Защита сети

Защитите общедоступную инфраструктуру
с помощью connectivity cloud от Cloudflare

Проблема: компромиссы между безопасностью и производительностью

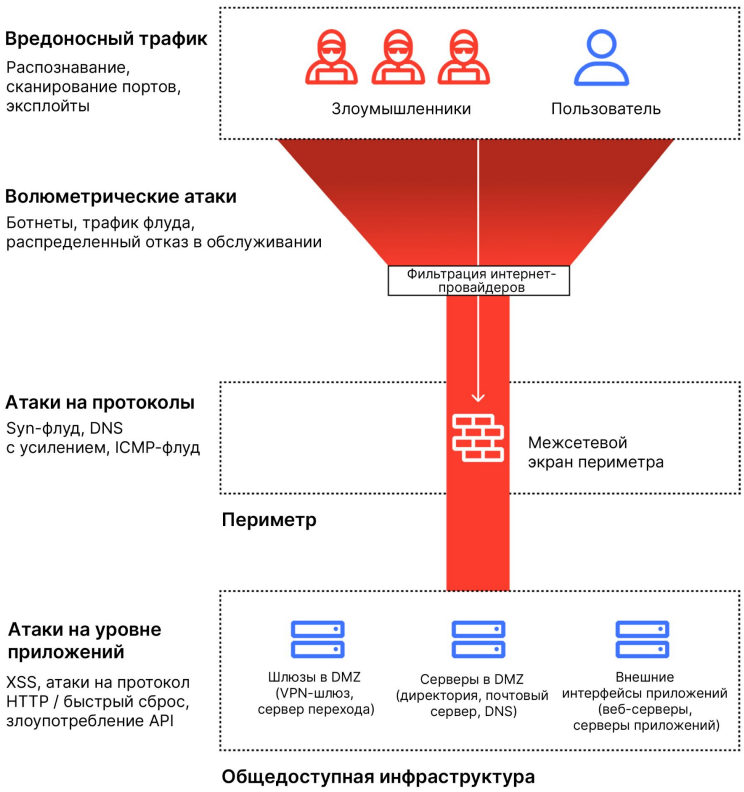
Общедоступная инфраструктура сталкивается с уязвимостями безопасности, поскольку ее доступность через Интернет делает ее мишенью для различных типов атак. Злоумышленники могут сканировать системы в поисках сервисов, использовать неисправленные уязвимости и запускать разрушительные DDoS-атаки, которые наносят финансовый ущерб, прежде чем службы безопасности успеют отреагировать.

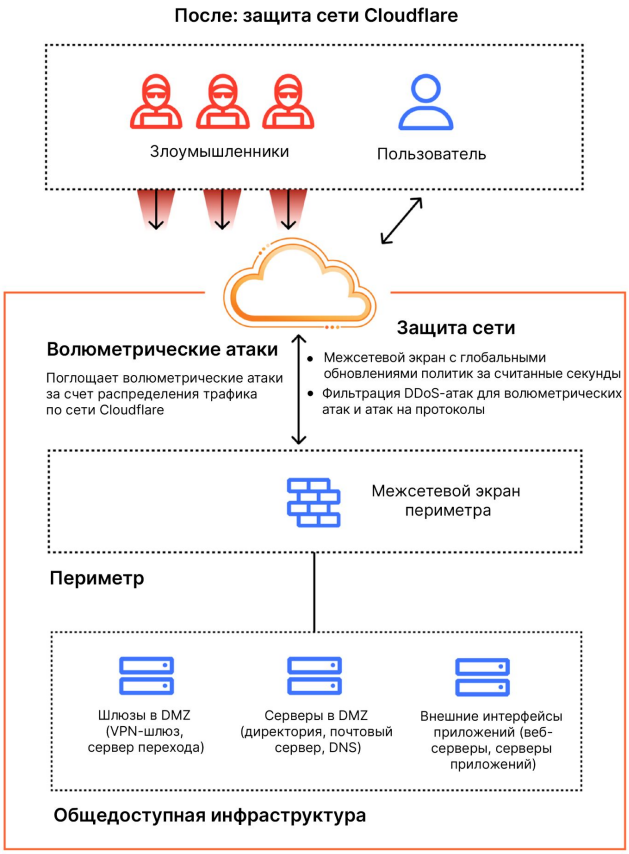
Организации развернули множество межсетевых экранов и сетевых устройств, но они часто снижают эффективность и по-прежнему не могут противостоять сложным угрозам.

Решение: защита сети

Упростите свою архитектуру и сделайте ее более безопасной, дополнив свою сеть connectivity cloud от Cloudflare.С легкостью добавляйте функциональные возможности, активируя облачные сервисы, а не добавляя устройства, и поддерживайте свою модернизацию сети с помощью платформы, которая удовлетворяет как текущие потребности, так и новые будущие варианты использования.

Cloudflare обеспечивает глобальный охват с помощью защиты в один проход, которая включает многоуровневую защиту от волюметрических атак, атак на уровне протоколов или приложений, а также мониторинг состояния, поведения и производительности сети.





Как это работает

1. Организуйте путь для трафика в сеть Anycast Cloudflare через туннели IPSec, туннели GRE или используя Cloudflare Network Interconnect (CNI)
2. Получите автоматическую защиту с помощью Magic Transit и Magic Firewall с минимальной настройкой
3. Развертывайте политики по всему миру за считанные секунды

Узнайте больше об архитектуре Cloudflare для защиты существующей сетевой инфраструктуры.

Преимущества

- **Гибкие ресурсы**: избегайте капитальных затрат, обеспечив глобальный характер в 1-й день
- **Упрощенное управление**: единая плоскость управления для всех сервисов, не требующая управления аппаратными средствами или перепроектирования сети
- **Улучшенная производительность**: оптимизированная маршрутизация трафика позволяет избежать перегрузок
- **Глобальное реагирование на угрозы**: сеть Cloudflare защищает около 20 % веб-сайтов, блокирует 227 миллиардов киберугроз ежедневно и использует ИИ для анализа глобальных моделей трафика для адаптации защиты в режиме реального времени.

Глобальное сетевое присутствие

В пределах ~50 мс от 95 % интернет-пользователей в мире

Подтвержденный опыт и результаты

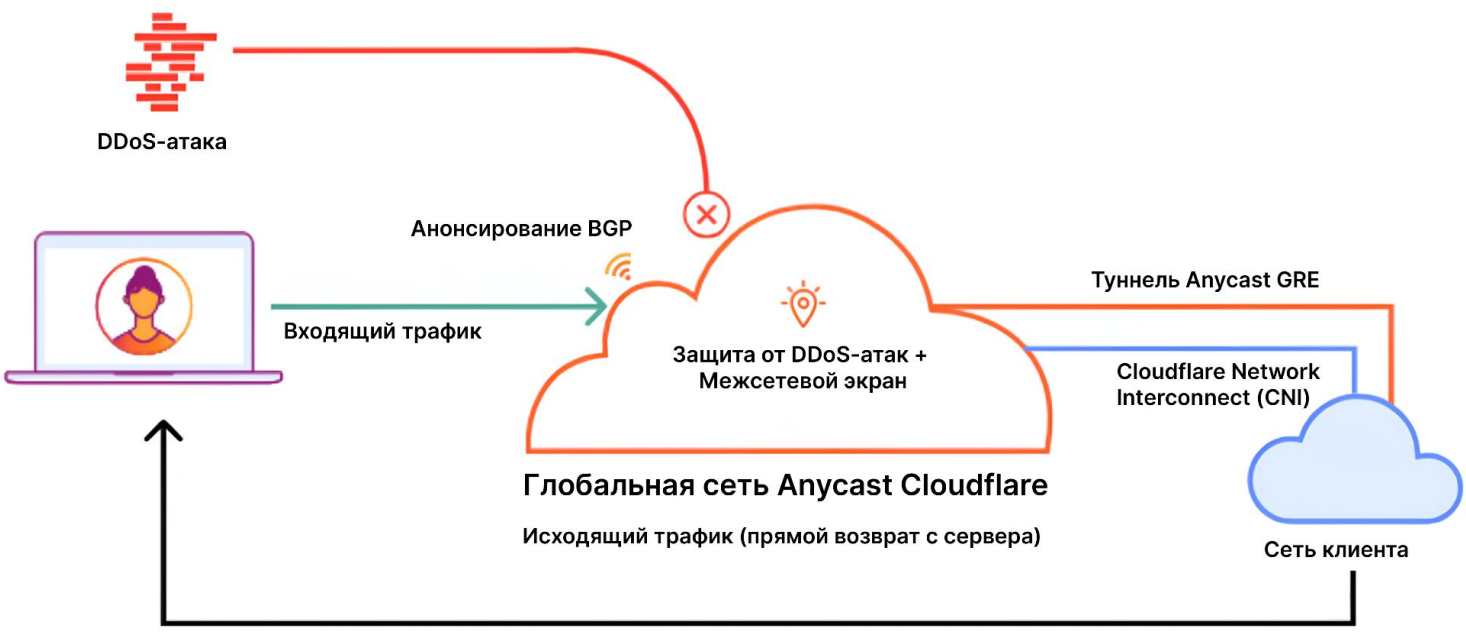
Защита миллионов интернет-ресурсов, а также 35 % компаний из списка Fortune 500

Постоянные инновации

Сетевые сервисы сети Cloudflare обеспечиваются 100%-ной доступностью по SLA

Экономически эффективная консолидация

Замените несколько точечных решений единой интегрированной платформой



Почему Cloudflare?

Каждый центр обработки данных, каждый сервис

Обрабатывайте трафик как можно ближе к источнику, чтобы снизить нагрузку на межсетевые экраны

Однопроходная многоуровневая защита

Избегайте нежелательной задержки и создавайте отказоустойчивость, используя глобальную сеть Anycast Cloudflare

Прямое подключение к Cloudflare

Обходите общедоступный Интернет и подключайтесь напрямую через наше межсетевое соединение

Запросить демо

Посмотрите живую демонстрацию средств защиты сети Cloudflare.

Запросить демо

Загрузить справочную документацию по защите сети

Узнайте о проблемах защиты общедоступной сетевой инфраструктуры и ограничениях межсетевых экранов

Загрузить

Дополнительные ресурсы

- Вебинар: «Прощание с устаревшими межсетевыми экранами: обеспечьте защиту, которую заслуживает ваша сеть»
- Эталонная архитектура: https://developers.cloudflare.com/reference-architecture/architectures/magic-transit/