УДК 004.62

А.В. МЕЛЕНЕЦ

Государственный департамент страхового фонда документации, Харьков, Украина

ЗАЩИТА CLOUD-АРХИТЕКТУР ОТ DDOS-АТАК

В статье рассмотрены схема и виды DDoS-атак, существующие техники защиты облака от DDoS-атак, предложена распределенная архитектура защиты облака от DDoS-атаки. Предложенная архитектура DDoS-щита для защиты облака лишает DDoS-атаку ее автоматичности, использует черный и белый списки, а также графические тесты. Архитектура DDoS-щита состоит из брандмауэра, который является точкой входа в облако и сервера защиты, который использует предложенный метод защиты от DDoS-атаки. Разработан пример архитектуры гибридного облака с DDoS-щитом и центром сертификации ключей.

Ключевые слова: *cloud computing, DDoS-атака, DDoS-щит, защита облака, графический тест, черный и белый списки, легитимный пользователь, распределенная архитектура защиты облака.*

Введение

Обеспечение надежности облачной инфраструктуры является на сегодняшний день основной проблемой для пользователей и провайдеров облачных служб. Кроме отказов облачной инфраструктуры, вызванных ошибками на различных уровнях проектирования и реализации, облака уязвимы к различным атакам, особенно DDoS-атакам. 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. Чтобы обеспечить полную доступность, провайдер может выделять все больше и больше ресурсов непосредственно запросам атаки, что увеличивает количество экземпляров служб, запущенных согласно SLA.

Таким образом, традиционная DDoS-атака может быть рассмотрена и как экономический отказ устойчивости.

В современных работах [6-9] посвященных технологиям защиты облачных инфраструктур, такие авторы как Zissis D., Irfan Gul, Qi Chen, Chonka A. и др. рассматривают техники защиты облаков от наиболее опасных DDoS-атак.

Однако предложенные техники защиты могут эффективно функционировать в комбинации, а методы, которые реализуются лишь в одной целевой машине, неэффективны, для защиты от DDoS-атаки необходим распределенный подход.

В данной статье рассматриваются вопросы построения распределенной архитектуры защиты облака от DDoS-атаки.

1. Отказы облачной инфраструктуры

Отказы облачной инфраструктуры возможно рассматривать как отказы компьютерной системы, при этом отказы классифицируются по таким группам: отказы по общей причине, отказы общего вида, каскадные отказы [1]. Приведенные отказы в облачной инфраструктуре возможны на таких уровнях:

модели развертывания;

сервисы (основа (Cloud OS, Виртуализация), инфраструктура (IaaS, PaaS и т.п.), приложения (SaaS, DaaS и т.п.);

конкретные приложения, платформы и т.п., развернутые в облаке.

Отказы по общей причине для облачной инфраструктуры, в соответствии с [1] можно определить таким образом:

ошибки при развертывании модели облака;

ошибки оператора при работе с облачными службами;

ошибки при проектировании модели облака;

неадекватность обслуживания;

процедурная неадекватность;

воздействия окружающей среды.

Наиболее специфичными для облачной инфраструктуры среди отказов по общей причине являются воздействия окружающей среды и неадекватность обслуживания.

1.1. Воздействия окружающей среды

Воздействие окружающей среды на облачную инфраструктуру возможно опосредовано, в случае природных или техногенных катастроф, которые выведут из строя дата-центр провайдера. В подавляющем большинстве случаев воздействие окружающей среды

не приводит к отказам облачной инфраструктуры, однако были исключения. В январе-феврале 2011 года над Восточным побережьем США прошел шторм, который только в Вашингтоне, округ Колумбия оставил без электроэнергии 1,3 млн. потребителей, при этом отключился сервис Amazon и остановились популярные веб-сайты, такие как Reddit, Quora и Foursquare. Этот пример не является единичным, однако такие отказы не выходили за пределы, установленные SLA. SLA Amazon EC2 составляет 99,95% для мульти-AZ развертывания, это означает, что возможно около 4,5 часов простоев каждый год [2].

1.2. Неадекватность обслуживания

Неадекватность обслуживания облака при удовлетворении требований SLA возможна прежде всего при DDoS-атаке на облако или провайдера в целом. 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, статистика наиболее резонансных DDoS-атак приведена в табл. 1.

Таблица 1

Статистика DDoS-атак

Сервис	Дата неадекватности обслуживания	Основа облака	Продолжительность
Amazon	февраль 2008 года	Amazon EC2/S3	2 час.
Microsoft Azure	март 2008 года	Microsoft	22 час.
Amazon	июль 2008 года	Amazon EC2/S3	3 час.
IMDB.com	июль 2008 года	Amazon EC2/S3	3 час.
FlexiScale	октябрь 2008 года	Flexiant	18 час.
Amazon	октябрь 2008 года	Amazon EC2/S3	27 час.
Google Search	январь 2009 года	Google	0,8 час.
Google Gmail	февраль 2009 года	Google	2,5 час
Google Gmail	март 2009 года	Google	22 час.
Microsoft Hotmail	март 2009 года	Microsoft	5 час.
Google Network	май 2009 года	Google	2 час.
Amazon	июнь 2009 года	Amazon EC2/S3	7 час.
Amazon, Salesforce, Oracle и Juniper	октябрь 2009 года	Amazon EC2/S3 Oracle	3 час.
Bitbucket	октябрь 2009 года	Amazon EC2/S3	19 час.
Microsoft Sidekick	октябрь 2009 года	Microsoft	144 час.
Amazon, Wal-Mart, Gap, Expedia, Salesforce, Linden Labs	декабрь 2009 года	Amazon EC2/S3	5 час.
Paypal API	декабрь 2010 года	Amazon EC2/S3	12 час.

Некоторые примеры таких атак и их последствий. Октябрь 2009 года – веб-сервис Bitbucket, предназначенный для хостинга проектов в области разработки программного обеспечения, столкнулся с многочисленными перебоями в работе на 19 часов [3]. Сбой произошел из-за DDoS-атаки на распределенную вычислительную инфраструктуру Amazon.com, мощности которой арендовал Bitbucket. 16 часов спустя Amazon блокировал вредоносный трафик и функционирование сервиса было восстановлено. Однако атака возобновилась, и Bitbucket на два часа вновь оказался парализован. Декабрь 2009 года – DDoS-атака, в результате которой резко упал уровень обслуживания торговых сайтов на Amazon, Wal-Mart, Gap, туристического сайта Expedia, Salesforce.com и Linden Labs. Продолжительность проблем составила 1 час. В апреле 2009 года DDoS-атака была направлена на Amazon, Salesforce, Oracle и Juniper в течение нескольких часов [4]. Декабрь 2010 года - DDoS-атака на Paypal API, в результате которой на время выведена из строя платёжная инфраструктура Paypal [5]. В процессе двух DDoS-атак, которые были проведены 6 и 9 июля 2008 г. трафик Amazon.com достигал 600-1000% от нормального значения в течение нескольких часов.

2. Защита облака от DDoS-атак

2.1. Схема и виды DDoS-атак

Технически 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. Ситуация усугубляется тем, что пользователи компьютеров, с которых направляются ложные запросы («зомби»), могут даже не подозревать о том, что их компьютеры используется троянами. Чаще всего злоумышленники при проведении DDoS-атак используют трехуровневую

архитектуру, которую называют «кластер DDoS». Общая схема DDoS атаки представлена на рис. 1.

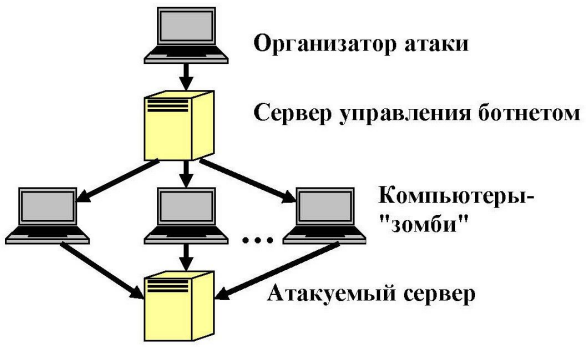

Рис. 1. Схема DDoS-атаки

Проследить такую структуру в обратном направлении и выявить адрес узла, организовавшего атаку, практически невозможно. Максимум того, что может атакуемый, это определить адреса зомби, в лучшем случае – центр управления ботнетом, но обычно это зараженные компьютеры и владельцы не подозревают о своем участии в атаке.

На сегодняшний день существуют следующие виды DDoS-атак:

UDP — отправка на адрес системы-мишени множества пакетов UDP (User Datagram Protocol). Этот метод в настоящее время считается наименее опасным. Программы, использующие этот тип атаки легко обнаруживаются, так как при обмене главного контроллера и агентов используются нешифрованные протоколы TCP и UDP.

TCP — отправка на адрес мишени множества TCP-пакетов, что также приводит к «связыванию» сетевых ресурсов.

TCP SYN — посылка большого количества запросов на инициализацию TCP-соединений с узлом-мишенью, которому, в результате, приходится расходовать все свои ресурсы на то, чтобы отслеживать эти частично открытые соединения.

Smurf-атака — пинг-запросы ICMP (Internet Control Message Protocol) по адресу направленной широковещательной рассылки с использованием в пакетах этого запроса фальшивый адрес источника в результате оказывается мишенью атаки.

ICMP — атака, аналогичная Smurf, но без использования рассылки.

Наиболее опасными являются программы, которые используют одновременно несколько видов описанных атак. Они получили название TFN и TFN2K и требуют от хакера высокого уровня подготовки.

Как вывод следует отметить, что основными объединяющими все виды DDoS-атак элементами является большое количество зараженных компьютеров, автоматически рассылающих запросы и ничего не подозревающие пользователи.

2.1. Механизмы защиты

В облаках используются различные механизмы защиты, как простые, например, черный и белый списки так сложные модели: система обнаружения вторжения, контроль виртуальной машины, и другие.

Распределенная модель обнаружения вторжения в облако [7].

Эта модель использует датчики, чтобы определить и контролировать сетевой трафик, а также проверку на нелегитимные пакеты. Работа системы состоит из трех фаз:

обработка и выявление подозрений,

анализ и обработка,

сообщение.

CBF (пакетный метод фильтрации) [8]. В этой модели есть два периода: атаки и неатаки. В период неатаки генерируется нормальный профиль, в течение периода атаки CBF прекращает генерировать профиль и извлекает атрибуты из пакета, проверяет их легитимность и тогда решает отбросить пакет или разрешить.

Контроль виртуальной машины (атака с VMM). VMM работает в изолированной среде и если доступные ресурсы являются ниже заранее установленного порога то VMM подозревает существование в DDoS-атаки. После выявления подозрения на атаку происходит дублирование гостевой операционной системы и приложения в изолированной среде.

Защита облака от HTTP-DoS и XML-DoS атак [9]. Для защиты от XML-DoS атак используется архитектура, которая включает в себя механизм детерминистской пакетной маркировки и сервис-ориентированной обратной трассировки. Обратная трассировка идентифицирует источник атаки и фильтрует его. Защита отслеживает метки, входящие пакеты и фильтрует пакеты. Облачное средство защиты является обучаемой нейронной сетью.

Выводы из статей [6-9]:

существующие методы не способны на высоком уровне обеспечить защиту от DDoS-атаки;

защитные механизмы, которые реализуются только в одной целевой машине, не эффективны, необходим распределенный подход;

для облачной среды хорошо подходят методы защиты по требованию;

механизм защиты, основанный на доверии, является плохим выбором;

отсутствие принятых стандартов приводит к тому, что поставщики услуг используют свои собственные механизмы безопасности;

наиболее эффективными являются средства защиты, основанные на работе с идентификационными данными пользователя;

необходимы более интеллектуальные методы текущего контроля трафика.

3. Распределенная архитектура защиты облака от DDoS-атаки

В работе [11] приведена схема и порядок действия при заражении и последующем использовании ресурсов зараженных компьютеров для проведения DDoS-атак. 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 ее автоматичность, т.е. автоматическое, без уведомления пользователя, использование ресурсов множества зараженных компьютеров. Таким образом, включив в процесс работы с облаком специфические возможности человека возможно не только защитить облако от множества запросов, но и обратить внимание владельца зараженного компьютера на наличие проблем. Наиболее простым 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 IP адресов - DDoS-щит (рис. 2).

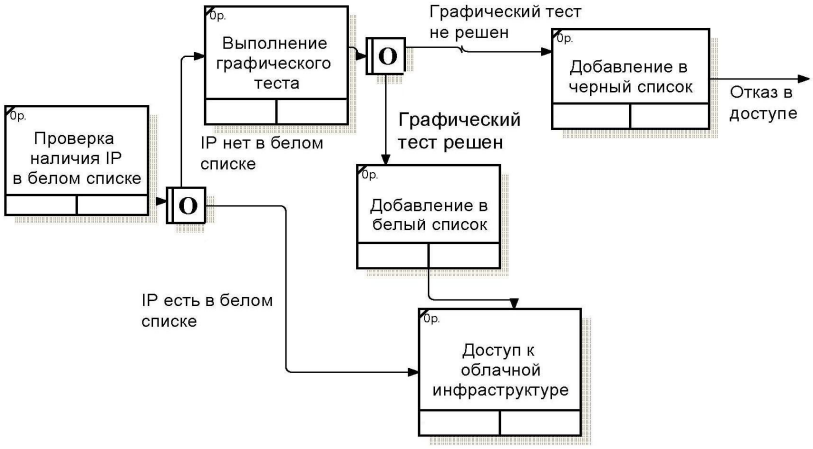

Рис. 2. IDEF-модель DDoS-щита

Однако следует учесть, что использование графических тестов занимает определенное время, что доставляет неудобство пользователям, в том числе проверенным, поэтому после проверки графическим тестом можно использовать простую схему черного и белого списка. 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.

4. DDoS-щит

Архитектура DDoS-щита приведена на рис. 3.

Описание работы с клиентом:

1. Для получения доступа к облачной службе пользовательский запрос клиента прерывается брандмауэром.

2. Брандмауэр перенаправляет запрос к серверу защиты, который является облачной службой по требованию.

3. Сервер защиты через брандмауэр отправляет клиенту задачу (графический тест) для решения.

4. Пользователь решает задачу и возвращает результат решения серверу защиты.

5. Сервер защиты проверяет результат решения и при верном решении отправляет подтверждение брандмауэру, при неверном решении – отправляет отказ в подтверждении брандмауэру.

6. Брандмауэр добавляет IP клиента к своему белому списку либо IP атакующего клиента к своему черному списку.

7. Брандмауэр перенаправляет пользователя, на получение доступа к "облачным" службам либо при атаке отбрасывает запрос.

5. Cloud-архитектура с DDoS-щитом

В [10] была предложена распределенная система 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. Для обеспечения защиты облака от DDoS-атак предлагается создать единую точку входа в облако, в которой размещается брандмауэр, прерывающий запросы пользователей на получение доступа к службам. Используя черный и белый списки, а также графические тесты брандмауэр совместно с сервером защиты отрабатывает запросы на доступ к облачным службам (рис. 4).

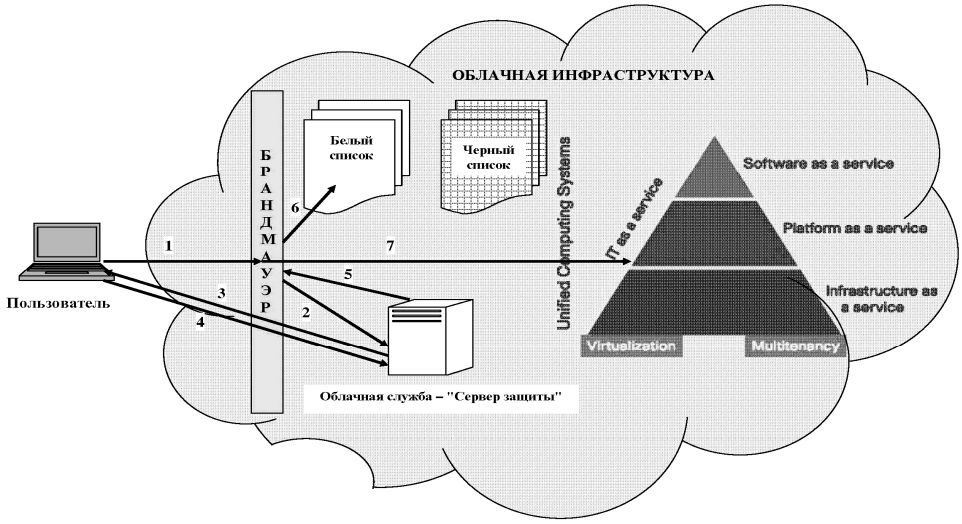

Рис. 3. Архитектура DDoS-щита

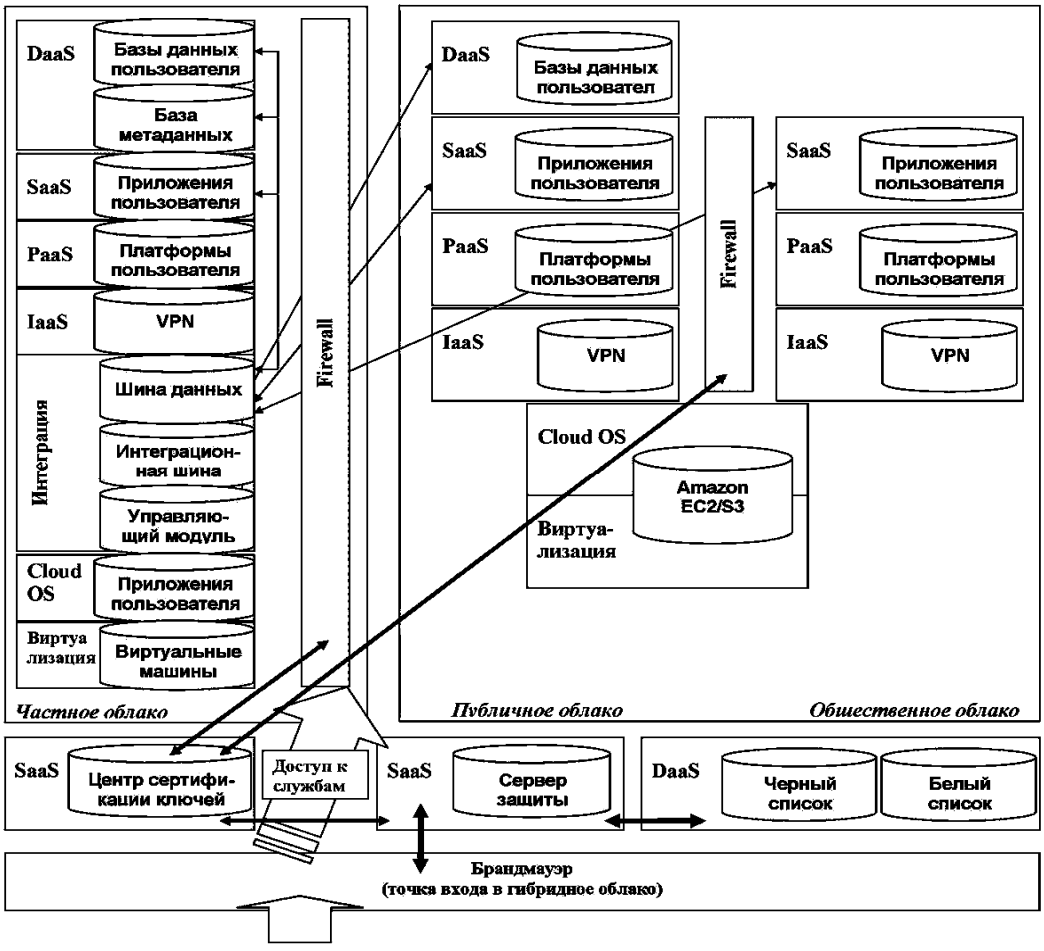

Рис. 4. Архитектура гибридного облака с DDoS-щитом

В такой архитектуре 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 службе центра сертификации ключей и соответственно возможность доступа к службам частного и общественного облаков.

Выводы

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

целом. В статье рассмотрены существующие техники защиты от DDoS-атак на облако и предложена общая распределенная архитектура защиты облака от DDoS-атаки. На основе этой общей архитектуры построена архитектура гибридного облака с DDoS-щитом и центром сертификации ключей. Дальнейшая работа в направлении защиты облаков состоит в разработке метода оценки надежности облаков.

Литература

1. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения [Текст] / В. Харченко, Е. Брежнев, В. Твердохлебов и др.. – Х.: ХАІ, 2011. – 640 с.

2. Theodoropoulos, T. Failing to Plan is Planning to Fail [Электронный ресурс] / T. Theodoropoulos. – Режим доступа: http://blog. acrowire.com/cloud-computing/ failing-to-plan-is-planning-to-fail. – 23.04.2011 г.

3. DDoS-атака вывела из строя распределенную сеть Amazon [Электронный ресурс]. – Режим доступа: http://www.xakep.ru/post/49669/ default.asp/. – 06.10.2009 г.

4. Modine, A. DDoS attack scrooges Amazon and others UltraDNS California facilities targeted [Электронный ресурс] / A. Modine. – Режим доступа: http://www.theregister.co.uk/2009/12/24/DDoS_attack_ ultradns_december_09. – 24.12.2009 г.

5. Началась DDoS-атака на Paypal API [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/109688/. – 09.12.2009 г.

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

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

8. 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.

9. 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.

10. Melenets, A. The State Corporate Cloud Computing- Based Network for Registration of Potentially Dangerous Objects [Text] / A. Melenets // Information & Security: An International Journal. – Sofia, Bulgaria. – 2012. – Vol. 28, Numb. 1 & 2. – P. 52 – 62.

11. Arbor White Paper: Anatomy of a Botnet [Электронный ресурс]. – Режим доступа: http://www. arbornetworks.com. – 19.09.2012 г.

Поступила в редакцию 28.02.2013, рассмотрена на редколлегии 20.03.2013

Рецензент: д-р техн. наук, проф., зав. каф. В.А. Краснобаев, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава, Украина.

ЗАХИСТ CLOUD-АРХІТЕКТУР ВІД DDOS-АТАК

А.В. Меленець

В статті розглянуті схема та види DDoS-атак, існуючі техніки захисту хмари від DDoS-атак; запропонована розподілена архітектура захисту хмари від DDoS-атаки. Запропонована архітектура DDoS-щита для захисту хмари залишає DDoS-атаку без її автоматичності, використовує чорний та білі списки, а також графічні тести. Архітектура DDoS-щита складається із брандмауера, який є крапкою входу у хмару та серверу захисту, який використовує запропонований метод захисту від DDoS-атаки. Розроблено приклад архітектури гібридної хмари с DDoS-щитом та центром сертифікації ключів.

Ключові слова: cloud computing, DDoS-атака, DDoS-щит, захист хмари, графічний тест, чорний та білий списки, легітимний користувач, розподілена архітектура захисту хмари.

PROTECTION OF CLOUD-ARCHITECTURE FROM DDOS-ATTACKS

A.V. Melenets

The article describes it's the scheme and the types of DDoS-attacks, and the existing technology protection of clouds from DDoS-attacks, and offered the distributed architecture of the protection of the clouds from DDoS-attacks. It's proposed architecture DDoS-shield to protect the clouds deprives the DDoS-attack her automaticity, using a black and white lists, and graphics tests. Architecture DDoS-shield consists of a firewall, which is the entry point into the cloud, and of the security server, which uses the method of protection against DDoS-attacks. It's designed the architecture of the hybrid cloud with DDoS-shield and center for certification of keys.

Keywords: cloud computing, DDoS-attack, DDoS-shield, cloud protection, graphics test, black and white lists, legitimate user, distributed architecture of protection of a cloud.

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.