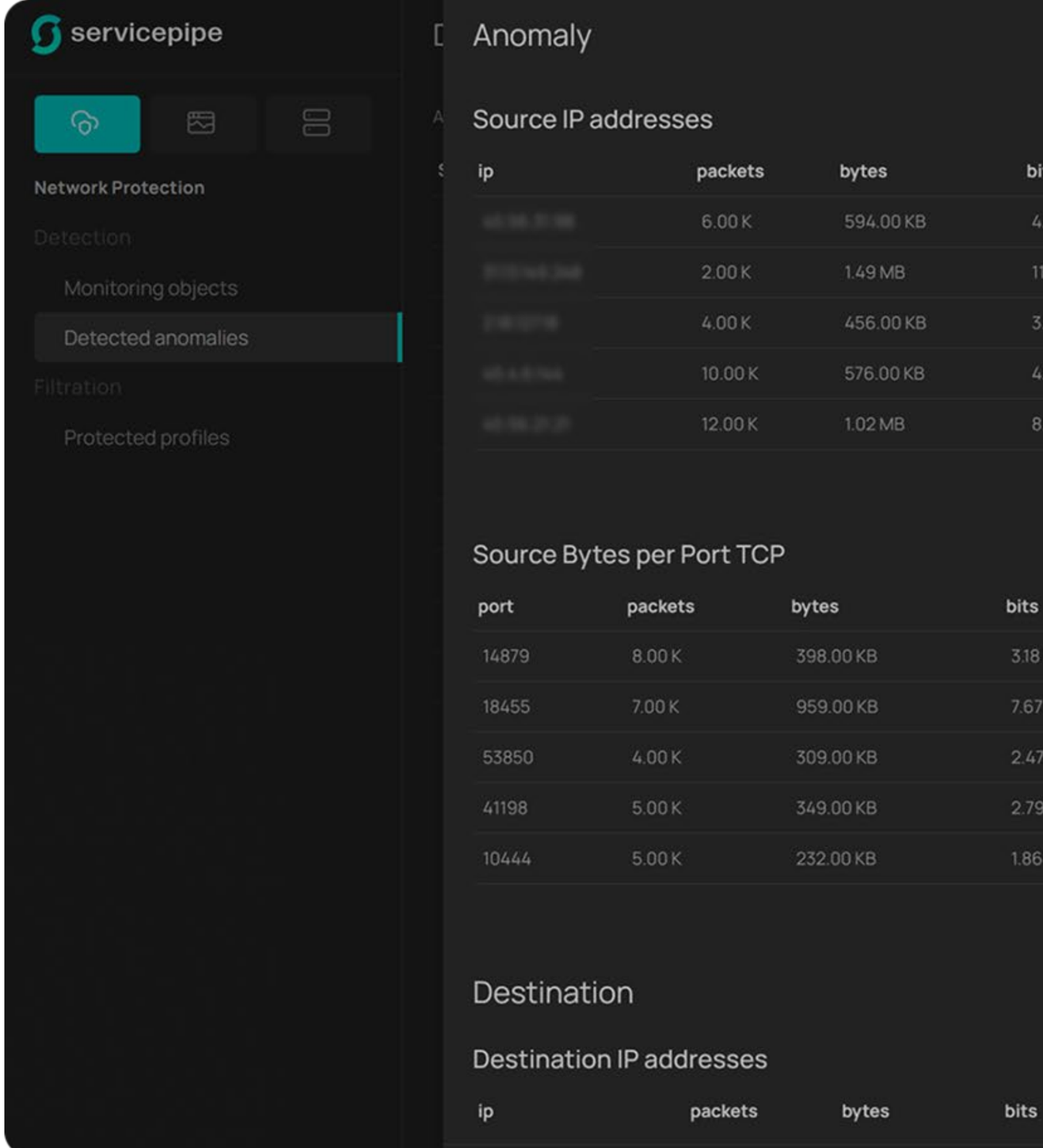
Network DDoS Protection

Защищённый IP-транзит. Защита сети от DDoS-атак с помощью мгновенной фильтрации трафика



servicepipe.ru
welcome@servicepipe.ru

Оглавление

Оглавление

servicepipe

Servicepipe

Sk Участник

Резидент ИНТЦ МГУ

2015

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 георапределённая отказоустойчивая платформа фильтрации с узлами в России и Германии

Built-to-suit подход к решению задач клиентов и развитию продуктов

Клиенты

Финтек

- Модульбанк
- точка
- БКС
- РоссельхозБанк
- Почта Банк

Логистика

- грузовичкоф
- Деловые Линии
- PONY EXPRESS
- 2ГИС
- tutu

Дата-центры

- DataSpace
- DATALINE
- КРОК
- Selectel
- INOVENTICA

Ритейл

- самокат
- ЕАПТЕКА
- OZON
- Все инструменты .ру
- OLDI

СМИ и медиа

- okko
- ТВ ЦЕНТР
- РБК
- KASSIR.RU
- interfax

Оглавление

servicepipe

Последствия

Финансовые

- Прямые финансовые потери из-за простоя сервисов
- Допзатраты на восстановление после атаки

Технологические

- Повреждение или потеря критически важных данных
- Нарушение работы IT-систем и простой производства
- Потеря сотрудниками доступа к корпоративным приложениям

Репутационные

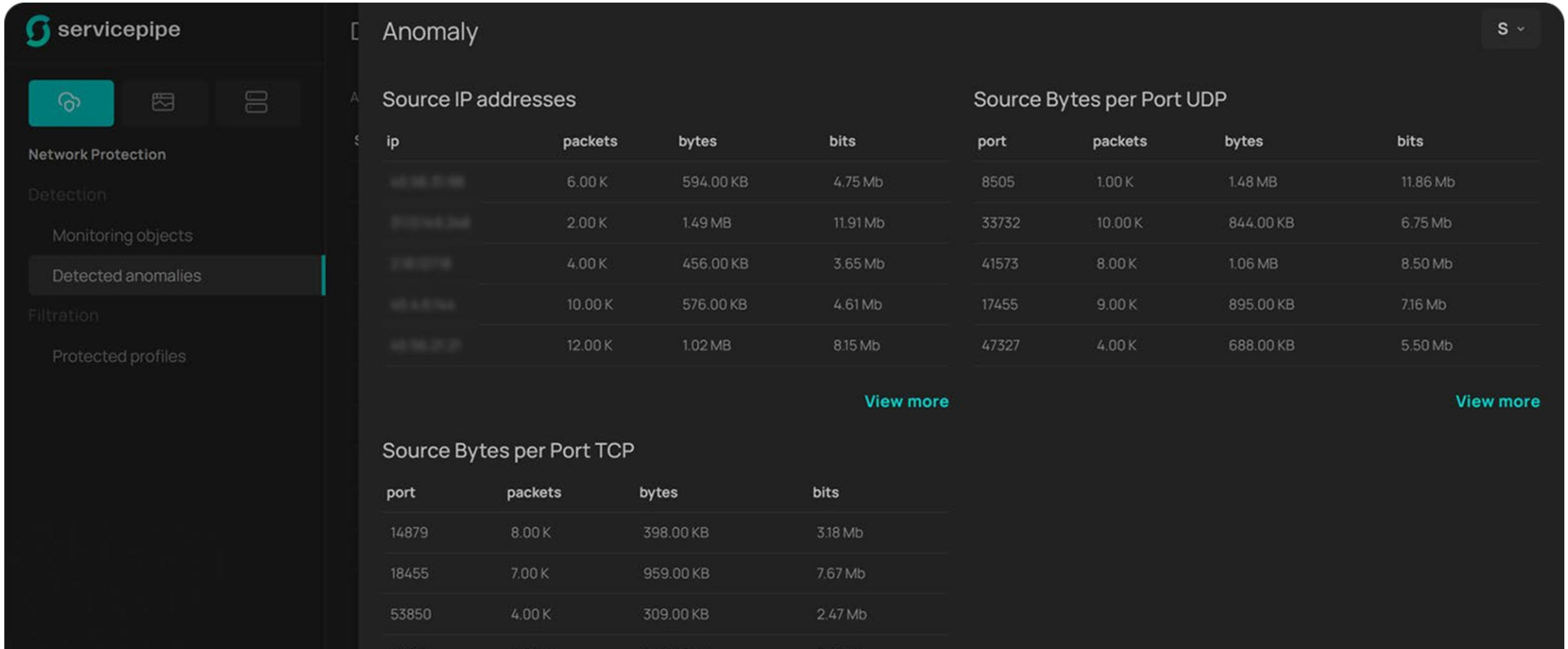
- Утрата доверия клиентов и партнёров
- Снижение лояльности и потенциальный отток клиентов
- Снижение стоимости бренда и падение биржевых индексов компании

Оглавление

servicepipe

Network DDoS Protection

Комплексная фильтрация всех сетевых ресурсов, подключенных к интернету, на сетевом и транспортном уровнях (L3–L4).
Защита для протоколов TCP и UDP, сервисов SMTP, FTP, SSH, VoIP, VPN и других.



Решаемые задачи

Доступность почтовых серверов, видео- конференций, IP-телефонии, корпоративных порталов, удалённых рабочих мест

1

Защита распределённой интернет-инфраструктуры

2

Соответствие требованиям регуляторов

3

servicepipe

Защита от всех типов DDoS-атак

L3—L4

UDP flood
NTP amplification
DNS amplification
SYN flood
Memcache amplification

CharGEN amplification
SNMP amplification
GRE-IP flood
CLDAP amplification
IP-Fragment attack

SSDP amplification
Jenkins amplification
TCP RST flood
TCP ACK flood
TCP connect flood

ARMS (ARD) amplification

И другие специфичные
для приложений
или протоколов атаки

1
2
3
4
5
6
7
8

Индивидуальная настройка защиты

В отличие от других продуктов, наше решение позволяет детализировать защиту по отдельным сервисам или сетевым сегментам, обеспечивая точную настройку для эффективного противодействия DDoS-атакам.

Детекция атак за <1 мс

1

2

3

4

5

6

7

8

Детекция атак за <1 мс

Решение быстро реагирует на угрозы за счёт Always-On фильтрации, помогая предотвращать возможный ущерб ещё до его возникновения.

Неограниченное кол-во правил

1
2
3
4
5
6
7
8

Неограниченное количество правил

Широкие возможности детекции и фильтрации, помогающие настроить высокоточную блокировку вредоносного трафика и адаптировать защиту для отдельных сетевых сегментов и сервисов заказчика.

Обширная база

Обширная база сигнатур атак

Благодаря наличию широкой клиентской базы, мы располагаем глубокими знаниями о сигнатурах атак и правилах их блокировки. Это гарантирует высокоэффективную защиту от самых разнообразных угроз.

Без блокировки

Без блокировки легитимных пользователей

Решение точно различает вредоносный и легитимный трафик, исключая риск ошибочной блокировки реальных пользователей. Это обеспечивает бесперебойный доступ к вашим сервисам для клиентов и партнёров в любой ситуации, даже во время DDoS-атаки.

Без ограничений

Без ограничений по объёму атак

706 Gbps и 288 Mpps — рекордные атаки, с которыми успешно справилось наше решение. Продемонстрировав в том числе и стабильную эффективность фильтрации на протяжении 336 часов, во время непрерывной DDoS-атаки.

Быстрое подключение

1
2
3
4
5
6
7
8

Быстрое подключение

Решение легко интегрируется с внешними анализаторами трафика и другими средствами защиты, обеспечивая гибкость и удобство использования в существующей IT-инфраструктуре.

Поддержка облачной сигнализации (Cloud

Поддержка облачной сигнализации (Cloud Signaling)

Система автоматически сообщает облачному сервису защиты об обнаружении атаки. Быстрая активация защитных мер минимизирует ущерб от атаки и обеспечивает непрерывность работы вашего сервиса.

Георасределённая сеть фильтрации

В России и глобально

Наша собственная инфраструктура обеспечивает эффективную фильтрацию трафика внутри России, гарантируя минимальные задержки и повышенную доступность сервисов для российских клиентов.

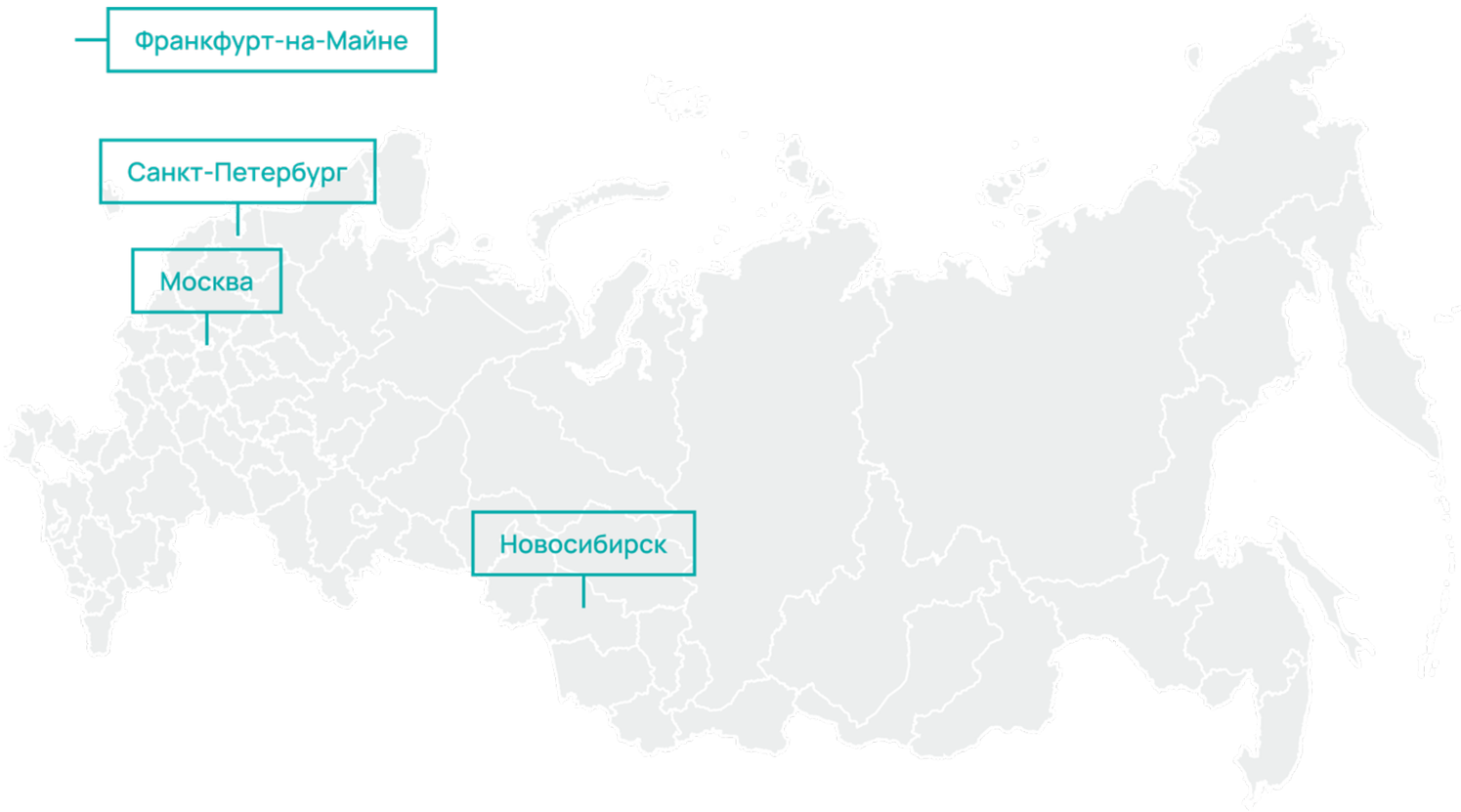
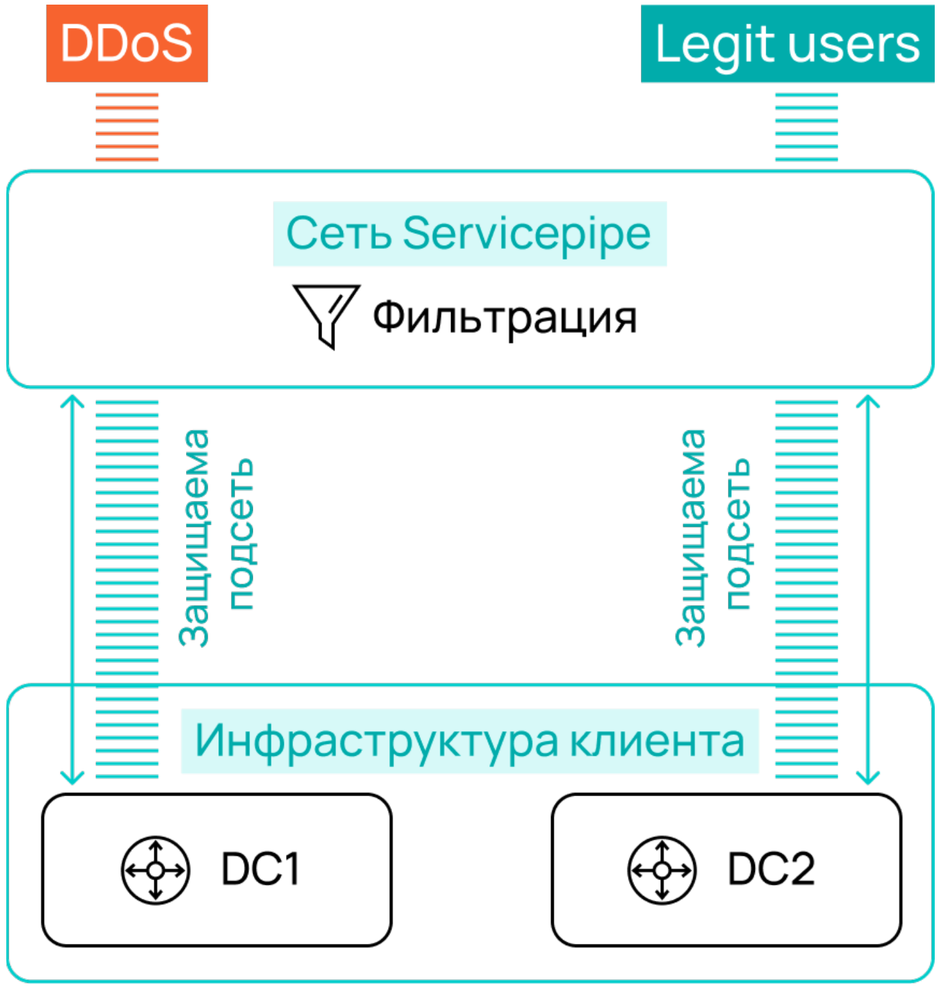


Схема работы

Network DDoS Protection

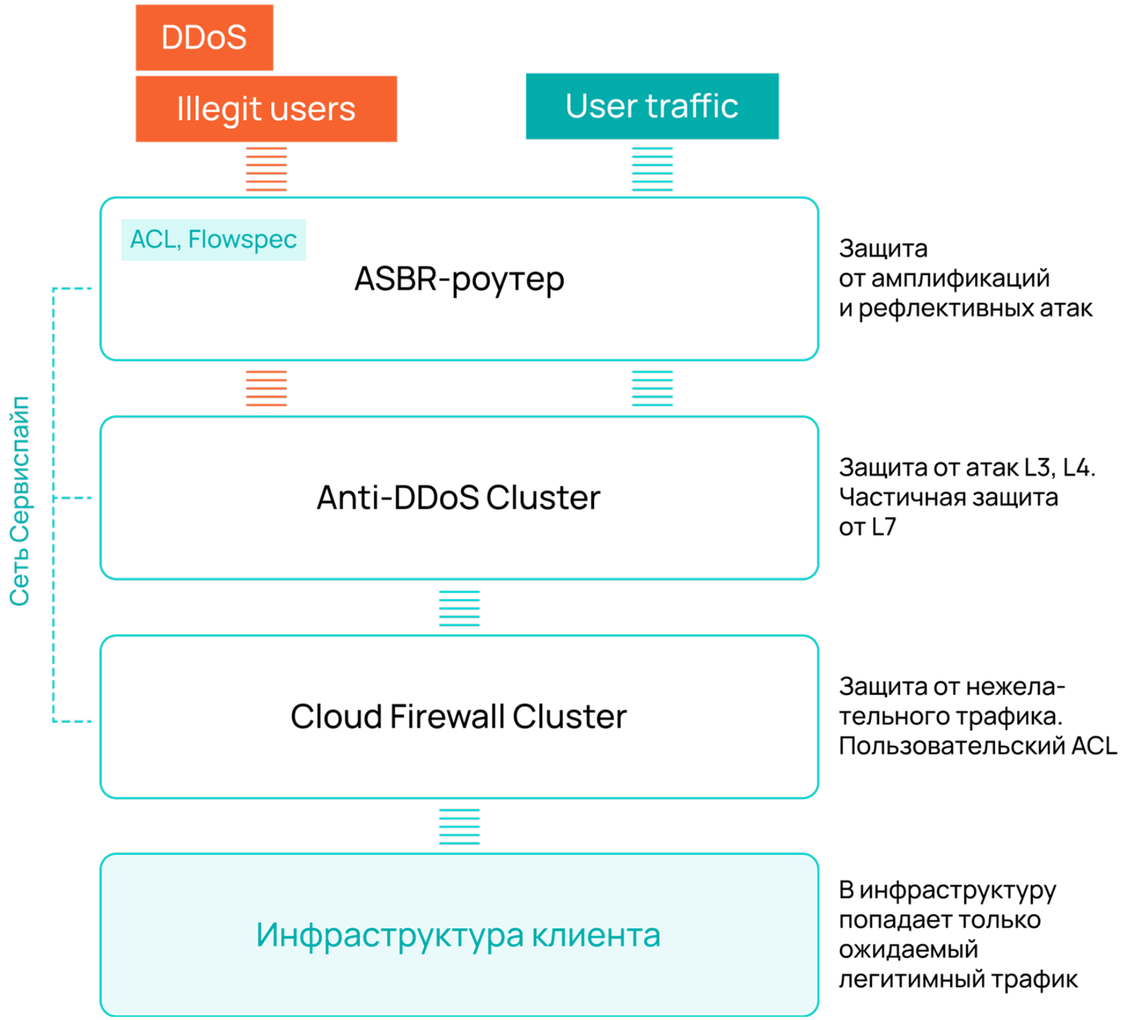
- Для защиты IT-инфраструктуры от DDoS-атак входящий трафик направляется через сеть Servicepipe (AS201706) и попадает на платформы фильтрации, распределённые по миру, на основании BGP Anycast
- Трафик постоянно анализируется на наличие аномалий. При их обнаружении — активируются правила фильтрации
- Правила фильтрации сбрасывают вредоносный трафик. При необходимости они меняются на основе автоматизированных алгоритмов, запроса клиента или решения нашего SOC 24/7/365. Легитимный трафик продолжает непрерывно доставляться клиенту



Servicepipe Cloud Firewall

Блокируйте нежелательный трафик, не относящийся к DDoS-атакам

С помощью собственных правил.
Наша собственная инфраструктура обеспечивает эффективную фильтрацию трафика внутри России, гарантируя минимальные задержки и повышенную доступность сервисов для российских клиентов.



servicepipe

Оглавление

NDA Кейс

Госорганизация

servicepipe

NDA Кейс

Госорганизация

Контекст

- 5 площадок ЦОД
- Высокие требования к резервированию и доступности

Задачи

- Защитить каналы связи площадок от DDoS-атак
- Построить отказоустойчивые каналы связи к каждой из площадок
- Создать специфичный ACL для разгрузки NGFW

Результаты

97% → 99,9995%

Доступность канала связи в интернет

98,55% → 99,9995%

Доступность сети

3 → 0 инцидентов за год

Отказоустойчивость

85% → 99%

Точность фильтрации

5 мин → 1 мс

Время активации защиты

5% → 1%

False positive

24/7/365

Техническая поддержка в SOC, SLA.
Ответ в течение 5 мин

Мгновенное подключение

В реестре отечественного ПО,
аккредитация Минцифры,
лицензии СЗИ и ТЗКИ

<1

Менее секунды на детекцию атак

Неограниченное количество правил + обширная база сигнатур

Без ограничений по объёму атак

SLA 99,99%

Минимизация простоев
и обеспечение непрерывности
вашего бизнеса

Геораспределённая сеть фильтрации

Cloud Signaling

Поддержка облачной
сигнализации

Что дальше?

1

2

3

Подготовим предложение по включению вашей инфраструктуры (BGP L2 или BGP over GRE), проанализируем результаты опросного листа и карты сервисов

Что дальше?

1

Подготовим предложение по включению вашей инфраструктуры (BGP L2 или BGP over GRE), проанализируем результаты опросного листа и карты сервисов

2

Сформируем коммерческое предложение

3

Что дальше?

1

Подготовим предложение по включению вашей инфраструктуры (BGP L2 или BGP over GRE), проанализируем результаты опросного листа и карты сервисов

2

Сформируем коммерческое предложение

3

Запустим пилотный проект. Поможем с настройкой сети и проведём работы по включению в удобное для вас время