Светлана Голубева,
Технический Университет Молдовы

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ЗАЩИТЫ ОТ DDOS

DDOS is a great problem for commercial and governmental INTERNET resources in our days. There doesn't exist any universal algorisms for defending against DDOS for one server. This article describes the possibilities for common and distributed defense against DDOS attacks.

Ключевые слова: *DDoS-атака, защита, CAPTCHA, «Оверлейная сеть», рассредоточение.*

1. Введение

Год за годом, мы становимся все более зависимыми от интернет сервисов, таких как: различные финансовые инструменты, IP-телефония, получение новостей, электронное правительство и т.д. Все эти сервисы представляют интерес для злоумышленников и нуждаются надежной защите. Наиболее часто Интернет-сервисы подвергаются, так называемым, DoS-атакам или DDoS-атакам[1].

DoS-атака (от англ. Denial of Service) и DDoS-атака (от англ. Distributed Denial of Service) – это разновидности атак злоумышленника на компьютерные системы. Цель этих атак – довести систему до отказа, то есть, создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён. Если атака производится одновременно с большого количества IP-адресов, то в этом случае она называется распределённой атакой на отказ в обслуживании (DDoS) [2].

Различные компании и производители предлагают и разрабатывают свои решения защиты. Проводятся тщательные исследования трафика. Составляется схема уже произошедших атак. Проводится анализ статистических данных как: частота атак определенного ресурса, количество вовлеченных в атаку компьютеров, а также качество методов, предотвративших атаку [5].

2. Методы защиты от DDoS-атак

Существуют различные методы защиты от DDoS-атак, причём как на уровне провайдера, так и на уровне конкретного конечного пользователя (непосредственно владельца сетевого ресурса). Ниже приведены основные способы защиты, которые можно комбинировать и совмещать [3]:

Владельцы веб-ресурсов защищаются с помощью:

- Искусственного ограничения пропускной способности сети.
- Периодического изменения адреса хостируемого ресурса.
- Использования Content Delivery Network (CDN) – географически распределенной сетевой инфраструктуры, предназначенной для доставки конечному пользователю высоко нагруженного по трафику цифрового контента на высоких скоростях [1].

Интернет-провайдеры используют такие методы защиты как:

- Blackhole маршрутизация – перевод запросов на несуществующий адрес.
- Фильтрация и блокирование – если не срабатывает хотя бы одно из условий, запрос отклоняется (например, не совпадает CAPTCHA (от англ. «Completely Automated Public Turing test to tell Computers and Humans Apart» [1]).
- Активные ответные меры – воздействие на источники, организатора или центр управления атакой, как технического, так и организационно-правового характера.

Но все эти методы не дают полной защиты от DDoS-атак ботов, а также могут отфильтровать запросы нормальных клиентов. Также они требуют правильной настройки непосредственно во время атаки, а, следовательно, нуждаются в постоянной поддержке опытного и дорогостоящего специалиста.

3. Рассредоточение или «Оверле́йная сеть» – как один из методов защиты от DDoS-атак

Рассредоточение является более глобальным подходом к решению проблемы DDoS-атак, позволяющим перенаправить и обработать запрос легитимного пользователя, даже если один из узлов системы заблокирован.

Процесс подтверждения, что пользователь является легитимным, происходит следующим образом [4]:

1. Пользователь обращается к интересующему его ресурсу
2. Ему присылается CAPTCHA – тест, определяющий является ли он человеком или ботом.
3. На основе правильно заполненного CAPTCHA формируется ключ доступа, который, в свою очередь, используется для создания Ticket-контракта между пользователем и «Оверле́йной сеть» на доступ в сеть.
4. И только пользователи, обладающие Ticket-ом, имеют доступ к целевому серверу.

Основные преимущества использования этого подхода заключаются в следующем:

- пользователям доступны все узлы рассредоточенной сети;
- любой узел может подтверждать, является ли пользователь легитимным или ботом;
- запросы пользователя, однажды признанного легитим-

ным, выполняются в первую очередь;
- сеть является «достаточно масштабной», чтобы заблокировать все узлы;
- одна распределенная сеть может предоставлять защиту множеству пользователей.

4. Заключение

Проблема DDoS-атак наиболее значимая в современном киберпространстве, поэтому различного уровня владельцы веб-ресурсов должны объединить свои усилия, чтобы найти максимально эффективное решение проблемы. Использование «Оверле́йной сети» является выгодным всем за счет ее независимого распределения от конкретного провайдера и невысокой цены для ее построения. Идея «Оверле́йной сети» может быть расширена путем использования в ее основе таких систем, как PlanetLab и GRID [2].

Литература:

1. Компьютерная документация от А до Я http://www.compdoc.ru/secur/xacer/what_is_ddos_attack/
2. Википедия – свободная энциклопедия http://wikipedia.org/
3. Internet – Technologies.RU http://www.internet-technologies.ru/articles/article_436.html
4. Angelos D. *Keromytis Network Security Lab Computer Science Department*, Columbia University «Denial of Service Attacks and Resilient Overlay Networks» http://www.nis-summer-school.eu/index.html
5. WebDocs.Ru документация от А до Я http://www.webdocs.ru/content-572.html