Servicepipe FlowCollector

Технология интеллектуального анализа
сетевого трафика

servicepipe

О Servicepipe

Компания Servicepipe работает на рынке защиты ИТ-инфраструктуры и веб-приложений с 2016 года. На этапе становления мы фокусировались на предоставлении провайдерам связи и дата-центрам услуг защиты сетевой инфраструктуры на базе технологий и оборудования от ведущих производителей российского и зарубежного рынков.

Благодаря работе с мультивендорным продуктовым портфелем мы обрели исчерпывающий опыт интеграции и комплексного оказания сервисов, повысили осведомленность о возможностях и ограничениях имеющихся на рынке решений. Мы осознали, что на рынке нет идеальных решений защиты от DDoS, и начали разработку собственных технологий, а также продуктов и сервисов на их базе.

Сегодня технологии Servicepipe обеспечивают высокую производительность, стабильность работы и защищенность ИТ-систем компаний, функционируя на базе собственной отказоустойчивой гео-распределенной сети узлов фильтрации. Servicepipe анализирует и очищает трафик клиентов, защищая их активы от DDoS-, целевых атак и нежелательных ботов, включая попытки взлома, фрод, парсинг и атаки на бизнес-логику. Поставка и внедрение технологий доступны как в виде облачной услуги SaaS (в частном или публичном облаке), так и в формате локальных интеграций внутри сетевого контура заказчика. Также возможны гибридные инсталляции, сочетающие фильтрацию на уровне защищенного облака с локальными вариантами внедрения.

Сегодня в команде Servicepipe более 50 экспертов по эксплуатации сетей передачи данных, разработке высоконагруженных систем, специалистов Data Science, фронтенд- и бэкенд-разработчиков.

Всестороннее тестирование собственных технологий перед выходом в свет обновлений позволяет нам на высоком профессиональном уровне проводить комплексные аудиты производительности и защищенности ИТ-систем заказчиков. Пентест и стресс-тест от команды опытных специалистов Servicepipe дают компаниям полноценную картину об актуальных уязвимостях в их сетевом периметре и эффективности работы используемых средств защиты. Всесторонние аудиты защищенности позволяют превентивно готовить критичные для бизнеса системы к хакерским атакам и высоким непрогнозируемым нагрузкам.

Нашим технологиям доверяют

2GIS

Miran data-center

РоссельхозБанк

Почта Банк

DATALINE

okko

РБК

tutu

окб

sales@servicepipe.ru
+7 495 374 62 65

FlowCollector

Servicepipe FlowCollector — это анализатор сетевого трафика. Он непрерывно отслеживает входящие и исходящие из сети пакеты, гибко реагируя на обнаруженные в них аномалии.

FlowCollector можно использовать для усиления безопасности внешней и внутренней сетевой инфраструктуры от DDoS-атак, настраивать на работу в связке с разными аппаратными комплексами для перенаправления вредоносного трафика через систему очистки, идентифицировать тип и объёмы потребления сетевого трафика в сети, наблюдать за состоянием сетевой инфраструктуры и направляемого трафика.

Servicepipe DosGate в паре с FlowCollector становится оптимальным средством защиты крупных сетей, например, федеральных интернет-провайдеров и дата-центров.

Ключевые возможности технологии

- Мгновенная реакция на аномалии сетевого трафика, в частности, на входящие и исходящие DDoS-атаки;
- Определение более 25 различных векторов DDoS-атак за 100 мс с момента появления аномалии;
- Повышение точности детектирования аномалий с помощью создания уникальных политик реагирования;
- Детекция как ковровых (распределенных по всей IP-маске), так и точечных атак (направленных в сторону конкретного IP получателя) DDoS-атак;
- Поддержка инкапсулированного сэмплинга.

Как это работает

При выявлении сетевой аномалии FlowCollector направляет трафик на фильтрацию (например, на Servicepipe DosGate или другой очиститель) или активирует BGP Blackhole в сторону атакуемой IP-маски. Либо производит сразу оба этих действия, в зависимости от достигнутого порога.

1. Динамические пороги.

   В отличие от других решений, FlowCollector позволяет задавать динамические пороги в виде относительных величин — коэффициентов или процентов от количества пакетов/байт в «плавающем» отрезке времени. А также в виде отклонений от последних записей в настроенных временных диапазонах анализа.

   Администратор сетевой инфраструктуры может указать, что если количество пакетов или байт выбранного вектора выросло больше чем в X раз за последние N секунд, то следует выполнить выбранное действие («Направить на очистку» или «Изолировать IP-адреса с помощью BGP Blackhole»).

2. Комбинации правил.

Flowcollector позволяет настраивать комбинации правил и порогов для каждого вектора, которые впоследствии работают как единый алгоритм.

Пример комбинации правил:

Превышение порога (количество пакетов достигло 15 000 pps) + Всплеск трафика (в 3 раза вырос параметр pps за последние 2 секунды) = Направить трафик на аппаратную платформу очистки через BGP next-hop.

3. Настройка разных правил на несколько порогов.

Если после применения одного из правил объёмы трафика всё равно продолжают кратно расти, угрожая стабильности работы инфраструктуры и аппаратной системы очистки, FlowCollector при достижении нового заведённого порога может применить новое правило/комбинацию правил. Например, активировать BGP Blackhole при достижении очередного заданного порога в рамках того же вектора.

Технические преимущества


Работа на стандартизированном серверном оборудовании;


Высокая производительность, до 100 Гбит/с и 100 млн пакетов в секунду на 1U-платформе;


Анализ flow (поддержка IPFIX);


Возможность установки произвольного интервала пересчёта трафика (например, 1000 мс, 5000 мс и т. д.);


Возможность просмотра детальной статистики:

- по любой IP-маске;
- по каждому объекту (группе IP-масок с общей конфигурацией);
- по каждому вектору внутри объекта или любой выбранной IP-маске;


Интеграция статистики через сервисы collectd (Grafana, Graphite, Clickhouse, Zabbix и другие)


HTTP API для интеграции с собственными сервисами


Настройка через конфигурационные файлы (GUI запланирован на Q2 2023)


2 варианта подключения: облачный сервис (SaaS) или локальное ПО (On-premise)

servicepipe

Мы будем рады
ответить на ваши вопросы
и обсудить параметры тестирования

Пожалуйста, свяжитесь с нами любым удобным способом

sales@servicepipe.ru https://servicepipe.ru