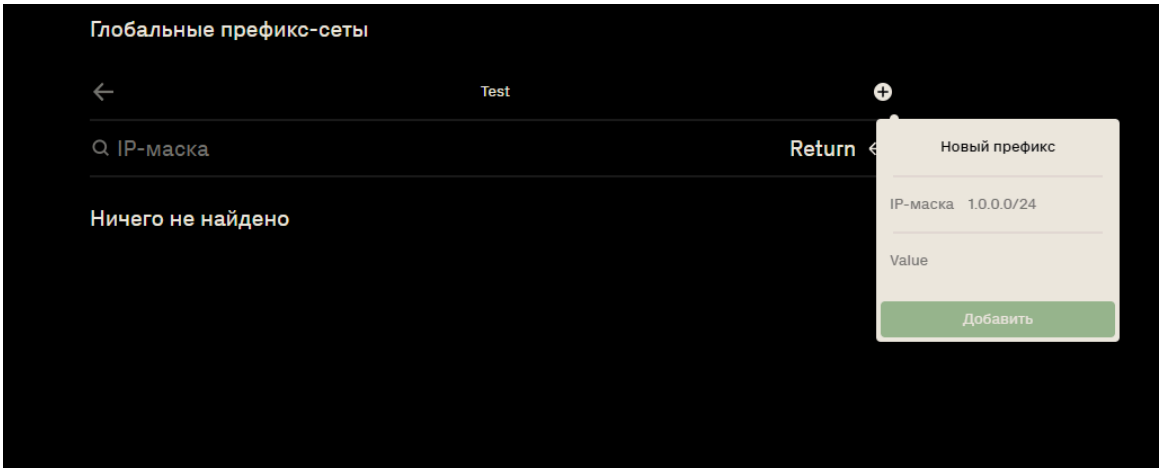
Добавление записи в префикс-сет

Префикс-сет представляет собой набор записей, каждая из которых содержит IP-префикс и value. Значение value служит идентификатором записи и используется для группировки записей при создании правил.

Value — это числовое значение, уникальное для каждой записи в префикс-сете. Оно не связано с самим префикс-сетом, а относится к конкретной записи.

В правилах фильтрации можно указывать конкретные значения value, чтобы применять правила только к соответствующим записям. Записи с одинаковым value могут быть объединены в группы для применения общих правил.

Для добавления записей в префикс-сет необходимо выбрать целевой префикс-сет и открыть его. В интерфейсе управления нажать значок плюса для добавления новой записи. В появившемся диалоговом окне указать **IP-адрес с маской** в формате `10.0.0.0/24` и задать числовое значение value, затем нажать "Добавить".



Примечание
Если при добавлении записи маска не указана, автоматически назначается маска /32.

Допустимо использовать альтернативный метод добавления записей путем перетаскивания файла формата TXT с префиксами в область

таблицы, что позволит автоматически загрузить и обновить содержимое префикс-сета.

Файл должен содержать список IP-префиксов в следующем формате:

```
192.168.1.0/24
10.0.0.0/8
1.1.1.0/24
```

При отсутствии указанного value автоматически устанавливается значение 1.

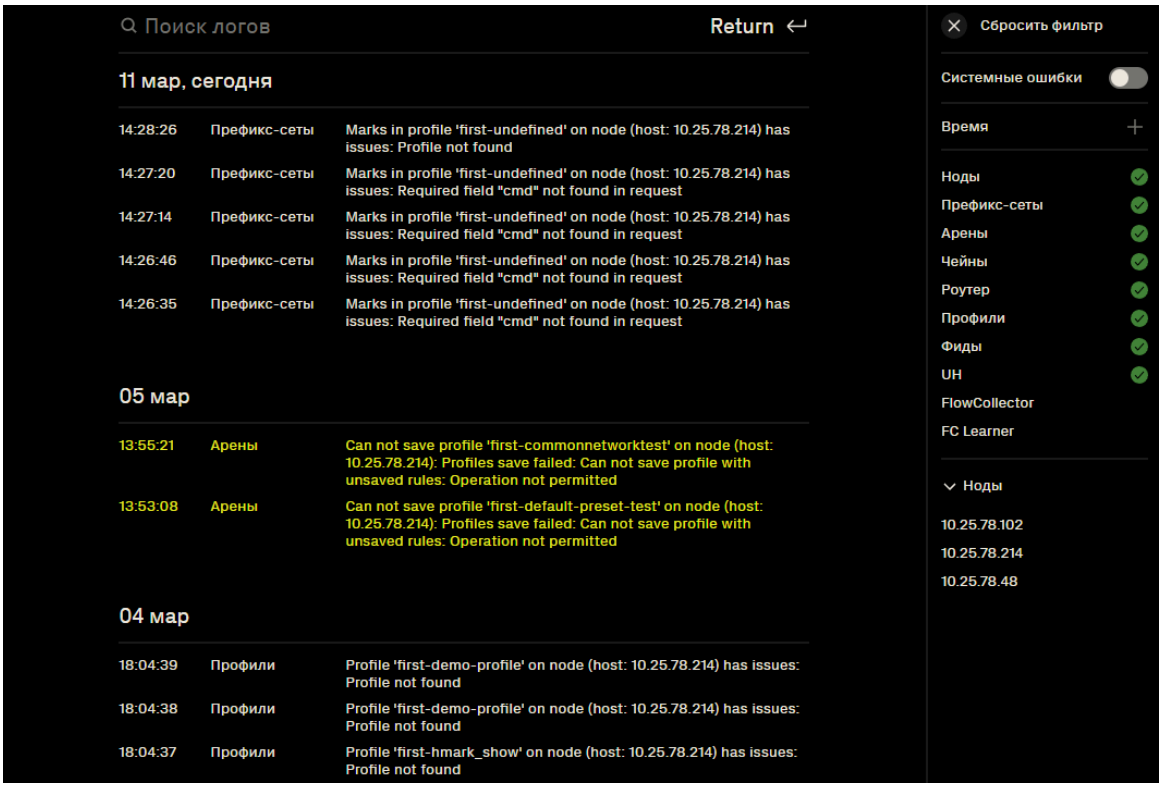
Для назначения value каждой записи формат файла может быть расширен:

```
192.168.1.0/24  1
10.0.0.0/8      2
1.1.1.0/24      1
```

Логи и дампы

Логи

Логи предназначены для мониторинга событий, возникающих в системе, и позволяет пользователю анализировать ошибки, предупреждения и другие системные сообщения.



Поле ввода в верхней части экрана, позволяющее осуществлять поиск по записям журнала.

Список логов отображает хронологический перечень событий, включающий:

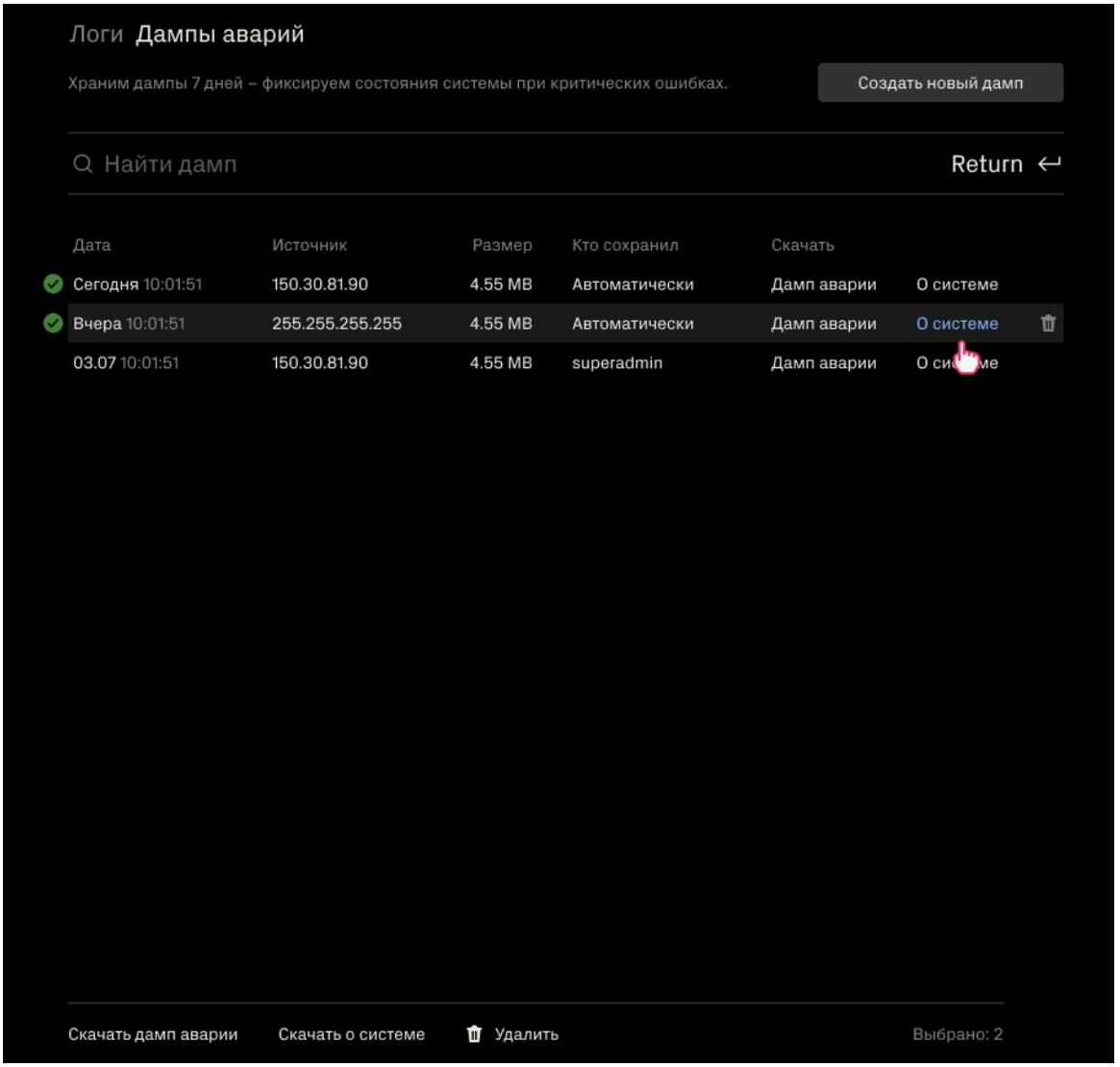
- Время события.
- Источник (Префикс-сеты, Профили, Арены и т.д).
- Описание события

Фильтр логов содержит следующие параметры:

- Системные ошибки – переключатель, позволяющий фильтровать критические ошибки.
- Время – настройка для ограничения выборки логов по дате и времени.
- Категории событий – возможность выбрать источники логов, такие как Ноды, Префикс-сеты, Роутеры, UH и другие.
- Ноды – меню для выбора ноды, логи которой отображаются.

Дампы аварий

Дампы аварий — это механизм быстрой диагностики. При сбое любого сервиса платформы система автоматически формирует архив с технической информацией за последние 5 минут.



Поиск дампов позволяет находить нужные записи журнала через поле ввода в верхней части экрана.

В верхней части интерфейса расположена кнопка **Создать новый дамп**. Она запускает ручное создание аварийного дампа. Система собирает данные и формирует архив.

Готовый дамп появляется в таблице. Его можно скачать или удалить.

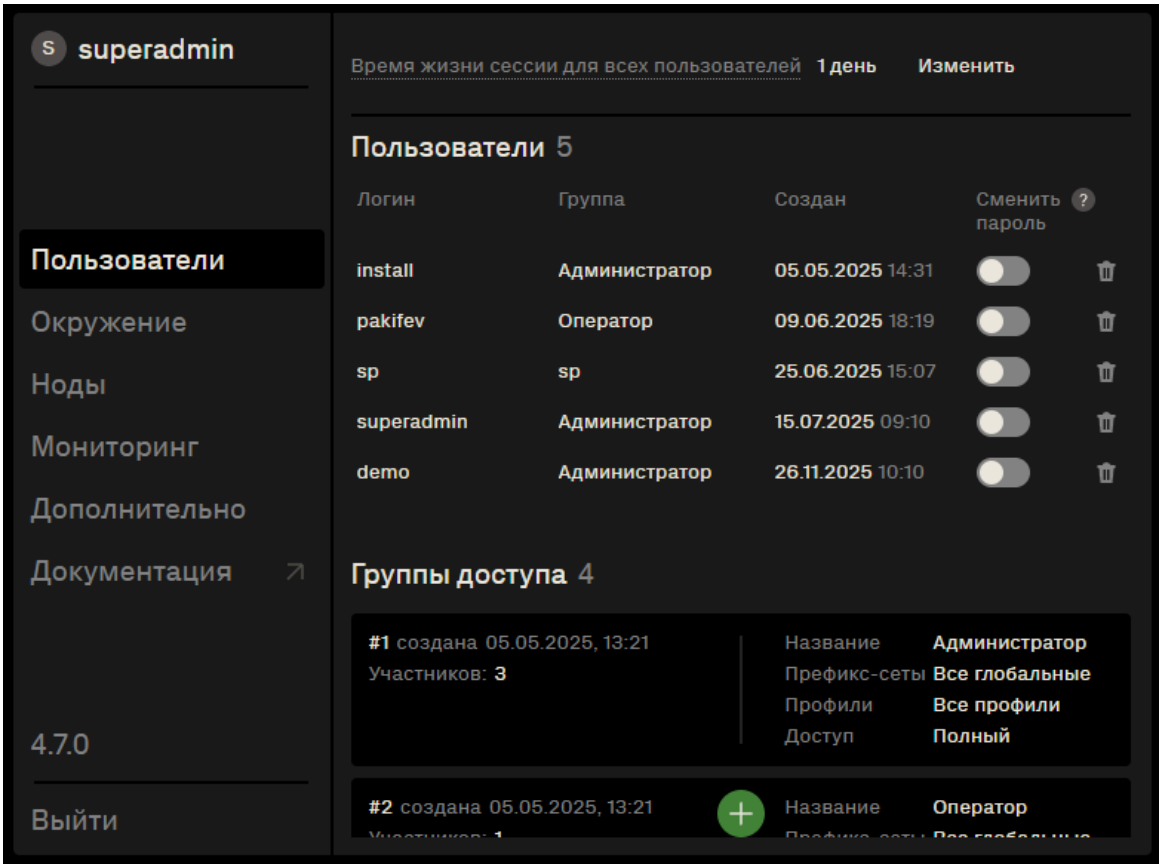
- **Дамп аварии** — полный архив с логами и служебными данными, собранными при сбое.
- **О системе** — краткая сводка о текущем состоянии сервера. Она включает информацию о оборудовании: сетевые интерфейсы, версию ядра, версию операционной системы и другие базовые параметры.

Дампы хранятся 7 дней и удаляются автоматически.

Настройки

Пользователи

Раздел **Пользователи** предназначен для управления пользователями системы и их принадлежностью к группам доступа.



Время жизни сессии для всех пользователей задаёт период, после которого пользователи должны заново войти в систему. При необходимости может быть изменено.

Пользователи - отображает учётные записи и их группы доступа. В списке можно удалить пользователя или включить переключатель **Сменить пароль** — в этом случае система завершит его сессию и попросит установить новый пароль при следующем входе.

Группы доступа - список доступных групп с детализацией параметров.

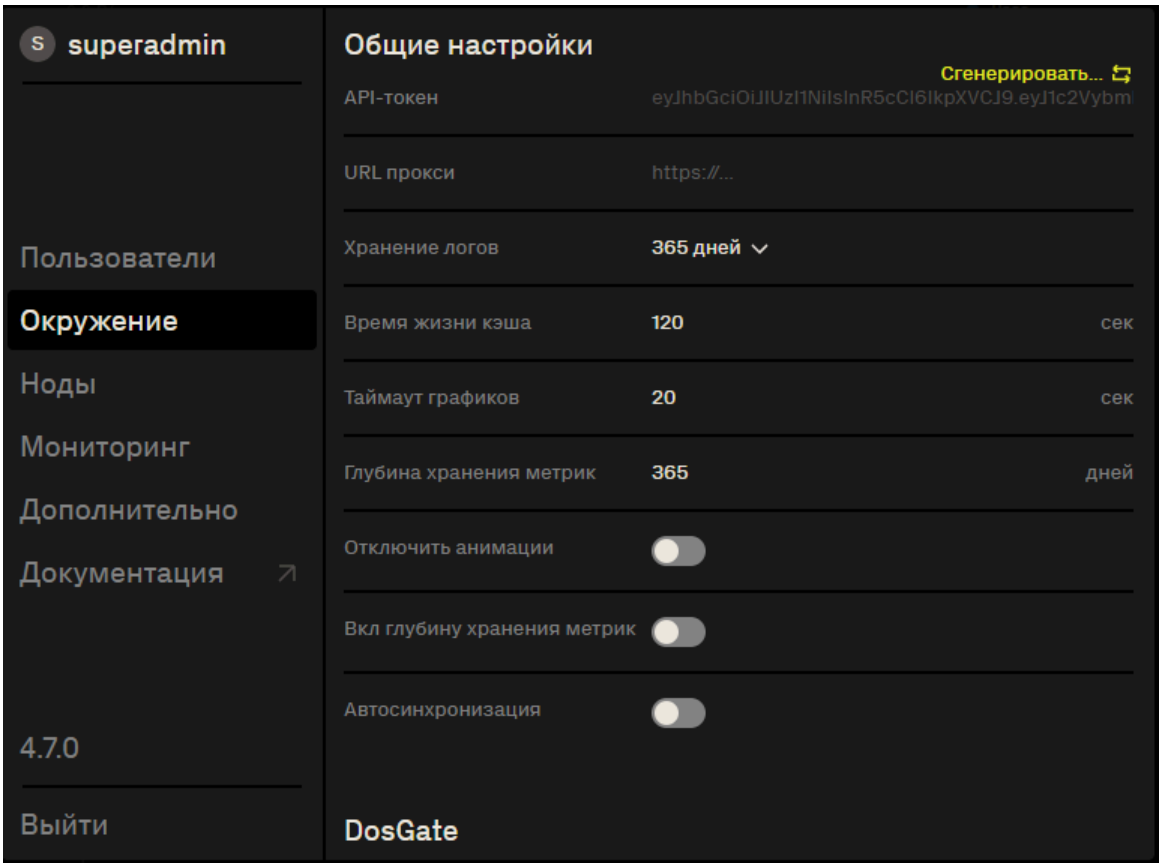
Группы доступа определяют права пользователей на доступ к профилям и префикс-сетам. По умолчанию в системе существуют три роли:

- Администратор
- Оператор
- Пользователь

Каждой группе можно назначить доступ ко всем или только определенным профилям и префикс-сетам. В системе есть возможность создавать собственные группы пользователей с индивидуальными правами доступа. Администратор может настраивать новые группы или изменять права существующих.
В нижней части интерфейса расположена кнопка "+", которая позволяет добавлять как новых пользователей, так и создавать новые группы доступа.

Окружение

Раздел **Окружение** содержит общие настройки системы, включая параметры API, прокси, кэширование, логи и интеграцию с внешними сервисами для работы с метриками и данными.



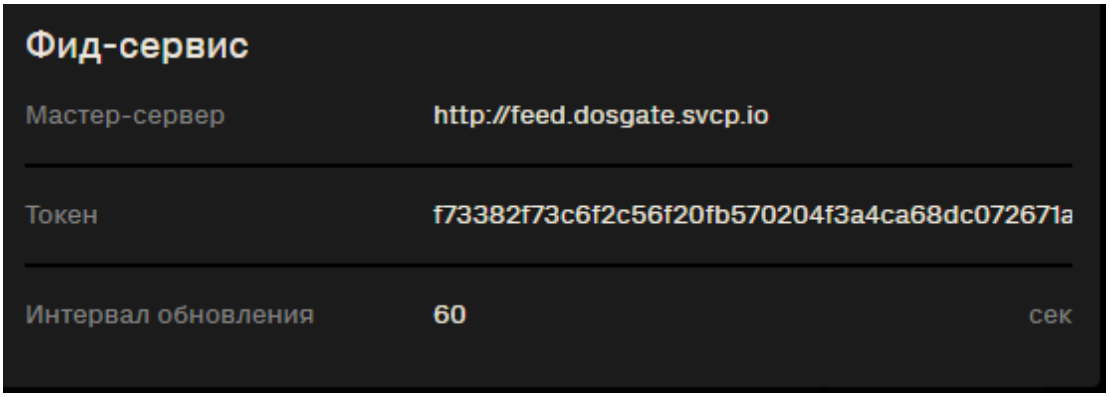
Общие настройки

- **API-токен** – позволяет сгенерировать уникальный ключ доступа к API.
- **URL прокси** – адрес прокси-сервера. Используется для доступа к фид-сервису Servicepipe через прокси-сервер
- **Хранение логов** – задает срок хранения логов в днях (по умолчанию 365 дней).
- **Время жизни кэша** – Хранит данные о профилях и их содержимом для ускорения работы системы. Чем больше значение кэша, тем реже он обновляется, что повышает производительность в крупных инсталляциях.
- **Отключить анимации** – переключатель, отключающий анимационные эффекты интерфейса. Рекомендуется отключать анимацию при подключении к веб-интерфейсу по RDP.
- **Автосинхронизация** – обеспечивает автоматическое приведение конфигурации узлов в соответствие с мастер-сервером при добавлении новых серверов или обнаружении расхождений в политиках.

DosGate

- **Graphite URL** – адрес сервера Graphite для сбора и отображения метрик.
- **Арена по умолчанию** – название арены, используемой в системе по умолчанию.
- **Обновление графиков** – интервал обновления графиков в секундах.

Фид-сервис

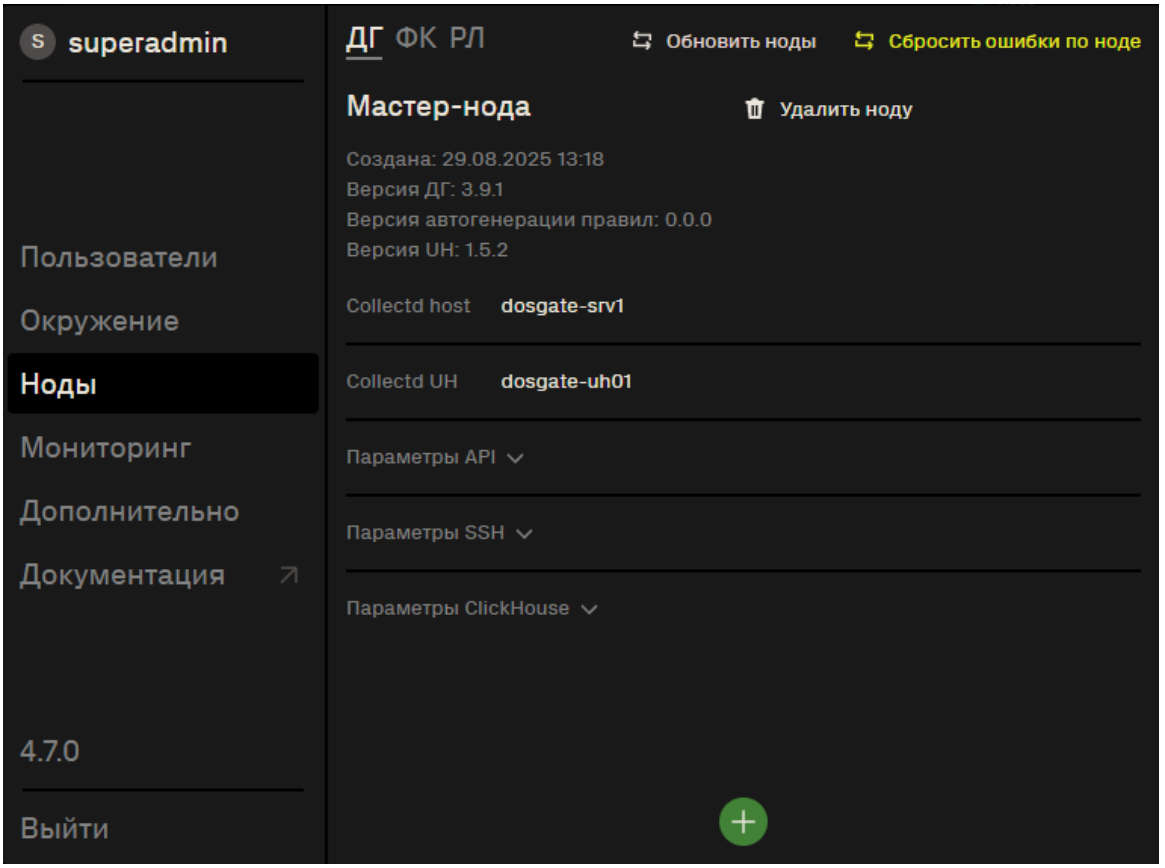


- **Мастер-сервер** – URL основного сервера фид-сервиса.

- **Токен** – ключ аутентификации, предоставленный вендором.
- **Интервал обновления**– частота обновления данных фид-сервиса в секундах.

Ноды

Раздел **Ноды** предназначен для управления узлами системы. Здесь отображается список доступных узлов, их статус и параметры.



Основные элементы:

- **Мастер-нода** — узел системы, на котором формируется бэкап настроек.
- **Collectd host** — имя хоста, с которого собираются системные и сервисные метрики.
- **Collectd UH** — имя хоста, с которого собираются системные и сервисные метрики для сессионой защиты.
- **Параметры API** — настройки доступа к API ноды.
- **Параметры SSH** — настройки SSH-доступа к ноде.

- **Параметры ClickHouse** — параметры подключения к базе данных ClickHouse для хранения и обработки аналитических данных.

Доступные действия:

- **Обновить ноды** – инициирует обновление данных о текущих узлах.
- **Синхронизировать** – выполняет принудительную синхронизацию конфигурации узлов с мастер-нодой.

Добавление новой ноды

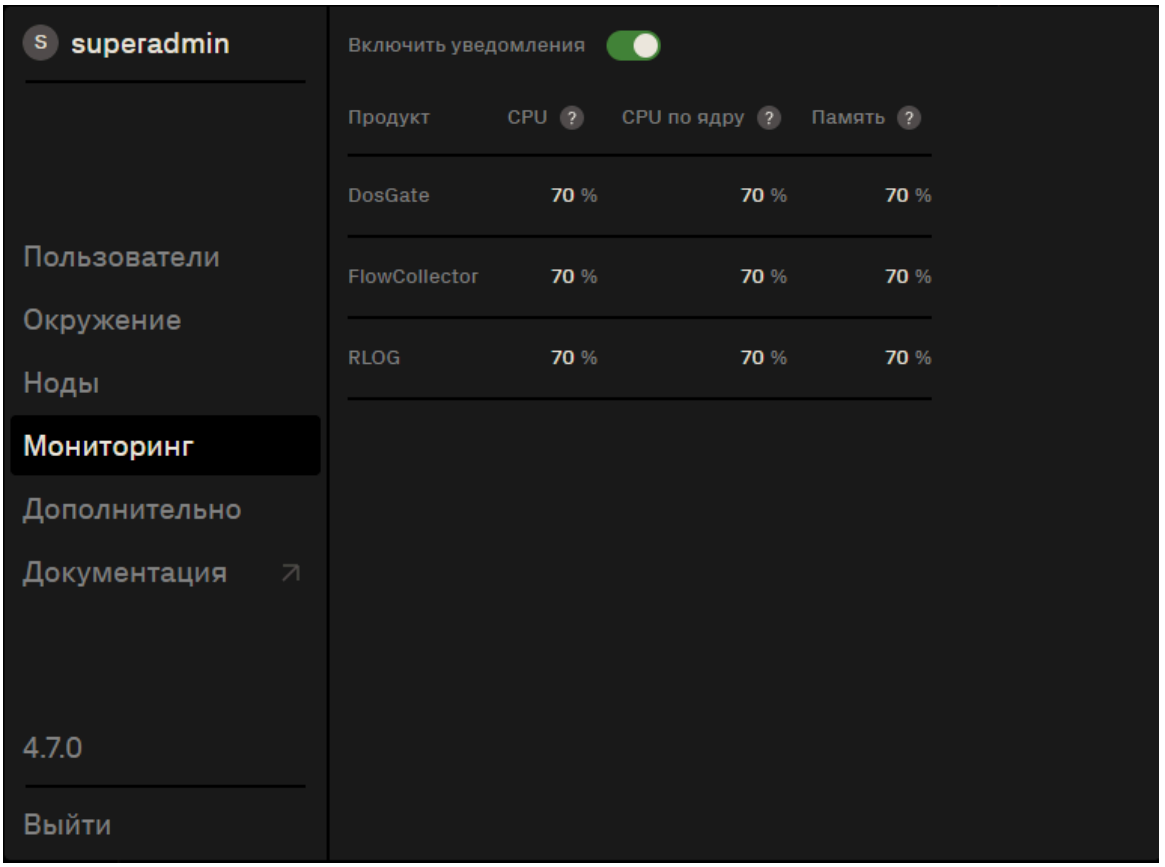
Для добавления нового узла в систему выполните следующие шаги:

1. Открыть раздел "Ноды" в интерфейсе.
2. Нажать кнопку "+" для создания новой ноды.
3. Заполнить параметры узла:
   - **Операционная система** – выбрать ОС из списка (Ubuntu 18, Альт 8 СП, Alma Linux).
   - **Модуль** – выбрать необходимый модуль (DosGate/FlowCollector).
   - **Collectd host** – указать имя хоста.
   - **Collectd UH** – указать имя сетевого модуля.
   - **HW Bypass** – функция управления сетевыми картами с поддержкой аппаратного байпаса, позволяющая включать или отключать режим прямой передачи трафика между портами на физическом уровне.
4. Нажать **Подключение**.
   - Доступны два способа соединения – API и SSH, выберите любой из них и настройте соответствующие параметры.
5. Нажать кнопку **Применить**.
6. Завершить добавление узла, нажав **Добавить ноду**.

После этого узел будет добавлен и отображён в общем списке нод.

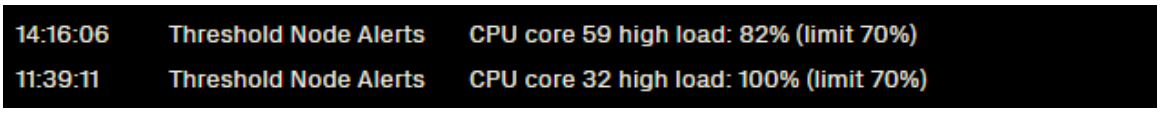
Мониторинг

Мониторинг отображает состояние ресурсов, используемых сервисами платформы. Интерфейс позволяет контролировать загрузку CPU, загрузку CPU по ядрам и объём используемой памяти для каждого продукта.

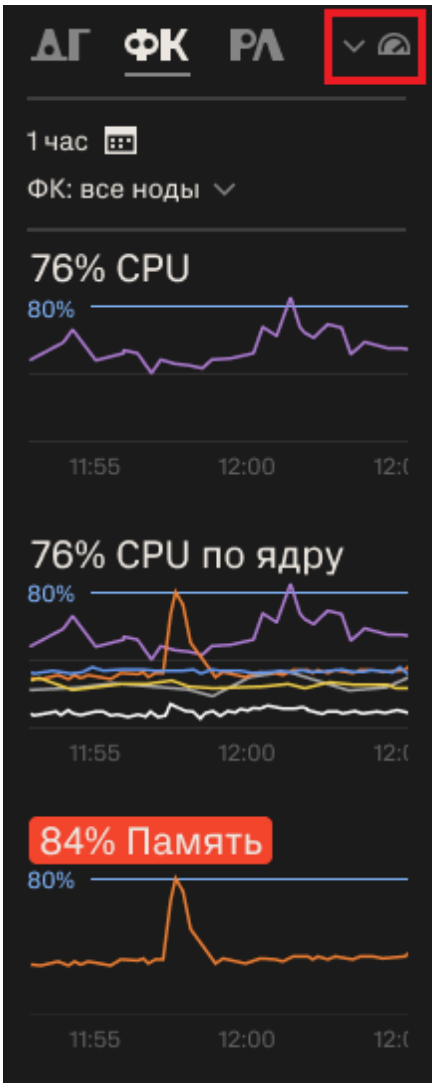


В верхней части расположен переключатель **Включить уведомления**, который активирует отправку предупреждений при превышении заданных порогов нагрузки.

Уведомления мониторинга отображаются в общем списке событий раздела **Логи**.



Для быстрого перехода к данным мониторинга в панели быстрого доступа доступна иконка мониторинга. Показатели, превышающие пороговые значения отображаются красным.

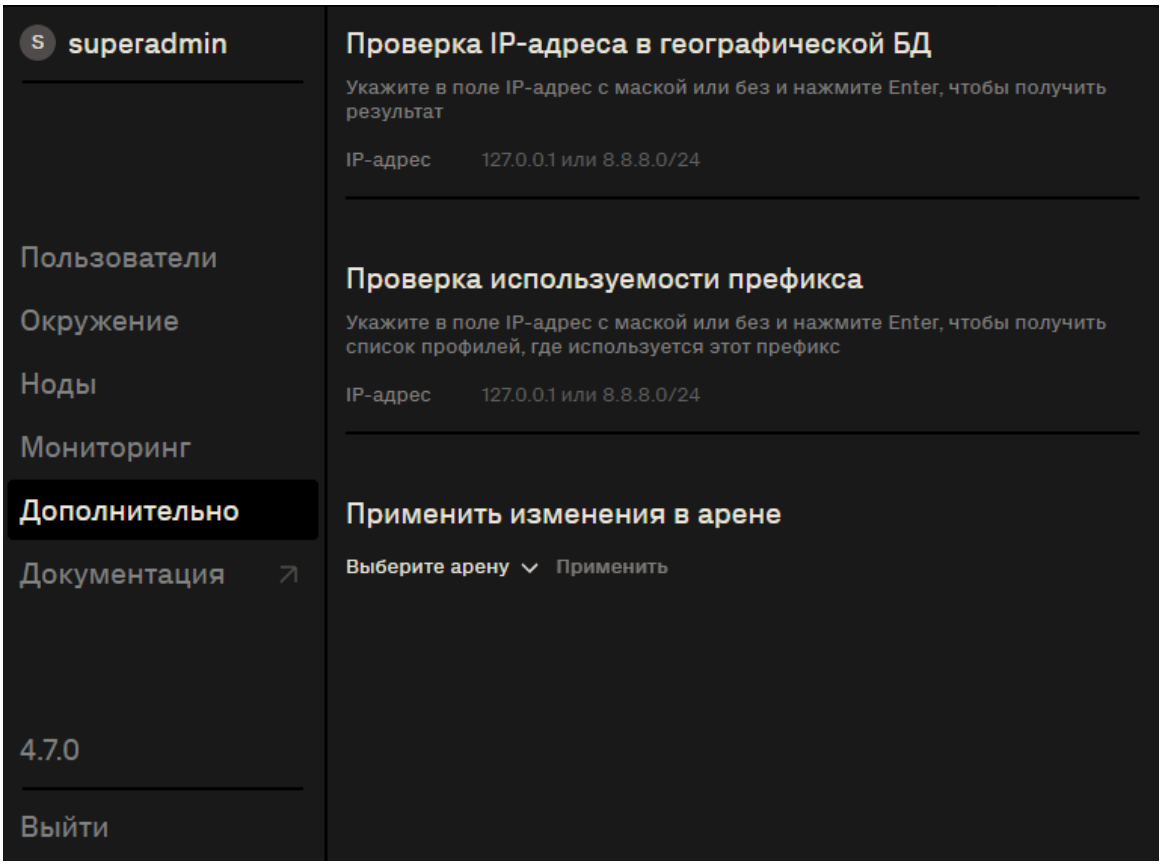


Дополнительно

Проверка IP-адреса в географической БД – позволяет определить географическую принадлежность IP-адреса.

Проверка используемости префикса – отображает список профилей, в которых используется заданный IP-адрес или префикс.

Применение изменений в арене – предоставляет возможность выбора арены из выпадающего списка и применения внесённых изменений с помощью кнопки **Применить**.



Документация

Раздел **Документация** в боковом меню является ссылкой, которая открывает справочные материалы по системе.

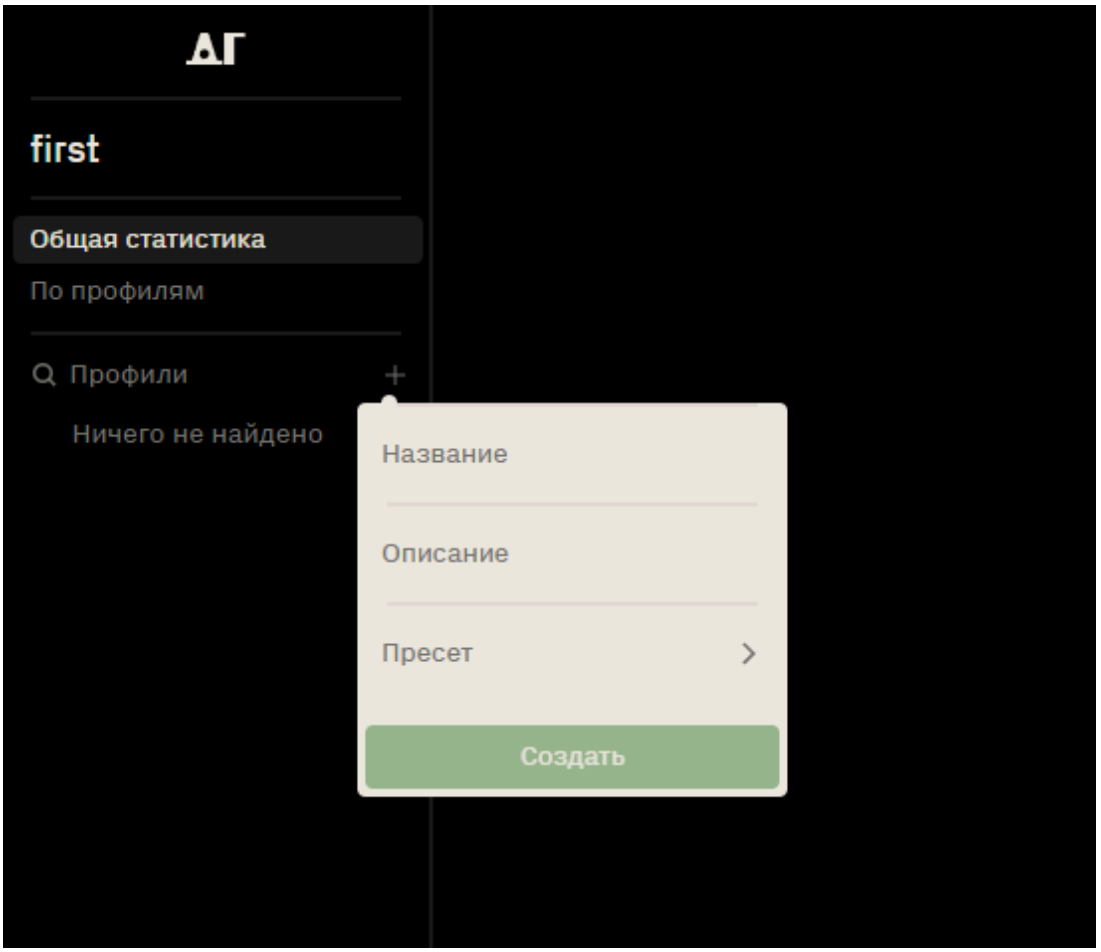
Профиль

Профиль – это набор правил, привязанных к конкретному префиксу назначения. Он определяет поведение системы в отношении маршрутизации и фильтрации трафика.

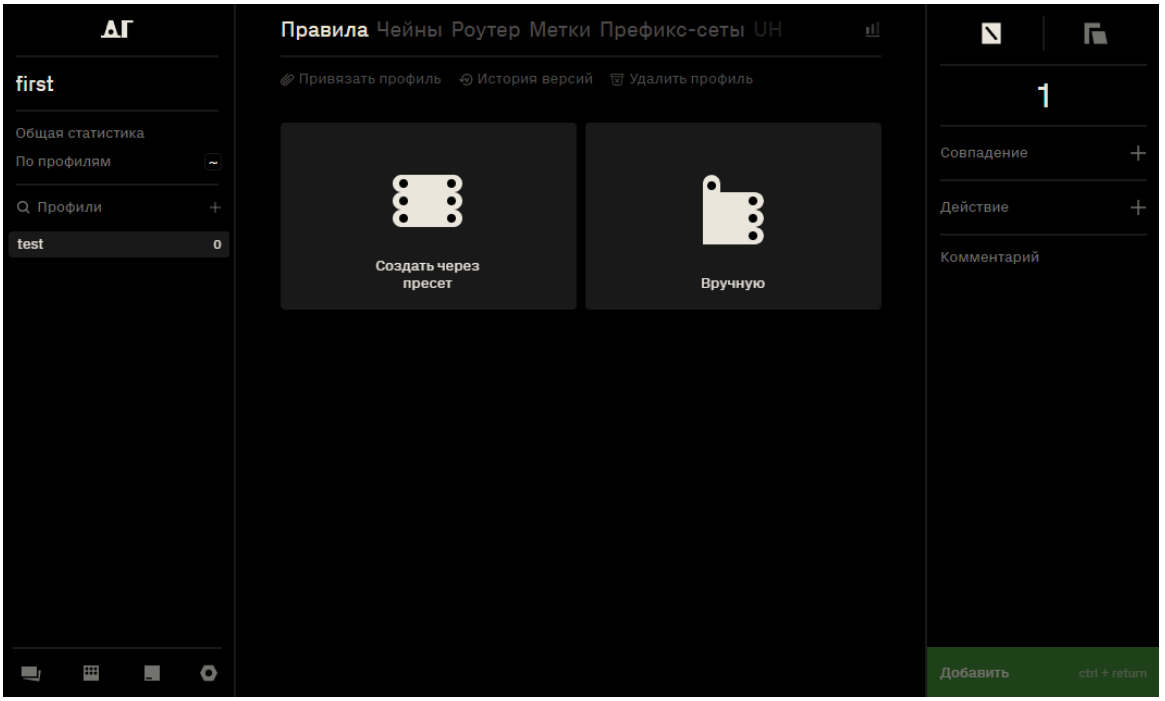
Создание профиля

Для создания нового профиля в системе выполнить следующие действия:

1. На главной странице в разделе **Профили** нажать кнопку "+".
2. Заполнить следующие поля для создания профиля:
    - **Название** - уникальное имя для профиля. Рекомендуется использовать комбинацию из обозначения сегмента инфраструктуры и названия сервиса, например, "zapadniy-filial-web" или "dmz-dns".
    - **Описание** - краткое текстовое пояснение, которое поможет понять назначение профиля.
    - **Пресет** - шаблон для быстрого создания профиля. Возможность выбрать из существующих пресетов, если подключена база вредоносных сигнатур. Использование пресета не является обязательным.
3. Нажать кнопку **Создать**.

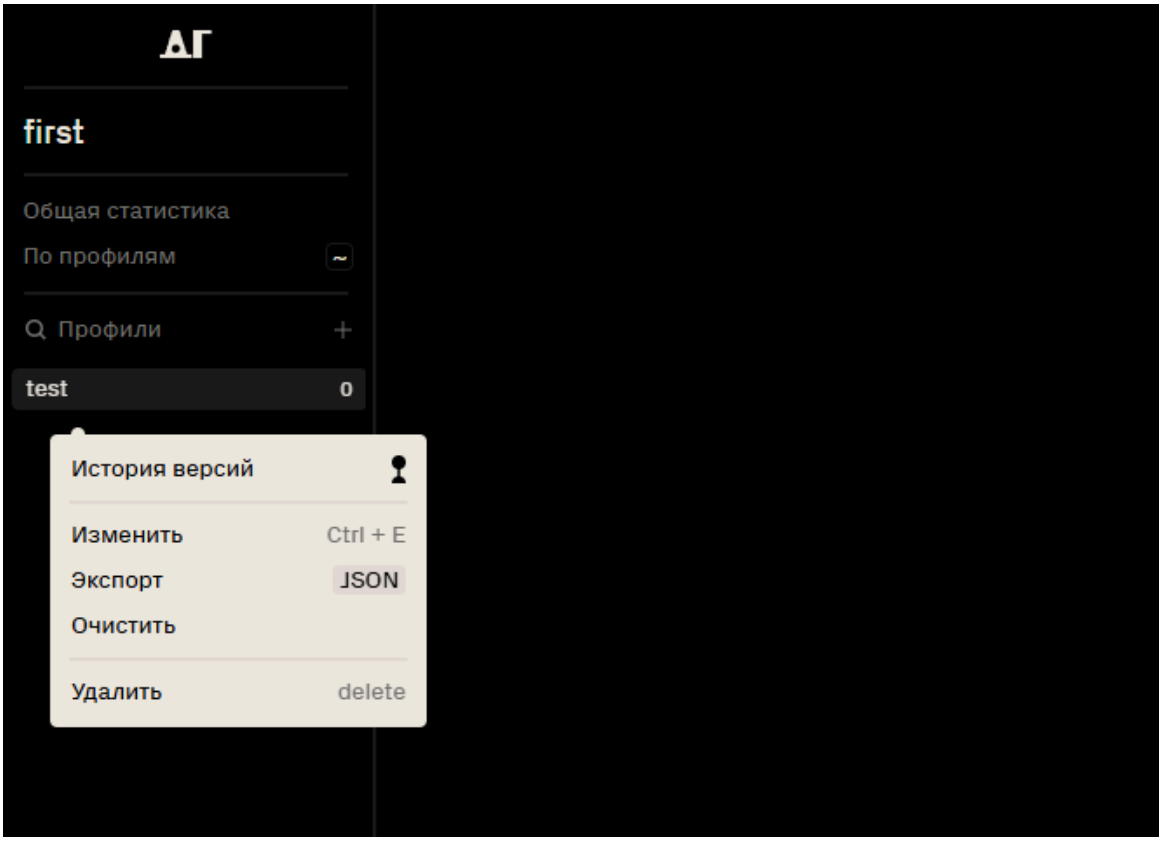


После создания профиля интерфейс переключится на страницу профиля.



Изменение профиля

Для изменения профиля необходимо нажать правой кнопкой мыши на его названии в общем списке профилей и выбрать пункт **Изменить**. Откроется окно, в котором можно изменить название и описание профиля.



Экспорт профиля

Для создания локальных пресетов реализована функция экспорта профилей в формате JSON. Для выполнения экспорта необходимо нажать правой кнопкой мыши на профиль в списке профилей и выбрать пункт **Экспорт**. После этого JSON-файл будет автоматически загружен.

Очистка профиля

Функция очистки профиля позволяет удалить все правила, оставляя неизменными остальные атрибуты профиля (чейны, роутер, метки и

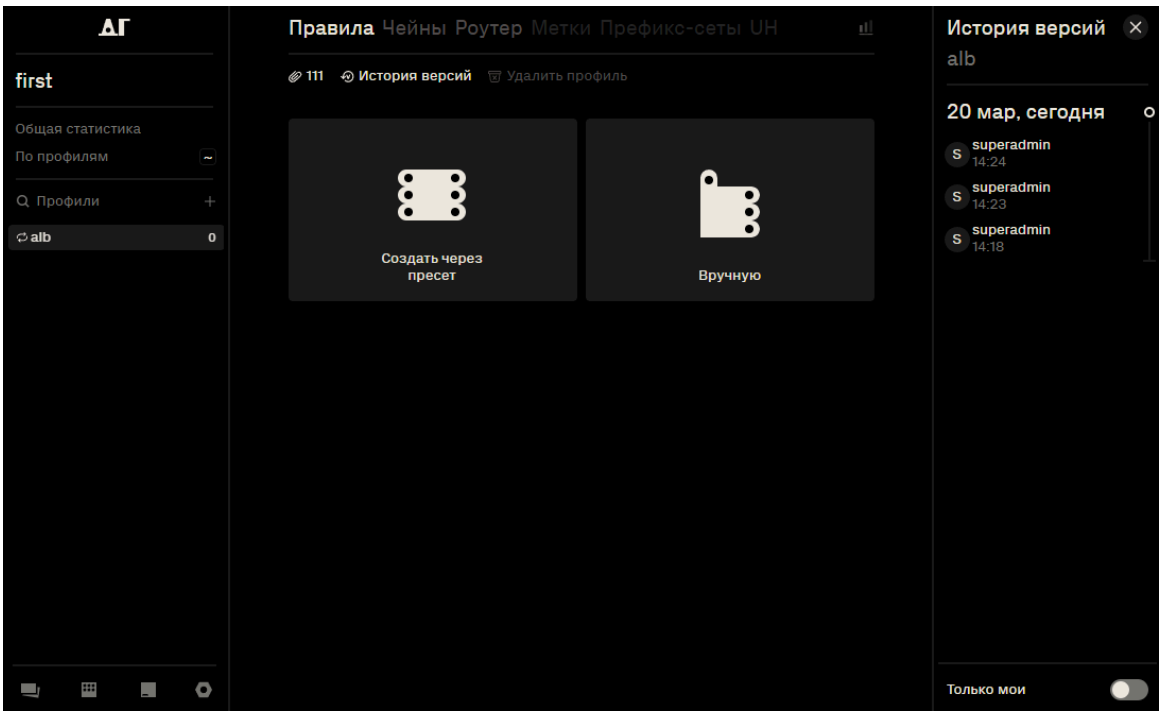
префикс-сеты). Для выполнения очистки нажмите правой кнопкой мыши на профиль в списке профилей и выберите пункт **Очистить**. После этого все правила будут удалены, а остальные атрибуты профиля останутся неизменными.

Удаление профиля

В профиле предусмотрена возможность его удаления. Для удаления профиля необходимо нажать правой кнопкой мыши на его названии в общем списке профилей и выбрать пункт **Удалить**. После этого профиль будет безвозвратно удален из системы.

История версий

История версий — это сохраненные состояния профиля, содержащие изменения следующих атрибутов: правила, чейны и роутер. Новая версия создается автоматически при применении изменений. Для просмотра истории версий необходимо нажать правой кнопкой мыши на профиль в общем списке профилей и выбрать пункт **История версий**.

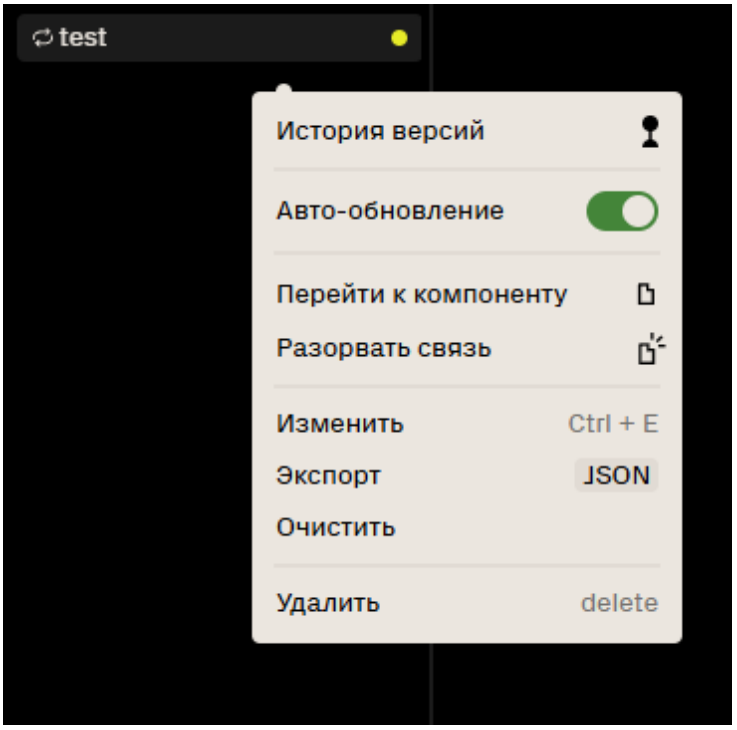


После этого в правой части интерфейса откроется панель **История версий**, содержащая список изменений, внесенных в профиль. Каждая

запись включает имя пользователя, выполнившего изменение и время сохранения версии. При необходимости возможно добавить комментарий. Записи отображаются в хронологическом порядке, начиная с самой последней. В нижней части раздела расположен переключатель «Только мои». При его активации отображаются изменения, внесенные текущим пользователем.

Автообновление

Если профиль создан на основе пресета, он автоматически получает обновления. При отключении функции «Авто-обновление» связь профиля с пресетом сохраняется, но изменения, поступающие в пресет, не будут автоматически применяться к профилю.



Переход к компоненту

Для перехода к компоненту щёлкните правой кнопкой мыши на его названии в общем списке профилей, выберите пункт **Перейти к компоненту**, после чего откроется окно редактирования пресета из которого был создан профиль.

Разрыв связи

Разрыв связи необходим в случае, если требуется внести изменения в правила профиля, созданного на основе пресета. Пока профиль остаётся связанным с пресетом, редактирование его правил невозможно — все настройки наследуются из пресета и обновляются автоматически. После разрыва связи профиль становится автономным, а изменения в пресете больше на него не распространяются.

Правила

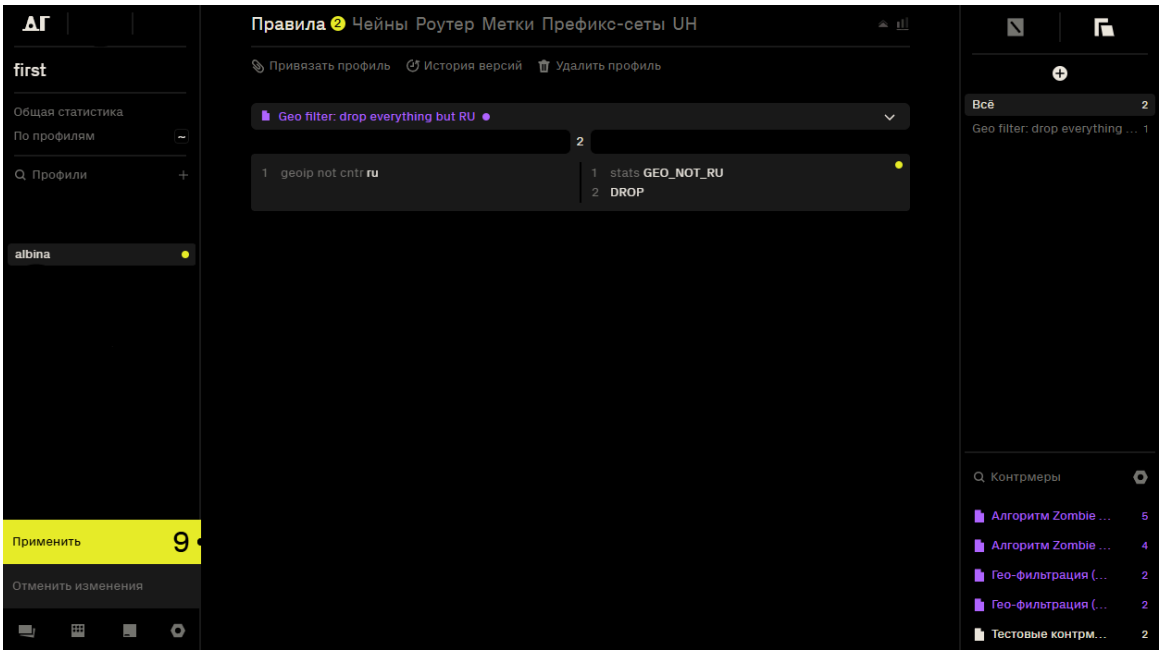
Правила – алгоритм (инструкция) для обработки трафика.

Создание и редактирование правил

Правила могут быть заданы одним из двух способов: с использованием пресета или вручную.

Создание правила через пресет

1. Перейти в необходимый профиль.
2. Выбрать опцию **Создать через пресет**.
3. В правом нижнем углу отобразятся доступные контрмеры:
    - Контрмеры отображаются **фиолетовым цветом**, если подключена база вредоносных сигнатур.
    - Контрмеры отображаются **белым цветом**, если они были созданы вручную в разделе **Пресеты**.
4. Выбрать необходимую контрмеру и перетянуть в поле **Правила**.
5. Для применения изменений необходимо нажать желтую кнопку **Применить**



Создание правила вручную

1. Перейти в необходимый профиль.
2. Выбрать опцию **Вручную**.

В DosGate правила создаются путем комбинирования совпадений и действий. Совпадения определяют условия, при которых правило срабатывает. Действия применяются к трафику, если условия совпадений выполнены. Такой процесс позволяет гибко настраивать фильтрацию и управление трафиком.

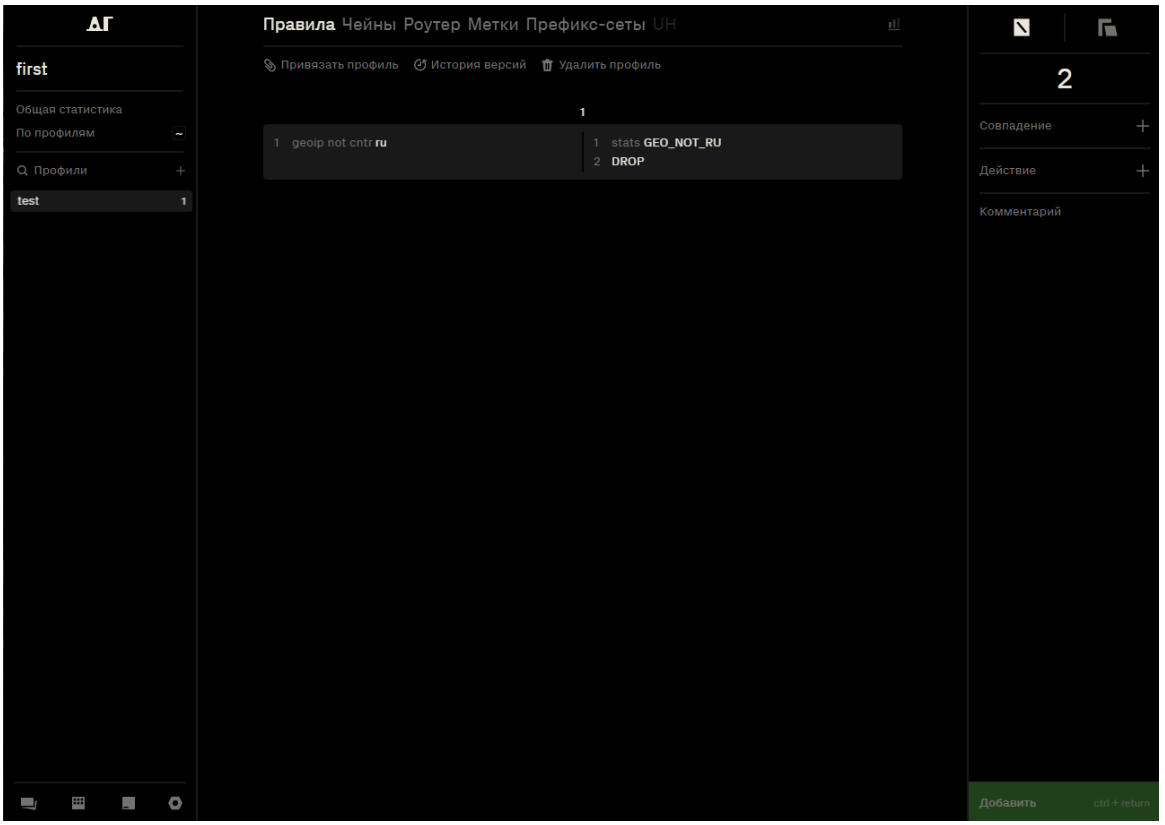
Пример №1

Назначение правила: Ограничения доступа на основе географического происхождения IP-адреса. Весь трафик, не относящийся к России, будет отброшен.

1. В интерфейсе профиля нажать кнопку **Вручную**. Это откроет форму для настройки совпадений.
2. В поле **Совпадение** выбрать параметр **geoip** → **country** → **RU**.
3. Активировать радиокнопку **NOT**, чтобы применить логическое отрицание. Условие будет выполняться для всех IP-адресов, не принадлежащих РФ.
4. В поле **Сверяем** установить **src**, правило будет охватывать весь трафик, *источник* которого находится за пределами РФ. Нажать

кнопку **Добавить**.

5. В поле **Действие** выбрать **STATS** — это позволяет записывать все срабатывания правила в отдельный счётчик. Ввести имя счётчика: *GEO_NOT_RU*, чтобы в дальнейшем можно было анализировать объём и частоту трафика, не относящегося к России. Нажать кнопку **Добавить**.
6. В поле **Действие** выберать **DROP** - это действие приведёт к немедленному отбрасыванию всех пакетов, соответствующих условию (т.е. всех, кто не из РФ). Пакеты будут сброшены без уведомления отправителя и без дальнейшей обработки.
7. При необходимости добавить комментарий к правилу. Это может быть пояснение или примечание для администратора.
8. Нажать зелёную кнопку **Добавить**, чтобы сохранить правило в список.
9. После добавления необходимо нажать жёлтую кнопку **Применить** в левой части интерфейса. Только после этого правило будет активно и начнёт применяться к обрабатываемому трафику.



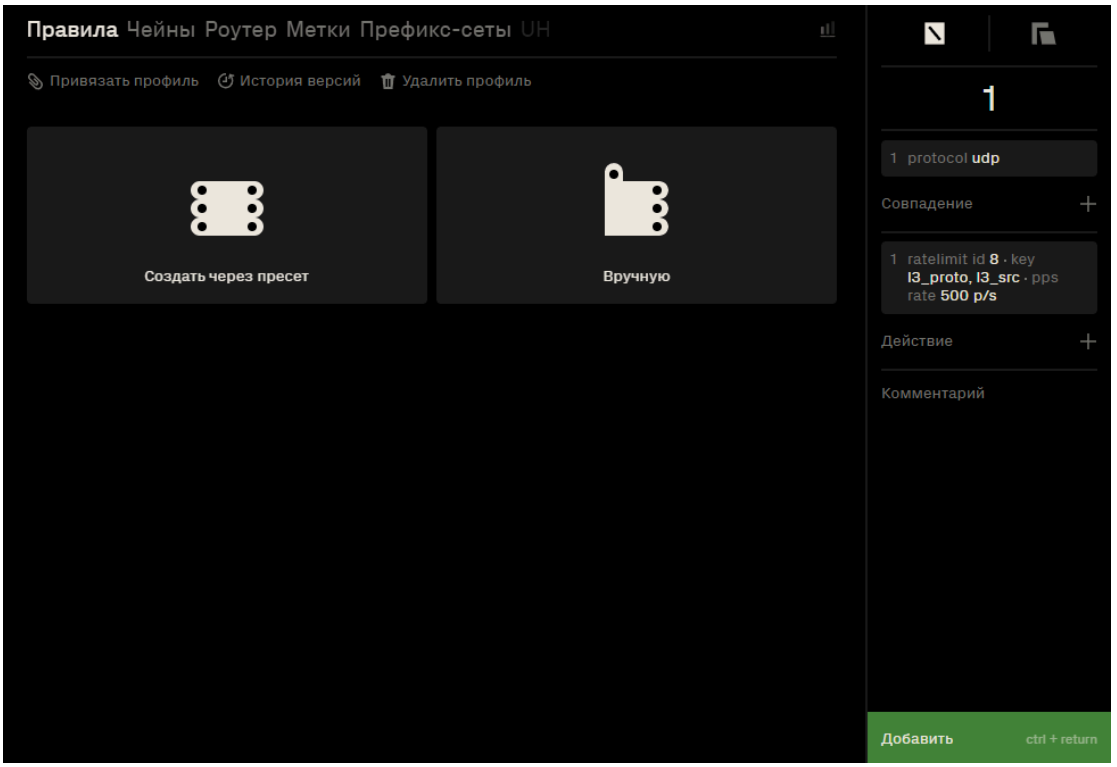
Пример №2

Назначение правила: Ограничение частоты UDP-трафика с последующей временной блокировкой IP-адреса-источника при

превышении лимита. Правило также регистрирует статистику по всем срабатываниям.

1. В интерфейсе профиля нажать кнопку **Вручную**. Это откроет форму для настройки совпадений.
2. В поле **Совпадение** выбрать параметр **protocol → udp**. Нажать зелёную кнопку **Добавить** Это ограничит обработку правил только UDP-трафиком.
3. В поле **Действие** выбрать **ratelimit**, указав параметры:
   - **id → 8**
   - **Bucket key → l3_proto** и **l3_src**
   - **pps → rate → 500**

   Нажать зелёную кнопку **Добавить**. Это ограничение установит максимум 500 пакетов в секунду от одного источника. В правом нижнем углу нажать зелёную кнопку **Добавить** для добавления первого правила.



4. Добавить второе правило. В поле **Совпадение** выбрать **verdict**, установить:
   - **type → ratelimit**
   - **value → exceed**

   Нажать зелёную кнопку **Добавить**.Это условие будет выполнено, если

лимит, указанный в предыдущем шаге, превышен.

5. В поле **Действие** поочередно выбрать:

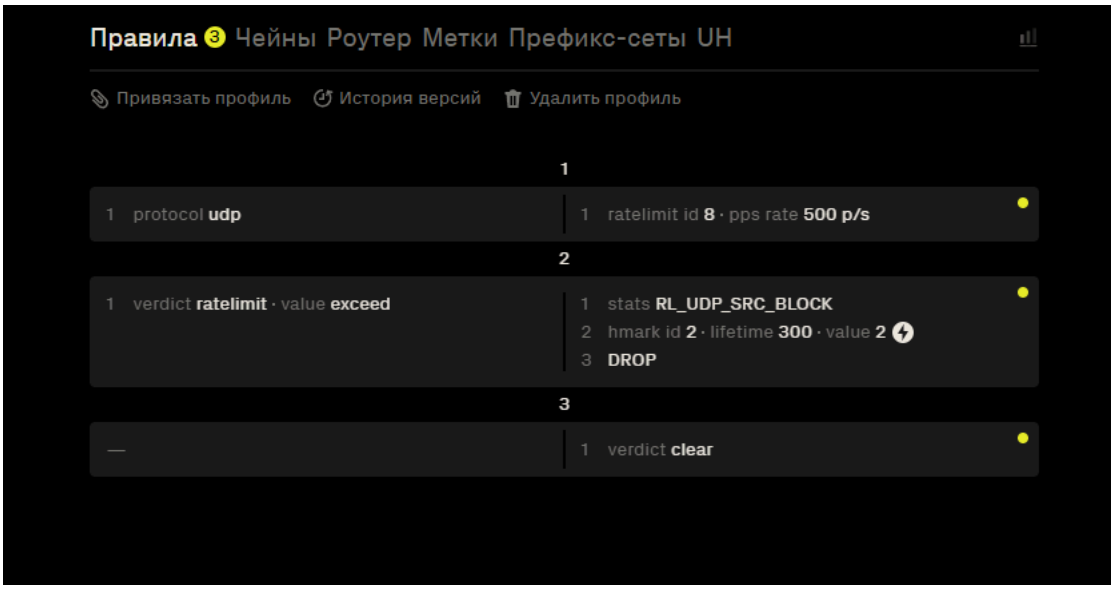
   - **STATS** – имя счётчика *RL_UDP_SRC_BLOCK*. Это позволит учитывать случаи превышения лимита. Нажать кнопку **Добавить**.
   - **HMARK**, указав: - **id → 2** - **value → 2** - **lifetime → 300**
     Нажать кнопку **Добавить**. Действие установит метку на IP-адрес на 300 секунд.
   - **DROP** – для немедленного отбрасывания пакета.

   В правом нижнем углу нажать зелёную кнопку **Добавить** для добавления второго правила.

6. Добавить третье правило. В поле **Действие** выбрать:

   - **verdict → clear**.

   Нажать кнопку **Добавить**. Сбрасывает **verdict** правила, если ни одно из предыдущих условий не выполнено.
   В правом нижнем углу нажать зелёную кнопку **Добавить** для добавления третьего правила.



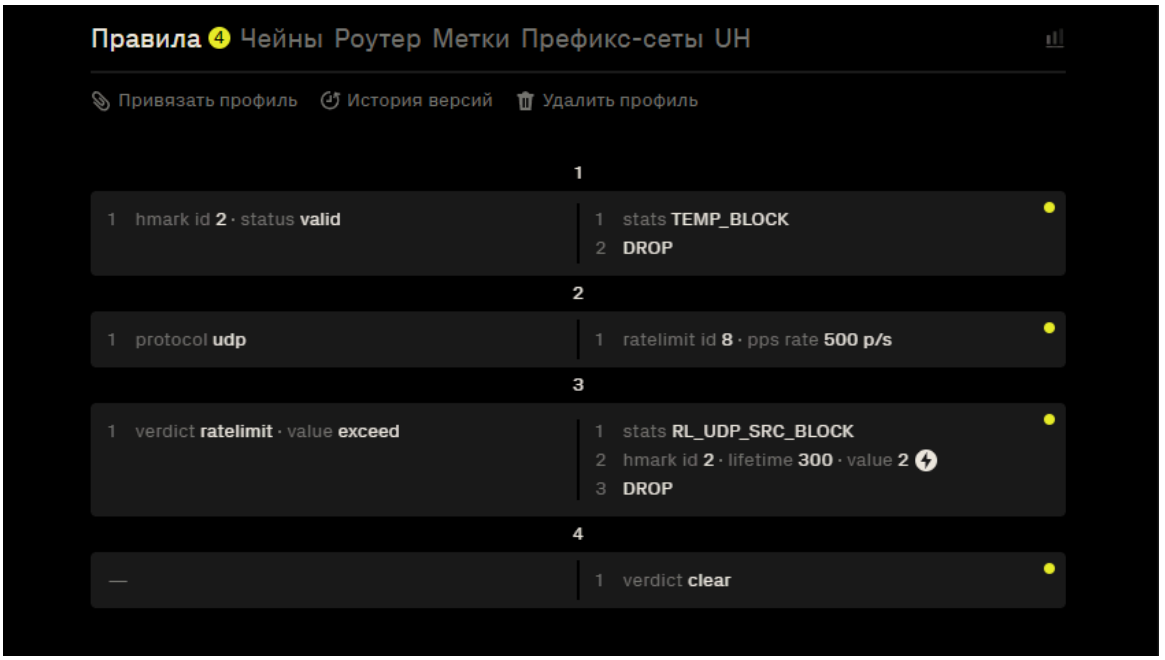
7. Добавить четвертое правило. В поле **Совпадение** добавить параметр **HMARK**, указав:

   - **id → 2**
   - **status → valid**
     Нажать кнопку **Добавить**. Это условие проверяет, что у пакета уже установлена действительная хеш-метка.

8. В поле **Действие** выбрать **STATS** и ввести имя счётчика: *TEMP_BLOCK*. Нажать кнопку **Добавить**. Это позволит отслеживать количество

срабатываний правила.

9. Добавить ещё одно действие: **DROP**.
   Все пакеты с валидной меткой **2** будут отброшены.
   Нажать зелёную кнопку **Добавить**, чтобы сохранить правило в список.
10. Необходимо переместить четвёртое правило в начало списка правил (сделать его первым). Это обеспечивает приоритетную фильтрацию пакетов, уже помеченных **HMARK id 2**, без повторной проверки всех условий, заданных ниже. Такое расположение позволяет сразу отбрасывать трафик, ранее идентифицированный как превышающий лимит, минимизируя нагрузку на последующую обработку.
11. Нажать жёлтую кнопку **Применить** в левой части интерфейса. Только после этого правила начнут применяться к трафику.



Совпадения

В системе Dosgate каждая проверка совпадения содержит один или несколько аргументов, настраиваемых пользователем. Для всех совпадений предусмотрена возможность включения флага **NOT**, реализованного в виде переключателя. **NOT** — логическая операция отрицания, при активации которой условие совпадения инвертируется: правило сработает для всех значений, кроме указанного.

dport - Порт получателя

Параметр	Описание
port	Номер порта, для которого применяется правило (диапазон от 0 до 65535)

dst - IP получателя

Параметр	Описание
IP-маска	Префикс, для которого применяется правило (Если маска подсети не указана, по умолчанию будет применена маска /32)

hmark - Метка для IP-отправителя

Параметр	Варианты	Описание
id		Идентификатор метки (диапазон от 1 до 255)
status		Состояние метки. Возможные значения:
	expired	Метка существует, но срок действия истёк
	valid	Метка активна, срок действия не истёк
age_op		Оператор сравнения для времени жизни метки:
	bw	Между двумя значениями
	eq	Равно указанному значению
	gt	Больше указанного значения
	lt	Меньше указанного значения
	null	Сравнение по времени не выполняется
age_value		Время жизни метки (например, 1200 секунд или диапазон 5m-10m)
value		Числовое значение метки, присвоенной пакету ранее с помощью действия **HMARK**

port - Порт отправителя и получателя

Параметр	Описание
port	Номер порта, для которого применяется правило (диапазон от 0 до 65535)

protocol - Протокол

Протокол	Описание
ipv4	Протокол интернета версии 4
ipv6	Протокол интернета версии 6
tcp	Протокол управления передачей (Transmission Control Protocol)
udp	Протокол пользовательских дейтаграмм (User Datagram Protocol)
ah	Протокол аутентификации заголовков (Authentication Header)
esp	Протокол безопасности IP (Encapsulating Security Payload)
eth	Протокол Ethernet
gre	Протокол инкапсуляции (Generic Routing Encapsulation)
icmp	Протокол управления интернет-сообщениями (Internet Control Message Protocol)
icmpv6	Версия ICMP для IPv6
ipip	Протокол туннелирования IP-в-IP, используется для инкапсуляции одного IP-пакета в другой
net	Группа протоколов сетевого уровня: включает *ipv4*, *ipv6*
sctp	Протокол управления потоками сообщений (Stream Control Transmission Protocol)
sec	Группа протоколов (IPsec): включает *ah*, *esp*
transport	Группа протоколов транспортного уровня: включает *tcp*, *udp*, *sctp*, *icmp*
tun	Группа туннельных протоколов: включает *gre*, *ipip*
tun_ah	Протокол *ah* с туннелированным заголовком
tun_esp	Протокол *esp* с туннелированным заголовком
tun_ipv4	Протокол *ipv4* с туннелированным заголовком
tun_ipv6	Протокол *ipv6* с туннелированным заголовком
tun_net	Группа протоколов сетевого уровня с туннелированным заголовком
tun_sec	Группа протоколов sec с туннелированным заголовком
vlan	Тегированный трафик

sport - Порт отправителя

Параметр	Описание
port	Номер порта, для которого применяется правило (диапазон от 0 до 65535)

verdict - Вердикт для предыдущего алгоритма

Тип	Значение	Описание
rate		Результат оценки текущей скорости трафика
	conform	Скорость не превышает заданное пороговое значение, соответствие норме
	cooldown	Сработал период охлаждения после зафиксированной перегрузки, трафик временно не считается превышающим
	exceed	Скорость превышена, текущий трафик нарушает установленный лимит
ratelimit		Результат проверки соблюдения ограничений скорости передачи битов или пакетов
	conform	Передача данных укладывается в установленные пределы
	cooldown	Включён период восстановления после превышения, трафик временно допускается
	exceed	Превышен первый порог (1-rate), допустим только краткосрочный допуск
	violate	Превышен второй порог (2-rate), нарушение лимита требует блокировки
sample		Результат применения механизма выборки трафика
	match	Пакет выбран согласно параметрам выборки
	skip	Пакет исключён из выборки, не обрабатывается по текущему правилу
tcpauth		Результат проверки подлинности TCP-пакета
	valid	TCP-пакет успешно аутентифицирован, подпись валидна
	invalid	TCP-пакет не прошёл проверку подлинности, подпись некорректна
	ignored	TCP-пакет не может быть аутентифицирован

connmark - Метка для соединений

Параметр	Варианты	Описание
id		Идентификатор метки (диапазон от 1 до 255)
status		Состояние метки. Возможные значения:

Параметр	Варианты	Описание
	expired	Метка существует, но срок действия истёк
	valid	Метка активна, срок действия не истёк
age_op		Оператор сравнения для времени жизни метки:
	bw	Между двумя значениями
	eq	Равно указанному значению
	gt	Больше указанного значения
	lt	Меньше указанного значения
	null	Сравнение по времени не выполняется
age_value		Время жизни метки (например, 1200 секунд или диапазон 5m-10m)
value		Числовое значение метки, присвоенной пакету ранее с помощью действия **CONNMARK**

dhmark - Метка для IP-получателя

Параметр	Варианты	Описание
id		Идентификатор метки (диапазон от 1 до 255)
status		Состояние метки. Возможные значения:
	expired	Метка существует, но срок действия истёк
	valid	Метка активна, срок действия не истёк
age_op		Оператор сравнения для времени жизни метки:
	bw	Между двумя значениями
	eq	Равно указанному значению
	gt	Больше указанного значения
	lt	Меньше указанного значения
	null	Сравнение по времени не выполняется
age_value		Время жизни метки (например, 1200 секунд или диапазон 5m-10m)
value		Числовое значение метки, присвоенной пакету ранее с помощью действия **DHMARK**

frag - Фрагмент сетевого уровня

Параметр	Описание
any	Соответствует любому фрагменту (первому, промежуточному или последнему)
df	Только пакеты с флагом *Don't Fragment* (IPv4)
first	Только первый фрагмент
internal	Только промежуточные фрагменты (не первый и не последний)
last	Только последний фрагмент
unfrag	Только целые (нефрагментированные) пакеты

geoip - Географическая БД для IP

Параметр	Варианты	Описание
Сверяем		Определяет, какой IP-адрес использовать для географической проверки:
	src	IP-адрес источника
	dst	IP-адрес назначения
country		Фильтрация по стране
continent		Фильтрация по континенту

icmp - Типы и коды ICMP

- **icmp type** — определение типа сообщения.
- **icmp code** — уточнение подтипа (если указано).

icmp type	icmp code	Описание
alt_addr		Сообщение ICMP об альтернативном адресе назначения
converr		Ошибка преобразования дейтаграммы при конвертации протоколов
echo_reply		Ответ на ICMP-запрос эха (проверка доступности узла)
echo_request		Запрос эха ICMP (диагностика доступности узлов)
ex		Превышено время жизни пакета (TTL)
defrag		Время ожидания сборки фрагментов превышено
ttl		Время жизни (TTL) истекло при транзите

icmp type	icmp code	Описание
info_reqply		Ответ на запрос информации об узле
info_request		Запрос информации об узле
ipv6_hia		Уведомление "Я здесь" (IPv6)
ipv6_way		Запрос "Где ты?" (IPv6)
mask_reply		Ответ ICMP с маской подсети
mask_request		Запрос маски подсети
mob_redir		Перенаправление пакетов мобильному хосту
mob_reg_reply		Ответ на регистрацию мобильного узла
mob_reg_request		Запрос на регистрацию мобильного узла
mobexp		Экспериментальные протоколы мобильности
name_reply		Ответ с доменным именем
name_request		Запрос доменного имени
param		Ошибка параметров заголовка IP-пакета
	len	Недопустимая длина заголовка
	opt	Отсутствует обязательная опция
	ptr	Указатель ссылается на некорректное значение
photuris		Ошибка механизма Photuris (безопасность обмена ключами)
quench		Уведомление об уменьшении скорости передачи
ra		Реклама маршрутизатора
redirect		Переадресация пакета на другой шлюз
	host	Переадресация для конкретного хоста
	net	Переадресация в пределах сети
	tos_host	Переадресация с учетом класса обслуживания и хоста
	tos_net	Переадресация с учетом класса обслуживания и сети
rs		Запрос маршрутизатора для обнаружения шлюза
skip_discover		Сообщение обнаружения SKIP
trace		ICMP-сообщение трассировки пути пакета
ts		Запрос временной метки
ts_reply		Ответ на временную метку
unreach		Пункт назначения недостижим

icmp type	icmp code	Описание
	frag	Требуется фрагментация, но установлен флаг DF
	host	Хост назначения недоступен
	hpv	Нарушение приоритета хоста
	iso_host	Изоляция источника
	net	Сеть назначения недоступна
	pc	Достигнут предел приоритета
	port	Порт назначения недоступен
	pr	Доступ запрещён администратором
	pr_host	Доступ к хосту запрещён
	pr_net	Доступ к сети запрещён
	proto	Протокол назначения недоступен
	sr	Сбой маршрутизации по заданному маршруту
	tos_host	Хост недоступен по классу обслуживания
	tos_net	Сеть недоступна по классу обслуживания
	unk_host	Хост назначения неизвестен
	unk_net	Сеть назначения неизвестна
xecho_reply		Расширенный ответ на эхо-запрос
	bad	Некорректный запрос
	intf	Нет интерфейса для ответа
	mult	Найдено несколько интерфейсов
	ok	Запрос выполнен успешно
	tbl	Таблица маршрутизации не содержит записи
xecho_request		Расширенный эхо-запрос с дополнительной информацией

icmp6 - Типы и коды ICMPv6

Тип сообщения	Название	Описание
cpa	Certification Path Advertisement	Используется для распространения информации о сертификационном пути
cps	Certification Path Solicitation	Применяется для запроса сертификационного пути
echo_reply	Echo Reply	Ответ на ICMPv6-эхо-запрос, применяется для диагностики сетевой доступности

Тип сообщения	Название	Описание
echo_request	Echo Request	Отправляется для проверки доступности узла (аналог ping)
ex	Time Exceeded	Генерируется при превышении времени жизни (Hop Limit) пакета
hadd_reply	Home Agent Address Discovery Reply	Ответ с адресом домашнего агента в мобильной IPv6-сети
hadd_request	Home Agent Address Discovery Request	Запрос адреса домашнего агента
inda	Inverse Neighbor Discovery Advertisement	Ответ, содержащий IPv6-адрес, связанный с MAC-адресом
inds	Inverse Neighbor Discovery Solicitation	Запрос IPv6-адреса по MAC-адресу
iniq	ICMP Node Information Query	Запрос информации об узле (например, hostname или адреса)
inir	ICMP Node Information Response	Ответ с запрошенной информацией об узле
mld	Multicast Listener Done	Оповещение о выходе из multicast-группы
mlq	Multicast Listener Query	Запрос о наличии подписчиков multicast-группы
mlr1	Version 1 Multicast Listener Report	Отчет о подписке на multicast-группу (версия 1)
mlr2	Version 2 Multicast Listener Report	Отчет о подписке на multicast-группу (версия 2)
mobexp	Experimental mobility protocols	Используется в экспериментальных протоколах мобильности
mpa	Mobile Prefix Advertisement	Реклама IPv6-префикса для мобильных узлов
mps	Mobile Prefix Solicitation	Запрос префикса у маршрутизатора мобильной сети
mra	Multicast Router Advertisement	Служебное сообщение для объявления маршрутизатора multicast
mrs	Multicast Router Solicitation	Запрос на обнаружение multicast-маршрутизаторов
mrt	Multicast Router Termination	Уведомление об отключении функции multicast-маршрутизатора
na	Neighbor Advertisement	Ответ на Neighbor Solicitation, содержит MAC-адрес узла
ns	Neighbor Solicitation	Используется для определения MAC-адреса по IPv6

Тип сообщения	Название	Описание
param	Parameter Problem	Указывает на ошибки в заголовке IPv6-пакета
ra	Router Advertisement	Используется маршрутизаторами для объявления себя в сети
redir	Redirect	Информирует хост об оптимальном маршруте к назначению
rr	Router Renumbering	Используется для перенумерации адресов маршрутизатора
rs	Router Solicitation	Запрос маршрутизатора для получения RA-сообщений
toobig	Packet Too Big	Указывает, что пакет превышает максимально допустимый размер MTU
unreach	Destination Unreachable	Уведомление о невозможности доставки пакета до получателя

len - Длина пакета

Параметр	Варианты	Описание
len		Числовое значение в диапазоне 0–65535.
level		Элемент кадра для анализа:
	application	Анализ содержимого данных приложений (HTTP, DNS и другие L7-протоколы)
	encap	Анализ инкапсуляции (PPPoE, MPLS и др.)
	mac	Анализ MAC-адресов и полей Ethernet-заголовка
	net	Анализ IP-заголовков (адреса, TTL, протокол)
	sec	Анализ IPSec (заголовки AH/ESP, параметры шифрования)
	transport	Анализ транспортных заголовков (TCP/UDP порты, флаги)
	tun	Анализ заголовков туннелирования
	tun_net	Анализ IP-заголовков внутри туннеля
	tun_sec	Анализ IPSec в туннелированном трафике
	vlan	Анализ VLAN-тегов
elm		Определяет конкретную часть сетевого кадра/пакета для анализа:
	header	Только заголовков пакета
	packet	Всего пакета целиком

Параметр	Варианты	Описание
	payload	Только полезной нагрузки

mark - Локальная метка на пакет

Параметр	Описание
value	Числовое значение метки, присвоенной пакету ранее с помощью действия **MARK**

pset - Префикс-сет

Параметр	Варианты	Описание
name		Имя предопределенного набора адресов
class		Тип префикс-сета:
	local	Локальные префикс-сеты
	global	Глобальные префикс-сеты
what		Какое поле анализировать:
	src	Адрес источника
	dst	Адрес назначения
value		Числовое значение или диапазон

sdhmark - Метка для IP отправителя и получателя

Параметр	Варианты	Описание
id		Идентификатор метки (диапазон от 1 до 255)
status		Состояние метки. Возможные значения:
	expired	Метка существует, но срок действия истёк
	valid	Метка активна, срок действия не истёк
age_op		Оператор сравнения для времени жизни метки:
	bw	Между двумя значениями
	eq	Равно указанному значению
	gt	Больше указанного значения

Параметр	Варианты	Описание
	lt	Меньше указанного значения
	null	Сравнение по времени не выполняется
age_value		Время жизни метки (например, 1200 секунд или диапазон 5m-10m)
value		Числовое значение метки, присвоенной пакету ранее с помощью действия **SDMARK**

seq - Последовательность байтов

Параметр	Варианты	Описание
level		Элемент кадра для анализа:
	application	Анализ содержимого данных приложений (HTTP, DNS и другие L7-протоколы)
	encap	Анализ инкапсуляции (PPPoE, MPLS и др.)
	mac	Анализ MAC-адресов и полей Ethernet-заголовка
	net	Анализ IP-заголовков (адреса, TTL, протокол)
	sec	Анализ IPSec (заголовки AH/ESP, параметры шифрования)
	transport	Анализ транспортных заголовков (TCP/UDP порты, флаги)
	tun	Анализ заголовков туннелирования
	tun_net	Анализ IP-заголовков внутри туннеля
	tun_sec	Анализ IPSec в туннелированном трафике
	vlan	Анализ VLAN-тегов
elm		Определяет конкретную часть сетевого кадра/пакета для анализа:
	header	Только заголовков пакета
	packet	Всего пакета целиком
	payload	Только полезной нагрузки
range		Диапазон байтов внутри полезной нагрузки пакета, в пределах которого осуществляется поиск. По умолчанию: 0-1500 (начальная часть кадра/пакета)
repeat		Количество повторений искомой последовательности в пределах указанного диапазона. По умолчанию: 0 (повторение не проверяется)
distance		Минимальное расстояние в байтах между повторяющимися

Параметр	Варианты	Описание
		вхождениями последовательности (если указан repeat)
seq		ASCII-строка для поиска в теле пакета. Поиск по декодированному содержимому (аналогично Wireshark)
b64seq		Строка в Base64, представляющая последовательность как в seq, но закодированную. Для точного соответствия бинарным данным или нестандартной кодировке

spi - IPSec SPI

Параметр	Описание
spi	Числовое значение или диапазон

src - IP отправителя

Параметр	Описание
IP-маска	Префикс, для которого применяется правило (Если маска подсети не указана, по умолчанию будет применена маска /32)

tcpflags - TCP Flags

- **flags** - список TCP-флагов, которые должны быть установлены в пакете (со значением 1). Указываются через запятую в левой части выражения.
- **mask** — список флагов, по которым производится сравнение (в правой части выражения). Если флаг указан в маске, то он обязательно проверяется: его наличие или отсутствие должно точно соответствовать соответствующему значению в flags.

Семантика работы следующая: каждый флаг из mask проверяется — если он присутствует в flags, то он должен быть установлен (равен 1), если отсутствует — то должен быть сброшен (равен 0).

Поддерживаются следующие TCP-флаги:

Флаг	Название	Описание
ack	Acknowledgement	Флаг подтверждения

Флаг	Название	Описание
all	All	Все флаги одновременно
cwr	Congestion Window Reduced	Флаг уменьшения окна перегрузки
ece	ECN Echo	Флаг ECN-Echo
fin	Finish	Флаг завершения соединения
psh	Push	Флаг принудительной отправки данных
rst	Reset	Флаг аварийного разрыва соединения
syn	Synchronization	Флаг синхронизации
urg	Urgent	Флаг срочных данных

tcpmss - TCP Maximum Segment Size

Параметр	Описание
value	Числовое значение или диапазон от 1 до 4096

tcpopts - TCP опции

- **left side** — список TCP-опций, которые должны быть установлены. Указывается в левой части выражения, через запятую.
- **right side** — маска TCP-опций, по которым будет производиться проверка. Указывается в правой части выражения, через запятую.

Семантика работы следующая: каждая опция из right side проверяется — если она присутствует в left side, то она должен быть установлена (равна 1), если отсутствует — то должна быть сброшена (равна 0).

Поддерживаются следующие TCP-опции:

Опция	Назначение
ECHO	Запрос проверки соединения. Измерение задержки (RTT)
ECHO_REPLY	Ответ на Echo Request
EOL	Маркер конца списка опций TCP. Выравнивание опционного поля
MSS	Максимальный размер TCP-сегмента. Определяет размер принимаемых данных

Опция	Назначение
NOOP	Пустая опция-заполнитель. Не содержит полезных данных
SACK	Выборочное подтверждение. Отслеживание полученных блоков при потерях
SACK_PERMIT	Разрешение использования SACK. Только в SYN-пакетах
TIMESTAMP	Измерение времени доставки. Защита от повторных передач
WSCALE	Масштабирование окна приёма. Для высокоскоростных сетей

tcpws - TCP Window Scale

Параметр	Описание
value	Числовое значение или диапазон

tdst - IP-получателя в туннеле

Параметр	Описание
value	Префикс, для которого применяется правило (Если маска подсети не указана, по умолчанию будет применена маска /32)

tgeoip - GeoIP в туннеле

Параметр	Варианты	Описание
Сверяем		Определяет, какой IP-адрес использовать для географической проверки:
	src	IP-адрес источника
	dst	IP-адрес назначения
country		Фильтрация по стране
continent		Фильтрация по континенту

tpset - Префикс-сет в туннеле

Параметр	Варианты	Описание
name		Имя предопределенного набора адресов
class		Тип префикс-сета:
	local	Локальные префикс-сеты
	global	Глобальные префикс-сеты
what		Какое поле анализировать:
	src	Адрес источника
	dst	Адрес назначения
value		Числовое значение или диапазон

tspi - Tunnelled IPSec SPI

Параметр	Описание
spi	Числовое значение или диапазон

tsrc - IP-отправителя в туннеле

Параметр	Описание
value	Префикс, для которого применяется правило (Если маска подсети не указана, по умолчанию будет применена маска /32)

ttl - TTL пакета

Параметр	Описание
ttl	Числовое значение или диапазон от 1 до 255

Действия

ACCEPT

Разрешает прохождение пакета, передавая его на выход.

DROP

Немедленно отбрасывает пакет, прекращая его обработку.

HMARK

Устанавливает или модифицирует метку для IP-отправителя на основе заданной операции и параметров. Применяется для маркировки пакетов с целью дальнейшей классификации или маршрутизации.

Параметр	Варианты	Описание
id		Число в диапазоне 1-255
how		Действие с меткой:
	add	Добавить значение
	and	Побитовое И
	dec	Декремент
	div	Деление на указанное значение
	inc	Инкремент
	mult	Умножение на указанное значение
	not	Побитовая инверсия
	or	Побитовое ИЛИ
	restore	Восстановить сетевую метку из общей метки
	save	Сохранить сетевую метку в общую метку
	set	Установить метку
	sub	Вычесть значение
	xor	Побитовое исключающее ИЛИ
value		Числовое значение 0 до 2^{32}-1
lifetime		Время жизни метки в секундах. Если значение равно 0 или не указано — метка считается постоянной

RATELIMIT

Действие **RATELIMIT** применяется для ограничения частоты обработки пакетов по заданным ключам агрегации (bucket key). Позволяет задавать

предельные значения по количеству пакетов в секунду (PPS) и/или объёму данных (BPS), а также управлять поведением при превышении лимитов.

Параметр	Варианты	Описание
id		Числовой идентификатор
Bucket key		Ключ агрегации: Определяет, по какому признаку (или их совокупности) будут сгруппированыпакеты при учёте скорости
	Any match	Все пакеты обрабатываются в одном общем bucket-е, без разделения
	l3_dst	По IP-адресу назначения
	l3_src	По IP-адресу источника
	l3_proto	По протоколу L3 (IPv4, IPv6)
	l3_tun_dst	По адресу назначения туннелированного L3
	l3_tun_src	По адресу источника туннелированного L3
	l3_tun_proto	По протоколу туннелированного L3
	l4_dst	По порту назначения
	l4_src	По порту источника
	l4_proto	По протоколу L4 (TCP, UDP)
	sec_id	По идентификатору IPsec
	sec_proto	По протоколу IPsec
	sec_tun_id	По SPI туннелированного трафика
	sec_tun_proto	По протоколу туннелированного IPsec
	tun_id	По ID туннеля
	tun_proto	По протоколу туннеля
cooldown		Интервал восстановления (в секундах). Время, в течение которого, после превышения лимита, новое срабатывание ограничения по данному bucket-ключу невозможно.
pps		Ограничение по количеству пакетов в секунду:
	rate	Максимальное количество пакетов в секунду (PPS)
	burst	Допустимый всплеск в миллисекундах. В течение указанного времени может быть превышен лимит rate, после чего срабатывает ограничение.
bps		Ограничение по объёму трафика (бит в секунду):

Параметр	Варианты	Описание
	rate	Предельная скорость передачи данных в битах в секунду (BPS)
	burst	Допустимое превышение в миллисекундах, В течение указанного времени может быть превышен лимит rate, после чего срабатывает ограничение

UH

Активирует сессионную защиту и анализ трафика на уровнях L3–L7. Выбор уровня определяет глубину проверки:

Параметр	Описание
L3-L4	Выполняется только отслеживание соединений (Connection Tracking); правила TLS и анализ L7 не применяются.
L3-L7	Выполняются все доступные проверки: от Connection Tracking до анализа TLS-пакетов

CAPTURE

Управляет захватом трафика с помощью dosgate-uh. Используется для сохранения копий трафика при выполнении конечного действия.

Параметр	Описание
on	Активирует захват трафика при достижении терминального действия
off	Отключает ранее назначенное действие захвата

CONNMARK

Устанавливает или модифицирует метку, связанную с TCP/UDP-соединением. Применяется для отслеживания состояния и последующей фильтрации пакетов в рамках одного соединения.

Параметр	Варианты	Описание
id		Число в диапазоне 1-255
how		Действие с меткой:

Параметр	Варианты	Описание
	add	Добавить значение
	and	Побитовое И
	dec	Декремент
	div	Деление на указанное значение
	inc	Инкремент
	mult	Умножение на указанное значение
	not	Побитовая инверсия
	or	Побитовое ИЛИ
	restore	Восстановить сетевую метку из общей метки
	save	Сохранить сетевую метку в общую метку
	set	Установить метку
	sub	Вычесть значение
	xor	Побитовое исключающее ИЛИ
value		Числовое значение 0 до 2^{32}-1
lifetime		Время жизни метки в секундах. Если значение равно 0 или не указано — метка считается постоянной

DHMARK

Присваивает метку, основанную на IP-адресе получателя. Используется для классификации трафика по адресу назначения.

Параметр	Варианты	Описание
id		Число в диапазоне 1-255
how		Действие с меткой:
	add	Добавить значение
	and	Побитовое И
	dec	Декремент
	div	Деление на указанное значение
	inc	Инкремент
	mult	Умножение на указанное значение
	not	Побитовая инверсия
	or	Побитовое ИЛИ

Параметр	Варианты	Описание
	restore	Восстановить сетевую метку из общей метки
	save	Сохранить сетевую метку в общую метку
	set	Установить метку
	sub	Вычесть значение
	xor	Побитовое исключающее ИЛИ
value		Числовое значение 0 до 2^{32}-1
lifetime		Время жизни метки в секундах. Если значение равно 0 или не указано — метка считается постоянной

DNAT

Выполняет Destination Stateless NAT — заменяет IP-адрес назначения в пакете без сохранения состояния соединения.

Параметр	Описание
prefix	Список IP-префиксов, разделённых запятыми, по одному на каждую поддерживаемую адресную семью (например, IPv4, IPv6)

DNSAUTH

Имитирует ответ DNS-сервера с установленным флагом **TC**, вынуждая отправителя повторить запрос по **TCP**.

EXPORT

Управляет экспортом трафика с помощью dosgate-uh. Применяется для передачи данных на внешний анализатор или систему хранения.

Параметр	Описание
on	Активирует захват трафика при достижении терминального действия
off	Отключает ранее назначенное действие захвата

GOTO

Выполняет передачу управления в чейн (другую цепь фильтрации).

Параметр	Описание
chain	Имя целевой цепи, в которую будет направлен пакет

MARK

Устанавливает метку (mark) непосредственно на обрабатываемый пакет. Может использоваться для последующей фильтрации или маршрутизации на основе значения метки.

Параметр	Варианты	Описание
how		Действие с меткой:
	add	Добавить значение
	and	Побитовое И
	dec	Декремент
	div	Деление на указанное значение
	inc	Инкремент
	mult	Умножение на указанное значение
	not	Побитовая инверсия
	or	Побитовое ИЛИ
	restore	Восстановить сетевую метку из общей метки
	save	Сохранить сетевую метку в общую метку
	set	Установить метку
	sub	Вычесть значение
	xor	Побитовое исключающее ИЛИ
value		Числовое значение 0 до 2^{32}-1

PASS

Операция PASS определяет правило передачи Ethernet-кадра либо в операционную систему, либо в сессионную защиту.

Параметр	Значение	Тип	Описание
to:			Направление передачи:
	os		Передача кадра в операционную систему

Параметр	Значение	Тип	Описание
	uh:		Передача кадра в сессионную защиту
		L3-L4	Выполняется только отслеживание соединений (Connection Tracking); правила TLS и анализ L7 не применяются
		L3-L7	Выполняются все доступные проверки: от Connection Tracking до анализа TLS-пакетов
vid			VLAN ID. Кадр передаётся в ОС только при совпадении указанного VLAN-тега с тегом в кадре
mac			MAC-адрес. Кадр передаётся в ОС только при совпадении MAC-адреса назначения с указанным

SDHMARK

Присваивает метку, основанную на IP-адресах как отправителя, так и получателя. Обеспечивает более точную идентификацию потоков трафика между конкретными хостами

Параметр	Варианты	Описание
id		Число в диапазоне 1-255
how		Действие с меткой:
	add	Добавить значение
	and	Побитовое И
	dec	Декремент
	div	Деление на указанное значение
	inc	Инкремент
	mult	Умножение на указанное значение
	not	Побитовая инверсия
	or	Побитовое ИЛИ
	restore	Восстановить сетевую метку из общей метки
	save	Сохранить сетевую метку в общую метку
	set	Установить метку
	sub	Вычесть значение

Параметр	Варианты	Описание
	xor	Побитовое исключающее ИЛИ
value		Числовое значение 0 до 2^{32}-1
lifetime		Время жизни метки в секундах. Если значение равно 0 или не указано — метка считается постоянной

SNAT

Выполняет Source Stateless NAT — заменяет IP-адрес источника в пакете без сохранения состояния соединения. Применяется для маскировки исходящего трафика.

Параметр	Описание
prefix	Список IP-префиксов, разделённых запятыми, по одному на каждую поддерживаемую адресную семью

STATS

Регистрирует статистику по обработанным пакетам. Используется для мониторинга, учёта и анализа трафика.

Параметр	Описание
name	Имя или числовой идентификатор счётчика, в который будут записаны данные

TCPAUTH

Операция **TCPAUTH** реализует механизм проверки TCP-соединений на этапе установления (SYN или SYN/ACK) с помощью одного из методов аутентификации. Результатом выполнения является вердикт *tcpauth valid* или *tcpauth invalid*, на основании которого принимается решение о дальнейшем прохождении трафика.

Параметр	Значение	Описание
id		Числовой идентификатор
syn		Метод аутентификации при получении TCP SYN:
	greylist	Сбрасывает все входящие пакеты от источника в течение

Параметр	Значение	Описание
		timeout, ожидая повторную попытку в интервале *window*
	hs	Полное TCP-рукопожатие. После успешного взаимодействия выносится вердикт *tcpauth valid*
	synack	В ответ на входящий SYN отправляется поддельный SYN-ACK. Источник должен корректно ответить RST. В случае правильной реакции — *tcpauth valid*
	none	Аутентификация не проводится
syn-ack		Метод аутентификации при получении SYN-ACK (реверсивная проверка):
	greylist	Сбрасывает все входящие пакеты от источника в течение *timeout*, ожидая повторную попытку в интервале *window*
	hs	Полное TCP-рукопожатие
	none	Аутентификация не проводится
timeout		Время ожидания завершения аутентификации. Если в течение этого времени клиент не проходит проверку, соединение признаётся неуспешным, выдаётся *tcpauth invalid*
window		Период, в течение которого ожидается повторный пакет от источника, успешно прошедшего аутентификацию

VERDICT

Изменяет общее значение вердикта действия для всех пакетов проходящих через правило

Тип	Значение	Описание
op		Операция с вердиктом
	clear	Сброс ранее установленного вердикта; используется для удаления текущего значения вердикта
	set	Устанавливает заданное значение вердикта; требует обязательного указания параметра value
rate		Результат оценки текущей скорости трафика
	conform	Скорость не превышает заданное пороговое значение, соответствие норме
	cooldown	Сработал период охлаждения после зафиксированной перегрузки,

Тип	Значение	Описание
		трафик временно не считается превышающим
	exceed	Скорость превышена, текущий трафик нарушает установленный лимит
ratelimit		Результат проверки соблюдения ограничений скорости передачи битов или пакетов
	conform	Передача данных укладывается в установленные пределы
	cooldown	Включён период восстановления после превышения, трафик временно допускается
	exceed	Зафиксировано превышение хотя бы одного из установленных лимитов (1-rate или 2-rate). Допускается краткосрочная передача трафика
	violate	Превышены оба установленных лимита (1-rate и 2-rate). Требуется блокировка трафика
sample		Результат применения механизма выборки трафика
	match	Пакет выбран согласно параметрам выборки
	skip	Пакет исключён из выборки, не обрабатывается по текущему правилу
tcpauth		Результат проверки подлинности TCP-пакета
	valid	TCP-пакет успешно аутентифицирован, подпись валидна
	invalid	TCP-пакет не прошёл проверку подлинности, подпись некорректна

Чейны

Чейны— это отдельная ветка правил, используемая для обработки и фильтрации сетевого трафика. Она представляет собой набор правил, определяющих порядок обработки пакетов.

Чейны используются для выборочного применения механизмов защиты в режиме постоянного трафика через DosGate. Это позволяет избежать непрерывной активации защитных мер, таких как TCP-аутентификация и другие контрмеры, которые могут негативно повлиять на легитимный трафик.

По своей структуре чейны аналогичны стандартным правилам фильтрации: в них можно задавать условия обработки пакетов, а также использовать готовые пресеты для унификации и удобства настройки.

Принцип работы

- Основной профиль содержит базовый набор правил обработки пакетов.
- В зависимости от условий, заданных в профиле, пакеты могут быть перенаправлены в определённый чейн.
- В чейне хранятся дополнительные правила, которые выполняются только для перенаправленных пакетов.
- Это позволяет изолировать специфические механизмы защиты и включать их только при превышении заданных порогов, минимизируя влияние на легитимный трафик.

Пример использования чейна на примере фильтрации трафика по географическому признаку

Рассмотрим работу чейна на примере разделения трафика по стране-источнику.

1. Анализ входящего трафика
   При поступлении пакета система анализирует его source-адрес и определяет страну-источник с использованием базы GeoIP.
2. Сопоставление с правилами профиля и перенаправление в чейн
   В профиле настроено правило, проверяющее, принадлежит ли трафик России. Если условие не выполняется, срабатывает действие **GOTO**, перенаправляющее пакет в отдельный чейн "Not-RU". Это логически изолированный блок правил, применяемых только к данному типу трафика.
3. Применение строгих политик фильтрации Внутри чейна "Not-RU" могут быть настроены дополнительные механизмы защиты, например:
   - Ограничение количества соединений с одного IP (rate limit).
   - Фильтрация по протоколам (например, блокировка UDP-амплификаций).
   - Блокировка трафика с известных вредоносных IP.
4. Принятие вердикта

Если пакет соответствует критериям блокировки, он отбрасывается. Если пакет проходит фильтры, он возвращается в основной профиль и продолжает обработку.

Роутер

Роутер — это IP-адрес или префикс, определяющий, к какому профилю будет применяться входящий трафик.

DosGate выполняет маршрутизацию пакетов внутри системы, сравнивая ip-адрес назначения в пакете с значением роутера. На основе этого сравнения принимается решение о том, в какой профиль следует направить трафик для дальнейшей обработки.

Роутеры могут быть настроены для маршрутизации как отдельных **IP-адресов, так и целых подсетей с различными масками**, что позволяет гибко управлять фильтрацией.

Принцип работы

1. Обнаружение интерфейса
    - Входящий трафик сначала попадает на интерфейс системы.
    - Интерфейсы могут быть сгруппированы в **арены**, которые представляют собой логические объединения интерфейсов.
2. Анализ назначения трафика
    - После определения интерфейса система анализирует destination-адрес пакета.
    - Далее ищется соответствующий роутер в профилях DosGate, где указана сеть или конкретный IP-адрес, совпадающий с адресом назначения пакета.
3. Выбор наилучшего совпадения

> Если в системе определено несколько роутеров для одной сети, выбирается наиболее специфичный (с наибольшей маской). Например, если присутствуют два роутера:

- 185.66.86.0/24
- 185.66.86.36/32

Трафик, адресованный **185.66.86.36**, будет направлен в профиль, содержащий роутер **185.66.86.36/32**, так как он более специфичен. Остальной трафик сети **185.66.86.0/24** будет обрабатываться в профиле с роутером **/24**.

Метки

Метки – это быстрые таблицы данных, предназначенные для временной фиксации информации о сетевых пакетах и соединениях. Они используются для управления трафиком, выявления угроз и отладки правил фильтрации.

Типы меток

Система поддерживает следующие типы меток:

- **HMARK** — фиксирует адрес источника.
- **DHMARK** — фиксирует адрес назначения.
- **SDHMARK** — фиксирует адрес источника и назначения.
- **CONNMARK** — фиксирует полный 5-tuple соединения: IP-адрес источника и назначения, порты источника и назначения, транспортный протокол (L4).
- **HMARKC** — административная метка для создания чёрных и белых списков. Префиксы вводятся вручную и не зависят от правил фильтрации.

Поля записи метки

- **ID** — идентификатор записи.
- **Value** — числовой счётчик, управляемый правилами.
- **Age** — время, прошедшее с момента добавления записи.
- **Lifetime** — время до истечения записи. Обновляется при поступлении подходящих пакетов. Когда срок заканчивается, запись получает статус **expired**.

Принцип работы

Исключение
Механизм ниже не применяется к **HMARKC**.

Создание метки

Когда срабатывает правило, система создаёт запись с параметрами трафика, характерными для конкретного типа метки.

Применение метки в правилах

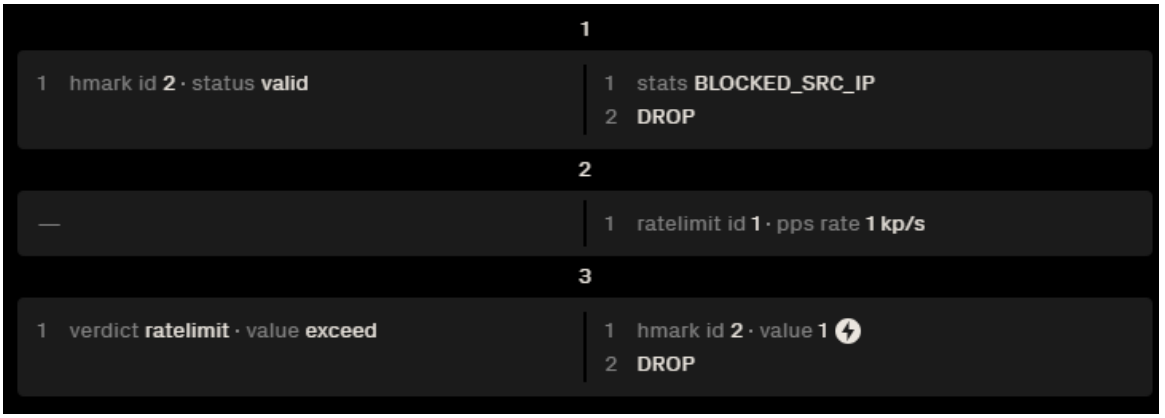
Для каждого нового пакета система проверяет, есть ли подходящая активная метка. Если метка найдена и она валидна, правило может применить действие: блокировку, перенаправление или другое требуемое поведение.

Обновление и удаление

При повторных нарушениях lifetime продлевается. Метка остаётся активной дольше. Когда срок истекает, метка автоматически удаляется. При необходимости её можно удалить вручную.

Пример использования HMARK

Сценарий: временная блокировка IP-адреса при превышении пороговой интенсивности пакетов.



Шаг 1. Блокировка по уже активной метке

Если у источника уже есть валидная метка в **HMARK id 2**, пакет сразу отбрасывается. Система фиксирует событие в статистике и завершает обработку.

Шаг 2. Измерение интенсивности

Если метки нет, система начинает измерять частоту пакетов. Порог — 1000 pps от одного источника.

Шаг 3. Реакция на превышение порога

При превышении порога создаётся запись в **HMARK id 2**. Текущие пакеты отбрасываются.

Жизненный цикл

Пока запись **HMARK id 2** валидна, трафик блокируется на шаге 1. После истечения lifetime измерения возобновляются. При повторном превышении порога создаётся новая запись и блокировка обновляется

Пример использования CONNMARK

Сценарий: временная блокировка TCP/UDP-сессий при превышении порога трафика.

Шаг 1. Блокировка по уже активной метке

Если у источника уже есть валидная метка в **CONNMARK id 111**, пакет сразу отбрасывается. Система фиксирует событие в статистике и завершает обработку.

Шаг 2. Измерение интенсивности

Если метки нет, система начинает считать пакеты для каждого соединения отдельно. Соединение определяется:

- l3_proto — IPv4 или IPv6
- l3_src и l3_dst — IP-адрес источника и назначения
- l4_proto — TCP или UDP
- l4_src и l4_dst — порт источника и назначения

Порог — 10 000 pps на одно соединение.

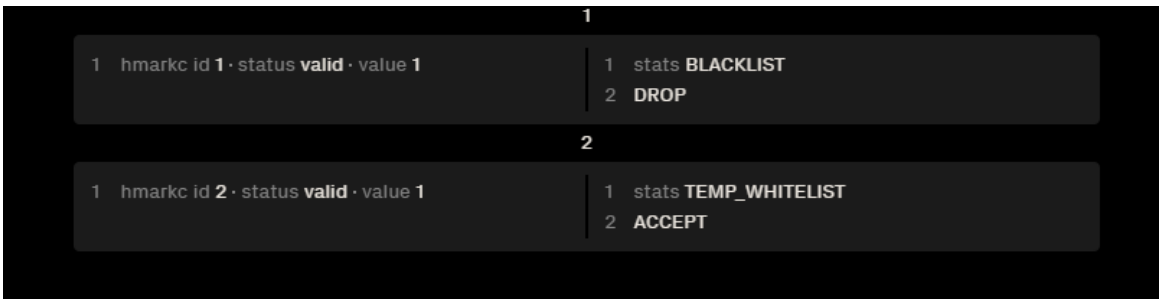
Шаг 3. Реакция на превышение порога

При превышении порога создаётся запись в **CONNMARK id 111** на 600 секунд. Текущий пакет и следующие отбрасываются шагом 1.

Жизненный цикл

Пока метка **CONNMARK id 111** активна, трафик блокируется на шаге 1 без повторных измерений. Когда lifetime истекает, пакеты снова проходят шаг 2. Если порог превышается, система обновляет метку и возвращает блокировку.

Пример использования HMARKC



Сценарий: адресное управление трафиком по заранее заданным префиксам.

Шаг 1. Добавление префикса

В разделе **Метки** создать новую метку **HMARKC** и добавить нужные префиксы.

Шаг 2. Применение в правилах

В условии совпадения выбрать **HMARKC** и задать действие:

- **DROP** — блокирует трафик указанных адресов. Правило работает как чёрный список.
- **ACCEPT** — пропускает трафик без дальнейшей фильтрации. Используется как белый список.

Жизненный цикл
Метка **HMARKC** управляется вручную. Автоматическое создание и продление **Lifetime** правилами не поддерживается.

Пример использования счётчика Value

Value помогает фиксировать повторные нарушения и усиливать реакцию системы при эскалации.

Первое срабатывание
При первом превышении порога создаётся метка **HMARK** со значением *value = 1*.

Повторные нарушения
Каждое новое превышение для того же источника увеличивает значение: *value = 2*, *value = 3* и далее.

Эскалация
Когда значение достигает порога источник можно обработать жёстче: добавить в префикс-сет или применить отдельное блокирующее правило.

Пример
10.0.0.1 отправил **600 TCP SYN-пакетов** → создаётся **HMARK** *value = 1*.
Через **100 секунд** тот же адрес отправил **700 пакетов** → *value = 2*.
Следующее превышение → *value = 3*, после чего источник блокируется через префикс-сет или соответствующее правило.

Префикс-сеты

Префикс-сет представляет собой набор IP-адресов, аналогичный списку управления доступом (ACL). Используется при создании правил для формирования белых и черных списков.

Префикс-сеты делятся на:

- **Глобальные** – распространяются на всю арену и используются во всех профилях.
- **Локальные** – применяются только в рамках конкретного профиля.

Добавление префикс-сета

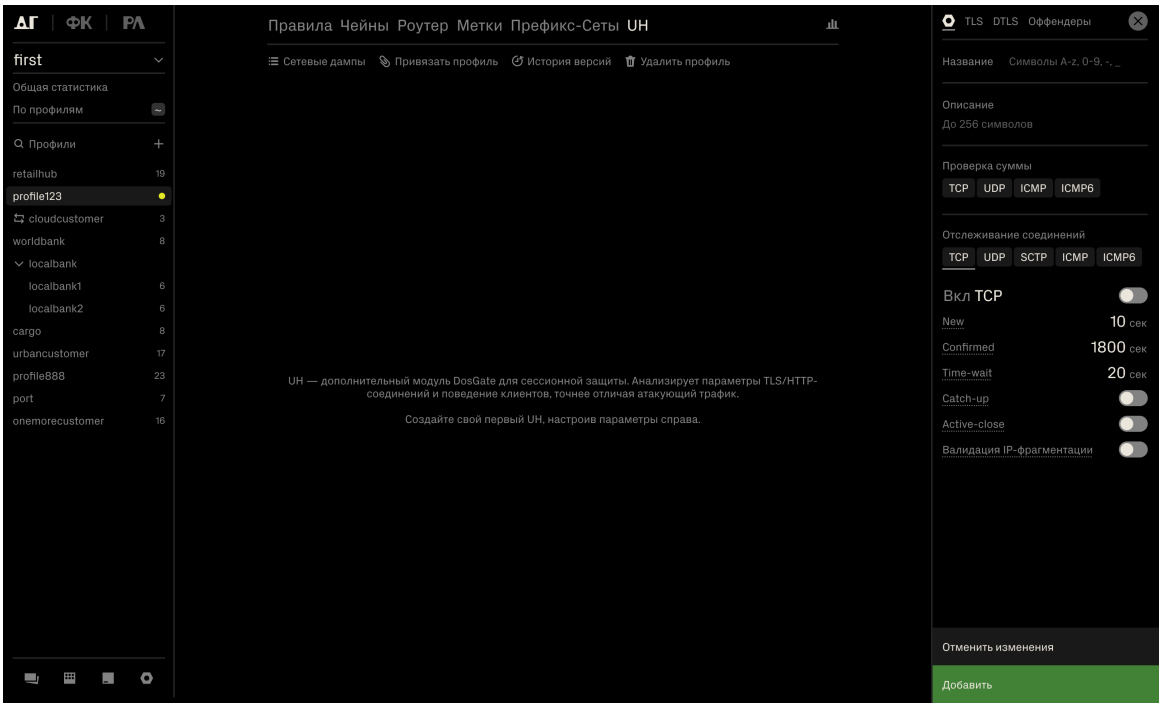
Сессионная защита

Принцип работы

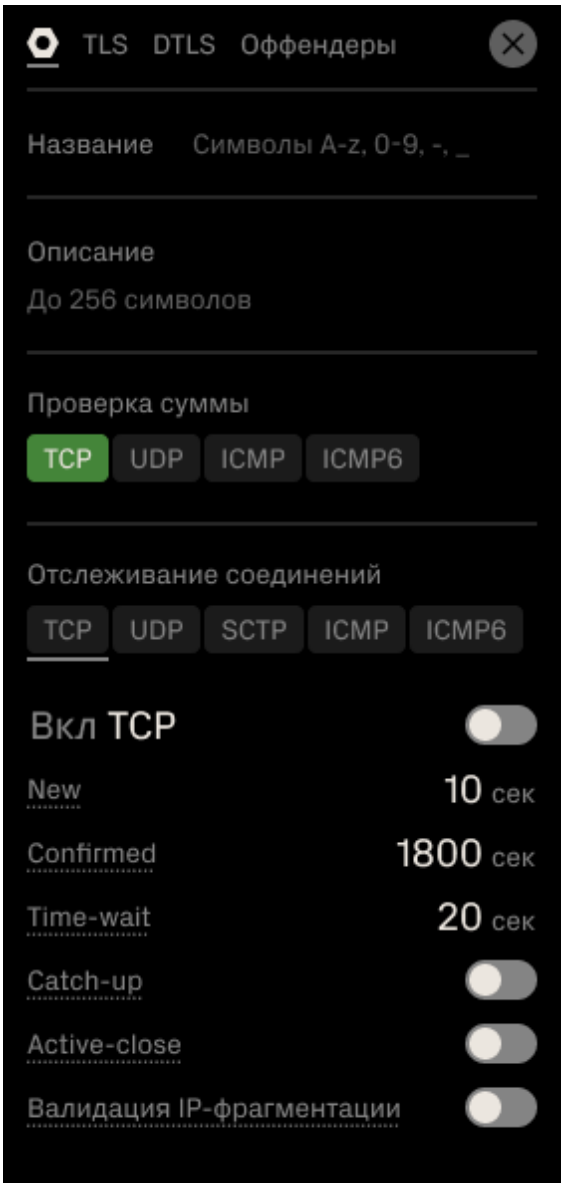
Сессионная защита анализирует сетевые соединения и параметры TLS/DTLS-рукопожатий (SNI, ALPN, JA3/JA4, наборы шифров). При обнаружении аномалий трафику назначается метка для последующей блокировки на сетевом уровне, что позволяет отсекать подозрительные соединения до глубокого анализа и снижать нагрузку на DosGate.

Настройка в веб-интерфейсе

При первом открытии раздела **UH** отображается пустая рабочая область. Справа расположена панель параметров для создания первой конфигурации.



Панель настройки параметров:



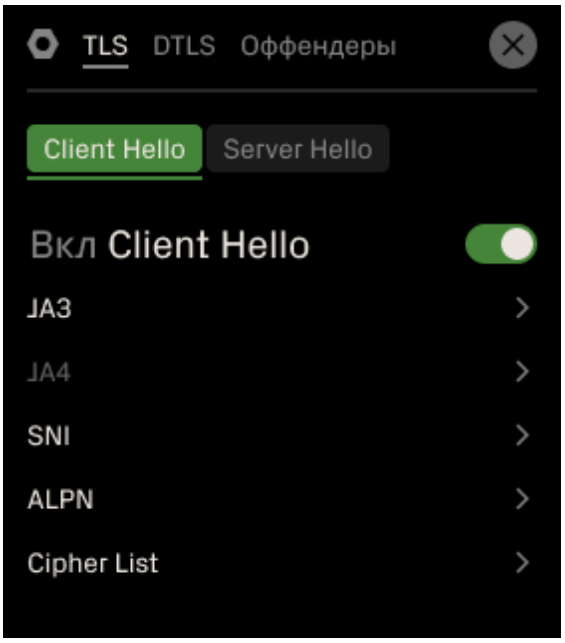
- **Название**: Указать имя конфигурации.
- **Описание**: Задать произвольное описание конфигурации.
- **Проверка контрольных сумм**: Включить проверку контрольных сумм для выбранных протоколов: TCP, UDP, ICMP, ICMPv6.
- **Отслеживание соединений**: Задать параметры сессионного отслеживания для протоколов TCP, UDP, SCTP, ICMP и ICMPv6. Активный протокол выделяется зеленым цветом, неактивные — серым.
  - **New** — ожидание установления неподтверждённого соединения (по умолчанию 10 секунд).
  - **Confirmed** — время жизни подтверждённого соединения (по умолчанию 1800 секунд).
  - **Time-wait** — ожидание полного закрытия соединения (по умолчанию 20 секунд).

- **Catch-up** — синхронизация состояний соединений при запуске сессионной защиты.
- **Active-close** — принудительное закрытие соединений при остановке сессионной защиты или при наступлении заданных условий.
- **Валидация IP-фрагментации** — проверять корректность фрагментированных IP-пакетов.

TLS и DTLS

Разделы **TLS** и **DTLS** предназначены для настройки анализа и обработки защищённого трафика. Они позволяют контролировать и идентифицировать сетевые соединения по параметрам TLS- и DTLS-рукопожатий.

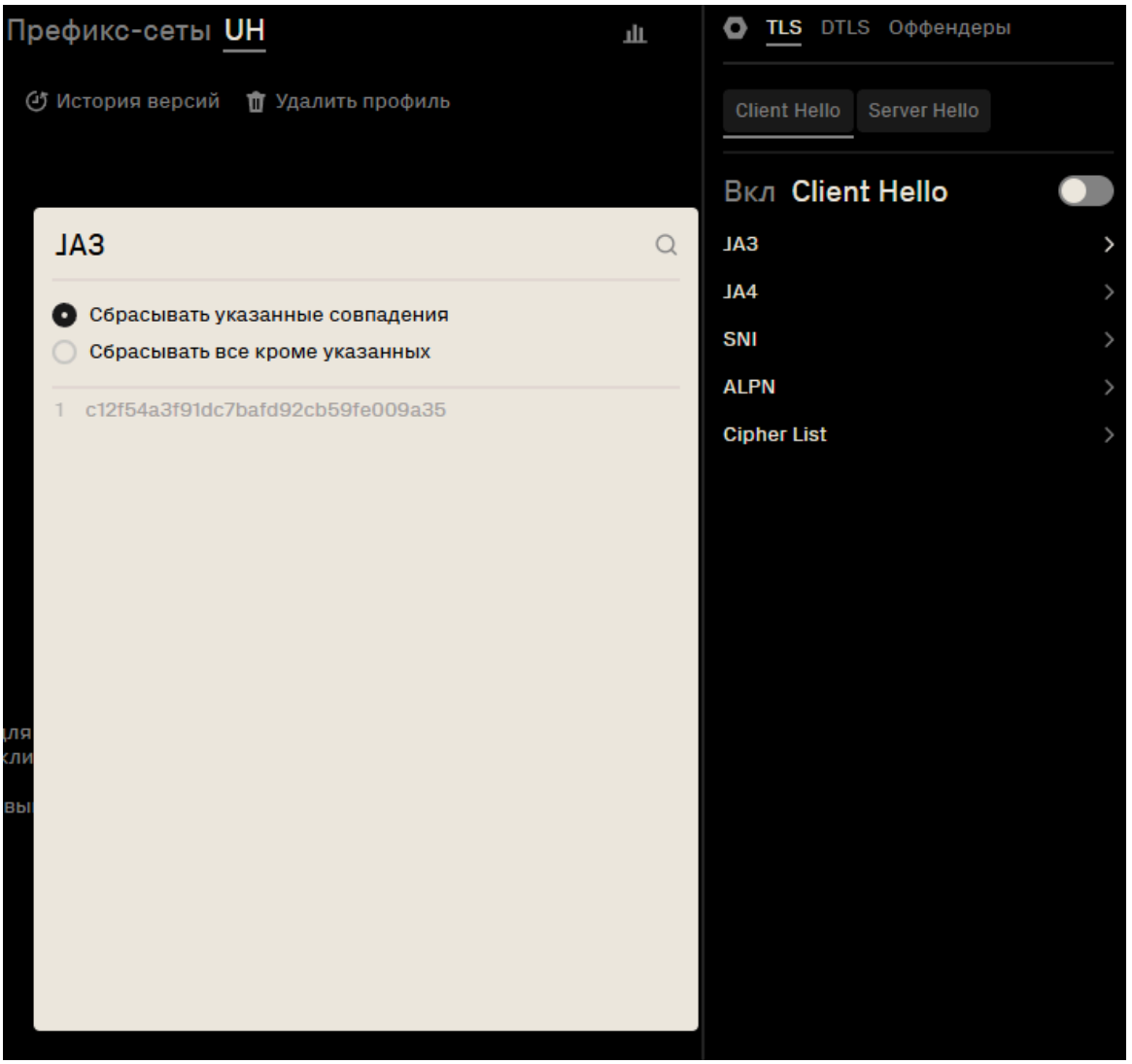
- **TLS** — используется для контроля защищённых потоковых соединений поверх TCP (например, веб-трафик).
- **DTLS** — используется для контроля защищённых датаграммных соединений поверх UDP (например, VoIP, видеоконференции и другие сервисы, чувствительные к задержкам).



- **Client Hello** — анализируются параметры ClientHello, исходящие от клиента.
- **Server Hello** — анализируются параметры ServerHello, исходящие от сервера.

Для включения анализа использовать соответствующий переключатель.

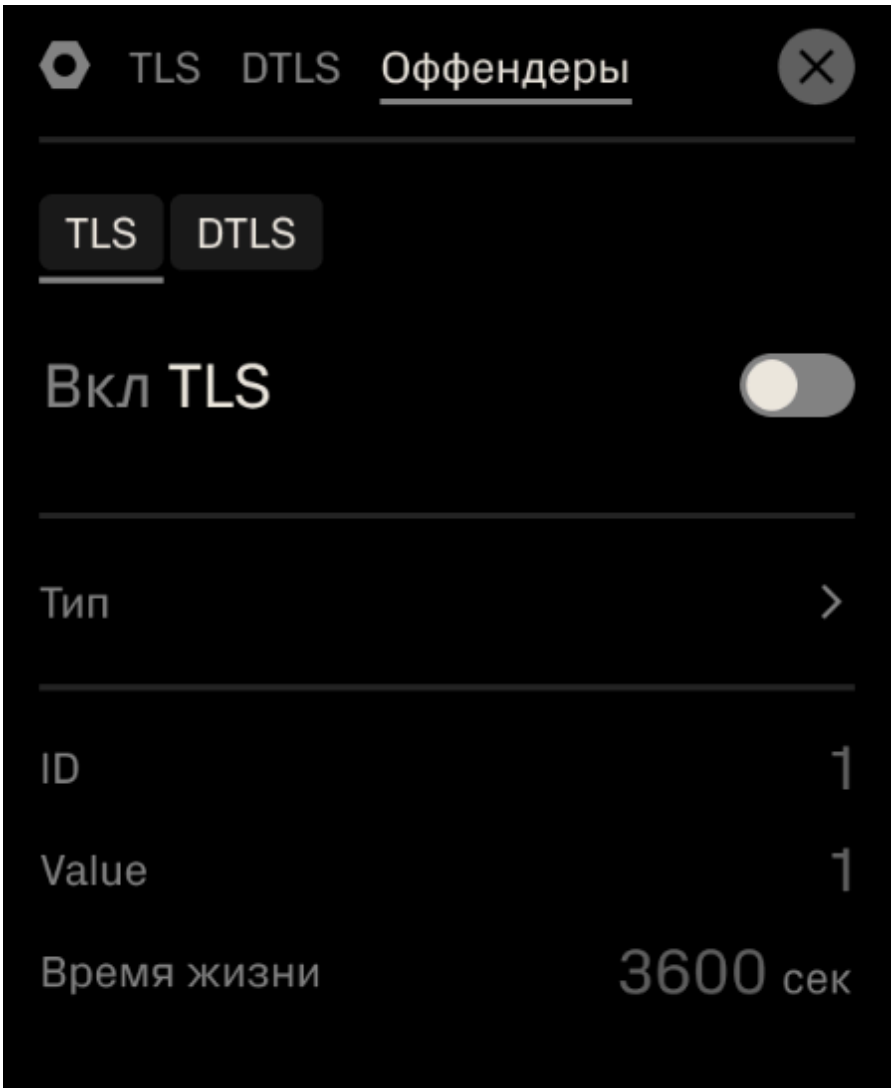
- **JA3**
  Фильтрация по JA3-хэшу. JA3-хэш — это отпечаток TLS-соединения, формируемый на основе параметров, согласуемых при его установлении.
- **JA4**
  Фильтрация по JA4-хэшу. JA4-хэш — это расширенный отпечаток TLS-соединения, формируемый на основе параметров, согласуемых при его установлении, с учётом дополнительных характеристик протокольного обмена.
- **SNI (Server Name Indication)**
  Фильтрация по имени хоста. Имя хоста объявляется клиентом при установлении TLS-соединения и используется для выбора целевого сервиса.
- **ALPN (Application-Layer Protocol Negotiation)**
  Фильтрация по значениям расширения ALPN. ALPN используется при установлении TLS-соединения для согласования протокола HTTP (например, http/1.1, h2, h3).
- **Cipher List**
  Фильтрация по наборам шифров. Наборы шифров объявляются в сообщении ClientHello, а выбранный набор подтверждается в сообщении ServerHello при установлении TLS-соединения.



- **Поле поиска** (значок в правом верхнем углу): Позволяет осуществлять быстрый поиск по списку указанных элементов.
- **Переключатели режима фильтрации**:
  - **Сбрасывать указанные** — режим, при котором соединения, соответствующие элементам списка, будут блокироваться или отбрасываться.
  - **Все кроме указанных** — режим, при котором соединения, не соответствующие элементам списка, будут блокироваться или отбрасываться.
- **Список элементов**: Содержит перечень заданных значений: идентификаторы, хэши, имена доменов и другие параметры, используемые для фильтрации.

Оффендеры

Оффендеры предназначены для маркировки и временного отслеживания сетевых объектов (сессий, хостов, потоков), распознанных как нарушители или аномальные участники TLS/DTLS-трафика. Маркировка используется для последующей фильтрации, ограничения или анализа таких соединений.



Верхняя часть интерфейса содержит переключатель между двумя типами защищённых протоколов: **TLS** и **DTLS**.

- **Тип**:
  - *CONNMARK* — Метка для соединений
  - *DHMARK* — Метка для IP-получателя
  - *HMARK* — Метка для IP-отправителя
  - *SDHMARK* — Метка для IP отправителя и получателя
- **ID**
  Целочисленный идентификатор группы или правила, к которому привязывается маркер. По умолчанию: 1.

- **Value**
  Значение метки, присваиваемое нарушителю. По умолчанию: 1.
- **Expire, сек**
  Время жизни (в секундах) метки после назначения. По истечении этого времени метка автоматически удаляется. Значение по умолчанию: 3600 (1 час).

Пример работы оффендеров

Сценарий: выявление вредоносных клиентов по признакам TLS/DTLS и их блокировка на уровне сетевого трафика.

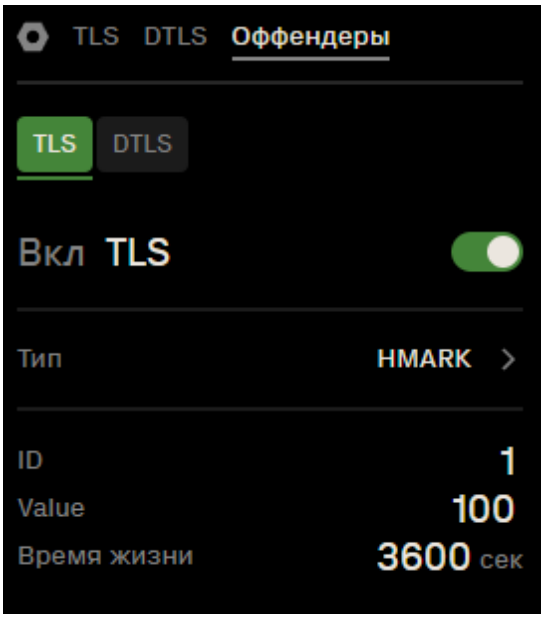
1. Обнаружение подозрительного клиента

Модуль TLS зафиксировал соединение с аномальными признаками, указывающими на потенциально нежелательный или вредоносный трафик.

2. Назначение метки

В настройках Оффендер задаются параметры метки, которые определяют, как именно будет помечен подозрительный IP-адрес:

Тип: HMARK
ID: 1
Value: 100
Expire: 3600



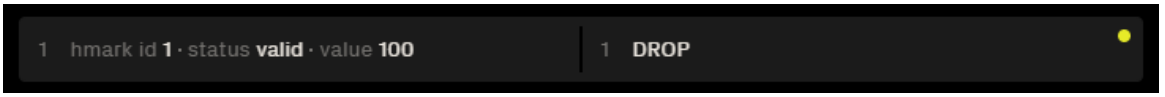
Это означает, что IP-отправителя будет отмечен меткой **100** на один час.

3. Блокировка по метке

Далее следует настроить правило блокировки для автоматической фильтрации нежелательного трафика. Для этого необходимо:

Перейти в нужный профиль → Правила → Создать новое правило

- **Совпадение**: hmark
  - **ID**: 1
  - **Status**: valid
  - **Value**: 100
- **Действие**: DROP



Нажать зелёную кнопку **Добавить**, а затем жёлтую кнопку **Применить**.

Переместите правило в начало списка, чтобы оно применялось в первую очередь. Таким образом, после первого подозрительного соединения все последующие попытки с этого IP будут блокироваться ещё до обработки TLS/DTLS.

Сетевые дампы

Функция захвата сетевых пакетов позволяет сохранить трафик для последующего анализа. Захват выполняется без потерь, без передачи пакетов в ОС и без дополнительной задержки.

Механизм записи сетевых пакетов можно держать постоянно-активным. Это не рекомендуется на платформах обрабатывающих более 30Mpps единовременно в рамках сессионной защиты из-за возможной деградации производительности.

Внимание!
При использовании действия захвата трафика рекомендуем использовать дополнительные совпадения для более частной выборки, или использовать захват в комбинации с рейтлимитом, захват на высокой скорости может негативно влиять на производительность платформы

1. Настройка конфигурационного файла

Во время установки dosgate-uh, вы должны будете указать следующую информацию в основном конфигурационном файле (/etc/dosgate-uh.conf):

```
capture:
  path: /var/cache/dosgate-uh/capture
  filename: cap_${DEV}_${ID}_${NUM}.pcap
  age: 3600
  count: 10
  size: 10M
```

- *path* — директория хранения дампов
- *filename* — шаблон имени файла: `dev` = network interface name, `id` = номер в очереди, `num` = номер в группе
- *age* — время жизни файла (сек)
- *count* — максимальное число файлов в ротации
- *size* — максимальный размер файла
- path, путь для сохранения файлов с захваченными пакетами.
- filename, сгенерированное название файла. `dev` = network interface name, `num` = номер в группе, `id` = номер в очереди.
- count, количество файлов в группе для ротации. Например 10.
- size, максимальный размер сохраняемого файла в мегабайтах. Например 10 мегабайт (10M).
- age, время ожидания до остановки записи файла. Например 3600 секунд.

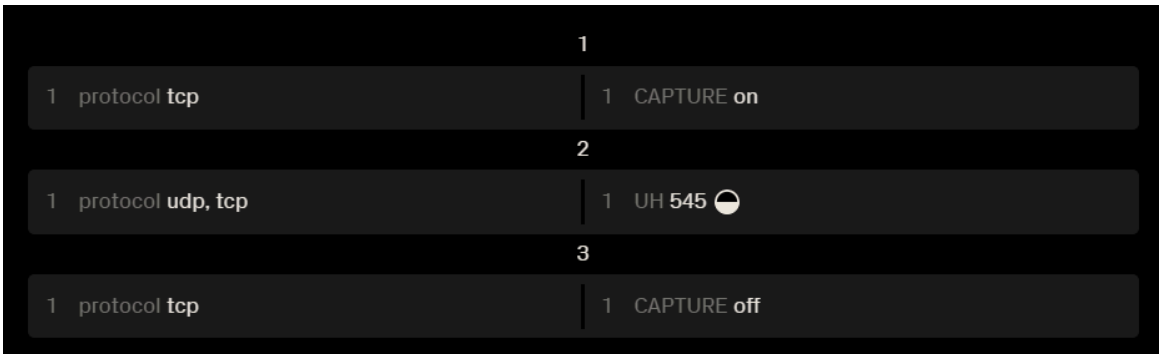
2. Создание правила с действием CAPTURE

Отправка трафика на анализ для построения правил автогенера

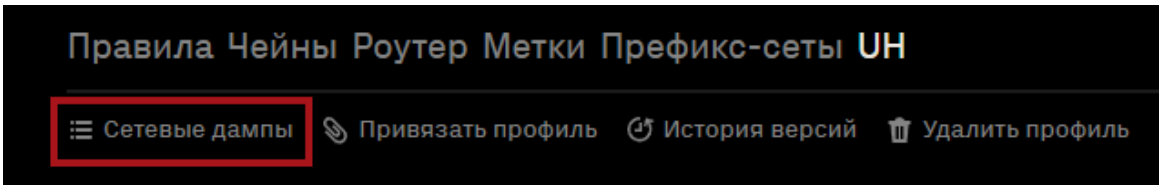
Создайте правило захвата сетевых пакетов (действие capture on) и его остановки (действие capture off).

Между capture on и capture off обязательно должно присутствовать правило передачи сетевых пакетов в любую из политик dosgate-uh. Именно на уровне dosgate-uh происходит захват пакетов.

Захват пакетов активируется раньше чем любые настроенные политики безопасности (терминальные действия сброса или передачи трафика конечному получателю).



Для профиля сессионного модуля доступна функция сохранения и загрузки сетевых дампов. В верхней панели необходимо нажать **Сетевые дампы**.



Откроется область управления дампами:

В блоке **Сетевые дампы** отображаются активные настройки:

- *path* — директория хранения дампов;
- *filename* — шаблон имени файла;
- *age* — время жизни файла (сек);
- *count* — максимальное число файлов в ротации;
- *size* — максимальный размер файла.

Алгоритм ротации

Файл в который сейчас ведется запись всегда имеет ID 0 (например, cap_ens35_000_00.pcap).

После того как размер файла соответствует size или заканчивается age (время в секундах которое выделяется на время записи), файл переименовывается в соответствии с очередью и лимитом count (например, cap_ens35_000_01.pcap или cap_ens35_000_02.pcap).

В случае, если все ID заняты - dosgate обнулит файл с последним ID и начнет его запись повторно. В таком цикле и ротации работа будет продолжаться и дальше.

Скачать дамп

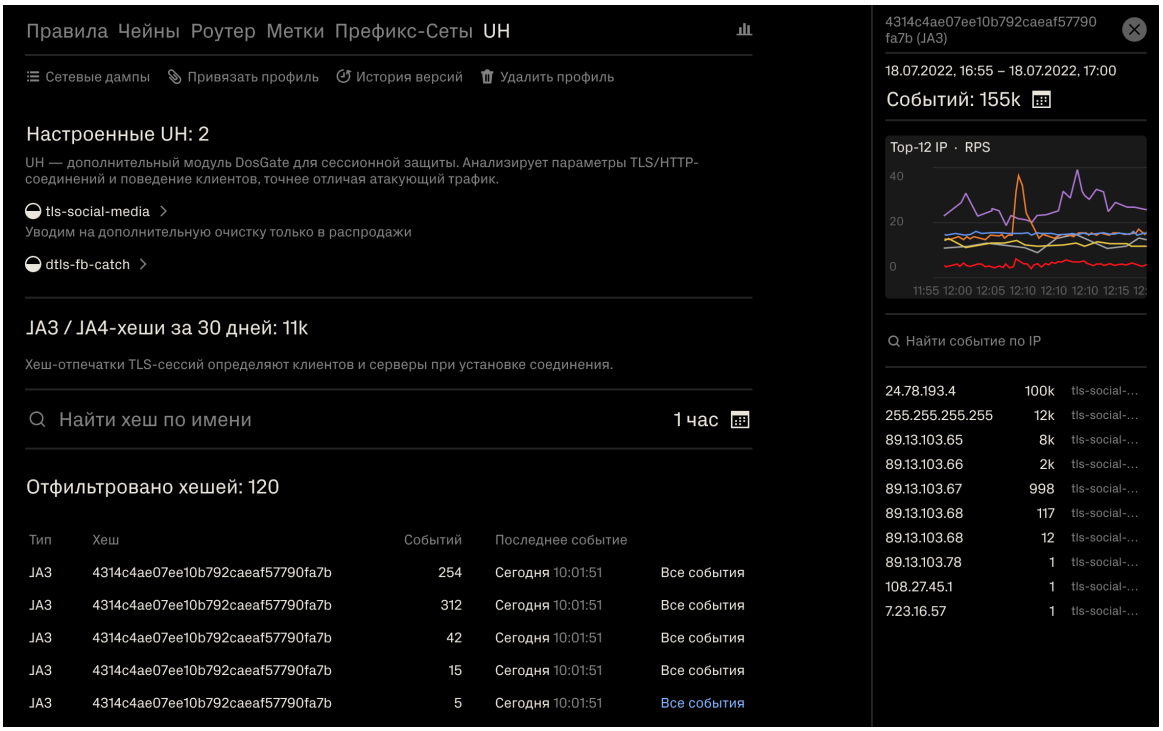
Для того чтобы **скачать дамп**, необходимо нажать на **название файла** в списке. Загрузка начнётся автоматически. Файл сохраняется в формате *.pcap*.

При скачивании **автоматически создаётся снэпшот** дампа. Найти и повторно скачать его можно в разделе **Снэпшоты**.

Срок хранения снэпшотов — 1 год.

Интерфейс после настройки

После настройки конфигураций в разделе отображается рабочая область с активными сессионными профилями.



В центральной части экрана показан список настроенных UH-профилей. Ниже отображается статистика по TLS-отпечаткам JA3/JA4 за выбранный период, включая количество событий и время последнего срабатывания.

В правой части экрана расположена аналитическая панель с детализацией по источникам трафика и динамикой событий. Панель позволяет быстро определить наиболее активные IP-адреса, частоту запросов и характер нагрузки, связанной с конкретными TLS-отпечатками.

Autopilot

Назначение модуля

Autopilot — это модуль интеллектуального анализа трафика, предназначенный для автоматической генерации правил защиты в реальном времени на основе текущего сетевого трафика. Он помогает оперативно реагировать на атаки, не требуя от администратора глубокого анализа трафика вручную.

Принцип работы

Модуль анализирует сетевой трафик, проходящий через **Сессионную защиту**, и автоматически формирует набор **контрмер**, которые можно применить для нейтрализации угроз. Эти меры строятся на основе математической модели. На выходе **Autopilot** предлагает готовые правила.

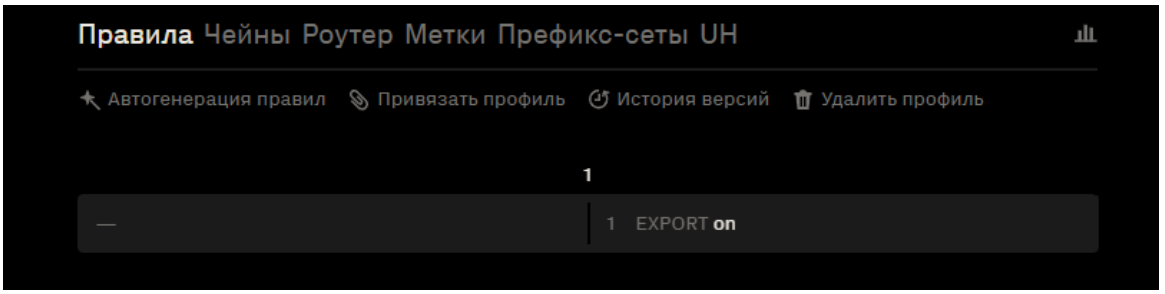
Настройка и запуск

1. Создание правила с действием EXPORT

Отправка трафика на анализ для построения правил автогенерации регулируется действием **EXPORT**. Без активного **EXPORT** трафик не попадёт в анализ, и кнопка **Автогенерация правил** останется недоступной.

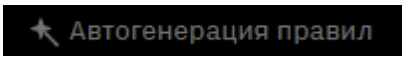
Если до **EXPORT** стоит действие **DROP** или **ACCEPT**, то экспортируемых пакетов не будет. Экспортируются только те пакеты, которые проходят через систему (то есть те, что "принимаются", а не блокируются или отбрасываются в следствии применения правил).

Допускается создание правила без указания **Совпадений**.

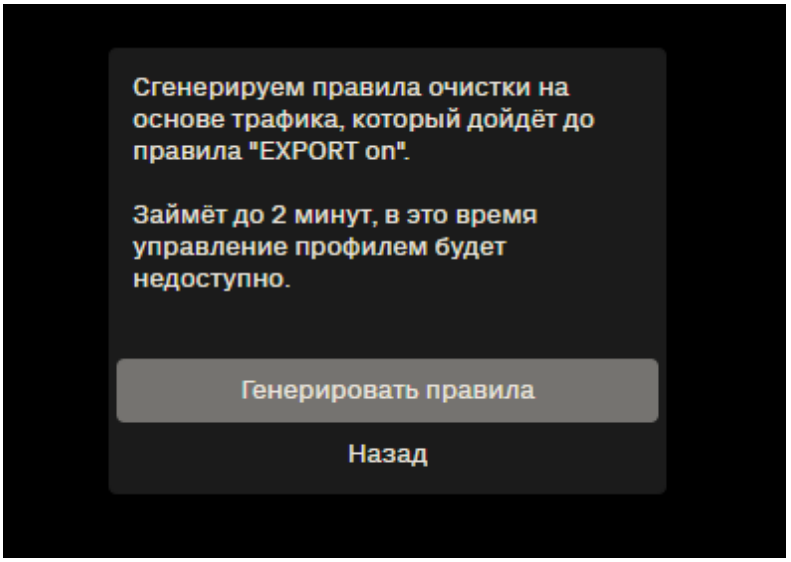


2. Запуск генерации правил

В интерфейсе станет активной кнопка



Нажать кнопку — запустится процесс сбора и анализа трафика на основе экспортируемых пакетов. На экране отобразится уведомление:

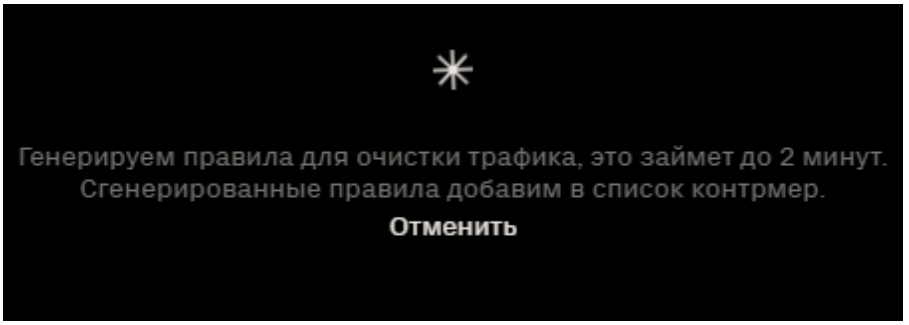


Ограничения при генерации контрмер:

- Во время выполнения автогенерации контрмер редактирование правил **блокируется для профиля**, на котором запущена генерация. Это связано с тем, что модуль анализирует трафик с учётом текущей политики фильтрации, заданной профиле.
- **Одновременная генерация контрмер невозможна** — запуск автогенерации правил поддерживается только для одного профиля в один момент времени.

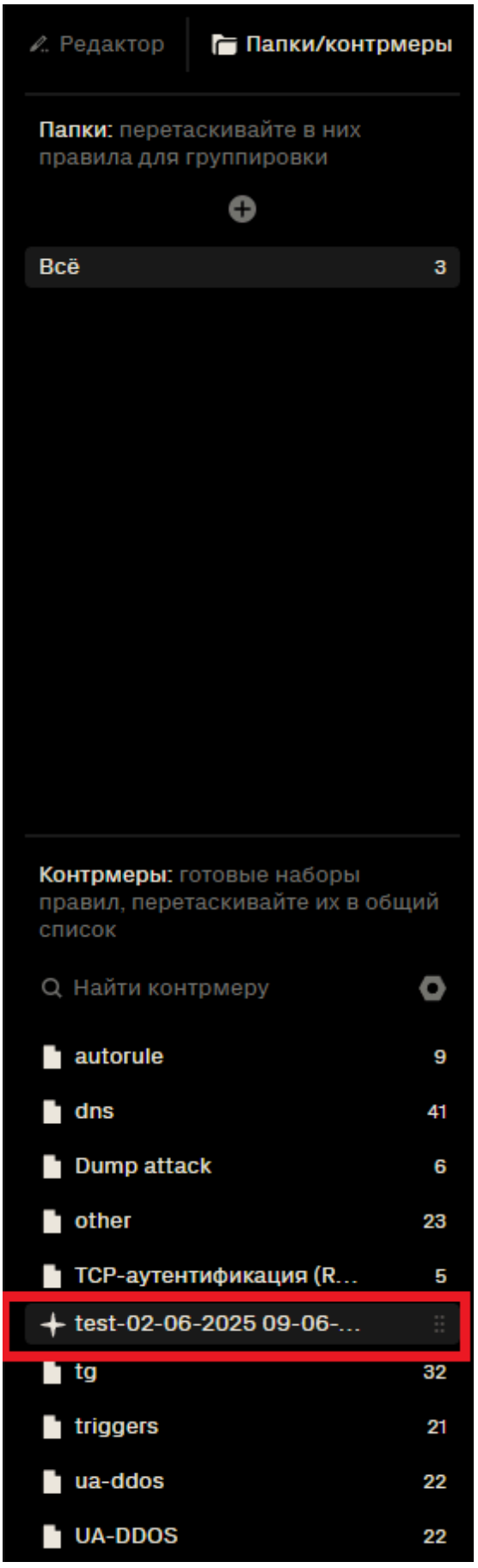
Нажать кнопку **Генерировать правила** для подтверждения запуска процесса. После подтверждения интерфейс отобразит статус

выполнения:



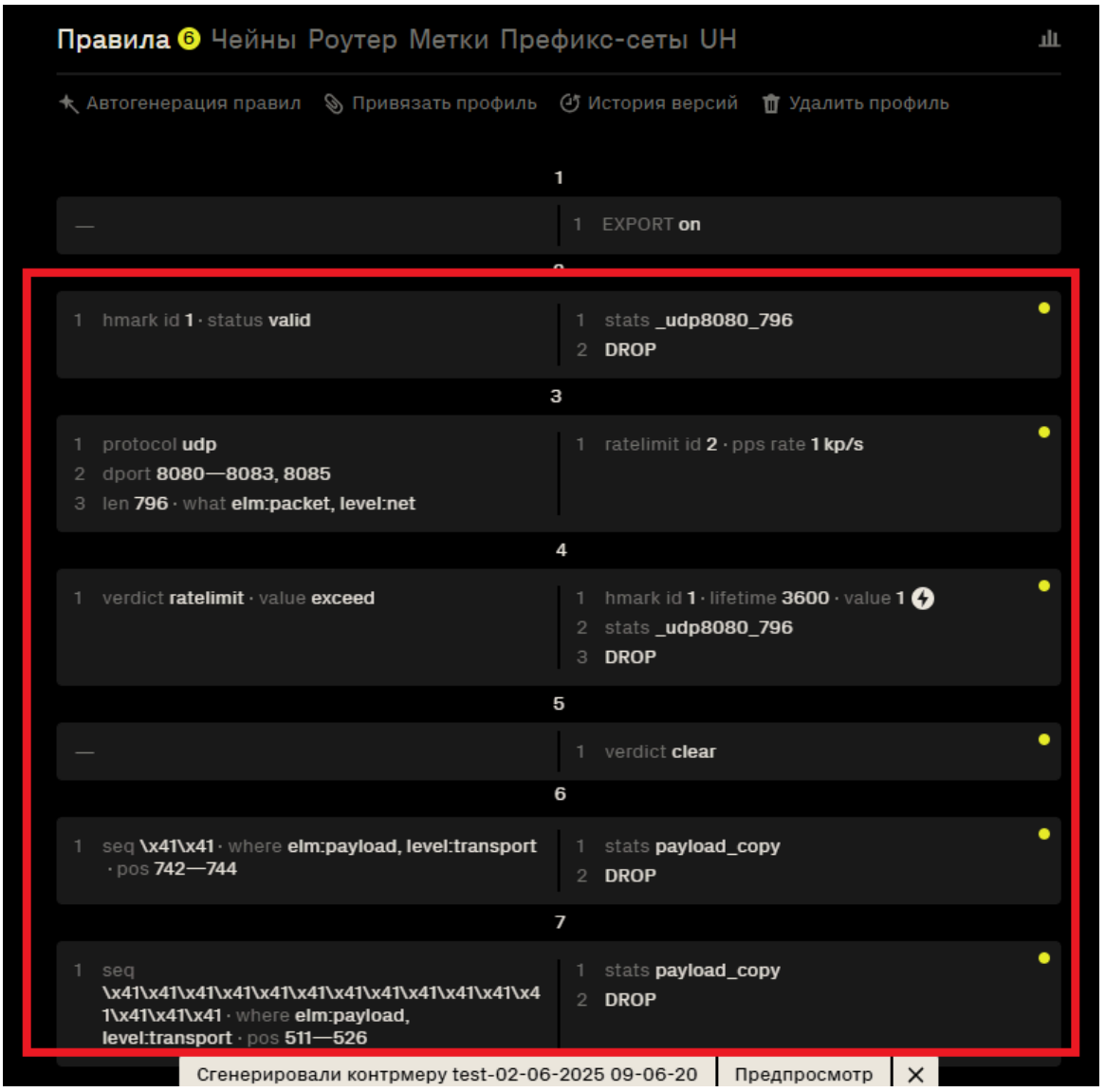
3. Получение и применение сгенерированных правил

После завершения генерации сгенерированный набор правил автоматически сохраняется в разделе **Контрмеры**, доступном во вкладке **Папки/контрмеры** на боковой панели интерфейса. Название набора формируется автоматически и включает имя исходного профиля, дату и время генерации.



Для применения набора необходимо перенести его в рабочий профиль. После переноса допускается просмотреть содержимое правил и внести

корректировки. Далее нажать жёлтую кнопку **Применить** для активации изменений.



RLOG

Назначение модуля

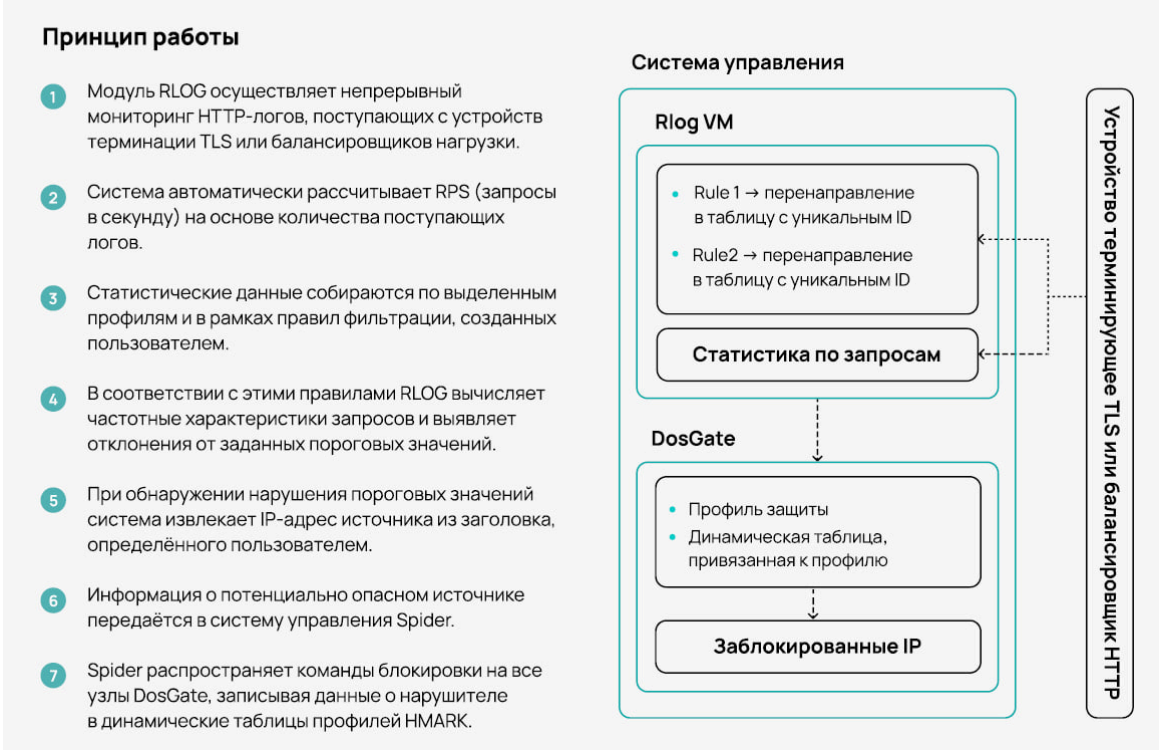
Модуль RLOG предназначен для анализа HTTP-логов от внешних систем терминирующих TLS. На основании полей логов позволяет формировать правила фильтрации для блокировки IP-адресов источника,тем самым обеспечивая возможность фильтрации зашифрованного L7-трафика.

Принцип работы

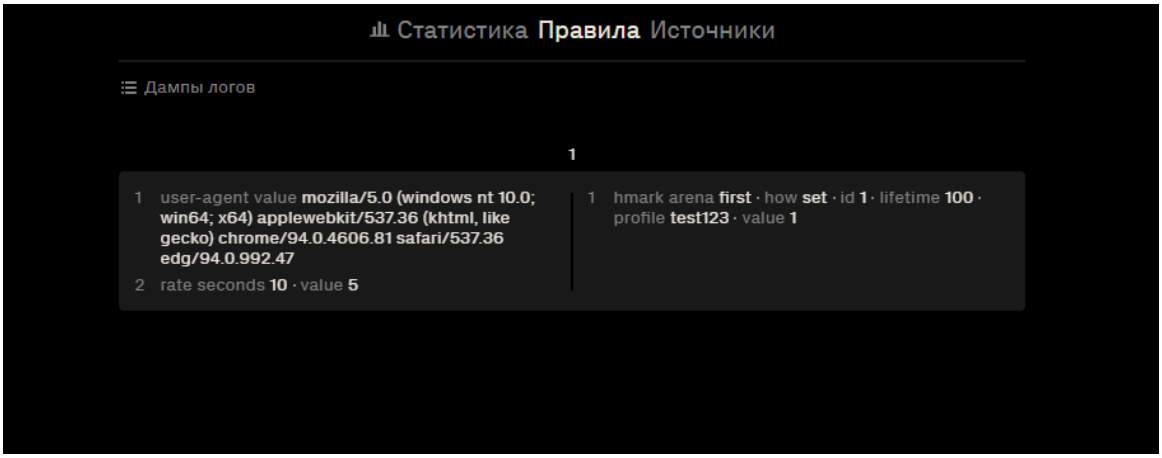
RLOG принимает входящий поток логов с одного или нескольких источников. Каждый лог анализируется в соответствии с предварительно заданным шаблоном. Извлечённые данные (статус-код, IP-адрес источника, время отклика, virtual IP и т.д.) используются для расчёта метрик.

На основе этих метрик могут быть активированы правила, определяющие допустимую частоту запросов (rate limit) и иные условия. При нарушении условий источник помечается, и его IP-адрес передаётся в систему DosGate для блокировки в соответствии с параметрами текущего профиля (арена, метка и пр.).

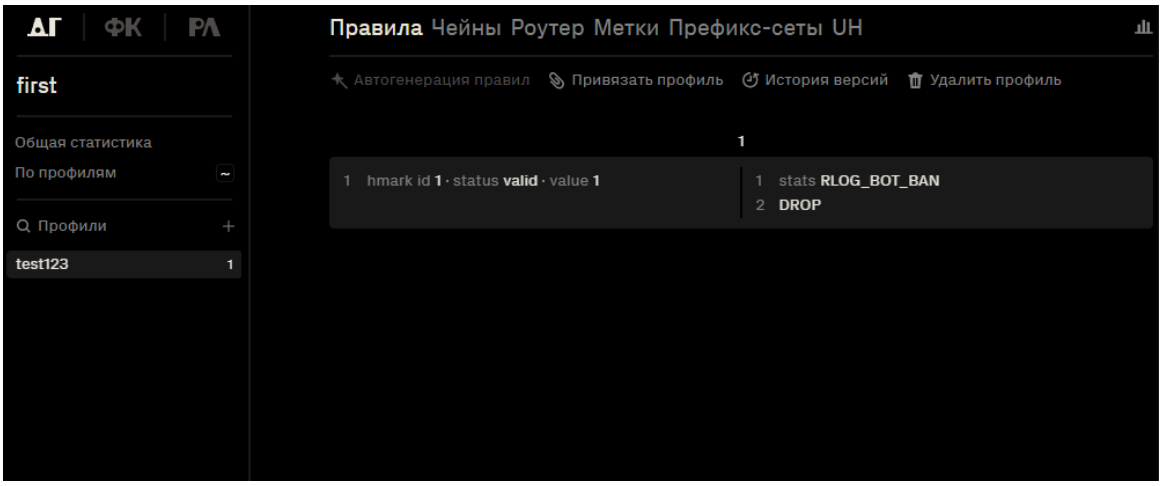
Для применения фильтрации на уровне DosGate необходимо создать правило, использующее соответствующую метку (HMARK) — с заданным действием, например, сбросить пакет (drop). Без такого правила IP-адрес, переданный из RLOG, не будет заблокирован на уровне трафика.



Пример работы RLOG с DosGate



Правило в **RLOG** отслеживает HTTP-запросы с определённым *User-Agent* и частотой более **5 запросов за 10 секунд**. При выполнении этих условий модуль присваивает IP-адресу временную метку **HMARK id 1, value 1**, сроком на **100 секунд** и передаёт её в **DosGate** — в арену *first* и профиль *test123*.



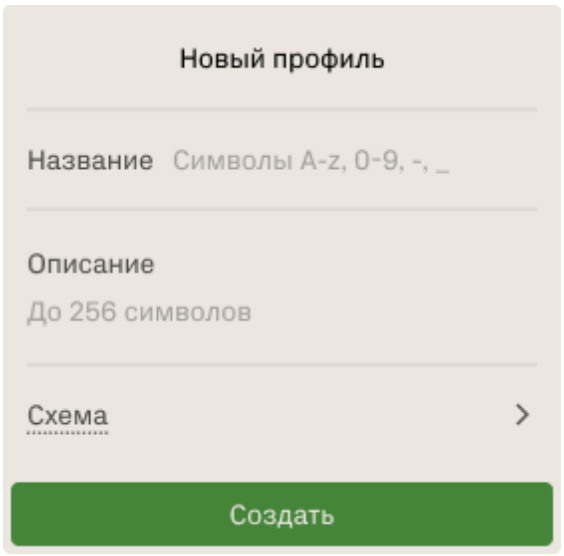
В **DosGate** настроено правило, реагирующее на наличие активной метки **HMARK id 1, value 1**. При наличии такой метки трафик от соответствующего IP-адреса блокируется действием **DROP**, а факт срабатывания фиксируется в счётчике **RLOG_BOT_BAN**. Таким образом обеспечивается автоматическая фильтрация подозрительных источников, выявленных на уровне логов.

Профиль

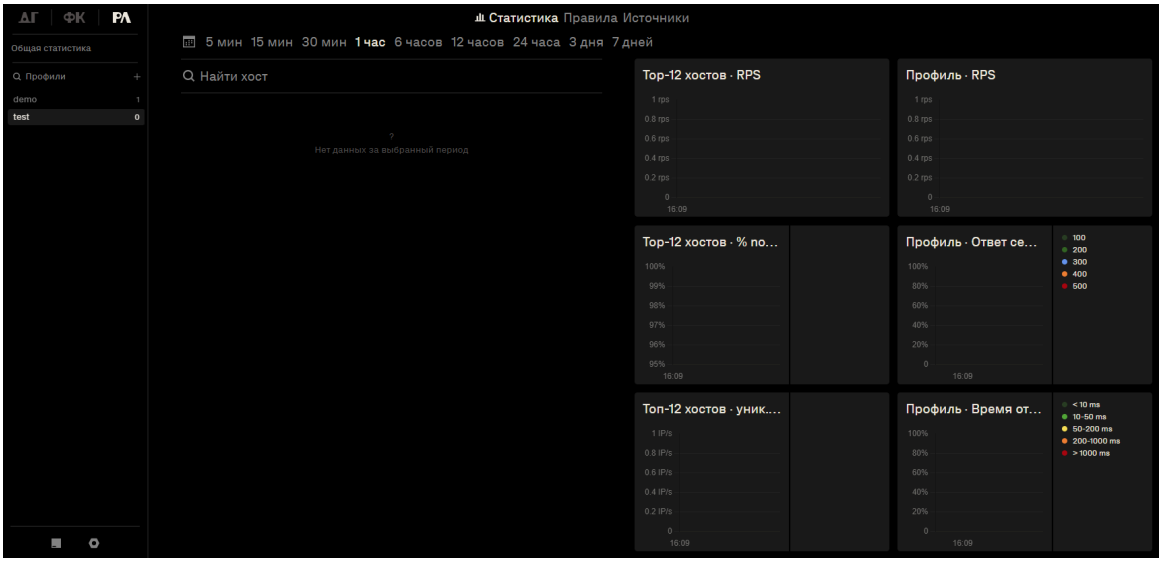
Создание профиля

Для создания нового профиля в системе выполнить следующие действия:

1. На главной странице в разделе **Профили** нажать кнопку "+".
2. Заполнить следующие поля для создания профиля:
   - **Название** - уникальное имя для профиля. Рекомендуется использовать комбинацию из обозначения сегмента инфраструктуры и названия сервиса, например, "zapadniy-filial-web".
   - **Описание** - краткое текстовое пояснение, которое поможет понять назначение профиля.
   - **Схема** - шаблон формата строк в логах. Определяет, как система будет разбирать поступающие журналы. После создания профиля изменить схему нельзя.
3. Нажать кнопку **Создать**.

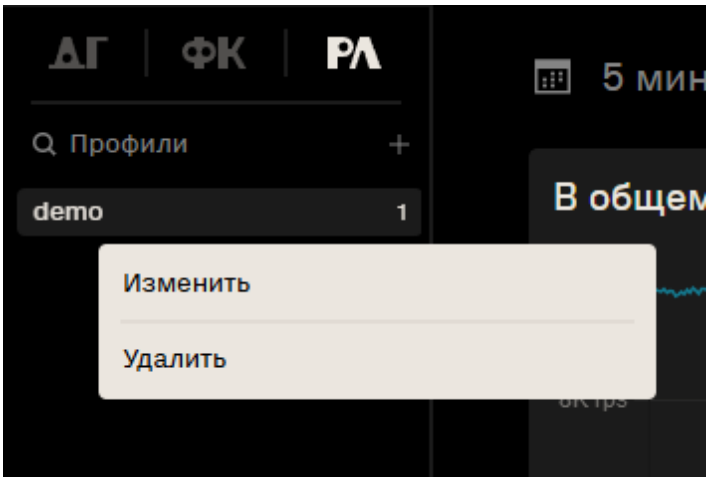


После создания профиля интерфейс переключится на страницу профиля.



Изменение профиля

Для изменения профиля необходимо нажать правой кнопкой мыши на его названии в общем списке профилей и выбрать пункт **Изменить**. Откроется окно, в котором можно изменить название и описание профиля.



Удаление профиля

Для удаления профиля необходимо нажать правой кнопкой мыши на его названии в общем списке профилей и выбрать пункт **Удалить**. После этого профиль будет безвозвратно удален из системы.

Статистика

Раздел **Статистика** предназначен для визуального мониторинга состояния трафика, поступающего в модуль RLOG в виде логов. Он позволяет выявлять потенциальные аномалии и источники нестандартного поведения на основе агрегации логов от разных хостов.

Навигация и фильтрация

- В верхней панели доступен выбор временного диапазона:
  5 мин, 15 мин, 30 мин, 1 час, 6 часов, 12 часов, 24 часа, 3 дня, 7 дней.
- Форма поиска по хосту — позволяет отфильтровать данные по доменному имени виртуального хоста.

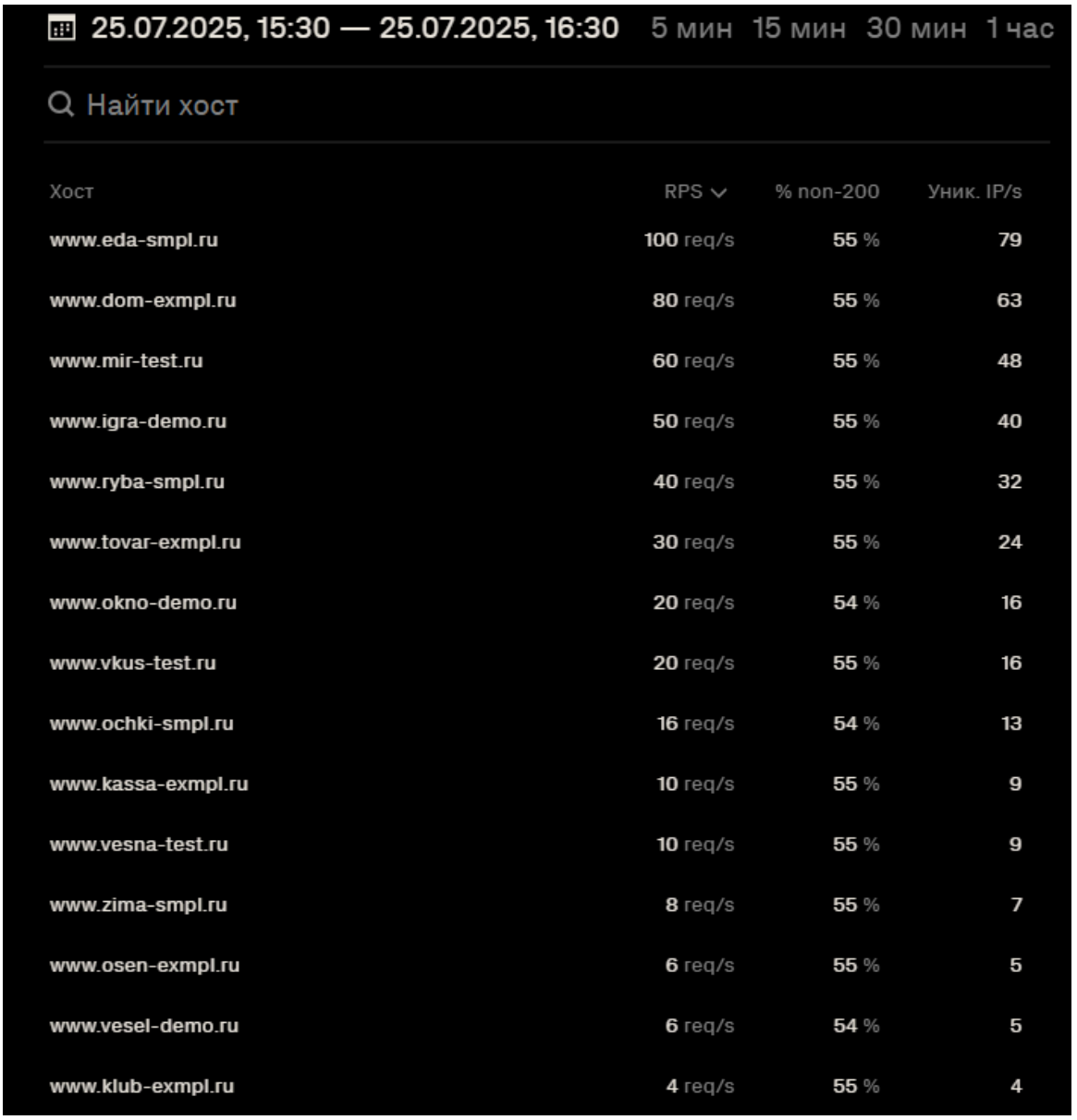


Таблица хостов

Отображается список хостов, по которым поступают HTTP-запросы.

Колонки таблицы:

- **Хост** — доменное имя виртуального хоста, извлечённое из логов.
- **RPS** — количество запросов в секунду, вычисляется как среднее значение за выбранный интервал.
- **% non-200** — процент ответов с HTTP-кодами, отличными от 200. Отражает долю ошибок и редиректов.
- **Уник. IP/s** — количество уникальных IP-адресов источников запросов в секунду.

Таблица поддерживает сортировку по каждому из столбцов. Для изменения порядка необходимо кликнуть по заголовку соответствующей колонки.

Графики

Top-12 хостов · RPS
Линейный график, отображающий интенсивность запросов по 12 наиболее активным хостам. Позволяет отследить пики и резкие изменения в трафике.

Top-12 хостов · % non-200
График показывает процент некорректных ответов (HTTP-коды, отличные от 200) по каждому из 12 наиболее активных хостов. Используется для выявления источников с высоким уровнем ошибок.

Top-12 хостов · Уник. IP/s
Отображает динамику количества уникальных IP-адресов, с которых поступают запросы. Является индикатором распределённости трафика или возможных сканирований.

Профиль · RPS
График суммарной нагрузки по запросам в секунду в рамках текущего выбранного профиля. Используется для мониторинга общего объёма входящего трафика.

Профиль · Ответ сервера
Диаграмма распределения ответов сервера по классам HTTP-кодов:

- 200 — успешные ответы.
- 300 — редиректы.
- 400 — ошибки клиента.
- 500 — ошибки сервера.
  Позволяет оценить качество работы приложения или выявить массовые сбои.

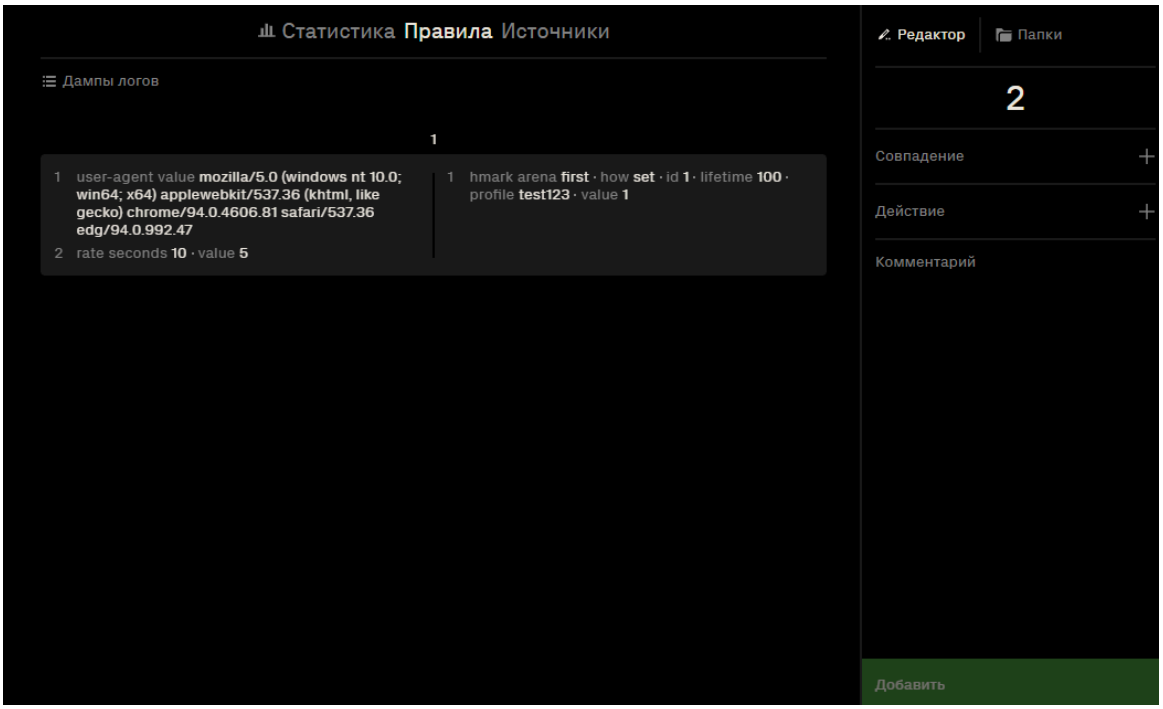
Профиль · Время ответа
Гистограмма распределения запросов по времени ответа сервера:

- менее 10 мс
- 10–50 мс

- 50–200 мс
- 200–1000 мс
- более 1000 мс
  Метрика отражает производительность backend-приложения и может сигнализировать о деградации.

Правила

Правила в системе RLOG создаются путем комбинирования совпадений и действий. Совпадения определяют условия, при которых правило срабатывает. Действия применяется, если условия совпадений выполнены.



Справа в интерфейсе расположена вкладка **Редактор**. В этой области задаются совпадения и действия. При необходимости можно добавить текстовый комментарий — он сохраняется вместе с правилом и используется для технических пометок или пояснений.

Справа находится вкладка **Папки**. В этой области можно вручную группировать правила по папкам для упрощения навигации и визуальной организации конфигурации.

Совпадения

Каждая проверка совпадения содержит один или несколько аргументов, настраиваемых пользователем. Для всех совпадений предусмотрена возможность включения флага **NOT**, реализованного в виде переключателя. **NOT** — логическая операция отрицания, при активации которой условие совпадения инвертируется: правило сработает для всех значений, кроме указанного.

Accept – Заголовок Accept

Параметр	Описание
value	Значение заголовка *Accept* (например, text/html).

Accept-Encoding – Заголовок Accept-Encoding

Параметр	Описание
value	Значение заголовка *Accept-Encoding* (например, gzip).

Accept-Language – Заголовок Accept-Language

Параметр	Описание
value	Значение заголовка *Accept-Language* (например, RU).

BIGIP_CACHED – Геолокация клиента

Используется код страны, полученный из внешних логов.

Параметр	Описание
CN	Китай
RU	Российская Федерация
TW	Тайвань (провинция Китая)
US	Соединённые Штаты Америки

Полный список кодов и стран

Параметр	Описание
CN	Китай
RU	Российская Федерация
TW	Тайвань (провинция Китая)
US	Соединённые Штаты Америки
AD	Андорра
AE	Объединённые Арабские Эмираты
AF	Афганистан
AG	Антигуа и Барбуда
AI	Ангилья
AL	Албания
AM	Армения
AO	Ангола

Параметр	Описание
AQ	Антарктида
AR	Аргентина
AS	Американское Самоа
AT	Австрия
AU	Австралия
AW	Аруба
AX	Аландские острова
AZ	Азербайджан
BA	Босния и Герцеговина
BB	Барбадос
BD	Бангладеш
BE	Бельгия
BF	Буркина-Фасо
BG	Болгария
BH	Бахрейн
BI	Бурунди
BJ	Бенин
BL	Сен-Бартелеми
BM	Бермудские острова
BN	Бруней-Даруссалам
BO	Боливия
BQ	Бонайре, Синт-Эстатиус и Саба
BR	Бразилия
BS	Багамские Острова
BT	Бутан
BV	Остров Буве
BW	Ботсвана
BY	Беларусь
BZ	Белиз
CA	Канада
CC	Кокосовые (Килинг) острова
CD	Демократическая Республика Конго

Параметр	Описание
CF	Центральноафриканская Республика
CG	Республика Конго
CH	Швейцария
CI	Кот-д'Ивуар
CK	Острова Кука
CL	Чили
CM	Камерун
CO	Колумбия
CR	Коста-Рика
CU	Куба
CV	Кабо-Верде
CW	Кюрасао
CX	Остров Рождества
CY	Кипр
CZ	Чехия
DE	Германия
DJ	Джибути
DK	Дания
DM	Доминика
DO	Доминиканская Республика
DZ	Алжир
EC	Эквадор
EE	Эстония
EG	Египет
EH	Западная Сахара
ER	Эритрея
ES	Испания
ET	Эфиопия
FI	Финляндия
FJ	Фиджи
FK	Фолклендские (Мальвинские) острова
FM	Федеративные Штаты Микронезии

Параметр	Описание
FO	Фарерские острова
FR	Франция
GA	Габон
GB	Великобритания
GD	Гренада
GE	Грузия
GF	Французская Гвиана
GG	Гернси
GH	Гана
GI	Гибралтар
GL	Гренландия
GM	Гамбия
GN	Гвинея
GP	Гваделупа
GQ	Экваториальная Гвинея
GR	Греция
GS	Южная Георгия и Южные Сандвичевы острова
GT	Гватемала
GU	Гуам
GW	Гвинея-Бисау
GY	Гайана
HK	Гонконг
HM	Острова Херд и Макдональд
HN	Гондурас
HR	Хорватия
HT	Гаити
HU	Венгрия
ID	Индонезия
IE	Ирландия
IL	Израиль
IM	Остров Мэн
IN	Индия

Параметр	Описание
IO	Британская территория в Индийском океане
IQ	Ирак
IR	Иран
IS	Исландия
IT	Италия
JE	Джерси
JM	Ямайка
JO	Иордания
JP	Япония
KE	Кения
KG	Киргизия
KH	Камбоджа
KI	Кирибати
KM	Коморы
KN	Сент-Китс и Невис
KP	Корейская Народно-Демократическая Республика
KR	Республика Корея
KW	Кувейт
KY	Острова Кайман
KZ	Казахстан
LA	Лаос
LB	Ливан
LC	Сент-Люсия
LI	Лихтенштейн
LK	Шри-Ланка
LR	Либерия
LS	Лесото
LT	Литва
LU	Люксембург
LV	Латвия
LY	Ливия
MA	Марокко

Параметр	Описание
MC	Монако
MD	Молдова
ME	Черногория
MF	Сен-Мартен (французская часть)
MG	Мадагаскар
MH	Маршалловы Острова
MK	Северная Македония
ML	Мали
MM	Мьянма
MN	Монголия
MO	Макао
MP	Северные Марианские острова
MQ	Мартиника
MR	Мавритания
MS	Монтсеррат
MT	Мальта
MU	Маврикий
MV	Мальдивы
MW	Малави
MX	Мексика
MY	Малайзия
MZ	Мозамбик
NA	Намибия
NC	Новая Каледония
NE	Нигер
NF	Остров Норфолк
NG	Нигерия
NI	Никарагуа
NL	Нидерланды
NO	Норвегия
NP	Непал
NR	Науру

Параметр	Описание
NU	Ниуэ
NZ	Новая Зеландия
OM	Оман
PA	Панама
PE	Перу
PF	Французская Полинезия
PG	Папуа — Новая Гвинея
PH	Филиппины
PK	Пакистан
PL	Польша
PM	Сен-Пьер и Микелон
PN	Питкэрн
PR	Пуэрто-Рико
PS	Палестина
PT	Португалия
PW	Палау
PY	Парагвай
QA	Катар
RE	Реюньон
RO	Румыния
RS	Сербия
RW	Руанда
SA	Саудовская Аравия
SB	Соломоновы Острова
SC	Сейшельские Острова
SD	Судан
SE	Швеция
SG	Сингапур
SH	Острова Святой Елены, Вознесения и Тристан-да-Кунья
SI	Словения
SJ	Шпицберген и Ян-Майен
SK	Словакия

Параметр	Описание
SL	Сьерра-Леоне
SM	Сан-Марино
SN	Сенегал
SO	Сомали
SR	Суринам
SS	Южный Судан
ST	Сан-Томе и Принсипи
SV	Сальвадор
SX	Синт-Мартен (нидерландская часть)
SY	Сирия
SZ	Эсватини
TC	Острова Тёркс и Кайкос
TD	Чад
TF	Французские Южные и Антарктические Территории
TG	Того
TH	Таиланд
TJ	Таджикистан
TK	Токелау
TL	Восточный Тимор
TM	Туркменистан
TN	Тунис
TO	Тонга
TR	Турция
TT	Тринидад и Тобаго
TV	Тувалу
TZ	Танзания
UA	Украина
UG	Уганда
UM	Внешние малые острова США
UY	Уругвай
UZ	Узбекистан
VA	Ватикан

Параметр	Описание
VC	Сент-Винсент и Гренадины
VE	Венесуэла
VG	Британские Виргинские острова
VI	Виргинские острова (США)
VN	Вьетнам
VU	Вануату
WF	Уоллис и Футуна
WS	Самоа
XK	Косово
YE	Йемен
YT	Майотта
ZA	Южно-Африканская Республика
ZM	Замбия
ZW	Зимбабве

CLIENT_IP – IP-адрес клиента

Параметр	Описание
ip	IP-адрес клиента (например, 192.168.74.164).

CLIENT_PORT – Порт клиента

Параметр	Описание
port	Номер порта клиента (диапазон от 0 до 65535).

DATE_DD – День запроса

Параметр	Описание
value	День месяца в формате *DD* (от 01 до 31).

DATE_MM – Месяц запроса

Параметр	Описание
value	Месяц в формате *MM* (от 01 до 12).

DATE_YYYY – Год запроса

Параметр	Описание
value	Год в формате *YYYY* (например, 2025).

Host – Заголовок Host

Параметр	Описание
value	Значение заголовка *Host* (например, 127.0.0.1).

HTTP_KEEPALIVE – Признак Keep-Alive

Параметр	Описание
status	Признак наличия заголовка *Connection: keep-alive*.

HTTP_REQUEST – Полный HTTP-запрос

Параметр	Описание
request	Полная строка запроса в формате `$METHOD $URI $VERSION`.

HTTP_STATCODE – HTTP-статус ответа

Параметр	Описание
status	Код статуса HTTP-ответа (например, 200, 403, 500).

ISO_CODE – Код страны по GeoIP

Геолокация вычисляется системой самостоятельно на основе IP-адреса клиента с использованием встроенной базы GeoIP.

Параметры и описание совпадают с описанием BIGIP_CACHED

RATE – Частота срабатываний

Параметр	Описание
seconds	Период времени в секундах, за который измеряется количество срабатываний.
value	Количество срабатываний за указанный период.

Referer – Заголовок Referer

Параметр	Описание
value	Значение заголовка *Referer* (например, localhost).

RESPONSE_MSECS – Время ответа

Параметр	Описание
value	Время ответа сервера в миллисекундах.

RESPONSE_SIZE – Размер ответа

Параметр	Описание
value	Размер тела ответа в байтах.

SERVER_IP – IP-адрес сервера

Параметр	Описание
ip	IP-адрес сервера, который обработал запрос.

SERVER_PORT – Порт сервера

Параметр	Описание
port	Номер порта сервера (диапазон от 0 до 65535).

TIME_HH24 – Час запроса (24-часовой формат)

Параметр	Описание
value	Час запроса в формате **HH** (от 00 до 23).

TIME_MM – Минута запроса

Параметр	Описание
value	Минута запроса в формате **MM** (от 00 до 59).

TIME_MSECS – Время запроса в миллисекундах

Параметр	Описание
value	Количество миллисекунд, прошедших с начала секунды.

TIME_SS – Секунда запроса

Параметр	Описание
value	Секунда запроса в формате **SS** (от 00 до 59).

User-Agent – Заголовок User-Agent

Параметр	Описание
value	Полное значение заголовка *User-Agent* (например, *Mozilla/5.0 ...*).

VIRTUAL_IP – Виртуальный IP-адрес

Параметр	Описание
ip	IP-адрес, на который был направлен запрос (виртуальный адрес сервиса).

VIRTUAL_PORT – Виртуальный порт

Параметр	Описание
port	Номер порта, к которому был направлен запрос (диапазон от 0 до 65535).

X-Forwarded-For – Заголовок X-Forwarded-For

Параметр	Описание
value	IP-адрес клиента, переданный через прокси в заголовке *X-Forwarded-For*.

X-Requested-With – Заголовок X-Requested-With

Параметр	Описание
value	Значение заголовка *X-Requested-With* (например, *XMLHttpRequest*).

Действие

HMARK

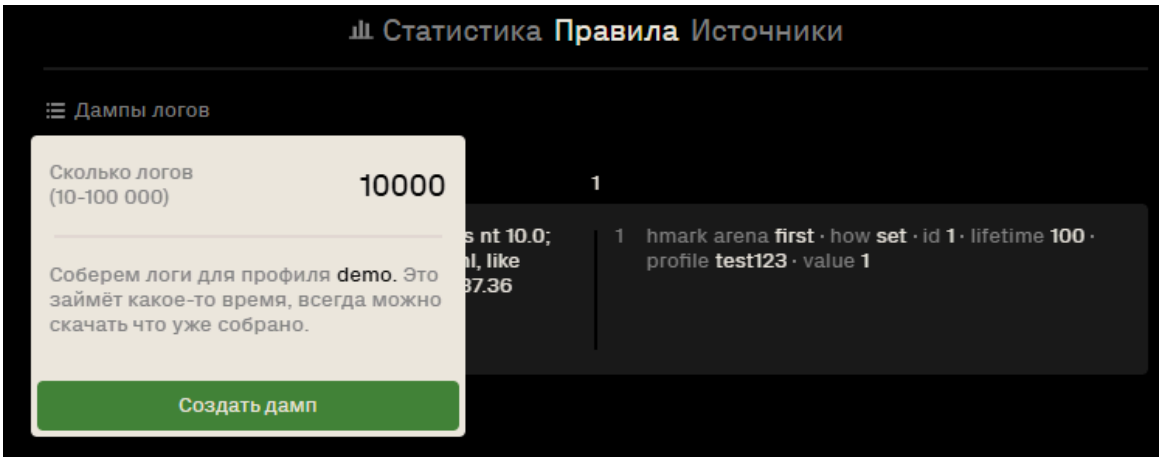
Устанавливает или модифицирует метку для IP-отправителя на основе заданной операции и параметров. Применяется для маркировки пакетов с целью дальнейшей классификации или маршрутизации.

Параметр	Варианты	Описание
id		Идентификатор метки (диапазон от 1 до 255).
how		Действие, выполняемое с меткой:
	add	прибавить значение.
	and	побитовая операция AND.
	dec	уменьшить значение на 1.
	div	разделить на указанное значение.
	inc	увеличить значение на 1.
	mult	умножить на указанное значение.
	not	побитовая инверсия.
	or	побитовая операция OR.
	restore	восстановить метку сети из общей метки.
	save	сохранить сетевую метку в общую метку.
	set	установить заданное значение.

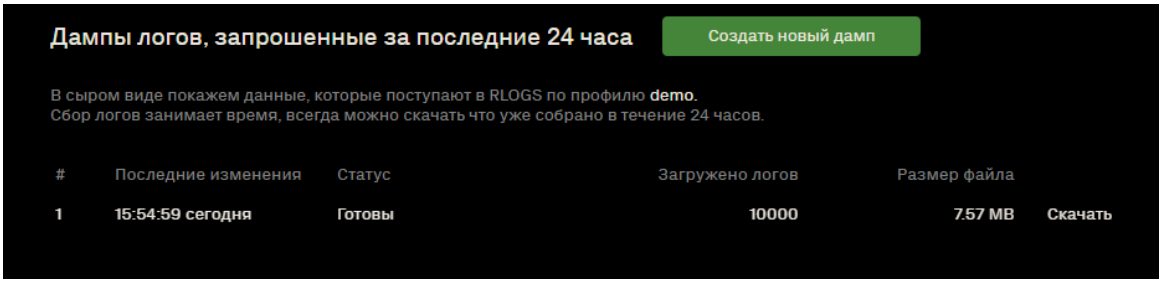
Параметр	Варианты	Описание
	sub	вычесть значение.
	xor	побитовая операция XOR.
value		Числовое значение 0 до 2^{32}-1
lifetime		Время жизни метки в секундах. Если не указано или равно 0 — метка считается постоянной.
arena		Имя арены DosGate, к которой относится метка.
profile		Имя профиля DosGate, в рамках которого применяется метка.

Дампы логов

Функция позволяет выгрузить в текстовом виде «сырые» данные, поступающие в модуль RLOG по выбранному профилю.



Кнопка **Создать дамп** запускает процесс выгрузки HTTP-логов по активному профилю. Объём дампа указывается вручную и может составлять от 10 до 100 000 записей. В выгрузку попадают «сырые» логи — без обработки, в том виде, в котором они поступили в систему. Сформированный дамп доступен для скачивания в течение 24 часов после создания.



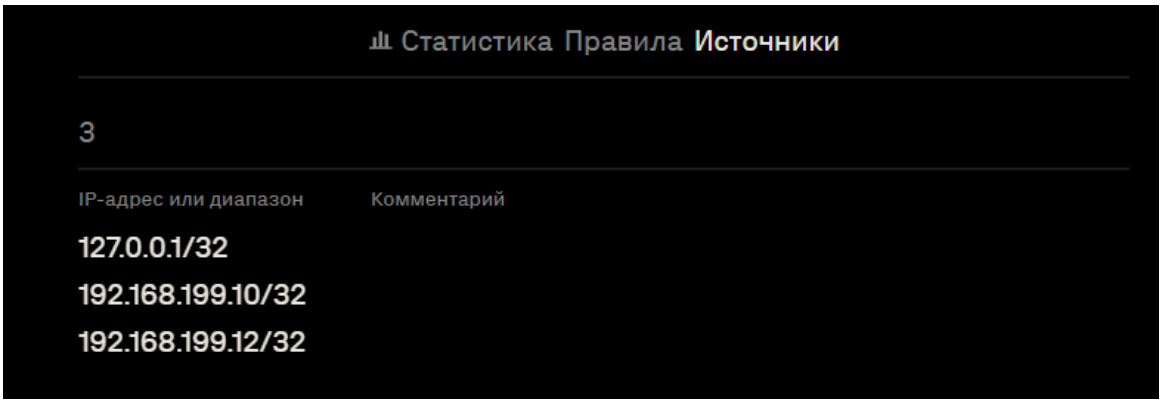
Сбор логов может занять некоторое время. Уже собранные данные можно скачать сразу, не дожидаясь завершения всей выборки.

Источники

Раздел **Источники** используется для указания IP-адресов или подсетей, от которых модуль RLOG принимает логи. Каждый источник задаётся в формате CIDR (например, 192.168.199.10/32).

Список служит фильтром: если адрес отправителя лога не входит ни в один из указанных диапазонов, лог не обрабатывается.

Механизм аналогичен «роутерам» в DosGate — используется для определения, к какому профилю привязать входящие данные. Допускается использование как отдельных IP, так и сетей с масками. Для каждого источника можно добавить комментарий.



Резервное копирование

Раздел описывает методы создания резервных копий. Поддерживается автоматизированное резервирование скриптом и ручное копирование.

Резервное копирование скриптом

Скрипт выполняет автоматическое формирование архивного файла, который включает резервные копии баз данных **PostgreSQL** и **MongoDB**, конфигурационные файлы сервисов, а также дополнительные данные: шаблоны и конфигурации **nginx**. Полученный архив может быть использован для восстановления системы при необходимости.

Для запуска необходимо выполнить команду:

```
curl -o "./backup.sh" "https://public-
repo.svcp.io/utility/backup.sh" && \
    sudo chmod +x "./backup.sh" && \
    ./backup.sh
```

Архив резервной копии сохраняется в директории: **/opt/backups/**

Ручное резервное копирование

Подготовка

Создать директорию для резервных копий:

```
sudo mkdir -p /opt/backups
```

Создать временную директорию:

```
sudo mkdir -p /opt/backups/node0
```

Резервное копирование базы данных PostgreSQL

Проверить наличие файла конфигурации:

```
sudo ls -la /opt/sp-spider-broker/.env
```

Открыть файл и посмотреть значения переменных подключения к базе (**DB_HOST**, **DB_PORT**, **DB_USER**, **DB_PASSWORD**, **DB_NAME**). Эти параметры понадобятся для бэкапа:

```
sudo grep -E '^DB_' /opt/sp-spider-broker/.env
```

Создать директорию для бэкапа PostgreSQL:

```
sudo mkdir -p /opt/backups/node0/postgres
```

Выполнить резервное копирование PostgreSQL с использованием считанных параметров:

```
sudo PGPASSWORD="DB_PASSWORD" pg_dump \
    -h "DB_HOST" \
    -p "DB_PORT" \
    -U "DB_USER" \
    "DB_DATABASE" \
    > /opt/backups/node0/postgres/DB_DATABASE.sql
```

Резервное копирование базы данных MongoDB

Проверить наличие утилиты **mongodump**:

```
sudo which mongodump
```

Если утилита не найдена — установить:

```
sudo apt-get update
sudo apt-get install -y mongodb-clients
```

Получить параметры подключения к MongoDB из PostgreSQL:

```
sudo PGPASSWORD="DB_PASSWORD" psql \
  -h "DB_HOST" \
  -p "DB_PORT" \
  -U "DB_USER" \
  -d "DB_DATABASE" \
  -t -A \
  -c 'SELECT "mongoConnection"::text FROM public.node LIMIT 1;'
```

Создать директорию для резервной копии MongoDB:

```
sudo mkdir -p /opt/backups/node0/mongo
```

Выполнить резервное копирование MongoDB (подставьте свои значения из mongoConnection):

```
sudo mongodump \
    --host "DB_HOST" \
    --port "DB_PORT" \
    --username "DB_USER" \
    --password "DB_PASSWORD" \
    --db "DB_DATABASE" \
    --out /opt/backups/node0/mongo
```

Резервное копирование конфигурационных файлов

Ядро системы (DosGate)

Создать директорию для резервной копии DosGate:

```
sudo mkdir -p /opt/backups/node0/dosgate
```

Скопировать конфигурационный файл:

```
sudo cp /etc/dosgate.conf /opt/backups/node0/dosgate/
```

Выполнить резервное копирование:

```
sudo dgadm --backup="/opt/backups/node0/dosgate/dgadm_backup" --
no-lic
```

Сессионная защита (DosGate-UH)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/dosgate-uh
```

Скопировать конфигурационный файл:

```
sudo cp /etc/dosgate-uh.conf /opt/backups/node0/dosgate-uh/
```

Веб-интерфейс (SP-Spider)

Внимание! Компонент может быть установлен на отдельной ноде. Операции выполняются на той ноде, где установлен веб-интерфейс.

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/sp-spider
```

Скопировать конфигурационный файл:

```
sudo cp /opt/sp-spider/.env /opt/backups/node0/sp-spider/
```

Брокер синхронизаций (SP-Spider-Broker)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/sp-spider-broker
```

Скопировать конфигурационный файл:

```
sudo cp /opt/sp-spider-broker/.env /opt/backups/node0/sp-spider-
broker/
```

Сервис событий (SP-Events)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/sp-events
```

Скопировать конфигурационный файл:

```
sudo cp /opt/sp-events/.env /opt/backups/node0/sp-events/
```

Скопировать каталог *template*:

```
sudo cp -r /opt/sp-events/template /opt/backups/node0/sp-events/
```

Модуль анализа логов (RLOG)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/rlog
```

Скопировать конфигурационный файл:

```
sudo cp /opt/rlog/.env /opt/backups/node0/rlog/
```

Посмотреть значение **RULES_FOLDER** в файле *.env* модуля RLOG:

```
grep "RULES_FOLDER" /opt/rlog/.env
```

Создать директорию для правил в резервной копии:

```
sudo mkdir -p /opt/backups/node0/rlog/rules
```

Скопировать директорию с правилами RLOG:

```
sudo cp -r RULES_FOLDER /opt/backups/node0/rlog/
```

Модуль автоматической генерации правил (AutoPilot)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/auto-rule
```

Скопировать конфигурационный файл:

```
sudo cp /opt/auto-rule/.env /opt/backups/node0/auto-rule/
```

Скопировать файлы лицензий:

```
sudo cp /opt/auto-rule/*.lic /opt/backups/node0/auto-rule/
```

Анализатор трафика (FlowCollector)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/spfc
```

Скопировать конфигурационный файл:

```
sudo cp /opt/spfc/etc/analyzer.yaml /opt/backups/node0/spfc/
```

Скопировать каталог *etc*:

```
sudo cp -r /opt/spfc/etc /opt/backups/node0/spfc/
```

Агент сбора метрик (Carbon-ClickHouse)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/carbon-clickhouse
```

Скопировать конфигурационный файл:

```
sudo cp /etc/carbon-clickhouse/carbon-clickhouse.conf
/opt/backups/node0/carbon-clickhouse/
```

Хранилище метрик (Graphite-ClickHouse)

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/graphite-clickhouse
```

Скопировать конфигурационный файл:

```
sudo cp /etc/graphite-clickhouse/graphite-clickhouse.conf
/opt/backups/node0/graphite-clickhouse/
```

Nginx

Создать директорию для резервной копии:

```
sudo mkdir -p /opt/backups/node0/nginx
```

Скопировать конфигурационный файл:

```
sudo cp /etc/nginx/nginx.conf /opt/backups/node0/nginx/
```

Скопировать каталоги *sites-enabled* и *sites-available*:

```
sudo cp -r /etc/nginx/sites-* /opt/backups/node0/nginx/
```

Создание архива

Создать архив:

```
sudo tar -czf /opt/backups/node0.tar.gz -C /opt/backups node0
```

Удалить временную директорию:

```
sudo rm -rf /opt/backups/node0
```

Проверить результат:

```
ls -la /opt/backups/node0.tar.gz
```

Проверить содержимое архива (отобразить первые 20 файлов):

```
sudo tar -tzf /opt/backups/node0.tar.gz | head -20
```

В результате выполнения шагов сформирован архив **/opt/backups/node0.tar.gz**, содержащий резервные копии PostgreSQL и MongoDB, конфигурационные файлы сервисов и дополнительные данные (шаблоны, лицензии, конфигурации nginx)

Восстановление системы

Перейти в каталог **/opt/backups/**, найти архив с резервной копией и распаковать:

```
sudo tar -xzvf node0.tar.gz
```

Восстановление базы данных PostgreSQL

Перейти в каталог базы:

```
cd node0/postgres
```

Найти файл с расширением **.sql**.

При необходимости создать базу и пользователя:

```
sudo -u postgres psql
```

- В консоли PostgreSQL выполнить:

```
CREATE DATABASE DB_DATABASE;
CREATE USER DB_USER WITH ENCRYPTED PASSWORD 'DB_PASSWORD';
GRANT ALL PRIVILEGES ON DATABASE DB_DATABASE TO DB_USER;
\q
```

Выполнить восстановление базы:

```
sudo PGPASSWORD="DB_PASSWORD" psql \
  -h "DB_HOST" \
  -p "DB_PORT" \
  -U "DB_USER" \
  -d "DB_DATABASE" \
  -f DB_DATABASE.sql
```

При необходимости обновить параметры подключения в конфигурационных файлах (.env) сервисов *sp-spider*, *sp-spider-broker*.

Перезапустить сервисы:

```
sudo systemctl restart sp-spider sp-spider-broker
```

Восстановление конфигурационных файлов

Ядро системы (DosGate)

Остановить Dosgate:

```
sudo systemctl stop dosgate
```

Очистить кэш:

```
sudo dgadm --batch=uh -y
```

Перейти в каталог с резервной копией:

```
cd node0/dosgate
```

Скопировать конфигурационный файл:

```
sudo cp ./dosgate.conf /etc/dosgate.conf
```

Выполнить восстановление конфигурации из резервной копии:

```
sudo dgadm --restore="/opt/backups/node0/dosgate/dgadm_backup" --
no-lic
```

Запустить сервис:

```
sudo systemctl start dosgate
```

Сессионная защита (DosGate-UH)

Перейти в каталог с резервной копией:

```
cd node0/dosgate-uh
```

Скопировать конфигурационный файл:

```
sudo cp ./dosgate-uh.conf /etc/dosgate-uh.conf
```

Перезапустить сервис:

```
sudo systemctl restart dosgate-uh
```

Веб-интерфейс (SP-Spider)

Внимание! Компонент может быть установлен на отдельной ноде. Операции выполняются на той ноде, где установлен веб-интерфейс.

Перейти в каталог с резервной копией:

```
cd node0/sp-spider
```

Скопировать конфигурационный файл:

```
sudo cp ./.env /opt/sp-spider/.env
```

Перезапустить сервис:

```
sudo systemctl restart sp-spider
```

Брокер сообщений (SP-Spider-Broker)

Перейти в каталог с резервной копией:

```
cd node0/sp-spider-broker
```

Скопировать конфигурационный файл:

```
sudo cp ./.env /opt/sp-spider-broker/.env
```

Перезапустить сервис:

```
sudo systemctl restart sp-spider-broker
```

Модуль анализа логов (RLOG)

Перейти в каталог с резервной копией:

```
cd node0/rlog
```

Скопировать конфигурационный файл:

```
sudo cp ./.env /opt/rlog/.env
```

Перезапустить сервис:

```
sudo systemctl restart rlog
```

Модуль автоматической генерации правил (Autopilot)

Перейти в каталог с резервной копией:

```
cd node0/auto-rule
```

Скопировать конфигурационный файл:

```
sudo cp ./.env /opt/auto-rule/.env
```

Скопировать файлы лицензий:

```
sudo cp ./*.lic /opt/auto-rule/*.lic
```

Перезапустить сервис:

```
sudo systemctl restart auto_rule
```

Агент сбора метрик (Carbon-ClickHouse)

Перейти в каталог с резервной копией:

```
cd node0/carbon-clickhouse
```

Скопировать конфигурационный файл:

```
sudo cp ./carbon-clickhouse.conf /etc/carbon-clickhouse/carbon-clickhouse.conf
```

Перезапустить сервис:

```
sudo systemctl restart carbon-clickhouse
```

Хранилище метрик (Graphite-ClickHouse)

Перейти в каталог с резервной копией:

```
cd node0/graphite-clickhouse
```

Скопировать конфигурационный файл:

```
sudo cp ./graphite-clickhouse.conf /etc/graphite-
clickhouse/graphite-clickhouse.conf
```

Перезапустить сервис:

```
sudo systemctl restart graphite-clickhouse
```

Nginx

Перейти в каталог с резервной копией:

```
cd node0/nginx
```

Скопировать конфигурационный файл:

```
sudo cp ./nginx.conf /etc/nginx/nginx.conf
```

Скопировать каталоги *sites-enabled* и *sites-available*:

```
sudo cp -r ./sites-* /etc/nginx/
```

Перезапустить сервис:

```
sudo systemctl restart nginx
```

Проверка целостности данных

Функционал вычисления хэш-сумм обеспечивает автоматическую генерацию и проверку хэш-суммы XDP-программы в процессе её передачи, хранении или обновления, что позволяет контролировать целостность данных.

Функция реализуется следующим образом:

Подсчет хэш-суммы

- Хэш-сумма рассчитывается на основе ELF-файла программы перед загрузкой в ядро.
- Для подсчета используется алгоритм, обеспечивающий высокую скорость и криптографическую стойкость (SHA-256).
  Сохранение хэш-суммы
- Хэш-сумма сохраняется вместе с метаданными программы в ядре (через BPF syscall или в логах).
- В случае изменения программы новая хэш-сумма вычисляется и сохраняется.

Сценарии применения

У Досгейта есть множество разных сценариев применения.

Он может быть использован как:

- пограничное устройство сети в виде пакетного фильтра
- stateless firewall
- полноценное standalone решение для защиты от ДДоС-атак.

Кроме этого, Досгейт может быть использован и напрямую интегрирован для разгрузки различных DPI, WAF, bot management, или NGFW систем.

Всё это доступно за счет **единого конструктора правил**, с помощью которого администратор системы сам выбирает какие функции и инструменты он комбинирует между собой для достижения той или иной цели.

В данной документации приведены примеры, как Досгейт может быть использован в разных случаях.

Incorrect TCP flags

Досгейт позволяет администратору системы завести набор правил, по которому можно сбрасывать некорректные TCP-флаги. Это может быть полезно как в случае эксплуатации Досгейта как Анти-ДДоС решения, так и пакетного файрволла

Данный набор правил рекомендуется для применения в внешних TCP-сервисах, например, на игровых серверах которые используют протокол TCP, а также веб-приложениях, которые защищаются только с использованием dosgate без WAF, bot management систем, и др. ПО которое обрабатывает HTTP/HTTPs трафик на прикладном уровне

Набор правил

Для каждого правила написан комментарий статистики для корректной визуализации в Collectd.

```
# В примере используется arena first и профиль test
# Создание цепочки правил (chain)
dgctl -u chain://first/test -c insert tcp_flags_chain Chain to
drop TCP packets with malicious flags

# Наполнение цепочки правил
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags fin,syn/fin,sin -j STATS INVALID_TCP_FLAG
-j DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags syn,rst/syn,rst -j STATS INVALID_TCP_FLAG
-j DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags fin,rst/fin,rst -j STATS INVALID_TCP_FLAG
-j DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags fin/fin,ack -j STATS INVALID_TCP_FLAG -j
DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags fin,psh,urg/fin,psh,urg -j STATS
INVALID_TCP_FLAG -j DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags /sin,rst,ack -j STATS INVALID_TCP_FLAG -j
DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags /syn,fin,rst,ack,psh,urg,ece,ecr -j STATS
INVALID_TCP_FLAG -j DROP
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m tcpflags syn ! -m tcpmss 536-65535 -j STATS
SUSPICIOS_MSS
dgctl -u chain://first/test/tcp_flags_chain -c insert -- -m
protocol tcp -m sport 21,80,443 -m dport 80,443 -j STATS
WEB_INVALID -j DROP

# Добавление правила в профиль защиты об отправке всех TCP пакетов
на обработку через ранее созданную цепочку
dgctl -u profile://first/test -c insert -- -m protocol tcp -j GOTO
tcp_flags_chain
```

Anti-DDoS

В качестве примера мы используем следующие вводные данные: Досгейт является устройством защиты внешнего периметра сети, на котором расположена 1 подсеть /24.

Основное преимущество Досгейта - возможность детализированного описания сервисов, как их легитимных, так и потенциальных вредоносных параметров, по которым можно сбрасывать атакующие пакеты, без привязанности к каким-то конкретным контрмерам и ограниченным настройкам.

Досгейт работает как единый конструктор правил, с помощью которого можно быстро и легко описать существующие сервисы, комбинировать наборы данных и функции между собой для создания эффективной ДДоС-защиты.

Правила фильтрации, созданные в данном документе являются примером использования существующих инструментов, а не регламентируют конкретный тип или порядок их использования.

В рамках сети работают как UDP, так и TCP сервисы. В рамках карты сервисов мы знаем, что:

- На IP-адресе .251 на порту TCP 8443 работает VPN, на порту TCP 22 работает SSH
- На IP-адресе .252 на порту TCP 443 работает веб-приложение с использованием HTTPs
- На IP-адресе .253 на порту UDP 53 и TCP 53 работает DNS-сервер
- На IP-адресах .251, .252, .253 - не живут никакие сервисы кроме описанных и они полностью под них зарезервированы

Помимо этих данных, мы знаем, что на остальных 252 адресах также время от времени появляются и удаляются внешние сервисы, которые тоже могут стать целью ДДоС-атаки, и мы должны защищать их в том числе.

В нашем примере arena имеет название `first`

Создание профиля защиты

```
dgctl -u arena://first -c add global all_services
```

Аллокация IP-адресов получателей к профилям

```
dgctl -u router://first/global -c insert -- x.x.x.0/24
```

Общие правила фильтрации

В рамках общих правил фильтрации мы сбрасываем самые популярные атаки, которые являются едиными для всех сервисов: VPN, WEB, DNS, SSH, и др.

Блокировка амплификаций

Сброс пакетов с вредоносных портов отправителя протокола UDP

```
dgctl -u profile://first/global -c insert -- -m protocol udp -m
sport
19,6881,389,751,11211,1434,5353,137,111,17,27960,520,1900,27015,7001
-j STATS amplifications -j DROP
dgctl -u profile://first/global -c insert -- -m protocol udp -m
sport 123 ! -m len what net:packet len 76 -j STATS amplifications
-j DROP
dgctl -u profile://first/global -c insert -- -m protocol udp -m
dport 53 -m len what net:packet len 1000-1500 -j STATS
amplifications -j DROP
dgctl -u profile://first/global -c insert -- -m protocol udp -m
sport 53 -m len what net:packet len 1000-1500 -j STATS dns_flood -
j DROP
```

Сброс всех протоколов кроме часто-используемых

В этом примере: TCP, UDP, ICMP, ESP, GRE, IPIP, AH

```
dgctl -u profile://first/global -c insert -- -m protocol
udp,tcp,icmp -j MARK how set value 2
dgctl -u profile://first/global -c insert -- -m protocol
ah,esp,ipip,gre -j MARK how set value 2
dgctl -u profile://first/global -c insert -- ! -m mark 2 -j STATS
incorrect_protocol -j DROP
```

Создание отдельных цепочек правил

Для каждого сервиса - своя индивидуальная цепочка правил, в которую пакет переходит из основного профиля

```
dgctl -u chain://first/global -c insert -- DNS
dgctl -u chain://first/global -c insert -- WEB
dgctl -u chain://first/global -c insert -- VPN_and_ssh
dgctl -u chain://first/global -c insert -- other
```

Маршрутизация сервисов

В зависимости от IP-получателя, пакет отправляется в специфичную для этого сервиса цепочку правил

```
dgctl -u profile://first/global -c insert -- ! -m dst
x.x.x.251,x.x.x.252,x.x.x.253 -j GOTO other
dgctl -u profile://first/global -c insert -- -m dst x.x.x.251 -j
GOTO VPN_and_ssh
dgctl -u profile://first/global -c insert -- -m dst x.x.x.252 -j
GOTO WEB
dgctl -u profile://first/global -c insert -- -m dst x.x.x.253 -j
GOTO DNS
```

Настройка цепочки правил other

Активация защиты по триггеру

В случае, если общий трафик, проходящий через это правило, составляет меньше 500 MBps, трафик пропускается сразу конечному получателю (bypass). Когда трафик становится выше 500 MBps - пакеты начинают проходить через остальные правила в профиле защиты (и в соединенных с профилем цепочках). В случае, если трафик стал ниже порога в 500 MBps - чтобы триггер перестал быть активным должно пройти еще 60 секунд (cooldown, для pulse wave атак)

```
dgctl -u chain://first/global/other -c insert -- -j RATELIMIT 2
key "" cooldown 60 bps 500m
dgctl -u chain://first/global/other -c insert -- -m verdict
ratelimit conform -j ACCEPT
```

TCP-авторизация

Методом RST для защиты от IP-spoofing атак, авторизация IP отправителя на 3600 секунд. TCP-авторизация

```
dgctl -u chain://first/global/other -c insert -- ! -m hmark id 2
status valid -j TCPAUTH id 1 type hs atype hs
dgctl -u chain://first/global/other -c insert -- -m verdict
tcpauth valid -j HMARK id 2 value 2 lifetime 3600
```

Защита от ботнетов

В случае, если 1 IP отправителя превышает 2000 пакетов в секунду, IP-адрес отправителя из пакета заносится в метку "hmark" ID 1 (быструю таблицу данных) и хранится там установленный lifetime (в нашем примере, 600 секунд). Правило по сбросу IP-адресов которые были заблокированы устанавливается на первое место после триггера о том что идет атака для ускорения работы системы, атаки ботнетами могут превышать сотни ГБит/с.

```
dgctl -u chain://first/global/other -c insert -i 3 -- -m hmark id
1 status valid -j STATS 2000pps -j DROP
dgctl -u chain://first/global/other -c insert -- -j RATELIMIT 1
key "l3_src" pps 2000
dgctl -u chain://first/global/other -c insert -- -m verdict
ratelimit exceed -j HMARK id 1 value 1 lifetime 600
```

ACL для TCP

```
dgctl -u chain://first/global/other -c insert -- -m protocol tcp -
m sport 0-1023 -j STATS bad_ports_tcp -j DROP
```

Защита от SYN flood ботами

Блокировка IP отправителя на 600 секунд при превышении 50 PPS SYN)

```
dgctl -u chain://first/global/other -c insert -- -m tcpflags
syn/syn -j RATELIMIT 3 key "l3_src" pps 50
dgctl -u chain://first/global/other -c insert -- -m verdict
ratelimit exceed -j HMARK id 1 value 2 lifetime 600
```

Сброс IP-фрагментации в UDP

```
dgctl -u chain://first/global/other -c insert -- -m protocol udp -
m frag -j STATS fragmentation -j DROP
```

Сброс QUIC-flood атак

```
dgctl -u chain://first/global/other -c insert -- -m protocol udp -
m sport 80,443 -m dport 80,443 -j DROP
```

Гео-шейпинг

Если может быть применим, для всех стран кроме России, Беларуси, Казахстана, Узбекистана, Кыргызстана, Грузии, Армении, и Азербайджана до 150 MBps

```
dgctl -u chain://first/global/other -c insert -- ! -m geoip cntr
RU,BY,KZ,UZ,KG,GE,AM,AZ -j RATELIMIT 4 key "" bps 150m
dgctl -u chain://first/global/other -c insert -- -m verdict
ratelimit exceed -j STATS geo_shaping -j DROP
```

Настройка цепочки правил DNS

ACL

Зная какой сервис расположен на этом адресе, мы заранее сбрасываем все проходимые пакеты не отправленные на порт получателя 53, а также те пакеты - которые не содержат DNS header в пакете.

```
dgctl -u chain://first/global/DNS -c insert -- ! -m dport 53 -j
DROP
dgctl -u chain://first/global/DNS -c insert -- ! -m dns -j DROP
```

Активация защиты по триггеру

В случае если общий трафик проходимый через это правило составляет меньше 100 MBps, трафик пропускается сразу конечному получателю (bypass). Когда трафик становится выше 100 MBps - пакеты начинают проходить через остальные правила в профиле защиты (и в соединенных

с профилем цепочках). В случае если трафик стал ниже порога в 100 MBps - чтобы триггер перестал быть активным должно пройти еще 60 секунд (cooldown, для pulse wave атак)

```
dgctl -u chain://first/global/DNS -c insert -- -j RATELIMIT 2 key
"" cooldown 60 bps 100
dgctl -u chain://first/global/DNS -c insert -- -m verdict
ratelimit conform -j ACCEPT
```

TCP-авторизация

Методом RST для защиты от IP-spoofing атак, авторизация IP отправителя на 3600 секунд. TCP-авторизация

```
dgctl -u chain://first/global/DNS -c insert -- ! -m hmark id 2
status valid -j TCPAUTH id 1 type hs atype hs
dgctl -u chain://first/global/DNS -c insert -- -m verdict tcpauth
valid -j HMARK id 2 value 2 lifetime 3600
```

Защита от ботнетов

В случае, если 1 IP отправителя превышает 2000 пакетов в секунду, IP-адрес отправителя из пакета заносится в метку "hmark" ID 1 (быструю таблицу данных) и хранится там установленный lifetime (в нашем примере, 600 секунд). Правило по сбросу IP-адресов которые были заблокированы устанавливается на первое место после триггера о том что идет атака для ускорения работы системы, атаки ботнетами могут превышать сотни ГБит/с.

```
dgctl -u chain://first/global/DNS -c insert -i 5 -- -m hmark id 1
status valid -j STATS 2000pps -j DROP
dgctl -u chain://first/global/DNS -c insert -- -j RATELIMIT 1 key
"l3_src" pps 2000
dgctl -u chain://first/global/DNS -c insert -- -m verdict
ratelimit exceed -j HMARK id 1 value 1 lifetime 600
```

DNS geo shaping для всех стран кроме России до 100 MBps

```
dgctl -u chain://first/global/DNS -c insert -- ! -m geoip cntr RU
-j RATELIMIT id 8 key "l3_dst" bps 100m
```

```
dgctl -u chain://first/global/DNS -c insert -- -m verdict
ratelimit exceed -j DROP
```

Настройка цепочки правил VPN_and_ssh

ACL

```
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -m dport
8443,22 -m protocol TCP -j MARK how set value 2
dgctl -u chain://first/global/VPN_and_ssh -c insert -- ! -m mark 2
-j DROP
```

Активация защиты по триггеру

В случае если общий трафик проходимый через это правило составляет меньше 100 MBps, трафик пропускается сразу конечному получателю (bypass). Когда трафик становится выше 100 MBps - пакеты начинают проходить через остальные правила в профиле защиты (и в соединенных с профилем цепочках). В случае если трафик стал ниже порога в 100 MBps - чтобы триггер перестал быть активным должно пройти еще 60 секунд (cooldown, для pulse wave атак)

```
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -j
RATELIMIT 2 key "" cooldown 60 bps 100m
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -m verdict
ratelimit conform -j ACCEPT
```

TCP-авторизация

Методом RST для защиты от IP-spoofing атак, авторизация IP отправителя на 3600 секунд. TCP-авторизация

```
dgctl -u chain://first/global/VPN_and_ssh -c insert -- ! -m hmark
id 2 status valid -j TCPAUTH id 1 type hs atype hs
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -m verdict
tcpauth valid -j HMARK id 2 value 2 lifetime 3600
```

Защита от ботнетов

В случае, если 1 IP отправителя превышает 2000 пакетов в секунду, IP-адрес отправителя из пакета заносится в метку "hmark" ID 1 (быструю таблицу данных) и хранится там установленный lifetime (в нашем примере, 600 секунд). Правило по сбросу IP-адресов, которые были заблокированы, устанавливается на первое место после триггера о том, что идет атака для ускорения работы системы, атаки ботнетами могут превышать сотни ГБит/с.

```
dgctl -u chain://first/global/VPN_and_ssh -c insert -i 4 -- -m
hmark id 1 status valid -j STATS 2000pps -j DROP
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -j
RATELIMIT 1 key "l3_src" pps 2000
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -m verdict
ratelimit exceed -j HMARK id 1 value 1 lifetime 600
```

GEO shaping для всех стран кроме России на 100 MBps на каждый IP-получателя

```
dgctl -u chain://first/global/VPN_and_ssh -c insert -- ! -m geoip
cntr RU -j RATELIMIT id 8 key "l3_dst" bps 100m
dgctl -u chain://first/global/VPN_and_ssh -c insert -- -m verdict
ratelimit exceed -j DROP
```

Настройка цепочки правил WEB

ACL

```
dgctl -u chain://first/global/WEB -c insert -- -m dport 443 -m
protocol TCP -j MARK how set value 3
dgctl -u chain://first/global/WEB -c insert -- ! -m mark 3 -j DROP
```

Активация защиты по триггеру

В случае если общий трафик проходимый через это правило составляет меньше 200 MBps, трафик пропускается сразу конечному получателю (bypass). Когда трафик становится выше 200 MBps - пакеты начинают проходить через остальные правила в профиле защиты (и в соединенных с профилем цепочках). В случае если трафик стал ниже порога в 200

MBps - чтобы триггер перестал быть активным должно пройти еще 60 секунд (cooldown, для pulse wave атак)

```
dgctl -u chain://first/global/WEB -c insert -- -j RATELIMIT 2 key
"" cooldown 60 bps 200m
dgctl -u chain://first/global/WEB -c insert -- -m verdict
ratelimit conform -j ACCEPT
```

TCP-авторизация

Методом RST для защиты от IP-spoofing атак, авторизация IP отправителя на 3600 секунд. TCP-авторизация

```
dgctl -u chain://first/global/WEB -c insert -- ! -m hmark id 2
status valid -j TCPAUTH id 1 type hs atype hs
dgctl -u chain://first/global/WEB -c insert -- -m verdict tcpauth
valid -j HMARK id 2 value 2 lifetime 3600
```

Защита от ботнетов

В случае, если 1 IP отправителя превышает 2000 пакетов в секунду, IP-адрес отправителя из пакета заносится в метку "hmark" ID 1 (быструю таблицу данных) и хранится там установленный lifetime (в нашем примере, 600 секунд). Правило по сбросу IP-адресов которые были заблокированы устанавливается на первое место после триггера о том что идет атака для ускорения работы системы, атаки ботнетами могут превышать сотни ГБит/с.

```
dgctl -u chain://first/global/WEB -c insert -i 4 -- -m hmark id 1
status valid -j STATS 2000pps -j DROP
dgctl -u chain://first/global/WEB -c insert -- -j RATELIMIT 1 key
"l3_src" pps 2000
dgctl -u chain://first/global/WEB -c insert -- -m verdict
ratelimit exceed -j HMARK id 1 value 1 lifetime 600
```

Stateless Firewall

В качестве примера мы используем следующие вводные данные: Досгейт является устройством защиты внешнего периметра сети, через которое ходит трафик. После этого трафик попадает внутрь сети. Досгейт

используется как промежуточный пакетный фильтр, выполняющий, в том числе функции файрволла.

В данном файле можно найти примеры использования Досгейта, как пакетного фильтра, для решения задач межсетевого экрана, ACL-фильтра, белых и черных списков, контроля доступа

В нашем примере, arena имеет название `first`, профиль имеет название `firewall`

Защита SSH-сервера от перебора паролей (bruteforce)

Блокировка IP-отправителя который перебирает пароль к SSH-сервису работающему на порту TCP 22 на 600 секунд, в случае если было больше 10 попыток установить соединение за минуту

```
# Проверка на IP-spoofing с помощью TCP-авторизации, чтобы атакующий не мог заблокировать легитимные IP-адреса от доступа к SSH

dgctl -u profile://first/firewall -c insert -- ! -m hmark id 1 status valid -j TCPAUTH id 1 type hs atype hs
dgctl -u profile://first/firewall -c insert -- -m verdict tcpauth valid -j HMARK id 1 value 1 lifetime 3600

# Блокировка IP-отправителя в случае если совершено больше 10 попыток соединения (определяется по пакету с SYN флагом в сторону TCP порта получателя 22) за 60 секунд с момента последней попытки

dgctl -u profile://first/firewall -c insert -- -m sdhmark id 1 status matches value 10-999 -j STATS ssh_bruteforce -j DROP
dgctl -u profile://first/firewall -c insert -- -m protocol tcp -m dport 22 -m tcpflags syn/syn -j SDHMARK id 1 how add value 1 lifetime 60
```

Сброс чужих IP-подсетей (тех, какие не занесены в белый список) в случае обращения к системным портам на сети

В этом примере системным является порт 22 по протоколам TCP и UDP. Это может применяться также на целые устройства на сети, например, когда нужно заблокировать доступ к определенному IP-получателя от всех кроме указанных масок, или даже стран (используя `-m geoip`)

```
# Создание локального префикс-сета, активного только для этого профиля

dgctl -u prefixset://first/firewall/ -c new internal_access

# Добавление IP-масок в префикс-сет
dgctl -u prefixset://first/firewall/internal_access -c insert -- 1.4.4.3/32 1,1.4.4.5/32 1,1.4.6.0/24 1

# Применение префикс-сета
dgctl -u prefixset://first/firewall/internal_access -c commit

# Создание правила, которое отрабасывает весь трафик на порт получателя 22 на протоколе UDP и TCP, в случае если IP-отправителя не находится в префикс-сете internal_access
dgctl -u profile://first/firewall -c insert -- -m dport 22 ! -m pset internal_access class local what src value 1 -j STATS no_internal_access -j DROP
```

Blackholing

В случае если нам нужно заблокировать доступ к определенному IP-адресу, или от определенных IP-адресов. В этом примере адреса находятся сразу в правиле, но они также могут забираться из созданного префикс-сета

```
dgctl -u profile://first/firewall -c insert -- -m dst 7.7.7.7 -j STATS dst_7_7_7_7_blackhole -j DROP
dgctl -u profile://first/firewall -c insert -- -m src 5.5.5.5 -j STATS src_5_5_5_5_blackhole -j DROP
```

Географический шейпинг

В некоторых случаях, требуется ограничить доступ к определенным ресурсам, например, только Российскими сетями. В этом примере мы ограничиваем трафик из всех стран кроме России в сторону указанных IP-масок получателей в 10 MBps.

```
dgctl -u profile://first/firewall -c insert -- ! -m geoip cntr RU
-m dst 3.3.3.3,3.2.2.0/24,3.7.6.2/28 -j RATELIMIT 1 key "" bps 10m
dgctl -u profile://first/firewall -c insert -- -m verdict
ratelimit exceed -j STATS geo_shape -j DROP
```

Bandwidth enforcement

В сетевой инфраструктуре находится несколько групп клиентов, которые отправляют и получают трафик

Администратору системы необходимо ограничить полосу пропускания на входящий и исходящий трафик индивидуально для каждой группы клиентов

Такое может быть применимо, например, в операторе связи, который продает разные группы тарификации разным клиентам, или хостингу, который хочет ограничить полосу пропускания определенных виртуальных или серверных платформ

В этом примере, трафик на постоянной основе маршрутизируется через аппаратную платформу на которой установлено ПО. Создано две арены: одна на входящий трафик, другая на исходящий

`arena:in eth1 > eth2 | arena:out eth2 > eth1`

В данном примере также всего 2 группы клиентов, их может быть больше

Первая группа клиентов ограничивается в `100 MBps входящего трафика` и `100 MBps исходящего трафика`

Вторая группа клиентов ограничивается в `50 MBps входящего трафика` и `25 MBps исходящего трафика`

Создание профилей

```
dgctl -u arena://in -c add bandwidth
dgctl -u arena://out -c add bandwidth
```

Настройка маршрутизации всего трафика через эти профили

```
dgctl -u router://in/bandwidth -c insert -- 0.0.0.0/0
dgctl -u router://out/bandwidth -c insert -- 0.0.0.0/0
```

Создание префикс-сетов, как определителя группы клиентов

```
# Входящий трафик
dgctl -u prefixset://in/bandwidth/ -c new group1
dgctl -u prefixset://in/bandwidth/ -c new group2

# Исходящий трафик
dgctl -u prefixset://out/bandwidth/ -c new group1
dgctl -u prefixset://out/bandwidth/ -c new group2
```

Добавление IP-адресов в префикс-сеты

```
# Адреса первой группы
dgctl -u prefixset://in/bandwidth/group1 -c insert -- 1.1.1.0/24 1
dgctl -u prefixset://out/bandwidth/group1 -c insert -- 1.1.1.0/24
1

# Адреса второй группы
dgctl -u prefixset://in/bandwidth/group2 -c insert -- 1.1.2.0/24 1
dgctl -u prefixset://out/bandwidth/group2 -c insert -- 1.1.2.0/24
1
```

Правила для входящего трафика

```
# Ограничения для первой группы
dgctl -u profile://in/bandwidth -c insert -- -m pset group1 class
local what dst -j RATELIMIT 1 key "l3_dst" bps 100m
dgctl -u profile://in/bandwidth -c insert -- -m verdict ratelimit
exceed -j DROP
dgctl -u profile://in/bandwidth -c insert -- -j VERDICT clear

# Ограничения для второй группы
dgctl -u profile://in/bandwidth -c insert -- -m pset group2 class
local what dst -j RATELIMIT 1 key "l3_dst" bps 50m
dgctl -u profile://in/bandwidth -c insert -- -m verdict ratelimit
exceed -j DROP
dgctl -u profile://in/bandwidth -c insert -- -j VERDICT clear
```

Правила для исходящего трафика трафика

```
# Ограничения для первой группы
dgctl -u profile://out/bandwidth -c insert -- -m pset group1 class
local what src -j RATELIMIT 1 key "l3_dst" bps 100m
dgctl -u profile://out/bandwidth -c insert -- -m verdict ratelimit
exceed -j DROP
dgctl -u profile://out/bandwidth -c insert -- -j VERDICT clear

# Ограничения для второй группы
dgctl -u profile://out/bandwidth -c insert -- -m pset group2 class
local what src -j RATELIMIT 1 key "l3_dst" bps 25m
dgctl -u profile://out/bandwidth -c insert -- -m verdict ratelimit
exceed -j DROP
dgctl -u profile://out/bandwidth -c insert -- -j VERDICT clear
```

Настройка и управление DosGate через CLI

Данная документация описывает взаимодействие с программным обеспечением DosGate с использованием командного интерфейса (CLI).

CLI является приоритетным способом управления системой, обеспечивая гибкость настройки и возможность автоматизации. Командный интерфейс позволяет администраторам работать с конкретными модулями системы, комбинировать параметры, правила и функции, что упрощает и ускоряет процесс конфигурирования.

Использование CLI обеспечивает полный доступ к функционалу системы и не ограничивает возможности администрирования, включая аварийные ситуации, в отличие от графических интерфейсов, подверженных перегрузке.

Адресация команд для управления таргетами системы

Взаимодействие с таргетами DosGate осуществляется через командный интерфейс (CLI) с использованием raw socket.

Команды делятся на два типа:

- Системные – выполняют общие операции с системой.
- Целевые – управляют конкретными таргетами системы.

1. Системные команды

Формат выполнения:

```
dgctl -c command
```

Доступные команды:

```
# Вывести справочную информацию
dgctl -c help

# Отобразить текущую версию DosGate.
dgctl -c version

# Отобразить список всех доступных таргетов
dgctl -c targets
```

2. Целевые команды

Формат выполнения:

```
dgctl -u target://arena-name/target-name/target-options -c command
-- command_options
```

Аргументы:

- `target://` – префикс, указывающий на обращение к целевому модулю.
- `<arena-name>` – имя арены, если требуется *(необязательный параметр)*.
- `<target-name>` – имя целевого модуля.
- `<target-options>` – дополнительные настройки *(необязательный параметр)*.
- `-c <command>` – команда, выполняемая в указанном модуле.
- `-- <command_options>` – дополнительные аргументы команды *(необязательный параметр)*.

Доступные целевые таргеты:

Таргет	Описание
system	Управление системными функциями.
license	Управление лицензиями.
daemon	Контроль фоновых процессов.

Таргет	Описание
geoip	Работа с географическими IP-базами.
context	Управление контекстами работы.
arena	Работа с аренами.
profile	Управление профилями.
router	Настройка маршрутизации.
mark	Управление метками.
prefixset	Работа с наборами префиксов.

Доступные команды:

```
# Вывести системную информацию
dgctl -u system:// -c sysinfo

# Получить идентификатор системы
dgctl -u system:// -c id

# Вывести справочную информацию.
dgctl -u system:// -c help

# Показать список лицензий
dgctl -u license:// -c list

# Отобразить информацию о лицензии
dgctl -u license:// -c show license
```

Управление таргетом: daemon

Для таргета daemon, не требуется указывать арену

daemon - полностью дублирует системные команды

Пример адресации таргета

`dgctl -u daemon:// -c help`

Управление таргетом: system

Таргет *system* предоставляет инструменты для получения информации о системе и проверки её состояния. Используется для мониторинга состояния системы, получения идентификационных данных и проверки доступности компонентов. Таргет не требует указания арены.

Формат выполнения:

```
dgctl -u system:// -c help
```

Доступные команды:

```
# Вывести справочную информацию
help

# Отобразить сведения о системе и использовании ресурсов DosGate
sysinfo

# Отобразить уникальный идентификатор системы
id

# Проверить доступность таргета
ping
```

Управление таргетом: license

Управление лицензиями включает в себя просмотр, добавление, удаление и откат изменений, а также их экспорт. Таргет не требует указания арены.

Формат выполнения:

```
dgctl -u license:// -c help
```

Доступные команды:

```
# Вывести список лицензий.
list

# Отобразить сведения о конкретной лицензии.
show

# Добавить новую лицензию.
add
```

```
# Удалить лицензию.
delete

# Отменить удаление лицензии (восстановление).
undelete

# Применить изменения (удаление или добавление лицензии).
commit

# Экспортировать (скачать) лицензию.
download

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

Управление таргетом: geoip

DosGate позволяет проверять IP-адрес отправителя и получателя на принадлежность определённому региону с использованием функции *geoip*.

Таргет не требует указания арены.

Формат выполнения:

```
dgctl -u geoip:// -c check -- <IP-адрес>
```

Пример:

```
dgctl -u geoip:// -c check -- 1.1.1.1
```

Вызов справки по таргету geoip:

```
dgctl -u geoip:// -c help
```

Загрузка собственной базы данных

По умолчанию DosGate загружает базу данных по пути:
/etc/dosgate/GeoLite2-Country.mmdb

Резервный путь: **/usr/share/dosgate/GeoLite2-Country.mmdb**

Чтобы использовать свою базу данных, необходимо:

1. Разместить файл *GeoLite2-Country.mmdb* в каталоге **/etc/dosgate/**.
2. Перезагрузить сервис DosGate:

```
sudo service dosgate restart
```

Содержимое базы данных

Для получения актуальной версии базы данных можно направить запрос по адресу: dosgate@servicepipe.ru

Теги geoip

Список всех тегов geoip

```
Countries
Code Name
=========================================================================

AF Afghanistan
AX Åland Islands
AL Albania
DZ Algeria
AS American Samoa
AD Andorra
AO Angola
AI Anguilla
AQ Antarctica
AG Antigua and Barbuda
AR Argentina
AM Armenia
AW Aruba
AU Australia
AT Austria
AZ Azerbaijan
BS Bahamas
BH Bahrain
BD Bangladesh
BB Barbados
BY Belarus
BE Belgium
```

BZ Belize
BJ Benin
BM Bermuda
BT Bhutan
BO Bolivia, Plurinational State of
BQ Bonaire, Sint Eustatius and Saba
BA Bosnia and Herzegovina
BW Botswana
BV Bouvet Island
BR Brazil
IO British Indian Ocean Territory
BN Brunei Darussalam
BG Bulgaria
BF Burkina Faso
BI Burundi
KH Cambodia
CM Cameroon
CA Canada
CV Cape Verde
KY Cayman Islands
CF Central African Republic
TD Chad
CL Chile
CN China
CX Christmas Island
CC Cocos (Keeling) Islands
CO Colombia
KM Comoros
CG Congo
CD Congo, the Democratic Republic of the
CK Cook Islands
CR Costa Rica
CI Côte d'Ivoire
HR Croatia
CU Cuba
CW Curaçao
CY Cyprus
CZ Czech Republic
DK Denmark
DJ Djibouti
DM Dominica
DO Dominican Republic
EC Ecuador
EG Egypt
SV El Salvador
GQ Equatorial Guinea
ER Eritrea
EE Estonia
ET Ethiopia
FK Falkland Islands (Malvinas)
FO Faroe Islands

FJ Fiji
FI Finland
FR France
GF French Guiana
PF French Polynesia
TF French Southern Territories
GA Gabon
GM Gambia
GE Georgia
DE Germany
GH Ghana
GI Gibraltar
GR Greece
GL Greenland
GD Grenada
GP Guadeloupe
GU Guam
GT Guatemala
GG Guernsey
GN Guinea
GW Guinea-Bissau
GY Guyana
HT Haiti
HM Heard Island and McDonald Islands
VA Holy See (Vatican City State)
HN Honduras
HK Hong Kong
HU Hungary
IS Iceland
IN India
ID Indonesia
IR Iran, Islamic Republic of
IQ Iraq
IE Ireland
IM Isle of Man
IL Israel
IT Italy
JM Jamaica
JP Japan
JE Jersey
JO Jordan
KZ Kazakhstan
KE Kenya
KI Kiribati
KP Korea, Democratic People's Republic of
KR Korea, Republic of
KW Kuwait
KG Kyrgyzstan
LA Lao People's Democratic Republic
LV Latvia
LB Lebanon

```
LS Lesotho
LR Liberia
LY Libya
LI Liechtenstein
LT Lithuania
LU Luxembourg
MO Macao
MK Macedonia, the Former Yugoslav Republic of
MG Madagascar
MW Malawi
MY Malaysia
MV Maldives
ML Mali
MT Malta
MH Marshall Islands
MQ Martinique
MR Mauritania
MU Mauritius
YT Mayotte
MX Mexico
FM Micronesia, Federated States of
MD Moldova, Republic of
MC Monaco
MN Mongolia
ME Montenegro
MS Montserrat
MA Morocco
MZ Mozambique
MM Myanmar
NA Namibia
NR Nauru
NP Nepal
NL Netherlands
NC New Caledonia
NZ New Zealand
NI Nicaragua
NE Niger
NG Nigeria
NU Niue
NF Norfolk Island
MP Northern Mariana Islands
NO Norway
OM Oman
PK Pakistan
PW Palau
PS Palestine, State of
PA Panama
PG Papua New Guinea
PY Paraguay
PE Peru
PH Philippines
```

```
PN Pitcairn
PL Poland
PT Portugal
PR Puerto Rico
QA Qatar
RE Réunion
RO Romania
RU Russian Federation
RW Rwanda
BL Saint Barthélemy
SH Saint Helena, Ascension and Tristan da Cunha
KN Saint Kitts and Nevis
LC Saint Lucia
MF Saint Martin (French part)
PM Saint Pierre and Miquelon
VC Saint Vincent and the Grenadines
WS Samoa
SM San Marino
ST Sao Tome and Principe
SA Saudi Arabia
SN Senegal
RS Serbia
SC Seychelles
SL Sierra Leone
SG Singapore
SX Sint Maarten (Dutch part)
SK Slovakia
SI Slovenia
SB Solomon Islands
SO Somalia
ZA South Africa
GS South Georgia and the South Sandwich Islands
SS South Sudan
ES Spain
LK Sri Lanka
SD Sudan
SR Suriname
SJ Svalbard and Jan Mayen
SZ Swaziland
SE Sweden
CH Switzerland
SY Syrian Arab Republic
TW Taiwan, Province of China
TJ Tajikistan
TZ Tanzania, United Republic of
TH Thailand
TL Timor-Leste
TG Togo
TK Tokelau
TO Tonga
TT Trinidad and Tobago
```

```
TN Tunisia
TR Turkey
TM Turkmenistan
TC Turks and Caicos Islands
TV Tuvalu
UG Uganda
UA Ukraine
AE United Arab Emirates
GB United Kingdom
US United States
UM United States Minor Outlying Islands
UY Uruguay
UZ Uzbekistan
VU Vanuatu
VE Venezuela, Bolivarian Republic of
VN Viet Nam
VG Virgin Islands, British
VI Virgin Islands, U.S.
WF Wallis and Futuna
EH Western Sahara
YE Yemen
ZM Zambia
ZW Zimbabwe
XK Kosovo
```

```
Continents
Code Name
=========================================================================

AF Africa
AN Antarctica
AS Asia
EU Europe
NA North America
OC Oceania
SA South America
```

Управление таргетом: context

Таргет *context* позволяет централизованно изменять параметры арен и управлять ими без необходимости указывать каждую арену отдельно.

Таргет *context* — необязательный компонент подсистемы, предназначенный для группировки нескольких арен в единый

логический объект. Это позволяет упростить массовое управление аренами в процессе конфигурирования dosgate через файл dosgate.conf.

Формат выполнения:

```
dgctl -u context:// -c help
```

Доступные команды:

```
# Отобразить список всех арен, включенных в контекст.
show

# Сохранить текущее состояние контекста.
save

# Применить изменения в контексте, включая все арены и профили,
входящие в него.
commit

# Откатить контекст к предыдущему сохраненному состоянию, если
команда commit не была выполнена.
rollback

# Пересобрать все программы dosgate. Используется для отладки. Не
рекомендуется запускать во время активной эксплуатации.
rebuild

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

Управление таргетом: arena

Таргет *arena* предоставляет ряд функций, позволяющих управлять профилями, их версиями и состоянием в системе DosGate.

Формат выполнения:

```
dgctl -u arena://arena-name -c help
```

Доступные команды:

```
# Добавить профиль.
add

# Удалить профиль.
delete

# Отобразить список всех профилей арены.
list

# Применить все профили арены.
commit

# Откатить контекст к предыдущему сохраненному состоянию, если
команда commit не была выполнена.
rollback

# Сохранить все профили арены.
save

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

Управление таргетом: profile

Таргет *profile* предназначен для управления профилями защиты в системе DosGate. Профиль представляет собой набор правил, применяемых к сетевому трафику, проходящему через систему. С его помощью можно управлять фильтрацией пакетов, анализировать их характеристики и применять необходимые действия.

Основные возможности профиля:

1. Определение IP-адресов получателей, привязанных к профилю (один IP-адрес не может быть закреплён за несколькими профилями одновременно).
2. Задание набора правил фильтрации трафика.
3. Применение правил в порядке следования (правила обрабатываются сверху вниз).
4. Использование трёх основных сущностей в правилах:
   - `Match` - параметры пакета, по которым выполняется фильтрация.

- `Action` - действие, выполняемое при соответствии пакета условиям фильтрации.
- `Stats` - запись статистики обработки трафика.

При отсутствии `match` в правиле действие `action` применяется ко всем пакетам. Если указан только `match` без `action`, правило не влияет на трафик.

Формат выполнения команд:

```
dgctl -u profile://arena-name/profile-name -c <команда>
```

Новые правила применяются только при использовании команды insert:

```
dgctl -u profile://arena-name/profile-name -c insert -- rule
```

Пример добавления правила с фильтрацией TCP-трафика:

```
dgctl -u profile://arena-name/profile-name -c insert -- -m
protocol tcp -j DROP
```

Пример адресации таргета

`dgctl -u profile://arena-name/profile-name -c command -- rule`

Команды для цели profile

```
# Добавить правило.
insert

#Можно указать позицию вставки (опция `-i`). Правило будет
добавлено на четвёртую позицию:

dgctl -u profile://first/test -c insert -i 4 -- rule

# Удалить правило. Указывается позиция (или диапазон через `-`).
remove

#Удаление правила на 4-й позиции:
dgctl -u profile://first/test -c remove -i 4

#Удаление нескольких правил на указанных позициях (например, 1, 3
```

```
и 5):
dgctl -u profile://first/test -c remove -i 1,3,5

#Удаление диапазона правил (например, с 1-й по 5-ю позицию):
dgctl -u profile://first/test -c remove -i 1-5

# Заменить правило на заданной позиции.
replace

#Замена правила другим правилом на 3 позиции:
dgctl -u profile://first/test -c replace -i 3 -- rule


# Отобразить список правил профиля.
list


# Применить набор правил.
commit


# Для сохранения набора правил в профиле. Команда доступна только
после выполнения *commit*. Сохраненный набор правил будет
автоматически применен при перезагрузке сервиса DosGate.
save

# Откатить профиль до предыдущей версии (если не был выполнен
commit).
rollback


# Переименовать профиль и изменить его описание.
rename

# Проверить доступность таргета.
ping


# Используется для внутренней отладки.
backref_stats

# Вывести справочную информацию.
help
```

Документация сущностей (match & action rule)

Основные параметры:

- `-m` (match) - определяет характеристики пакетов для фильтрации.

- `-j` (action) - указывает действие, выполняемое при соответствии условиям.
- `-c` (comment) — добавляет комментарий к правилу.

```
Usage: [-m <match>]... [-j <action>]... [-c <comment>...]
```

Комбинирование параметров match и action
Параметры match и action могут использоваться совместно для точного определения характеристик пакета и применения соответствующих действий.

В командной строке двойное тире `--` используется для разделения команды и параметров правила (match & action).

Вызов справки по match и action

Для просмотра доступных параметров фильтрации и возможных действий используйте команду:

```
dgctl -u profile://arena-name/profile-name -c insert -- help
```

Пример комбинации правил

Пример 1: Фильтрация по протоколу TCP с выполнением действий `STATS` и `DROP`:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -j
STATS TCP_protocol -j DROP
```

Пример 2: Фильтрация по протоколу TCP, TTL, геолокации с выполнением действий `STATS` и `ACCEPT`:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -m ttl
155 -m geoip cntr RU -j STATS bypass_for_ru_ttl_155_tcp -j ACCEPT
```

Пример 3: Фильтрация ACL для веб-ресурса, с выполнением действий `MARK` и `DROP`:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -m
dport 80,443 -j MARK value 1 ! -m mark 1 -j STATS WEB_ACL -j DROP
```

Получение справки по параметрам

В справке (help) подробно описано, как использовать каждый параметр match и action, а также доступные для них опции.

Пример:

```
dgctl -u profile:/arena-name/profile-name -c insert -- -m protocol
help

dgctl -u profile://first/test -c insert -- -j RATELIMIT help

dgctl -u profile://first/test -c insert -- -m icmp help

dgctl -u profile://first/test -c insert -- -m geoip help
```

Опция "NOT"

Перед параметром `match` допустимо использование символа `!`, который выполняет функцию логического оператора **NOT**.

Пример:

```
-m protocol tcp ! -m dport 443,80 -j DROP
```

Данное правило означает: если пакет использует протокол TCP, но порт получателя не 80 или 443 — сбросить пакет.

Примечание:

> Оператор `!` нельзя использовать с `-m protocol`.

Список доступных match & action

Просмотреть все доступные параметры можно с помощью команды:

```
dgctl -u profile://arena-name/profile-name -c insert -- help
```

Match

Match	Описание
protocol	Протокол
mark	Общая метка фрейма
len	Длина элемента фрейма
ttl	Время жизни (TTL)
frag	Фрагментация пакета на сетевом уровне
src	Сетевой адрес источника
dst	Сетевой адрес получателя
spi	IPSec SPI
tsrc	Туннелированный адрес источника
tdst	Туннелированный адрес назначения
tspi	Туннелированный IPSec SPI
dport	Порт назначения на транспортном уровне
sport	Порт источника на транспортном уровне
gre	Элементы GRE-заголовка
tcpflags	Флаги TCP
hmark	Метка хоста источника
sdhmark	Метка хоста источника и назначения
connmark	Метка соединения
dhmark	Метка хоста назначения
verdict	Результат предыдущего действия
seq	Последовательность байтов
dns	Заголовок DNS
tcpopts	Опции TCP
tcpmss	Максимальный размер сегмента TCP
tcpws	Масштаб окна TCP
icmp	Тип/код ICMP
icmp6	Тип/код ICMPv6
pset	Совпадение с префиксом из набора, заданного на основе IP-адреса
tpset	Совпадение с префиксом из набора, заданного на основе туннелированного IP-адреса
geoip	Совпадение с данными в GeoIP-базе на основе IP-адреса

Match	Описание
tgeoip	Совпадение с данными в GeoIP-базе на основе туннелированного IP-адреса

Action

Action	Описание
ACCEPT	Принять фрейм и прекратить дальнейшую обработку
DROP	Немедленно отбросить фрейм
PASS	Передать пакет в сетевой стек ОС
STATS	Собирать статистику по всем обрабатываемым пакетам
MARK	Изменить общий маркер фрейма
HMARK	Добавить запись в таблицу меток для источника
SDHMARK	Добавить запись в таблицу меток для источника и назначения
CONNMARK	Добавить запись в таблицу меток для соединения
DHMARK	Добавить запись в таблицу меток для назначения
VERDICT	Изменить вердикт
RATELIMIT	Применить ограничение скорости
SAMPLE	Провести выборку трафика
TCPAUTH	Выполнить авторизацию TCP
SNAT	Источник статического NAT
DNAT	Назначение статического NAT
CAPTURE	Захватить пакет
GOTO	Перейти к указанной цепочке правил
RATE	Механизм ограничения скорости с расширенными возможностями подсчёта

Управление таргетом: router

Таргет *router* используется для настройки маршрутизации пакетов в рамках профиля. Каждому профилю назначается индивидуальный набор IP-префиксов, которые определяют, какие пакеты должны обрабатываться данным профилем.

Пакеты, чей IP-адрес получателя соответствует указанному в конфигурации префиксу, направляются на профиль. Если IP-адрес отсутствует в маршрутизаторе и пакет не является L2-multicast (при работе в режимах inline или transparent), он передается в операционную систему.

Формат выполнения:

```
dgctl -u router://arena-name/profile-name -c command -- prefix
```

Добавление и удаление префиксов поддерживает указание нескольких значений через запятую, а также диапазонов (через тире `-`).

После внесения изменений в конфигурацию маршрутизатора требуется применить их с помощью команд:

```
dgctl -u profile://first/test -c commit
```

```
dgctl -u profile://first/test -c save
```

Доступные команды:

```
# Добавить указанный IP-префикс в таблицу маршрутизации профиля.
insert

# Удалить указанный префикс из таблицы маршрутизации.
remove

#Удаляет указанный префикс, автоматически разбивая оставшиеся
адреса по маскам.
pin

#Пример: Если в маршрутизаторе имеется запись 1.1.1.0/24 и
требуется удалить 1.1.1.88/32, выполняется команда:

 #dgctl -u router://first/test -c pin -- 1.1.1.88

#Система автоматически удалит только 1.1.1.88/32, разделяя
оставшийся диапазон на соответствующие маски.


# Выводит полный список маршрутов, заданных в профиле.
list
```

```
# Выводит список маршрутов непосредственно из программы dosgate в ядре Linux.
list_kernel

# Показывает несохраненные изменения в таблице маршрутизации профиля.
diff

# Вывести справочную информацию.
help


# Проверяет доступность таргета.
ping
```

Управление таргетом: mark

Таргет *mark* используется индивидуально для каждого профиля и представляет собой механизм хранения и обработки меток. Метки позволяют временно сохранять информацию о пакетах и использовать её в последующих правилах фильтрации.

Метка (mark) может как записывать информацию из пакета (например, `-j HMARK id 1 value 1 lifetime 600`), так и проверять её наличие (`-m hmark id 1 status valid`).

Важно: в метках поддерживаются только адреса с маской /32. Другие маски не применяются.

Типы меток

Метки представляют собой быстрые таблицы данных:

- **hmark** - Хранит в себе IP-адреса отправителя.
- **sdhmark** - Хранит в себе IP-адреса отправителя и IP-адрес получателя.
- **dmark** - Хранит в себе IP-адрес получателя.
- **connmark** - Хранит в себе IP-адрес отправителя, IP-адрес получателя, протокол, порт отправителя и порт получателя.

Формат выполнения:

```
dgctl -u mark://arena-name/profile-name -c command --
```

```
command_options
```

Доступные команды:

```
# Отобразить содержимое метки.  (Не рекомендуется использовать без фильтров
# которые указываются в \<command-options\>, при большом объёме данных.)
list

# Добавить информацию в метку.
insert

# Удалить информацию из метки.
delete

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

Опции команд

```
Usage: [[type] <type>] id <id> [<field_name> <field_value>]... value <val> [expire <exp>]
```

Параметры метки:

- **type** – Тип метки. По умолчанию `shost`.
- **id** – Идентификатор метки, диапазон: 0, 2^32-1.
- **field_name** – Имя поля метки. См. ниже.
- **field_value** – Значение поля метки, специфично для протокола.
- **val** – Значение метки, диапазон: 0, 2^32-1.
- **exp** – Время жизни в секундах, начиная с текущего момента. По умолчанию – без срока действия.

Названия полей:

- **l3_proto** – Протокол сетевого уровня
- **l3_src** – Исходный адрес сетевого уровня
- **l3_dst** – Адрес назначения сетевого уровня

- **sec_proto** – Протокол безопасности IP
- **sec_id** – Идентификатор безопасности IP (SPI)
- **tun_proto** – Протокол туннеля
- **tun_id** – Идентификатор туннеля
- **l3_tun_proto** – Туннелируемый протокол сетевого уровня
- **l3_tun_src** – Исходный адрес туннелируемого сетевого уровня
- **l3_tun_dst** – Адрес назначения туннелируемого сетевого уровня
- **sec_tun_proto** – Туннелируемый протокол безопасности IP
- **sec_tun_id** – Идентификатор безопасности туннелируемого IP (SPI)
- **l4_proto** – Протокол транспортного уровня
- **l4_src** – Исходный адрес транспортного уровня (порт)
- **l4_dst** – Адрес назначения транспортного уровня (порт)

Протоколы сетевого уровня:

- **ipv4** – IPv4
- **ipv6** – IPv6

Протоколы безопасности:

- **ah** – Заголовок аутентификации (AH)
- **esp** – Инкапсулированная полезная нагрузка безопасности (ESP)

Протоколы туннелей:

- **ipip** – Туннель IP-IP (ipencap)
- **gre** – Универсальная инкапсуляция маршрутизации (GRE)

Туннелируемые протоколы сетевого уровня:

- **tun_ipv4** – Туннелируемый IPv4
- **tun_ipv6** – Туннелируемый IPv6

Туннелируемые протоколы безопасности:

- **tun_ah** – Туннелируемый заголовок аутентификации (AH)
- **tun_esp** – Туннелируемая инкапсулированная полезная нагрузка безопасности (ESP)

Протоколы транспортного уровня:

- **udp** – Протокол пользовательских датаграмм (UDP)

- **tcp** – Протокол управления передачей (TCP)
- **sctp** – Протокол управления потоком передачи (SCTP)

Типы меток:

- **shost** – Исходный адрес сетевого уровня
- **dhost** – Адрес назначения сетевого уровня
- **sdhost** – Исходный и адрес назначения сетевого уровня
- **conn** – Полное соединение (Ntuple)

Управление таргетом: prefixset

Таргет *prefixset* может быть двух типов:

- **Глобальный**: применяется ко всей системе.
- **Индивидуальный**: специфичен для конкретного профиля.

В *prefixset* поддерживаются все маски IP-адресов. Префикс-сет представляет собой таблицу данных, которую может редактировать только администратор вручную. Данные в префикс-сет нельзя добавить автоматически через правила, что отличает его от меток (быстрых таблиц данных).

Функциональность

- **Поиск**: По префикс-сету можно осуществлять поиск с использованием команды `match`. Поиск может выполняться как по IP-адресу отправителя, так и по IP-адресу получателя.
- **Применение изменений**: После внесения изменений в префикс-сет необходимо применить их с помощью команды `-c commit`. Сохранение (`-c save`) не требуется.

Формат выполнения:

Примеры индивидуального префикс-сета:

```
dgctl -u prefixset://arena-name/profile-name/prefixset -c command
```

```
dgctl -u prefixset://arena-name/profile-name/ -c command
```

Примеры глобального префикс-сета:

```
dgctl -u prefixset://arena-name/prefixset-name -c command
```

```
dgctl -u prefixset://arena-name/ -c command
```

Доступные команды:

```
#Показать список префикс-сетов или их содержимое.
list

#Создать новый префикс-сет.
new

# Переименовать префикс-сет.
rename

# Очистить префик-сет.
free

# Отменить очистку (до применения commit).
unfree

# Применить изменения.
commit

# Откатить изменения (до применения commit).
rollback

# Добавить данные в префикс-сет.
insert

# Заменить данные в префикс-сете.
replace

# Удалить данные из префикс-сета.
delete

# Удалить все указанные суб-префиксы.
# Например, указав delete_sub 0.0.0.0/0 - префикс-сет полностью
```

```
очистится.
delete_sub

# Удалить префикс, автоматически разбивая его
# Например, если в префикс-сете есть 1.1.1.0/24, и нужно удалить
1.1.1.88/32,
# выполните команду: dgctl -u prefixset://first/test/test -c pin -
- 1.1.1.88/32
# Система удалит только .88/32, оставив остальные префиксы
(1.1.1.0/25, 1.1.1.128/25 и т.д.)
pin


# Показать изменения, ожидающие применения (до выполнения commit).
diff

# Используется для внутренней отладки.
backref

# Проверить доступность таргета.
ping

# Вывести справочную информацию.
help
```

Управление таргетом: chain

Таргет *chain* позволяет создавать дополнительные цепочки правил, которые могут использоваться для перенаправления пакетов с помощью команды `-j GOTO chain-name`. Цепочки уникальны для каждого профиля защиты.

Перед этим – chain нужно создать

- **Применение изменений**: Применение (`-c commit`) и сохранение (`-c save`) цепочек происходит автоматически при применении профиля. Отдельно применять цепочки не требуется.

Формат выполнения:

```
dgctl -u chain://arena-name/profile-name/chain-name -c command --
command options` или `dgctl -u chain://arena-name/profile-name -c
command
```

Доступные команды:

```
# Показать список цепочек в профиле или правила в цепочке.
list

# Добавить новую пустую цепочку или правила в существующую
цепочку.
insert

# Удалить цепочку или правила в цепочке.
delete

# Заменить правила в цепочке.
replace

# Удалить все правила из цепочки.
clear

# Отменить предыдущее удаление цепочки.
undelete

# Переименовать существующую цепочку.
rename

# Показать все ссылки на цепочку (используется для внутренней
отладки).
backref

# Показать справку по командам.
help

# Проверить доступность таргета.
ping
```

Примеры использования

Создать цепочку под именем "acl" с описанием "access list rules set":

```
dgctl -u chain://first/test -c insert acl access list rules set
```

Добавить правило в цепочку:

```
dgctl -u chain://first/test/acl -c insert -- ! -m dport 80,443 -j
STATS incorrect_proto_and_ports -j DROP
```

Добавить второе правило:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -j GOTO
acl
```

Применить и сохранить измнения:

```
dgctl -u profile://first/test -c commit
dgctl -u profile://first/test -c save
```

TCP авторизация

TCP-авторизация предназначена для защиты сетевой инфраструктуры от атак, связанных с подменой IP-адресов (IP-spoofing), а также от ситуаций, когда злоумышленник не может установить полноценное TCP-соединение. Данный механизм позволяет проверить подлинность отправителя TCP-пакетов и минимизировать риски несанкционированного доступа.

Основные команды и их назначение

Проверка наличия IP-адреса в таблице доверенных узлов

```
-c insert -- ! -m hmark id 77 status valid -j TCPAUTH 1 type hs
atype hs
```

Если IPv4-адрес отправителя отсутствует в таблице "host mark" ID 77 или его статус "valid" истёк, выполняется TCP-авторизация с применением RST на SYN и RST на SYN+ACK.

Добавление IP-адреса в доверенную таблицу

```
-c insert -- -m verdict tcpauth valid -j HMARK id 77 value 1
lifetime 3600
```

При успешном прохождении TCP-авторизации IPv4-адрес отправителя добавляется в "host mark" ID 77 со значением "1" и временем жизни 3600 секунд.

Обработка неудачной авторизации

```
-c insert -- -m verdict tcpauth invalid -j STATS TCP_AUTH -j DROP
```

В случае неуспешной авторизации пакет фиксируется в статистике с тегом "TCP_AUTH" и отбрасывается.

Полный пример конфигурации:

```
-c insert -- ! -m hmark id 77 status valid -j TCPAUTH 1 type hs
atype hs
-c insert -- -m verdict tcpauth valid -j HMARK id 77 value 1
lifetime 3600
-c insert -- -m verdict tcpauth invalid -j STATS TCP_AUTH -j DROP
-c insert -- -j VERDICT clear
```

Рекомендации по применению

Выбор метода TCP-авторизации определяется характеристиками сервиса и параметрами сети, инициирующей или принимающей подключение. В зависимости от этих факторов рекомендуется применять различные механизмы проверки.

Настоящий документ предоставляет сведения о применении TCP-авторизации в различных сетевых инфраструктурах. Перед внедрением рекомендуется тестирование специфических сценариев, включая нестандартные приложения.

Определение совместимости: Авторизация считается прозрачной для пользователя, если выполняется автоматически и не требует дополнительных действий, таких как обновление страницы или повторное установление соединения.

Веб-приложения

Браузер	Операционная система	Исходящая сеть	Совместимость SA-авторизации	Совместимость RST-авторизации
PC				
Google Chrome	Windows 10,11	РТК-бизнес		
Google Chrome	Mac OS 13.4	РТК-бизнес		
Google Chrome	Linux Ubuntu 22.04.2 LTS	РТК-бизнес		
Atom	Windows 10,11	РТК-бизнес		

Браузер	Операционная система	Исходящая сеть	Совместимость SA-авторизации	Совместимость RST-авторизации
Safari	Mac OS 13.4	РТК-бизнес		Требуется перезагрузка страницы
Яндекс Браузер	Windows 10,11	РТК-бизнес		
Яндекс Браузер	Mac OS 13.4	РТК-бизнес		
Mozilla Firefox	Windows 10,11	РТК-бизнес		
Opera	Windows 10,11	РТК-бизнес		
TOR Browser	Windows 11	РТК-бизнес	Отсутствует	
Brave Browser	Windows 11	РТК-бизнес		
Mobile				
Google Chrome	Android 11,12,13	РТК-бизнес, МТС, Билайн, Мегафон		
Google Chrome	iOS 16	РТК-бизнес, МТС, Билайн, Мегафон		
Safari	iOS 16	РТК-бизнес, МТС, Билайн, Мегафон		Требуется перезагрузка страницы
Яндекс Браузер	Android 11,12,13	МТС, Билайн, Мегафон		

Последнее обновление рекомендаций: 13 июля 2023 г.

Техническая поддержка DosGate

По умолчанию на выбор заказчика существует два уровня оказывания услуг технической поддержки.

Поддержка	Описание
DosGate Gold Support	Поддержка 24/7/365. Включает в себя техническую поддержку уровня Gold: обновление системы и работа по TAC-кейсам.
DosGate Advanced Support	Условия Gold Support + техническая поддержка в чате, комплексное сопровождение решения, в том числе удалённое управление инсталляцией (включено 40ч.), доступ к базе вредоносных сигнатур.

Обновление системы

Включает предоставление обновлений программного обеспечения, исправлений уязвимостей, новых функциональных возможностей и оптимизаций производительности. Обновления предоставляются в рамках поддерживаемых версий продукта и могут включать рекомендации по установке.

Обработка обращений по TAC-кейсам

Техническая поддержка по зарегистрированным запросам пользователей (TAC-кейсы). Включает диагностику проблем, рекомендации по настройке, помощь в устранении неисправностей, а также консультации по использованию продукта.

Техническая поддержка в чате

Оперативная помощь специалистов в режиме онлайн-общения. Позволяет быстро решать вопросы, связанные с эксплуатацией, настройкой и устранением неисправностей. Подходит для консультаций в реальном времени без необходимости регистрации TAC-кейса.

Комплексное сопровождение решения

Включает полный цикл поддержки: анализ текущего состояния системы, рекомендации по оптимизации, помощь в адаптации решения под специфические требования заказчика, мониторинг работоспособности и консультирование по наилучшим практикам эксплуатации.

Удалённое управление инсталляцией (включено 40 часов)

Удалённая техническая поддержка специалистов для настройки, обновления и устранения проблем в системе. В рамках пакета предоставляется до 40 часов удалённой работы.

Доступ к базе вредоносных сигнатур

Обеспечивает актуальную защиту от угроз за счёт автоматического обновления базы сигнатур вредоносного трафика. Используется для проактивного выявления и блокировки потенциально опасных атак, фишинговых попыток и других видов вредоносной активности.

DosGate ведет собственную обновляющуюся базу вредоносных сигнатур которая поддерживается внутренней командой аналитики ServicePipe и обновляется каждый час. База вредоносных сигнатур применяется на решении в автоматическом или полу-автоматическом режиме

Ответы на популярные вопросы

Логирование каждого пакета (SIEM, детальная аналитика)