

ТЕХНОЛОГИИ ЗАЩИТЫ ОТ DDoS-АТАК

Карпеченко В.А., студент гр.272303, Липницкая Н.И., ассистент кафедры ЭИ

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Ефремов А.А. – канд. эк. наук, доцент кафедры ЭИ

Аннотация. Данная работа представляет собой анализ технологий защиты от DDoS-атак. В процессе анализа будут рассмотрены определение DDoS-атак их типы и особенности. Описываются технологии защиты. В статье акцентируется внимание на преимуществах и недостатках различных типов защиты от DDoS-атак

Ключевые слова. DDoS-атаки, защита DfY, локальное решение, автономное облачное решение, симметричный тип подключения, ассиметричный тип подключения.

DDoS-атака - это вид кибер-атаки, при которой недоброжелатель создает множество запросов к серверу, генерируемых компьютером [1]. Обычно они поступают из бот-сети – сети устройств, зараженных вредоносным ПО, которое дает злоумышленнику возможность контролировать сервер, – волна запросов перегружает сеть и делает сайт недоступным для клиентов. В результате компания испытывает простой и не может обслуживать клиентов в течение неизвестного периода времени [2].

Существует несколько подходов для решения проблемы с защитой от DDoS-атак. К ним относятся:

- DfY защита;
- локальные решения;
- автономные облачные решения.

В практическом плане защита DfY опирается на установку статических пороговых значений трафика и неизбирательных правил черного списка IP-адресов. Основным недостатком решений DfY является то, что они часто используются в качестве реактивной меры. Еще одна проблемой данного подхода заключается в том, что он всегда ограничен пропускной способностью сети.

Локальный подход к защите от DDoS-атак использует аппаратные устройства, развернутые внутри сети, размещенные перед защищенными серверами. К недостаткам данного подхода можно отнести:

- ограничение масштабируемости;
- локальные устройства необходимо развернуть вручную. Это влияет на время реагирования;
- стоимость покупки, установки и обслуживания оборудования относительно высока.

Облачные решения предоставляют дополнительные возможности фильтрации, необходимые для предотвращения атак на уровне приложений. Значительными преимуществами данного подхода являются:

- практически неограниченная масштабируемость;
- не требуют инвестиций в персонал безопасности или техническое обслуживание.

Сравнивая данные подходы по защите от DDoS-атак можно заметить, что облачные решения являются наиболее эффективными и менее затратными по сравнению с DIY защитой и локальными решениями. Так как не требуют каких-либо инвестиций в персонал безопасности или техническое обслуживание, требуемое решениями DIY и локальным оборудованием [4].

По типу подключения защиту от DDoS-атак можно классифицировать на симметричную и асимметричную [5].

В заключении можно сказать, что DDoS-атака является основной угрозой для компаний. Злоумышленники постоянно стараются находить новые уязвимые места для нанесения ущерба. Поэтому необходимо постоянно работать над совершенствованием методов защиты и противодействия DDoS-атакам.

Список использованных источников:

1 Как предотвратить DDoS-атаки: рекомендации и стратегии [Электронный ресурс] // Radware. – Режим доступа: [Как предотвратить DDoS-атаки: лучшие практики и стратегии | Radware](#). – Дата доступа: 08.04.2023.

2 Параматаров, М. DDoS-атаки и как защитить себя [Электронный ресурс] / Параматаров, М //CloudDNS блог. – Режим доступа [DDoS-атаки и как защитить себя - CloudDNS Блог](#). – Дата доступа: 08.04.2023.

3 Титов, Ф.М. Исследование методов защиты от атаки DDOS / Титов, Ф.М. // Научные междисциплинарные исследования: материалы 16 науч.-практ. конф. аспирантов, магистрантов и студентов, Саратов, 30 июня 2021 г. /Научная общественная организация "Цифровая наука" ; редкол.: Н. В. Емельянов (гл. ред.) [и др.]. – Саратов, 2021. – С. 36-41.

4 Как остановить DDoS-атаки [Электронный ресурс] // Imperva. – Режим доступа: [\(1\) New Messages! \(imperva.com\)](#). – Дата доступа: 08.04.2023.

5 Хантимиров, Р. Выбираем и проверяем технологии защиты от DDoS-атак [Электронный ресурс] /Хантимиров, Р //Anti-malware. – Режим доступа: [Выбираем и проверяем технологии защиты от DDoS-атак \(anti-malware.ru\)](#). – Дата доступа: 08.04.2023.