Servicepipe DosGate

Адаптивная система защиты IT-инфраструктуры
от DDoS-атак и сетевых угроз

servicepipe

Состав решения

I Сетевая защита

Встроенные механизмы проверок и возможность создания правил защиты, основанных на детальных комбинациях содержимого пакетов.

- Комбинации правил между собой
- Таблицы данных, счётчики, алгоритмы rate limit, etc.
- Максимальная точность фильтрации с минимальным false positive

II Сессионная защита

Обеспечивает защиту веб-приложений с помощью интеллектуального отслеживания соединений и автоматического разрыва сессий для минимизации простоя.

- Анализ отпечатков JA3 и JA4, а также TLS Cipher Suite
- Эффективная защита промежуточных узлов от переполнения сессий
- Connection Tracking для TCP, UDP, SCTP, ICMP, ICMPv6

✳ Гибкие пакеты правил

DosGate сочетает сетевую и сессионную защиту и даёт возможность пользователям подключить готовые комплекты правил, быстро и без дополнительных настроек.

- ✓ Управление базой вредоносных сигнатур, в том числе через удаление/изменение отдельных сигнатур в ответ на критические угрозы
- ✓ Автоматическое обновление сигнатур 24/7 в реальном времени при обнаружении новых угроз
- ✓ Автообновление списка вредоносных IP-адресов для своевременной защиты

Показатели фильтрации

› 30 000
Атак отражено

1500 Gbps
Пропускная способность кластера крупнейшего заказчика

› 10 000
Профилей защиты

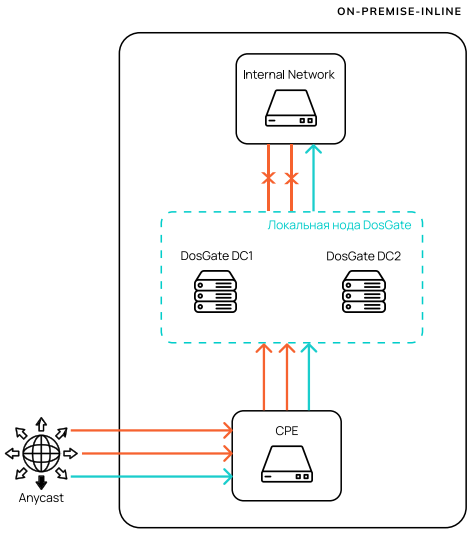
706 Gbps
288 Mpps
Самая крупная отражённая атака

336 часов
Самая длительная атака

Inline

Установка Inline («в разрыв») подразумевает, что трафик постоянно маршрутизируется через ПО DosGate. Трафик приходит на один сетевой интерфейс и возвращается с другого.

Поддерживается L2 multicast, ARP, LACP, LAG

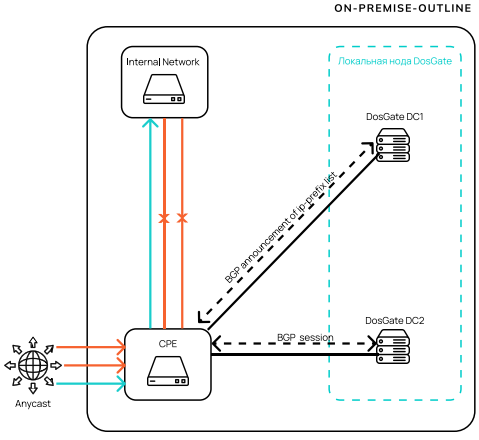


Outline

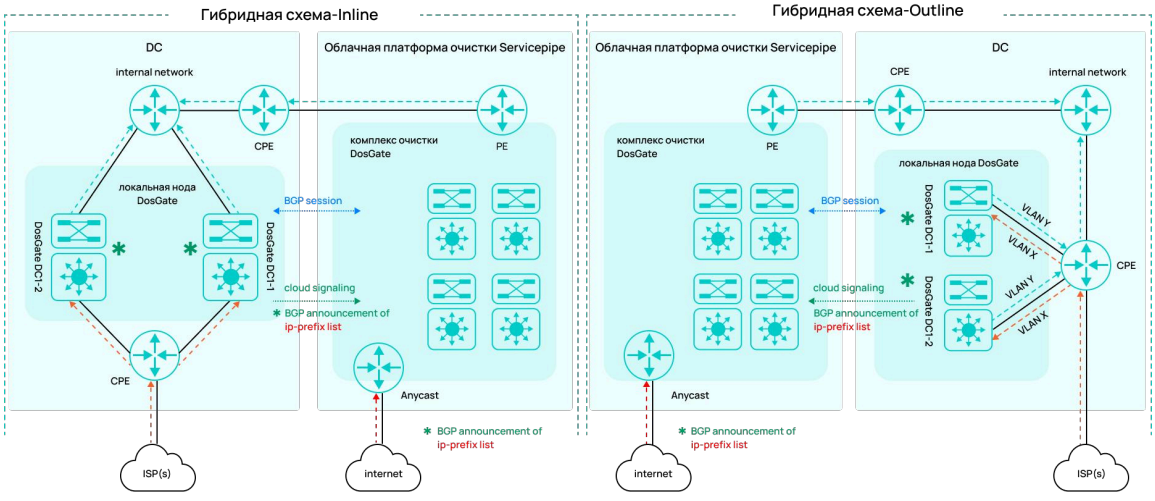
Установка Outline (или VLAN swap) подразумевает, что DosGate может принимать и возвращать трафик в рамках одного интерфейса, например, принимая трафик с одним VLAN tag и возвращая с другим.

DosGate 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).

Поддерживается L2 multicast, ARP, LACP, LAG



Hybrid



Гибридная схема инсталляции подразумевает комбинацию локального DosGate (On-prem Inline или On-prem Outline) и облачного (Cloud Inline или Cloud Outline).

Собственное ядро обработки трафика на XDP и eBPF

- Многоуровневая защита: сетевая и сессионная
- Защита от L3–L7 DDoS-атак до 100 Gbps и 100 Mpps на одно устройство
- До 150 млн уникальных правил по всей системе
- Always-on или Ultra-low Time to Mitigate (TTM) — меньше 1 секунды

Удобная система управления

- Управление правилами через интуитивно понятный веб-интерфейс
- Возможность быстро создавать детализированные отчёты для анализа
- Техническая поддержка 24/7/365 в SOC, SLA — ответ в течение 5 минут

Любые варианты интеграции

- On-premise: ПО и ПАК в инфраструктуру
- Hybrid: On-premise + Cloud Signaling + Cloud

Полностью российское ПО

- DosGate входит в реестр отечественного ПО
- Servicepipe имеет лицензии ФСТЭК на разработку СЗИ и ТЗКИ, а также аккредитацию Минцифры

Интерфейс DosGate

История защиты

МКБ

1. Выстроенная эшелонированная защита IT-инфраструктуры, сайта и веб-приложений от DDoS-атак и ботов на L3–L7
2. Старт фильтрации DDoS-атаки за <1 с
3. Минимальный уровень ложноположительных срабатываний

Прочитать подробнее →

> «Мы получили комплексную защиту от DDoS-атак, и на данный момент решения Servicepipe играют ключевую роль в поддержании защищённости инфраструктуры и доступности веб-сервисов МКБ».
>
> **Вячеслав Касимов**
> Директор департамента информационной безопасности МКБ

О компании

servicepipe

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

120+

технических экспертов в команде, включая специалистов highload и big data

Собственная геораспределённая отказоустойчивая платформа фильтрации с узлами в России и Германии

Built-to-suit

Индивидуальный подход к решению задач клиентов и развитию продуктов

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 welcome@servicepipe.ru Оставить заявку на сайте

Интуитивно понятный веб-интерфейс для создания правил фильтрации

Возможность быстро создавать детализированные отчёты для анализа

Поддержка Hardware Bypass

BGP FlowSpec

Поддержка BGP FlowSpec вместе с FlowCollector

Cloud Signaling

Внедрение механизма Cloud Signaling для эшелонированной защиты