МНОГОВЕРСИОННОСТЬ ЗАЩИТЫ ОБЛАЧНЫХ ИНФРАСТРУКТУР ОТ DDOS-АТАК

Меленец А. В.

Государственный департамент страхового фонда документации, г. Харьков

Многоверсионность защиты облака от DDoS-атак заключается в определении наличия атаки на облако, при этом атака обходит используемую в данный момент базовую модель защиты, определения цели и трафика атаки и последующего применения другого механизма защиты для обработки запросов на использование только атакуемых ресурсов облака, что снизит нагрузку на ресурсы и не будет увеличивать нагрузку на пользователей неатакуемых ресурсов.

Обязательным элементом архитектуры облачной инфраструктуры с многоверсионной защитой от DDoS-атак является единая точка входа в облако, в которой размещается брандмауэр, прерывающий запросы пользователей на получение доступа к службам и декомпозиция логической структуры облака на классы: основа, инфраструктура и приложения.

В качестве базовой модели защиты в брандмауэре предлагается использовать технику DDos-щита. В такой модели защиты запрос пользователя на получение доступа к службам прерывается брандмауэром, который в соответствии с техникой DDoS-щита обрабатывает запрос и предоставляет доступ к службам, либо запрос отбрасывается, IP пользователя добавляется в белый или черный списки. После добавления IP в белый список предоставляется доступ к облачным службам.

В случае обнаружения атаки на определенный класс служб облака все запросы на использование ресурсов класса будут проходит через выбранную модель защиты, например, защита от flooding DDoS-атаки, если после этого атака не прекратилась, запросы проходят через следующую модель защиты, например, защита от SYN Flooding DDoS-атаки и так далее до выбора модели, которая отразит атаку. Подобная схема используется параллельно для всех классов служб облака.

Для обнаружения атаки и ее трафика (нападающих пользователей облака), пользователей и классы облака можно представить в виде матрицы, ячейки столбцов которой соответствуют состоянию работы пользователя с определенным классом сервисов облака. Матрица строится дискретно, в интервал обнаружения. Для обнаружения используется фиксированный порог. Наличие превышения фиксированного порога для отдельных классов означает наличие атаки.