ООО "ВАС Экспертс"
191028, Санкт-Петербург,
Литейный пр. д. 26 Лит. А,
БЦ «Преображенский», офис 5-23
Телефон: +7 (812) 313-8815
Эл. Почта: info@vasexperts.ru

Опция: Защита от DOS и DDOS атак

В системе реализованы следующие механизмы противодействия DoS и DDoS:

- Защита от TCP SYN Flood
- Защита от fragmented UDP Flood
- Защита от DDoS (LOIC и т.п.) на основе теста Тьюринга (HumanDetection)

1. Механизмы защиты от DoS атак

В случае DoS атаки злоумышленнику важно замаскировать обратный адрес, чтобы его было невозможно блокировать по IP. Поэтому DoS атака представляет собой бомбардировку серверов жертвы отдельными пакетами с фиктивным обратным адресом. Отказ в обслуживании в этом случае наступает либо вследствие переполнения (забивания трафиком) арендуемой клиентом полосы, либо при бомбардировке пакетами, которые вызывают повышенный расход ресурсов на атакуемой системе.

СКАТ содержит высоко производительный механизм защиты от TCP SYN Food и fragmented UDP Flood атак, позволяет обработать в зависимости от конфигурации до 20 млн. пакетов в секунду.

1.1 TCP SYN Flood защита

Атака SYN flood вызывает повышенный расход ресурсов атакуемой системы, так как на каждый входящий SYN пакет система должна зарезервировать определенные ресурсы в памяти, либо сгенерировать специальный SYN+ACK ответ, содержащий криптографическую cookie, осуществлять поиск в таблицах сессий и т.п., т.е. затратить существенные процессорные ресурсы. В обоих случаях отказ в обслуживании наступает при потоке SYN-flood 100000-500000 пакетов в секунду. В тоже время даже гигабитный канал позволит злоумышленнику направить на атакуемый сайт поток до 1,5 миллионов пакетов в секунду.

СКАТ осуществляет защиту от SYN flood следующим образом:

- обнаруживает атаку по превышению заданного порога неподтвержденных клиентом SYN запросов
- самостоятельно, вместо защищаемого сайта отвечает на SYN запросы
- организует TCP сессию с защищаемых сайтом после подтверждения запроса клиентом

В зависимости от настроек СКАТ может не применять данный тип защиты (активация в ручную), автоматически активировать защиту или быть в постоянном режиме защиты от данного типа атак.

1.2. Fragmented UDP Flood защита

Данный тип атаки осуществляется фрагментированными udp пакетами, обычно короткого размера, на сборку и анализ которых атакуемая платформа вынуждена тратить много ресурсов.

Защита осуществляется путем отбрасывания неактуального для защищаемого сайта набора протоколов, или жесткого ограничения их по пропускаемой полосе.

Например, для WEB-сайтов рабочими протоколами являются HTTP, HTTPS. В этом случае не актуальные протоколы можно отбросить путем настройки СКАТ.

2. Механизм защиты от DDoS

Для осуществления DDoS атаки злоумышленник имеет в распоряжении большую сеть удаленно управляемых компьютеров (BOTNET) и ему уже нет необходимости скрывать IP-адрес каждого из них. В этом случае злоумышленник может просто имитировать действия легитимных пользователей сайта, но благодаря большому количеству участвующих в атаке компьютеров (иногда сотен тысяч), даже такие действия вызовут большую нагрузку на сайт и приведут к отказу в обслуживании. Обычно злоумышленники выбирают для вызова наиболее ресурсоемкие запросы к атакуемому сайту, чтобы минимизировать число участвующих в атаке компьютеров, IP адреса которых будут после атаки засвечены.

Часто для защиты от подобных атак с разной степенью эффективности применяются различные поведенческие стратегии (behavioralDDoSprotection), которые позволяют определить отклонения в нормальном поведении. Мы же предлагаем простой и очень эффективный подход - использование теста Тьюринга (странички с CAPTCHA, от англ. CompletelyAutomatedPublicTuringtesttotellComputersandHumansApart), компьютерного теста, используемого для того, чтобы определить, кем является пользователь системы: человеком или компьютером.

Защита работает следующим образом:

- при превышении порогового значения, например, комфортного для сайта количества запросов в секунду, активируется защита
- к работе с сайтом допускаются только пользователи, находящиеся в белом списке, все остальные перенаправляются на страничку с CAPTCHA для проверки на «человечность». Эта страничка расположена на отдельном сервере в интернет, способном выдержать нагрузку BOTNET любого размера (возможно использование сервера компании).
- пользователи, успешно прошедшие тест, добавляются в белый список и дальнейшая их работа с сайтом ничем не омрачена
- пользователи, не прошедшие тест (BOTы), не могут продвинуться дальше детектирующей странички и создать какую-либо нагрузку на атакуемый сайт