cloudfresh

CLOUDFLARE

Как предотвратить DDoS-атаку в зависимости от типа

Борьба с DDoS может быть похожа на мигрень. В одну минуту все в порядке, а в другую вы испытываете цифровую боль. Но знаете что? Вы не должны страдать от этого. Мы расскажем вам о различных видах этих атак и, что более важно, о том, как нейтрализовать каждую из них и сохранить ваш бизнес.

01

DNS-флуд

Используйте Cloudflare DNS в качестве основного или дополнительного резолвера и включите DNS Firewall или Magic Transit для усиленной защиты. Глобальная сеть Cloudflare фильтрует вредоносный или избыточный DNS-трафик, кэшируя и обслуживая запросы, поступающие от легитимных пользователей. Она обрабатывает десятки миллионов DNS-запросов в секунду, автоматически блокируя флуд до того, как он достигнет вашего источника.

02

SYN-флуд

Разверните Cloudflare Magic Transit, чтобы остановить SYN-флуд на границе. Он использует SYN-куки, отслеживание соединений и поведенческий анализ, чтобы отделить реальных пользователей от поддельных IP-адресов или вредоносного трафика. Для дополнительной защиты направляйте трафик через Cloudflare Spectrum (для TCP) или Cloudflare CDN/Web Application Firewall (для HTTP). Эти обратные прокси предотвращают прямой доступ к вашему источнику и блокируют DDoS-трафик на основе TCP до того, как он нанесет урон.

03

UDP-флуд

Вы задавались вопросом, как предотвратить DDoS-атаку, посылающую UDP-трафик? Используйте Magic Transit или Spectrum, чтобы идентифицировать и отбросить его в режиме реального времени. В сочетании с Magic Firewall применяйте интеллектуальное ограничение скорости или полностью блокируйте нежелательные UDP-пакеты, защищая свою инфраструктуру от объемных наплывов.

04

Teeworlds

Защитите свои игровые серверы с помощью Cloudflare Spectrum или Magic Transit. Cloudflare автоматически определяет отпечатки и отфильтровывает DDoS-трафик, позволяя реальным игрокам подключаться. Для дополнительного контроля используйте Magic Firewall для создания пользовательских правил, которые останавливают атаки на уровне пакетов.

05

RIPv1

Отключите RIPv1 на всех маршрутизаторах и переключитесь на RIPv2 с аутентификацией, если требуется маршрутизация. Блокируйте входящий UDP-порт 520 из недоверенных сетей и следите за необычной маршрутизацией, чтобы выявить потенциальные злоупотребления на ранней стадии.

06

RDP

Используйте Magic Transit для блокировки поддельного или вредоносного трафика RDP до того, как он попадет на ваш сервер. Чтобы защитить удаленный доступ на уровне приложений, переместите RDP за Cloudflare Gateway или Zero Trust Network Access (ZTNA), которые требуют аутентификации и помогают предотвратить злоупотребления открытыми службами RDP.

07

DemonBot

Как защититься от DDoS, осуществляемого с помощью DemonBot? Обратитесь к Magic Transit, который фильтрует массивные потоки на уровнях 3 и 4. Cloudflare выявляет зараженный трафик с помощью анализа в реальном времени и обнаружения сигнатур. Для атак седьмого уровня используйте WAF и защиту от DDoS от Cloudflare, чтобы блокировать HTTP-флуд и злоупотребление соединениями.

08

VxWorks Flood

Разверните Magic Transit для фильтрации DDoS-трафика со взломанных устройств VxWorks. Cloudflare обнаруживает и блокирует этот трафик с помощью кастомной эвристики и отпечатков в режиме реального времени. Для защиты на уровне приложений используйте службу Cloudflare Gateway и WAF для защиты от злоупотреблений на уровне протоколов.

Никаких отказов: Ваша защита от DDoS выиграет с Cloudfresh!

cloudfresh.com

hi@cloudfresh.com