УДК 004.62

А. В. МЕЛЕНЕЦ

Государственный департамент страхового фонда документации, Украина

МНОГОВЕРСИОННАЯ МОДЕЛЬ ЗАЩИТЫ ОБЛАКА ОТ DDOS-АТАКИ

В статье рассмотрены схема DDoS-атак, существующие механизмы защиты облака от DDoS-атак, предложена многоверсионная модель защиты облака от DDoS-атаки. Предложенная многоверсионная модель заключается в определении наличия атаки на облако, при этом базовая модель защиты не отражает атаку, определения цели и трафика атаки, и последующего применения другой модели защиты для обработки запросов на использование только атакуемых ресурсов облака. В качестве базовой модели защиты в брандмауэре предлагается использовать технику DDos-щита. Модель предусматривает декомпозицию логической структуры облака на классы. Разработан пример архитектуры гибридного облака с многоверсионной моделью защиты облака от DDoS-атаки.

Ключевые слова: *cloud computing, DDoS-атака, многоверсионная модель защиты облака от DDoS-атаки, DDoS-щит, классы облака.*

Введение

DDoS-атаки - это на сегодняшний день самое заметное последствие применения cloud computing – в облаке есть все необходимое для проведения эффективных атак: SaaS с удобными web-интерфейсами и простаивающие ресурсы множества зараженных компьютеров. В облаке очень сложно идентифицировать легитимные запросы и запросы атаки. 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). Чтобы обеспечить полную доступность, провайдер может выделять все больше и больше ресурсов непосредственно запросам атаки, что увеличивает количество экземпляров служб, запущенных согласно SLA.

DDoS-атаки могут осуществляются на сетевом уровне или на уровне приложений. DDoS атаки сетевого уровня, такие как ICMP flooding, SYN flooding и UDP flooding занимают полосу пропускания сети и легитимные пользователи получают отказ в обслуживании от атакуемой системы. При отражении DDoS атаки сетевого уровня, организатор атаки может перенести ее на уровень приложений и создать более сложный тип DDoS-атак. В современных работах [1-4] посвященных технологиям защиты облачных инфраструктур, такие авторы как Zissis D., IrfanGul, Qi Chen, Chonka A. и др. рассматривают техники защиты облачной инфраструктуры от наиболее опасных DDoS-атак. Однако предложенные техники защиты могут эффективно функционировать только в их комбинации и методы, которые реализуются только в одной целевой машине, не эффективны, для защиты от DDoS-атаки необходим распределенный подход. Кроме того, предложенные модели работают в основном на физическом уровне аппаратного обеспечения, анализируя трафик в коммутаторах и другом сетевом оборудовании.

В статье предлагается метод обнаружения цели DDoS-атаки и использование распределенного многоверсионного метода защиты.

1. Схема DDoS-атаки

DDoS-атака заключается в скоординированной посылке огромного количества ложных запросов на атакуемый ресурс от множества компьютеров. В результате атакуемый сервер тратит все свои ресурсы на обслуживание этих запросов и становится практически недоступным для обычных пользователей. Ситуация усугубляется тем, что пользователи компьютеров, с которых направляются ложные запросы, могут даже не подозревать о том, что их компьютеры используются специальными троянами. Чаще всего злоумышленники при проведении DDoS-атак используют трехуровневую архитектуру. Проследить такую структуру в обратном направлении и выявить адрес узла, организовавшего атаку, практически невозможно. Максимум того, что может атакуемый, это определить адреса атаки, специальные мероприятия в лучшем случае приведут к центру управления ботнетом, но обычно это зараженные компьютеры и владельцы не подозревают о своем участии в атаке.

2. Механизмы защиты от DDoS-атак

Существует несколько механизмов защиты, используемых в облаке, таких как система обнаружения вторжения, фильтрование пакета, контроль виртуаль-

ной машины, маркировка пакета и другие. Используются как простые механизмы, такие как черный и белый списки так сложные модели.

На сегодня стандартным механизмом защиты от DDoS-атак является механизм CAPATCHA, который работает посредством создания и сортировки наборов визуальных тестов, которые разрешимы на человека, но выходят за пределы возможностей существующих программ компьютера.

Предотвращение атаки является самым распространенным механизмом в успешных реализациях защиты от DDoS-атак. Этот механизм направлен на фильтрацию и отбрасывание пакетов атаки. Одним из таких механизмов является anti-spoofing, который использует определенные правила с целью предотвращения подмены адреса источника атаки, используя уязвимости протоколов.

Обнаружение атаки. Обнаружение DDoS-атак основано на использовании сигнатур известных атак или обнаружении аномального поведения трафика во время атаки. Схема обнаружения основана на том, что нормальное соединение TCP начинается пакетом SYN и заканчивается пакетом FIN или RST, поэтому, когда начинается атака, пакетов SYN будет больше чем сумма FIN и RST пакетов. Наиболее проста схема D-WARD защиты от DDoS-атак, которая работает путем сравнения статистики входящего и исходящего трафика с нормальным трафиком для каждого типа трафика с целью обнаружения потока атаки. Основная идея этой схемы заключается в суммировании количества SYN пакетов за период обнаружения и если оно превышает определенный порог, то существует вероятность атаки, эта схема обнаружения является масштабируемой для больших сетей, но не дает никакой информации о IP-адресе с которого происходит атака [4].

Ответ на атаку. Ответ на DDoS-атаку заключается в определении источника атаки и блокировке его трафика. Одной из схем ответа на атаку является хэш-IP техника трассировки, которая использует изоляцию исходного пути. Эта схема формирует аудит движения и может проследить происхождение каждого, доставленного сетью пакета IP. Основой хэш-IP техники трассировки является метод хранения информации о прохождении пакетом определенных маршрутизаторов, с которыми далее проводится работа, вплоть до блокировки их пакетов.

Уменьшение атаки. Методы уменьшения атаки исходят из понимания невозможности полностью предотвратить или остановить DDoS-атаку и фокусируются на минимизации воздействия атаки. Через наличие перегрузки в буфере маршрутизатора обнаруживается трафик, создавший перегрузки и на него накладывается ограничение скорости.

2.1. Защита от flooding DDoS-атаки

Общая методика flooding DDoS-атаки состоит в отправке flooding пакетов с имитированными IP-адресами от нескольких агентов к жертве, с целью загрузки ресурсов жертвы таких как пропускная способность и вычислительные ресурсы. Основой предотвращения такой атаки является отбрасывание пакетов с имитированным IP-адресом (фильтрация source-end).

Наиболее простой и эффективной является схема вход/выход. Фильтрация входа предусматривает фильтрацию трафика в конечную сеть и фильтрация выхода – трафика из конечной сети. Основной идеей схемы вход/выход является разрешение обработки пакета если его исходный адрес находится в пределах ожидаемого IP-адреса (это может быть исходный IP-адрес с определенным префиксом либо белый список).

2.2. Защита от SYN flooding DDoS-атаки

В TCP SYN flooding атаке используются ограничения TCP в поддержании частично открытого соединения. В этом типе DDoS-атаки атакующий атакует сервер путем отправки одновременно потока flooding SYN пакетов с имитированными IP-адресами, так, что очередь сервера для частично открытых соединений будет исчерпана, и любые новые лингитимные пакеты SYN будут отброшены. Основным механизмом защиты от TCP SYN flooding атаки является анализ аномального поведения пары TCP пакетов SYN-SYN/ACK во время атаки (SYN-dog Detection Scheme).

Так как один SYN пакет нормального соединения TCP приведет к SYN/ACK пакету в обратном направлении в течение одного периода то в нормальных условиях разница между количеством исходящих SYN пакетов и входящих пакетов SYN/ACK в отдельной подсети мала. Во время TCP SYN flooding атаки число исходящих пакетов SYN от подсети атакующего будет значительно выше, чем число входящих SYN/ACK пакетов.

Чтобы обнаружить источник атаки, исходя из аномального поведения трафика, SYN-dog Detection Scheme анализирует общее число исходящих пакетов SYN и входящих пакетов SYN/ACK в течение каждого периода наблюдения. Затем вычисляется разность между количеством этих двух потоков пакетов и нормируется с учетом среднего количества входящих SYN/ACK пакетов, с целью исключения зависимости от времени наблюдения и размера сети. В завершении, на основе этой разницы принимается решение о возможной атаке.

3. Многоверсионность защиты облака от DDoS-атак

Многоверсионность защиты облака от DDoS-атак заключается в определении наличия атаки на облако, при этом базовая модель защиты не отражает атаку, определения цели и трафика атаки, и последующего применения другой модели защиты для обработки запросов на использование только атакуемых ресурсов облака, что снизит нагрузку на ресурсы и не будет увеличивать нагрузку на пользователей неатакуемых ресурсов.

3.1. Архитектура многоверсионной модели защиты облака от DDoS-атак

Обязательным элементом архитектуры облачной инфраструктуры с многоверсионной моделью защиты от DDoS-атак является единая точка входа в облако, в которой размещается брандмауэр, прерывающий запросы пользователей на получение доступа к службам и использующий базовую модель защиты. В качестве базовой модели защиты в брандмауере предлагается использовать технику DDos-щита [5]. Модель предусматривает декомпозицию логической структуры облака на классы. В [5] (Том 3. Cloud) используется декомпозиция логической структуры облака на основу, инфраструктуру и приложения.

Рис. 1. Схема работы многоверсионной модели защиты облака от DDoS-атак.

В случае обнаружения атаки на определенный класс служб облака все запросы на использование ресурсов класса будут обрабатываться другой моделью защиты. Например, если базовая модель DDoS-щита стала неэффективной то, используется защита от flooding DDoS-атаки, если после этого атака не прекратилась, запросы обрабатываются моделью защиты от SYN flooding DDoS-атаки и так далее до выбора модели, которая отразит атаку. Подобная схема должна использоваться параллельно для всех классов служб облака. Схема работы такой модели представлена на рис. 1.

3.2. Определение цели атаки

Сервисы, предоставляемые в облачной инфраструктуре можно разделить на классы K, наиболее простым будет K=3, это – основа (Cloud OS, Виртуализация), инфраструктура (IaaS, PaaS и т.п.), приложения (SaaS, DaaS и т.п.). Затем ввести и рассчитать максимальную совокупную емкость обслуживания каждого класса E, которая измеряется числом запросов в единицу времени, и зафиксировать E при нормальных условиях, которые удовлетворяют требованиям SLA. Во время DDoS-атаки число пакетов с запросами от нападающих будет значительно выше, чем число пакетов, которые могут быть обработаны без превышения условий SLA и для отдельных классов сервисов число запросов от пользователей будет превышать определенный порог. Порог согласно [7] предлагается считать через определенные интервалы времени I как:

$$P = (E * I) / K. \qquad (1)$$

Для обнаружения атаки и ее трафика, пользователей и классы облака можно представить в виде матрицы A, ячейки столбцов которой соответствуют состоянию работы пользователя с определенным классом сервисов облака. Матрица A строится дискретно, в интервал обнаружения. Для обнаружения используется фиксированный порог P. Наличие превышения фиксированного порога P для отдельных классов означает необходимость включения иных методов защиты для них.

3.3. Пример работы

Для примера используется облако, разделенное на 3 класса (основа, инфраструктура и приложения) с 4 пользователями облачных служб, пользователь 1 работает с Cloud OS, пользователь 2 – с PaaS и Cloud OS, пользователь 3 – с DaaS, IaaS и Виртуализация, пользователь 4 – с SaaS и Виртуализация (таблица 1). Совокупная емкость обслуживания каждого класса E=6 запросов в секунду. При этом пользователи 1, 3 и 4 отправляют 1 запрос/сек., а пользователь 2 атакует облако и направляет 2 запроса в сек. к выбранным службам.

В таблице 1 представлена матрица A работы пользователей с классами облака в определенный момент времени I.

Таблица 1

Матрица работы в определенный момент времени I

Классы облака	Пользователь 1	Пользователь 2	Пользователь 3	Пользователь 4
основа	1	0	1	1
инфраструктура	0	1	1	0
приложения	0	1	1	1

Наличие запроса клиента на использование ресурсов определенного класса регистрируются в соответствующей ячейке матрицы и обозначается как 1 (например пользователь 4 работает с основой, не работает с инфраструктурой и работает с приложениями). Если интервал измерения I составляет 2 сек., то: порог $P = (6*2)/3 = 4$, нагрузка на классы облака будет такой:

Таблица 2

Нагрузка на классы облака

Классы облака	Число запросов
основа	3
инфраструктура	5
приложения	6

Число запросов на классы «инфраструктура» и «приложения» превышают порог, таким образом определяется наличие атаки на определенные классы облака и для этих классов активизируется модель защиты N, если она не сработала то используется модель защиты N+1 и так далее. Пример схемы работы многоверсионной модели защиты облака от DDoS-атак представлен на рисунке 2.

5. Гибридная cloud-архитектура с многоверсионной защитой облака от DDoS-атаки

В работе [5] была предложена архитектура гибридного облака с DDoS-щитом распределенной системы хранения, оперативного обновления и предоставления данных о потенциально опасных объектах на основе технологии cloud computing. Предложенное к реализации гибридное облако распределенной системы основано на комбинации частного облака, развернутого в локальном дата-центре, публичного и общественного облака, развернутого на Amazon и развернутой внутри облака интеграции как услуге. Гибридное облако разворачивается на уровнях DaaS, SaaS, PaaS, IaaS, Интеграция как сервис, Cloud OS и Виртуализация.

Для обеспечения защиты облака от DDoS-атак предлагается создать единую точку входа в облако, в которой размещается брандмауэр с моделью защиты DDos-щит, прерывающий запросы пользователей на получение доступа к службам.

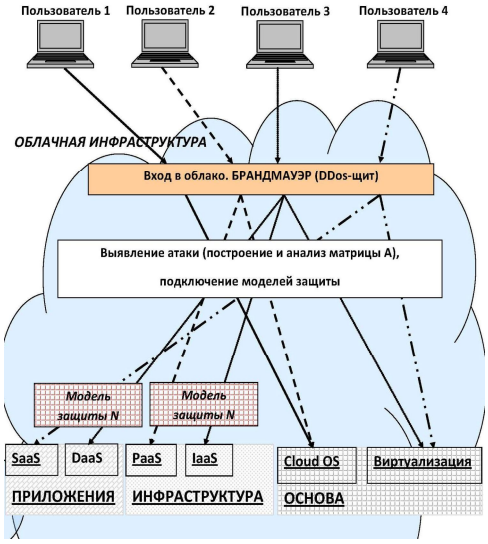

Рис. 2. Пример схемы работы многоверсионной модели защиты облака от DDoS-атак

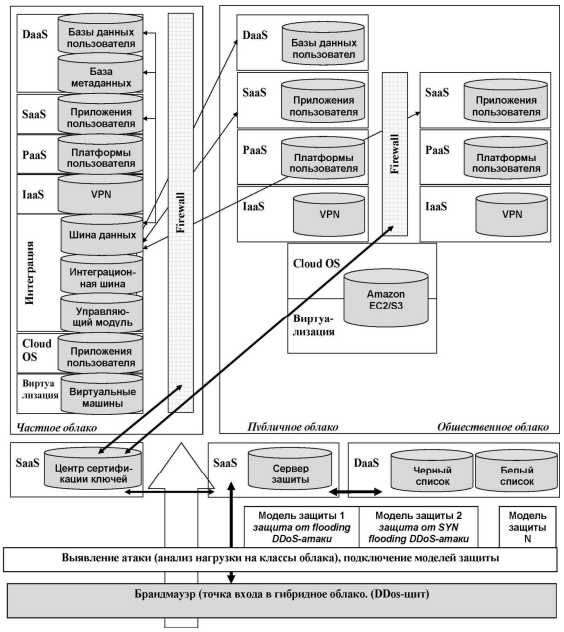

Рис. 3. Архитектура гибридного облака многоверсионной защитой от DDoS-атаки

В случае обнаружения атаки на определенный класс служб облака все запросы на использование ресурсов класса будут обрабатываться другой моделью защиты. Если базовая модель DDoS-щита стала неэффективной то, используется защита от flooding DDoS-атаки, далее – от SYN flooding DDoS-атаки и так далее. Подобная схема должна использоваться параллельно для всех классов служб облака.

Выводы

Неадекватность обслуживания облака при удовлетворении требований SLA возможна прежде всего при DDoS-атаке на облако или провайдера в целом.

Применение многоверсионности в защите облака от DDoS-атак позволить повысить уровень надежности функционирования облачной инфраструктуры и заключается в определении наличия атаки на облако, при этом базовая модель защиты не отражает атаку, определения цели и трафика атаки, и последующего применения другой модели защиты для обработки запросов на использование только атакуемых ресурсов облака, что снизит нагрузку на ресурсы и не будет увеличивать нагрузку на пользователей неатакуемых ресурсов. Дальнейшая работа будет состоять в математическом описании предложенной многоверсной защиты облака от DDoS-атак и построении математической, в частности марковской модели.

Литература

1. Zissis, D. Addressing cloud computing security issues [Text] / D. Zissis, D. Lekkas // Future Generation Computer Systems. – 2012 – №. 28. – P. 583-592.

2. Irfan, G. Distributed Cloud Intrusion Detection Model [Text] / G. Irfan, M. Hussain // International Journal of Advanced Science and Technology. – 2011. – №. 34. – P. 71-81.

3. CBF A Packet Filtering Method for DDoS Attack Defense in Cloud Environment [Text] / Q. Chen, L. Wenmin, D. Wanchun, Y. Shui // Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing. – 2011. – P. 428 – 433.

4. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks [Text] / A. Chonka, Y. Xiang, W. Zhou, A. Bonti // Journal of Network and Computer Applications. – 2010. – № 34. – P. 1097–1107.

5. Меленец, А. Защита Cloud-архитектур от DDoS-атак [Текст] / А. Меленец // Радіоелектронні і комп'ютерні системи. –2013. – № 5(64). – С. 64–69.

6. Технологии web, grid, cloud для гарантоспособных IT-инфраструктур [Текст] : лекционный материал / под ред. В. С. Харченко, А. В. Горбенко ; Министерство образования и науки Украины, НАУ им. Н.Е. Жуковского «ХАИ». – Х. : НАУ им. Н.Е. Жуковского «ХАИ», 2013. – 868 с.

7. Mohamed, D. Defense Against Distributed Denial of Service Attacks in Computer Networks [Text] / D. Mohamed, N. Mohamed // Graduate School of Information Sciences Tohoku University, 2010. – 98 p.

Поступила в редакцию 11.02.2014, рассмотрена на редколлегии 25.03.2014

Рецензент: д-р техн. наук, проф. И. Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

БАГАТОВЕРСІЙНА МОДЕЛЬ ЗАЩИСТУ ХМАРИ ВІД DDOS-АТАК

А. В. Меленець

В статті розглянута схема DDoS-атак, існуючі механізми захисту хмари від DDoS-атак, запропонована багатоверсійна модель захисту хмари від DDoS-атаки. Багатоверсійна модель захисту хмари від DDoS-атаки, що запропонована, складається з визначення наявності атаки на хмару, при цьому базова модель захисту не спроможна відбити атаку, визначення цілі та трафіка атаки, та подальшого застосування іншої моделі захисту для опрацювання запитів на використання ресурсів, що атакуються. В якості базової моделі захисту в брандмауері запропоновано використовувати техніку DDos-щита. Модель передбачає декомпозицію логічної структури хмари на класи. Розроблено приклад архітектури гібридної хмари з багатоверсійною моделлю захисти хмари від DDoS-атаки.

Ключові слова: cloud computing, DDoS-атака, багатоверсійна модель захисту хмари від DDoS-атаки, DDoS-щит, класи хмари.

MULTIVERSION MODEL OF PROTECTION OF THE CLOUD FROM DDOS-ATTACK

A. V. Melenets

The article describes the scheme of DDoS-attacks, existing protection mechanisms clouds from DDoS-attacks, the security model proposed multiversioning clouds from DDoS-attack. The proposed multiversion model of protection of the cloud from DDoS-attack is to determine whether the attack on the cloud, and the basic security model does not reflect the attack, determine goals and attack traffic, and then use another security model to handle requests to use only attacked cloud resources. As a basic model in the firewall protection is offered to use the technique DDos-shield. The model provides the logical structure of clouds decomposition into classes. Developed example of the architecture of the hybrid cloud model to multi- cloud protection from DDoS- attack.

Keywords: cloud computing, DDoS-attack , multiversion model, cloud protection from DDoS-attacks , DDoS-shield, clouds classes.

Меленец Андрей Викторович – заместитель директора – начальник управления ведения государственных реестров, мониторинга и научной политики Государственного департамента страхового фонда документации, Харьков, Украина, e-mail: andrey_melenets@ukr.net.