EDGE ЦЕНТР

Стресс-тестирование в борьбе с DDoS-атаками: Практические применения для улучшения внутреннего контроля

Артём Избаенков

Директор по развитию направления кибербезопасности

Член правления АРСИБ

Член ISDEF

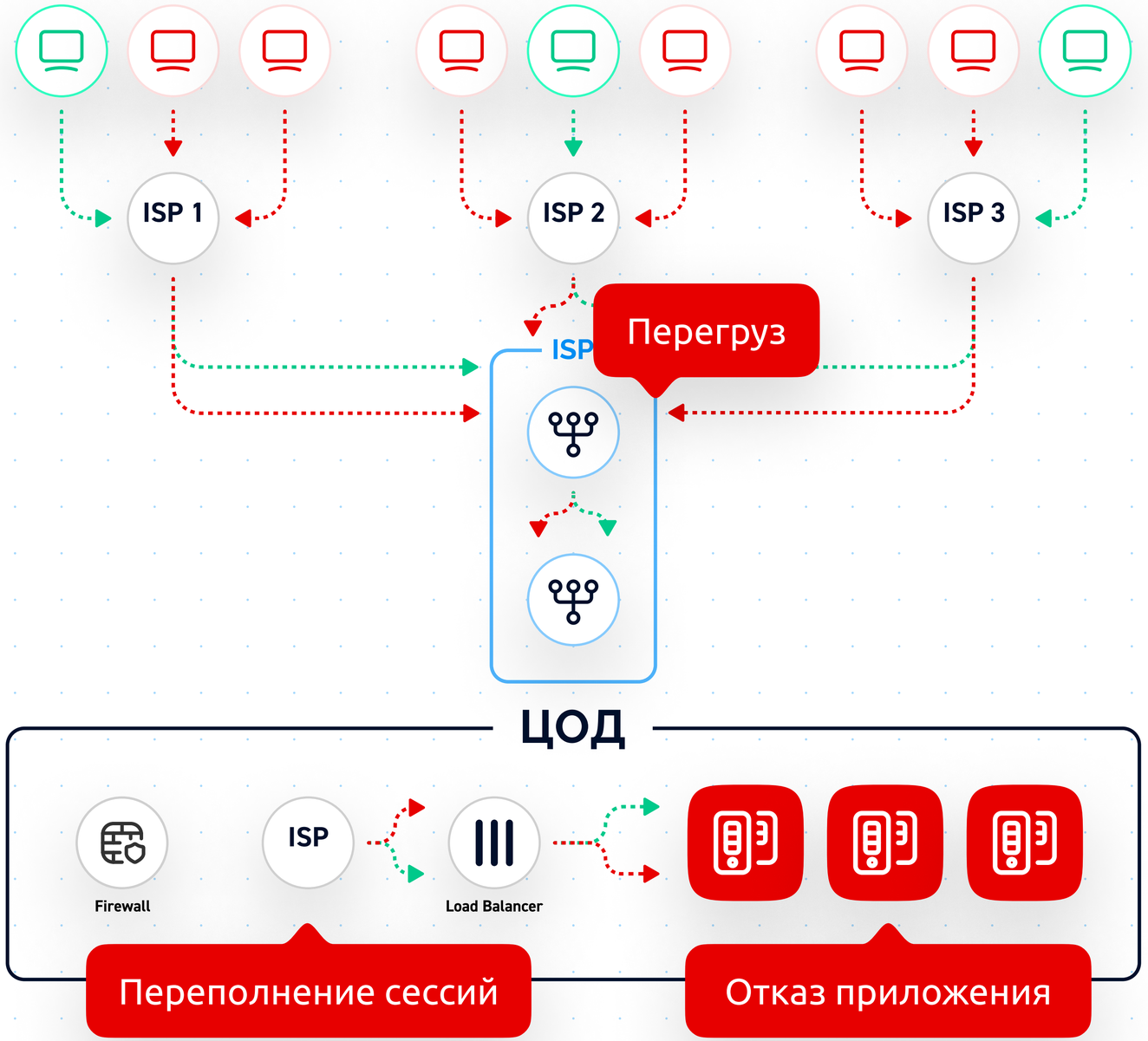
DDoS-атака

Во время DDoS-атаки заражённые хосты (боты) из разных сетей перегружают ресурсы сервера, канала или приложения нелегитимным трафиком. Тем самым они не позволяют легитимным пользователям получить доступ к информации.

Сложность современных DDoS-атак

Сегодня DDoS можно разделить на 3 типа:

1. Перегрузку канала
2. Переполнений таблиц сессий
3. Отказ сервиса (приложения)



Что такое боты и как они вредят?

Бот – программа, которая автоматически выполняет заданные действия.

Создать вредоносный ботнет из тысяч и миллионов взломанных устройств становится всё легче из-за растущего количества IoT-устройств с плохой защитой.

Хорошие боты

Автоматизируют рутинную работу, разные бизнес-процессы, применяются в поисковых системах, инструментах аналитики.

Плохие боты

Создаются злоумышленниками из взломанных устройств, используются для разных кибератак.

Тренды DDoS атак 2023

- Атаки уровня L7 (Приложения) на web инфраструктуру
- Целенаправленные атаки на DNS сервера компаний
- Обьем атак ботнетов на РФ легко перешел границу в 1,2 Тбит/с и более 500 Mpps
- Рост Мощности + Длительности атак >1 Тбит/с >10 дней
- Существенную долю ботов составляют боты из РФ
- Использование облачных ЦОДов для организации и монитизации DDoS атак
- Атаки на API

Планирование рисков

DDoS-атаки — угроза доступности №1 – должны быть частью анализа рисков.

Измеряя риски доступности и надежности сервиса, необходимо понять, где риск угрозы DDoS-атак в вашем случае?

1. Выбор площадки
2. Физическая безопасность
3. Пожарная безопасность
4. Электричество
5. Окружающая среда
6. DDoS-атаки

Стресс-тестирование

Это процесс проверки устойчивости и способности системы, сети или веб-ресурса к отражению DDoS и бот атак. DDoS-атака направлена на перегрузку ресурса большим количеством запросов или трафика с целью временно либо полностью обесточить или ограничить доступ к ресурсу для легитимных пользователей.

Стресс-тестирование DDoS проводится с целью определения, каким образом целевой объект будет реагировать на подобную атаку и насколько эффективно он сможет справиться с ней. Это позволяет выявить уязвимости в инфраструктуре и принять меры для улучшения защиты от DDoS-атак и понять предельные возможности инфраструктуры или веб-сайта.

Виды стресс-тестирования

Нагрузочное тестирование (Load Testing): Проверка системы под типичной рабочей нагрузкой для оценки производительности.

Стресс-тестирование (Stress Testing): Тестирование с экстремальной нагрузкой для выявления точки деградации или сбоев.

Долговременное тестирование (Endurance Testing): Проверка устойчивости системы при продолжительной нагрузке.

Производительное тестирование (Performance Testing): Оценка скорости и отклика системы при разной нагрузке.

Объемное тестирование (Volume Testing): Тестирование на обработку больших объемов данных или запросов.

Атакующее тестирование (Spike Testing): Проверка реакции системы на резкие пики нагрузки с эмуляцией DDoS атакой ботами.

Методы стресс-тестирования по модели OSI инфраструктуры

L3 Уровень по модели OSI

Синфлуд (SYN Flood): На этом уровне можно сгенерировать большое количество недостоверных SYN-запросов, чтобы перегрузить маршрутизаторы и коммутаторы.

MAC-флуд (MAC Flood): Атака на адреса MAC, перегружая коммутаторы и сетевую инфраструктуру.

ARP-флуд (ARP Flood): Атака на таблицы ARP, затрудняя разрешение IP-адресов в MAC-адреса.

ICMP-флуд (ICMP Flood): Атака с использованием множества ICMP-запросов, что может привести к перегрузке маршрутизаторов.

UDP-флуд (UDP Flood): Генерация большого объема ненадежных UDP-пакетов для перегрузки сети.

L4 Уровень по модели OSI

SYN-ACK-флуд (SYN-ACK Flood): Отправка большого количества недостоверных SYN-ACK-ответов для перегрузки серверов.

Методы стресс-тестирования по модели OSI приложений

L7 Уровень по модели OSI

HTTP/HTTPS-флуд (HTTP/HTTPS Flood): Атака на серверы, генерируя большое количество HTTP/HTTPS-запросов, чтобы перегрузить веб-приложения.

DNS-амплификация (DNS Amplification): Злоумышленник отправляет DNS-запросы с подделанным адресом источника, чтобы перегрузить DNS-серверы.

Slowloris: Эта атака направлена на веб-серверы. Злоумышленник открывает множество недостаточно завершенных HTTP-соединений с сервером, что замедляет его отклик и перегружает ресурсы.

RUDY (R-U-Dead-Yet): Этот метод заключается в отправке большого количества POST-запросов на веб-сервер с медленной передачей данных. Это может замедлить сервер, так как он должен будет обрабатывать каждый запрос.

Запросы на ресурсы с высокой вычислительной нагрузкой: Например, множество запросов на выполнение сложных математических операций или генерацию больших объемов данных может перегрузить сервер.

Интересные кейсы

Клиент

Крупный интернет-магазин

Проблема

Во время пика популярности товара и сезона распродаж, веб-сервера работали с задержками в обработке заказов, что приводило к ухудшению опыта пользователей и потере продаж.

Решение

Командой EdgeЦентр Security было проведено стресс-тестирование для определения максимальной пропускной способности валидных пользователей. Было предложено оптимизировать инфраструктуру серверов, внедрить кеширование и масштабирование (включая CDN), чтобы обеспечить плавную обработку большого числа заказов.

Клиент

Биржевой холдинг

Проблема

При волатильных рыночных условиях, торговая платформа может столкнуться с задержками в обработке ордеров и обновлении информации о ценных бумагах, что может повлиять на точность торгов.

Решение

Командой EdgeЦентр Security было проведено стресс-тестирование для определения максимальной пропускной способности валидных пользователей. Было предложено оптимизировать инфраструктуру серверов, внедрить кеширование и масштабирование (включая CDN), чтобы обеспечить плавную обработку большого числа заказов.

Клиент

Международное СМИ

Проблема

В случае публикации важных новостей или проведения онлайн-трансляций мероприятий, сервер может перегрузиться и не справиться с высоким числом одновременных пользователей, что приведет к сбоям и недоступности контента.

Решение

Командой EdgeЦентр Security было проведено стресс-тестирование для определения максимальной пропускной способности валидных пользователей. Было предложено оптимизировать сервера, использовать CDN (сеть доставки контента) для распределения нагрузки и масштабировать ресурсы по мере необходимости.

EDGE ЦЕНТР

edgecenter.ru

8 800 775 08 54