АРХИТЕКТУРА ЗАЩИТЫ ОБЛАКА ОТ DDOS-АТАКИ

Меленец А.В.

Государственный департамент страхового фонда документации, г. Харьков

Обеспечение надежности облачной инфраструктуры, в т.ч. и для страхового фонда документации, является на сегодняшний день основной проблемой для пользователей и провайдеров облачных служб.

Поскольку облачная среда является хорошо масштабируемой, при DDoS-атаке службы используют больше ресурсов в течение периода атаки, чтобы поддержать уровень SLA (соглашение об уровне обслуживания), что приводит либо к неадекватности обслуживания клиентов облака или заказчика, который будет вынужден оплачивать провайдеру использование ресурсов, которые выделяются при атаке. Чтобы обеспечить полную доступность, провайдер может выделять все больше и больше ресурсов непосредственно запросам атаки, что увеличивает количество экземпляров служб, запущенных согласно SLA.

В случае обхода защиты и заражения компьютера, пользователь в большинстве случаев и не подозревает о том, что его компьютер участвует в DDoS-атаке. Одним из аспектов удачной DDoS-атаки является автоматическое, без уведомления пользователя, использование ресурсов множества зараженных компьютеров. Таким образом, включив в процесс работы с облаком специфические возможности человека, можно защитить облако от множества спам-запросов. Наиболее простым и распространенным методом обязательного использования человеческих способностей являются графические тесты. При добавлении в процесс работы с облаком человека существенно снижается интенсивность возможной атаки и повышается уровень защиты.

Для защиты облака от DDoS-атак возможно использовать графические тесты совместно с методом черного и белого списка (DDoS-щит). Однако использование графических тестов занимает определенное время, поэтому после проверки графическим тестом можно использовать простую схему черного и белого списка IP адресов для ускорения процесса принятия решения о доступе к ресурсам облака.

Для обеспечения функционирования DDoS-щита в случае атаки на провайдера в целом, DDoS-щит должен располагаться в ином, чем облако дата-центре, либо, как минимальное решение – под другим IP.

Предложенная архитектура защиты облака, прежде всего лишает DDoS-атаку ее автоматичности, использует черный и белый списки, а также графические тесты. Архитектура состоит из брандмауэра, который является точкой входа в облако и сервера защиты, который использует вышеприведенный метод защиты от DDoS-атаки.