Н.В. Щетинин

ИЗУЧЕНИЕ ПОЛЬЗОВАТЕЛЬСКОЙ АУДИТОРИИ ДЛЯ ЗАДАЧ СЕТЕВОЙ БЕЗОПАСНОСТИ

(Самарский государственный аэрокосмический университет имени академика С.П. Королева (национальный исследовательский университет))

Работа посвящена защите от сетевых DDoS-атак и изучению аудитории Интернет-сервисов. Проведены эксперименты в условиях реальной сетевой атаки на популярный Интернет-портал. Для предотвращения DDoS-атак нами был разработан алгоритм, позволяющий эффективно бороться с ними.

DDoS атака (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании») – это такой тип атак, при котором некоторое множество компьютеров в сети Интернет, называемых «зомби», «ботами» или бот-сетью (ботнет), по команде злоумышленника начинают отправлять запросы на сервис жертвы. Такие сети имитируют действия обычных пользователей, поэтому их крайне сложно выявить и заблокировать. Когда число запросов превышает возможности серверов жертвы, новые запросы от настоящих пользователей перестают обслуживаться и становится недоступным. При этом жертва несёт финансовые убытки. В настоящее время DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик.

Алгоритм заключается в:

- Выявлении пользовательского ядра (постоянных посетителей) сайта и составлении их списка;
- Создании разрешительных и запретительных списков доступа;
- Анализе и блокировании поступающего UDP-траффика на основании списков доступа;
- Написании скриптов, автоматизирующих данные алгоритмы;
- Налаживание взаимодействия с провайдерами для организации защиты.

Рассмотрим подробнее предложенный алгоритм.

Пользовательское ядро – постоянные посетители Интернет-сервиса, которые регулярно обращаются к исследуемому ресурсу. Все остальные IP-адреса будем считать новыми.

Для определения постоянной аудитории нужно:

- определить период времени, за которое анализ статистики посещений позволит выявить пользовательское ядро;
- оценить предельную долю адресов из пользовательского ядра в общей базе IP адресов;
- определить особенности поведения новых (посетивших ресурс впервые) пользователей и процента запросов, принадлежащих им.

Особенно важным аспектом является определение особенностей поведения новых пользователей. К ним можно отнести количество и долю запросов новых пользователей при пользовании сервисом (включая их ранжированный список), период времени непрерывного пользования сервисом и т.д. Прежде всего, следует сравнить поведение новых и старых пользователей, и найти степень различия между частотой посещений и количеством запросов к сервису.

Чтобы определить постоянных пользователей Интернет-сервиса можно использовать любые журналы доступа, в которые вносятся IP адреса посетителей, либо данные NetFlow (в нашем случае используются файлы журналов веб-сервера Nginx). Далее производится формирование постоянной аудитории сайта в виде списка IP-адресов. После формирования такого списка, все остальные IP-адреса считаются новыми.

На основе этих данных формируется разрешающий список адресов, для которых можно разрешить доступ в начале сетевой атаки.

Также, после начала атаки необходимо сформировать запрещающий список (стоп-лист) атакующих адресов. Он будет ограничивать UDP пакеты, поступающие с атакующих адресов. Тем самым можно избежать переполнения канала (атака типа flood).

Во время сетевой атаки очень важно оперативно составить список атакующих адресов для блокировки на фильтрующем оборудовании затем, чтобы сервис смог отвечать на запросы обычных пользователей вне пользовательского ядра как можно скорее. Для этого эффективно применить одновременно сразу два критерия выявления источников атаки: превышение порогового уровня для предельной скорости UDP потоков (объему входящего трафика (UDP, ICMP или TCP)) и для количества потоков, генерируемых с исследуемого IP адреса.

После формирования стоп-листа нужно просто заменить разрешающий список на запрещающий.

В заключение этого раздела необходимо установить, какой части пользователей будет отказано в обслуживании при установке фильтра, позволяющего обслуживать запросы только с IP адресов, входящих в пользовательское ядро. Из расчетов следует, что всего, в среднем, только 8% от среднесуточной аудитории будет отказано в обслуживании.

Как было сказано выше, испытания проводились на реальном Интернет-портале. Он был перемещен на веб-хостинг с созданной на нем сетевой инфраструктурой, принципиальная схема которой приведена на Рис. 1. Также в течение пяти месяцев собиралась статистика использования данного сервера.

В процессе комбинированной DDoS-атаки был записан сетевой трафик, собрана статистика NetFlow и сделаны выводы об эффективности способов обнаружения и методов противодействия.

Проводились атаки на количество запросов к веб-серверу и UDP flood атака, а также проводилось испытание скорости фильтрации IP-адресов. Ни

одна из атак не вывела из строя оборудование, а веб-сервер отвечал на запросы пользователей. Можно сделать вывод, предложенный алгоритм показал себя очень эффективным при защите от DDoS-атак.

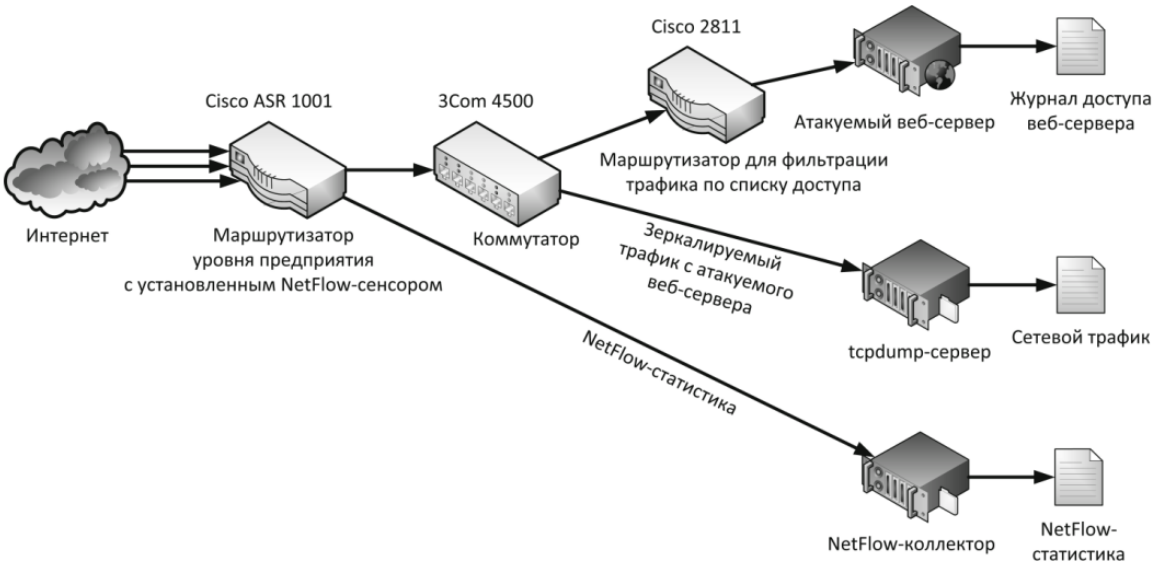

Рис.1 – Сетевая инфраструктура для проведения исследований

Для организации эффективной защиты от подобных атак необходимо наладить взаимодействие с провайдерами верхнего уровня. Если организовать автоматизированный процесс передачи списка блокированных IP-адресов, то такая защита будет эффективной против подавляющего большинства существующих бот-сетей.

Литература

1. Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms //ACM SIGCOMM Computer Communication Review. – 2004. – Т. 34. – №. 2. – С. 39-53.

2. Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art //Computer Networks. – 2004. – Т. 44. – №. 5. – С. 643-666.

3. Singh S., Gyanchandani M. Analysis of Botnet behavior using Queuing theory //International Journal of Computer Science & Communication. – 2010. – Т. 1. – №. 2. – С. 239-241.

4. Stanton J. M., Stam K. R., Mastrangelo P., Jolton, J. Analysis of end user security behaviors //Computers & Security. – 2005. – Т. 24. – №. 2. – С. 124-133.

5. Sukhov A. M., Sidelnikov D. I., Platonov A. P., Strizhov M. V., Galtsev A. A. Active flows in diagnostic of troubleshooting on backbone links //Journal of High Speed Networks. – 2011. – Т. 18. – №. 1. – С. 69-81.

6. Sukhov A.M., Sagatov E.S., Baskakov A.V., Analysis of Internet service user audiences for network security problems //2014 IEEE 2nd International Symposium on Telecommunication Technologies, 24-26 November 2014, Langkawi, Malaysia, p. 191-196.