Servicepipe FlowCollector

servicepipe

Система интеллектуального анализа сетевого трафика

FlowCollector непрерывно отслеживает входящие и исходящие из сети пакеты, обнаруживая аномалии и переводя DDoS-атаки на фильтрацию в течение 100 мс.

Интегрируется как ПО или ПАК. Работает как в связке с DosGate, так и с любым другим очистителем.

Формирует детальные отчёты по сетевым аномалиям, расширяя возможности аналитики.

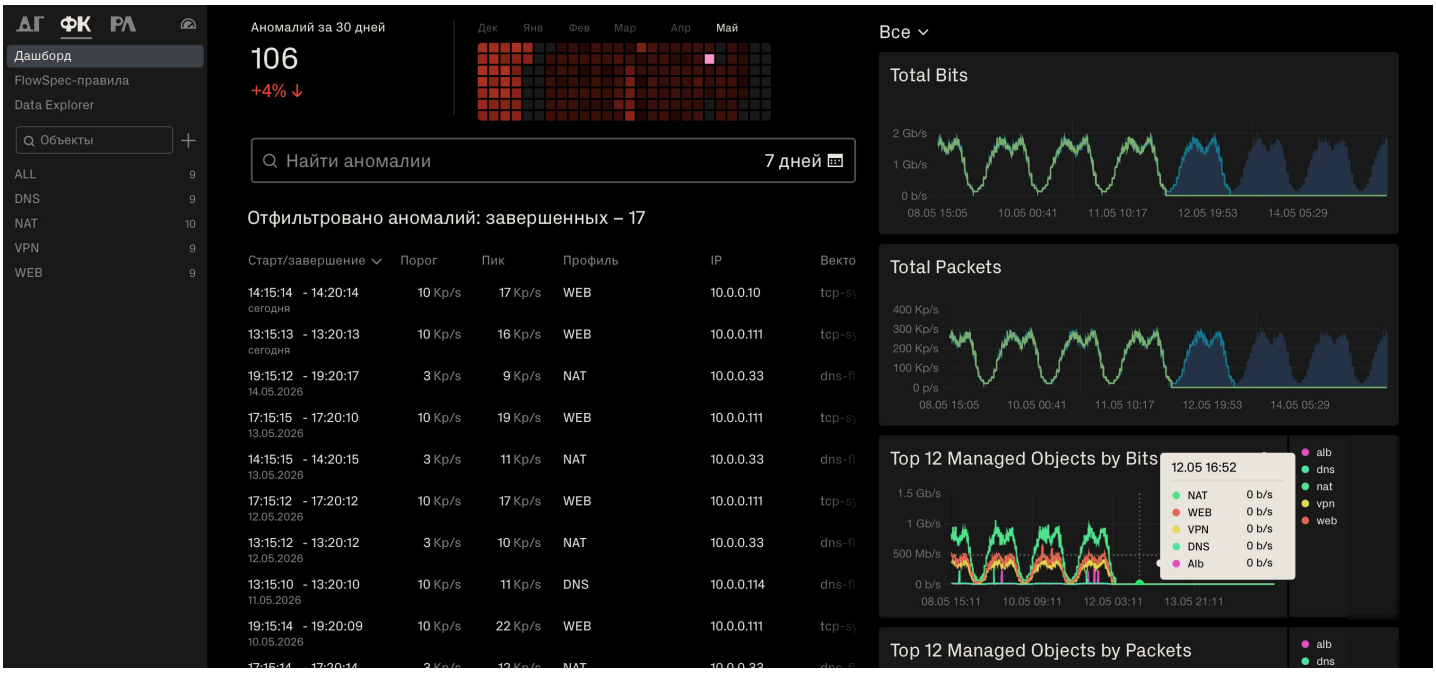
Области применения

Усиление безопасности внешней и внутренней сетевой инфраструктуры от DDoS-атак

Наблюдение за состоянием сетевой инфраструктуры и направляемого трафика

Идентификация типа и объёма потребления сетевого трафика

Веб-интерфейс



Возможности

Быстрое и точное выявление аномалий

Определение более 30 различных векторов DDoS-атак за 100 мс с момента появления аномалии.

Детекция как ковровых DDoS-атак (распределённых по всей IP-маске), так и точечных (направленных в сторону конкретного IP-адреса получателя).

Тонко настраиваемые политики реагирования

Динамические пороги

Задаются как относительные значения или отклонения на основе анализа данных из выбранных временных диапазонов.

Дополнительные правила

При недостаточной эффективности начальных мер FlowCollector включает дополнительные правила.

Комбинации правил и порогов

Функционируют как единый алгоритм для точной настройки под каждый тип атаки.

Интервал пересчёта трафика

Настройка произвольных интервалов, например, 1 000 мс или 5 000 мс.

Детальная статистика

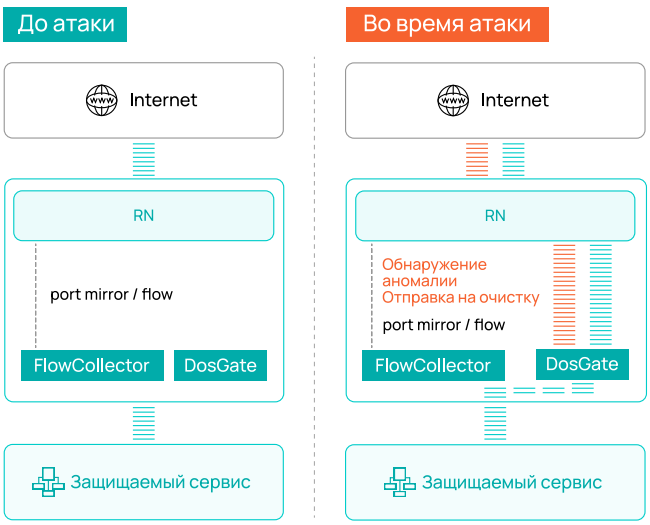
По любой IP-маске, по объекту (группе IP-масок с общей конфигурацией), по вектору внутри объекта.

Модуль Data Explorer

Сохраняет параметры трафика для анализа и визуализации, помогая выявлять аномалии и исследовать сетевые события за всё время с момента подключения.

Схема работы

1. От CPE идёт Flow sampling (IPFIX) во FlowCollector.
2. FlowCollector держит BGP-сессию с очистителем. Если FlowCollector детектирует атаку, он анонсирует префиксы (IP-адреса получателей), которые находятся под DDoS.
3. Очиститель, замечая новые адреса в анонсе, также их анонсирует в свою BGP-сессию с CPE.
4. Когда атака заканчивается, FlowCollector убирает адреса из анонса, так как в IPFIX больше не виден вредоносный трафик. Соответственно, очиститель также убирает эти адреса из своих анонсов, и трафик идёт напрямую к конечному получателю.
5. Трафик всегда проходит мимо, и FlowCollector автоматически указывает, какой трафик должен быть перенаправлен в очиститель при обнаружении атаки.



Преимущества

Стабильно высокая производительность

- Обработка NetFlow до 250 000 fps (flows per second) на 1 платформу
- Производительность платформ анализа и очистки не деградирует даже при сложных комплексных атаках

Standalone-решение

- 100% автономная работа в инфраструктуре
- Совместимость с любым стандартизированным серверным оборудованием
- Совместимость с SIEM
- Интеграция с сервисами через HTTP API

Гибкая система управления

- Автоматическая фильтрация трафика с помощью BGP FlowSpec
- Управление правилами и политиками через интуитивно понятный веб-интерфейс
- Техническая поддержка 24/7/365 в SOC, SLA — ответ в течение 5 минут

О компании

ИНТЦ МГУ
ВОРОБЬЕВЫ ГОРЫ

servicepipe

Servicepipe основана в 2015 году ведущими экспертами из крупных российских и зарубежных IT-компаний

120+

Технических экспертов в команде, включая специалистов highload и big data

Built-to-suit

Индивидуальный подход к решению задач клиентов и развитию продуктов

Собственная геораспределённая отказоустойчивая платформа фильтрации с узлами в России и Германии

Пилот — лучшее доказательство нашей эффективности

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

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

Оставить заявку на сайте