Servicepipe HUB + Flowcollector

Защита инфраструктуры телеком-операторов от DDoS-атак

servicepipe

Servicepipe HUB

Заранее подготовленный физический и BGP-стык с сетью Servicepipe на портах от 10 до 100 Гбит/с, который можно организовать в любом дата-центре Москвы.

\+

Servicepipe FlowCollector

Интеллектуальный анализатор сетевого трафика, специально адаптированный для работы в условиях динамичного и интенсивного обмена данными, характерного для телекоммуникационных сетей.

О Servicepipe HUB

Решение предназначено для защиты инфраструктуры операторов связи от масштабных ковровых DDoS-атак, когда атака направлена сразу на всю автономную систему и все входящие в неё префиксы.

Защита отдельных клиентских префиксов по AS-SET с возможностью перепродажи услуги конечным абонентам и гарантированным SLA предоставляется как отдельная опция с собственной тарификацией.

О Servicepipe FlowCollector

FlowCollector поставляется в виде программного обеспечения для внедрения внутри вашей инфраструктуры и может быть развернут как на выделенном, так и на виртуальном сервере.

Продукт поддерживает RTBH (Remote Triggered Blackhole) и генерацию BGP FlowSpec как в ручном, так и в автоматическом режиме.
Эти инструменты могут применяться как самостоятельный **механизм противодействия атакам, нацеленным на отдельные адреса или сегменты сети оператора.**

Также система может по заданным правилам формировать BGP-анонсы, которые позволяют перенаправлять входящий DDoS-трафик для последующей фильтрации, в том числе в сети Servicepipe.

Правила смены маршрутизации и сценарии перевода трафика определяются совместно с оператором, исходя из особенностей его сетевой архитектуры и политики эксплуатации.

В штатном режиме весь трафик проходит через существующие апстримы оператора. При обнаружении атаки в зависимости от преднастроенных политик **FlowCollector создаёт FlowSpec-правило или соответствующий BGP-анонс, которые применяются в отношении атакуемых префиксов.**

При перенаправлении трафика через сеть Servicepipe выполняется его фильтрация. После этого легитимный трафик возвращается в сеть оператора. При этом для очистки достаточно маршрутизировать только входящий трафик.

Эксперты Servicepipe готовы предоставить примеры успешной интеграции и варианты практического использования FlowCollector как инструмента управления BGP-маршрутизацией для перенаправления DDoS-трафика на площадки фильтрации.

Принцип работы

1. Оператор подключает порт на Servicepipe HUB и устанавливает BGP-пиринг с Servicepipe (принимаются анонсы AS оператора, но не AS-SET*);
2. В штатном режиме трафик проходит через существующие апстримы оператора;
3. При обнаружении DDoS-атаки FlowCollector инициирует специализированные BGP-анонсы: входящий трафик к атакуемым префиксам перенаправляется в сторону Servicepipe, проходит фильтрацию и «чистым» возвращается в сеть оператора через порт Servicepipe HUB;
4. После завершения атаки маршрутизация автоматически возвращается в исходный режим с соответствующим cooldown, учитывающим вероятность повторения атаки;

Почему это выгодно для операторов связи

Быстрое подключение

- Порт на Servicepipe HUB + BGP-пиринг — без атак порт не нагружен и не используется.
- Переключение при атаке — автоматически, без ручных операций.

Экономически оправданно

- Прозрачные эксплуатационные затраты: порт/сервис вместо закупки и поддержки «тяжёлого» оборудования.
- На старте нужны: порт на Servicepipe HUB и сервер под FlowCollector — это существенно дешевле, чем сразу покупать полноценный On-Premise AntiDDoS (например, Servicepipe DosGate).

Контроль

- Защищаем только атакуемые префиксы, остальной трафик не затрагивается.
- Гибкая политика (BGP, FlowSpec, communities), белые/серые списки.

Для кого особенно актуально

Компаниям, которым требуется старт без CAPEX и постепенное наращивание защиты.

Инфраструктурам с критичными сервисами, где нужен автоматический переключатель на время атак.

servicepipe

Компания основана в 2015 году ведущими экспертами из крупных российских зарубеж ных ИТ-компаний

120+

Технических экспертов в команде, включая специалистов highload и big data

Собственная георасспредёленная отказоустойчивая платформа фильтрации с узлами в России и Германии

500+

Клиентов, включая ведущие компании в различных секторах: банки, маркетплейсы, СМИ, телеком и другие

Пилот — лучшее доказательство нашей эффективности

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

+7 (495) 374-62-65

servicepipe.ru/flowcollector

Написать в Telegram