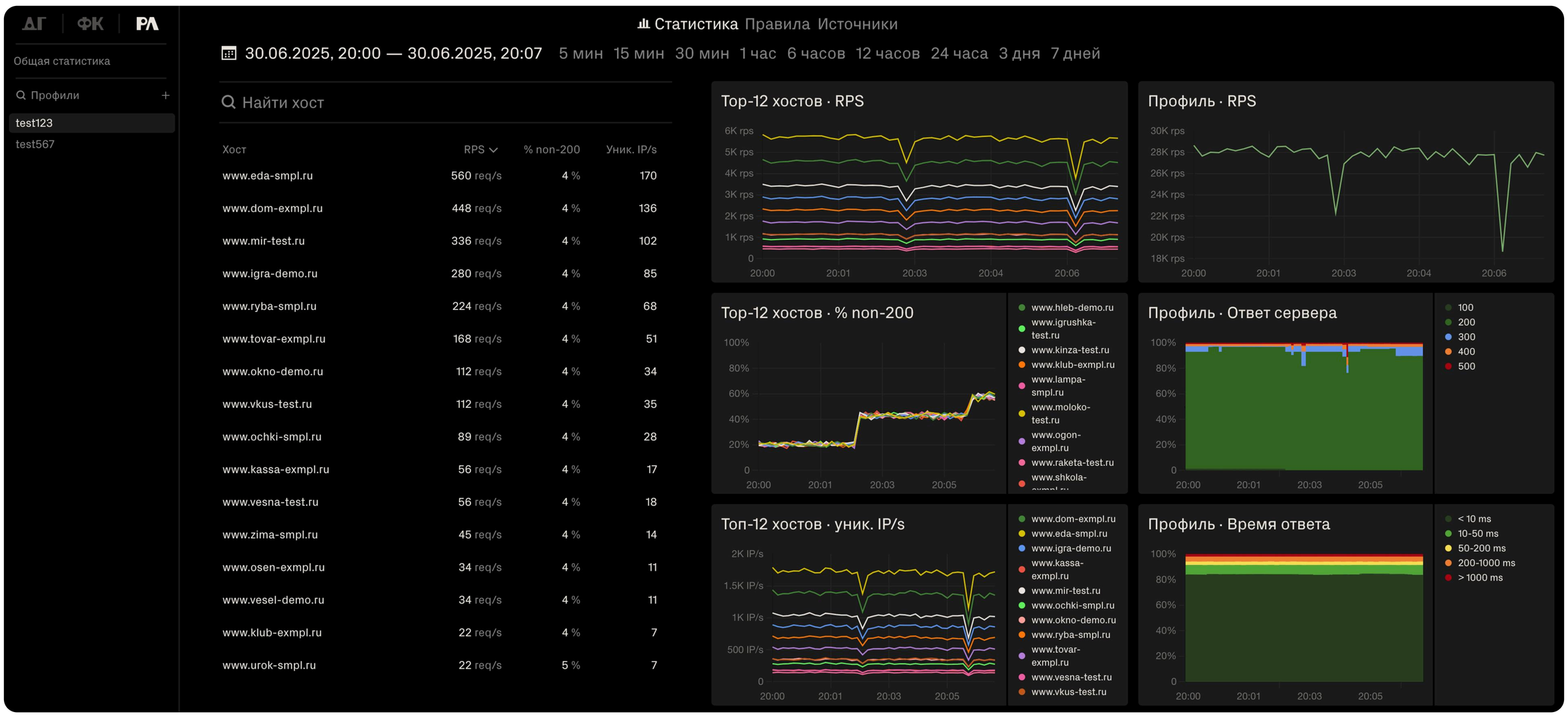
Модуль DosGate RLOG

servicepipe

Модуль анализа логов веб-сервера, предназначенный для автоматического выявления аномального поведения пользователей на уровне HTTP и передачи IP-адресов нарушителей в систему DosGate для фильтрации.



DosGate — адаптивная система защиты IT-инфраструктуры от DDoS-атак и сетевых угроз. Благодаря высокой производительности (до 400 Gbps и 400 Mpps на одной аппаратной платформе) продукт способен обрабатывать большие объёмы трафика, эффективно отражать атаки на уровнях L3–L7 и обеспечивать стабильную работу критически важных сервисов.

Возможности RLOG

1 Анализ логов в реальном времени

- Обработка access-логов веб-сервера.
- Поддержка всех стандартных полей: IP, метод, URI, user-agent, referer, код ответа и т. д.
- Поддержка access-логов от WAF, прокси, балансировщиков и веб-серверов после TLS/SSL-терминации. Совместимость с NGINX, F5, Apache и HAProxy.

2 Конструктор правил через веб-интерфейс

- Условие ЕСЛИ — фильтрация по полям логов и скорости.
- Действие ТО — занесение IP-адреса в таблицу временной блокировки DosGate.
- Создание цепочки правил с определённым порядком обработки.

3 Производительность и масштабируемость

- До 160K RPS на ядро благодаря анализу логов без TLS-терминации и с масштабированием более 10M RPS на сервер.
- Правила работают независимо, сохраняется линейная производительность при росте числа профилей.
- Гибкая фильтрация по конкретным URI, сервисам, user-agent и другим параметрам.

4 Детектирование на основе частоты запросов

- Подсчёт количества совпадающих запросов от одного IP в заданный временной интервал.
- Реализация скоростных лимитов (rate-limiting) с пороговыми условиями: например, 100 запросов за 10 секунд — заблокировать.

5 Гибкость и универсальность

- Независимость от протоколов и серверов — RLOG работает с любыми версиями HTTP (1.x, 2, 3).
- Быстрое подключение новых логов — добавление поддержки нестандартных форматов или источников (WAF, прокси, балансировщики).
- Гибкая настройка источника IP — возможность выбирать, из какого параметра лога брать IP-адрес клиента, включая специальные заголовки, передающие реальные IP при использовании прокси или балансировщиков (например, X-Real-IP, X-Forwarded-For).

Преимущества модуля в интеграции с Servicepipe DosGate

Точная фильтрация L7-угроз

RLOG анализирует содержимое логов HTTP-запросов, позволяя выявлять и блокировать нежелательную активность, которую не видно на уровне сетевых фильтров (классического антиDDoS).

Мгновенная реакция на угрозы

RLOG срабатывает в реальном времени — при превышении лимита запросов IP-адрес моментально передаётся в DosGate, где начинается фильтрация.

Без раскрытия TLS-сертификата

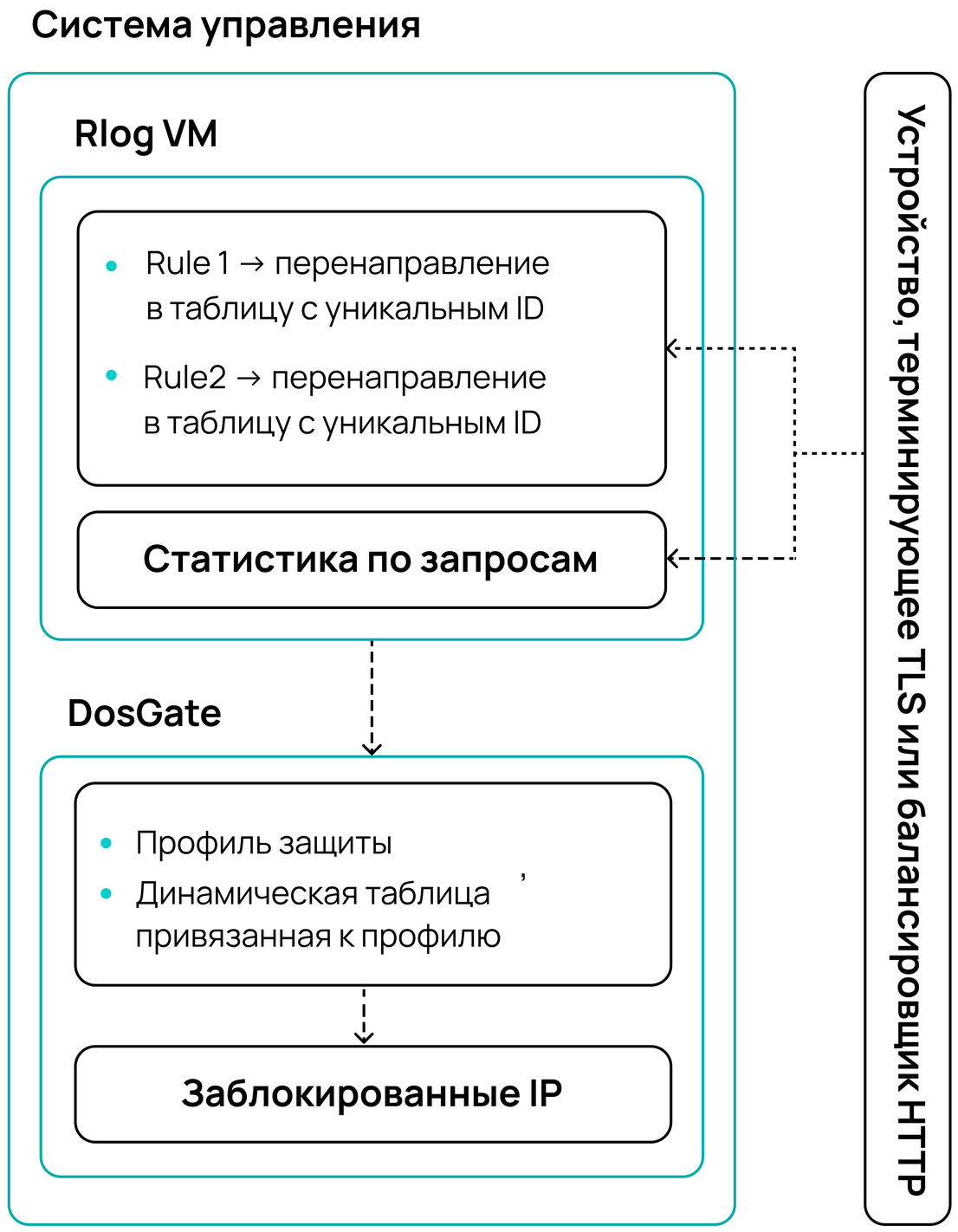
RLOG анализирует уже сформированные логи, без доступа к приватным ключам и вмешательства в TLS-сессии.

Работа в формате on-premises

Решение разворачивается в инфраструктуре клиента, обеспечивая автономность, безопасность, соответствие PCI-DSS и ГОСТ Р 57580.1–2017.

Принцип работы

1. Модуль RLOG осуществляет непрерывный мониторинг HTTP-логов, поступающих с устройств терминации TLS или балансировщиков нагрузки.
2. Система автоматически рассчитывает RPS (запросы в секунду) на основе количества поступающих логов.
3. Статистические данные собираются по выделенным профилям и в рамках правил фильтрации, созданных пользователем.
4. В соответствии с этими правилами RLOG вычисляет частотные характеристики запросов и выявляет отклонения от заданных пороговых значений.
5. При обнаружении нарушения пороговых значений система извлекает IP-адрес источника из заголовка, определённого пользователем.
6. Информация о потенциально опасном источнике передаётся в единую систему управления.
7. Система передаёт команды блокировки на узлы DosGate, занося IP-адреса нарушителей в динамические таблицы блокировки выбранных профилей защиты.



DosGate — это:

- Защита от L3–L7 DDoS-атак до 400 Gbps и 400 Mpps на устройство
- Гибкие пакеты правил
- Удобный и простой интерфейс
- Отчёты по клику
- Эшелонированная защита
  On-premise + Cloud Signaling + Cloud
- Техническая поддержка 24/7/365. SLA: ответ в течение 5 минут
- On-premise
  ПО и ПАК в инфраструктуру
- Менее секунды на Always-on или Ultra-low Time to Mitigate
- Модуль DosGate Autopilot
  Автоматическая генерация правил фильтрации
- В реестре отечественного ПО, аккредитация Минцифры
- Модуль DosGate RLOG
  Анализ логов веб-сервера
- Сетевая и сессионная защита: до 150 млн правил в системе
- Подключаемая система интеллектуального анализа трафика FlowCollector

Пилот — лучшее доказательство нашей эффективности

Оставьте заявку на пилот или свяжитесь с нами, чтобы обсудить технические детали и получить дополнительные материалы о продукте.

+7 (495) 374-62-65
servicepipe.ru/dosgate
welcome@servicepipe.ru