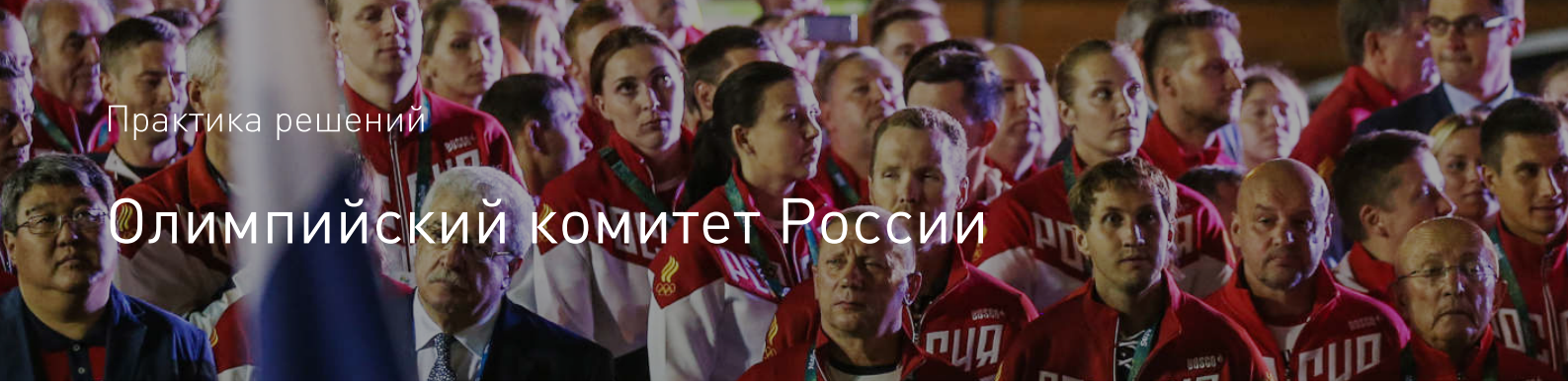


Практика решений

Олимпийский комитет России

> NGENIX оказался самым надежным решением из тех, которые мы рассматривали. Веб-сайт работал без сбоев, как во время атак, так и при резких всплесках интереса к контенту сайта.

Андрей БОРОДИНОВ
Руководитель отдела технического обеспечения службы информации Олимпийского комитета России

ОСОО «Олимпийский комитет России»

Сфера

Государственный веб-портал

Отражено атак

10

Максимальная мощность атаки

8 Gbit/s

Максимальная длительность атаки

7 дней 22 часа 6 минут

Веб-сайт

www.olympic.ru

Используемые решения

- NGENIX Secure Cloud

Защита от кибератак и ускорение веб-сайта

В предверии Олимпийских игр 2016 официальный веб-сайт Олимпийского комитета России столкнулся с проблемой кибератак. Обстановка вокруг олимпийской сборной привлекала повышенное внимание киберприступников. Стабильность работы веб-ресурса стала одной из приоритетных задач технической команды Олимпийского комитета России.

Решение NGENIX Secure Cloud, совмещающее в себе преимущества распределенной доставки контента и противодействия киберугрозам, было выбрано в качестве наиболее оптимального варианта. В рамках единого контракта было создано несколько уровней защиты инфраструктуры веб-ресурса. Интеграция NGENIX с системой противодействия атакам национального оператора Ростелеком позволила обеспечить защиту от DDoS-атак, сохранив высокую скорость работы веб-сайта для легитимных пользователей. Сервис Web Application Firewall позволил решить проблему безопасности на уровне приложений.

Сервисы доставки контента Олимпийского комитета были развернуты на узлах, входящих в состав защищённого сегмента распределенной облачной платформы NGENIX. Система защиты Arbor PeakFlow, работающая на базе сети Ростелекома, обеспечила своевременную очистку вредоносного трафика и сохранила доступность сайта для всех неравнодушных к происходящему в российском спорте.

> «Государственный и банковский сектор – одна из главных целей для хакеров. Сейчас каждый может заказать атаку на любой веб-ресурс. В случае с Олимпийским комитетом – это репутационные потери не только для организации, но и для бренда нашей страны. Поэтому мы очень тщательно подошли к выбору партнера»

Какие задачи стояли перед NGENIX?

- Обеспечить доступность веб-сайта во время DDoS-атак
- Защитить веб-сайт на уровне приложений
- Ускорить доставку контента

Доступность веб-сайта во время DDoS-атак

Решение NGENIX Secure Cloud позволило обеспечить несколько уровней защиты. В рамках сервиса DDoS Protection программно-аппаратный комплекс Ростелекома Arbor PeakFlow защитил ресурс от DNS/NTP Amplifiction атак. Путем переноса статического и динамического трафика на инфраструктуру сети доставки контента был создан дополнительный эшелон защиты, который полностью экранирует сервера заказчика от внешних запросов. Только за 2016 год система Arbor зафиксировала и отразила 10 атак мощностью до 8 Гбит/с, фильтрация трафика одной из атак длилась более 7 дней. Своевременная классификация типов киберугроз и непрерывная работа системы защиты сохранили полную доступность веб-сайта в течение всего периода атаки.

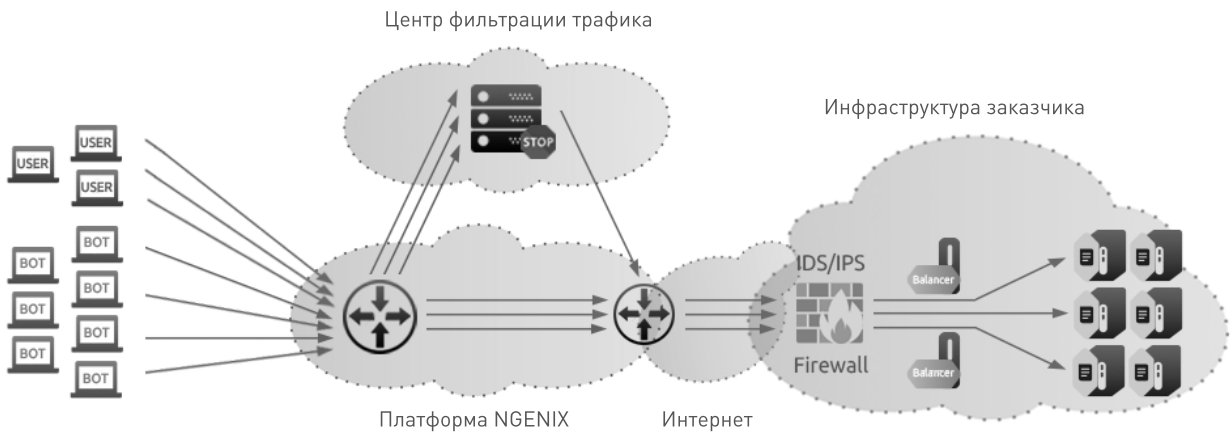
Защита веб-сайта на уровне приложений

Одной из ключевых задач по противодействию атакам на веб-ресурсы Олимпийского комитета стала защита от взломов на уровне приложений. Сервис Web Application Firewall (WAF) позволил обнаружить уязвимости приложений веб-сайта и своевременно принять меры по выявлению и блокированию вредоносного трафика, направленного на эксплуатацию уязвимостей.

Ускорение доставки защищаемых ресурсов

Повышенное внимание СМИ к российскому спорту в 2016 году привело не только к интересу киберпреступников, но и к росту трафика на веб-сайте Олимпийского комитета России. Перенаправление запросов в центр очистки трафика в период активных атак могло негативно сказаться на скорости загрузки ресурса при резком росте количества посетителей. Подключение распределенной облачной платформы NGENIX уменьшило время загрузки веб-страниц. Таким образом, доставка всего содержимого веб-сайта стала не только дополнительным эшелоном защиты, но также позволила сохранить высокую скорость работы ресурса без дополнительных вложений в инфраструктуру.

Как происходит фильтрация трафика при DDoS-атаке?



NGENIX – провайдер облачных сервисов для киберзащиты и ускорения веб-ресурсов, лидер в области доставки медиаконтента в российском интернете. Мы первыми вывели на российский рынок технологию CDN и первыми разработали универсальный набор облачных услуг для обеспечения безопасности веб-сайта и доставки контента на высокой скорости.

Услуги NGENIX сокращают время вывода на рынок контент-сервисов и позволяют избежать затрат на проектирование, разработку, построение, развертывание и поддержку собственных решений. Распределенная облачная платформа NGENIX позволяет доставлять видео по запросу, вести прямые интернет-трансляции, организовать надежную дистрибуцию цифрового контента, ускорять загрузку сайтов и повышать производительность веб-приложений.

Поговорите с экспертом

sales@ngenix.net
+7 (495) 737-57-43
/ngenix.net
/company/ngenix
127083, Россия, Москва, ул. 8 Марта, д. 1, стр. 12, подъезд 1, этаж 7