ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ № 4(8), 2011, с. 61–70

УДК 004.042

А. А. Кондратьев, И. П. Тищенко, В. П. Фраленко

# Разработка распределенной системы защиты облачных вычислений

Аннотация. Рассмотрены вопросы построения исследовательского стенда для организации сетевых атак на системы облачных вычислений. Предложена концепция распределенной системы защиты с использованием перспективного модуля мониторинга аномальной сетевой активности, учитывающая основные направления возможных атак.

*Ключевые слова и фразы:* стенд, сетевая атака, облачные вычисления, концепция защиты, безопасность.

## Введение

Облачные вычисления (англ. cloud computing) — технология распределенной обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Предоставление пользователю услуг как Интернет-сервис является ключевым, причем доступ к сервису может осуществляться также и через обычную локальную сеть с использованием веб-технологий. Основой для создания и быстрого развития облачных вычислительных систем послужили крупные интернет сервисы, такие как Google, Amazon и др., а также технический прогресс: развитие многоядерных процессоров, увеличение емкостей носителей информации, развитие технологии многопоточного программирования (гибкое распределение вычислительных мощностей облаков), развитие технологий виртуализации, снижение стоимости хранения информации (безграничное увеличение объемов хранимой информации для «облаков»). Перечисленные факторы привели к существенному повышению конкурентоспособности облачных вычислений в сфере информационных технологий. Несмотря на имеющийся прогресс в создании программных средств информационной безопасности, необходимо отметить насущную необходимость в защите облачных вычислений, имеющих ряд

специфических особенностей по сравнению с обычными вычислениями. Вопрос требует тщательной проработки особенностей облачных вычислений с целью выявления требований к системе их информационной защиты. Данная работа является продолжением исследований, начатых в [1–4].

## 1. Состав исследовательского стенда

В состав разработанного исследовательского стенда входят:

(1) Кластерное вычислительное устройство семейства «СКИФ» с не менее чем двумя узлами, имеющее сетевое оборудование и программное обеспечение, необходимое для организации облачных вычислений (рис. 1, где Frontend — управляющая машина, HV — гипервизор, VM — виртуальная машина, а Node 1, Node 2, ... — вычислительные узлы).
(2) Тестовая программа, проводящая некоторые облачные вычисления на КВУ и подвергающаяся атакам. В качестве тестовой программы использовалась программа распределенных вычислений, построенная на базе параллельной программной системы «ППС ИНС», разработанная в ИПС им. А.К.Айламазяна РАН [5].
(3) Сеть из персональных компьютеров, подключенных к сети с установленным программным обеспечением (генератором) для организации сетевых атак видов «сканирование портов» и DDoS.

В качестве основного средства защиты, устанавливаемого в критических узлах, предполагается IDS Snort с подключенной обновленной версией модуля мониторинга аномальной сетевой активности на основе искусственных нейронных сетей «Эгида-НС» [6], который включает в себя следующие компоненты:

- нейросетевые анализаторы сетевого трафика,
- анализаторы на основе сравнения долгосрочных и краткосрочных сетевых профилей,
- анализаторы на основе полиномиального расстояния Евклида-Махаланобиса,
- анализаторы на основе метода опорных компонент.

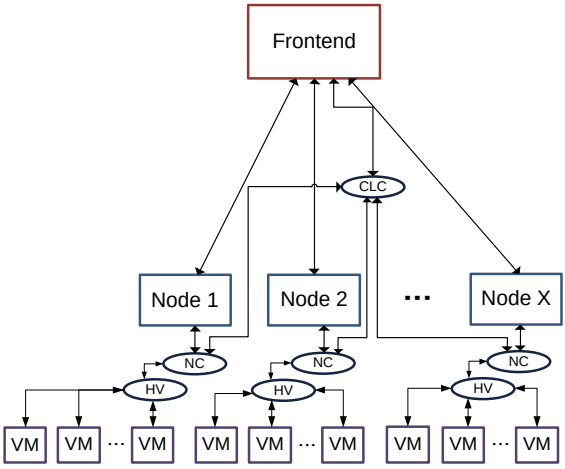


Рис. 1. Архитектура типовой системы облачных вычислений

## 2. Создание виртуальных машин и организация сетевого обмена

Для организации работы виртуальных машин была выбрана система OpenVZ [7]. OpenVZ — это реализация технологии виртуализации на уровне операционной системы, которая базируется на ядре Linux. В качестве образов для виртуальных машин использовался заранее подготовленный вариант CentOS 6 x86 с установленными необходимыми версиями библиотек для IDS. В гостевой системе настроен один сетевой интерфейс для взаимодействия с внешней сетью и один виртуальный — для организации доступа к виртуальным машинам. Каждой виртуальной машине определен IP-адрес. Все виртуальные машины находятся в одном адресном пространстве. Для обеспечения доступа к сети из виртуальных машин в системе включена переадресация. Для обеспечения доступа к виртуальным машинам по ssh извне организовано перенаправление портов, начиная с 23, на виртуальные машины (23, 24 и 25). Примерная схема отображена на рис. 2. В разработанной сетевой модели есть доступ к вычислительному узлу, а также организован доступ ко всем виртуальным машинам. Это не ограничивает использование сети внутри машины,

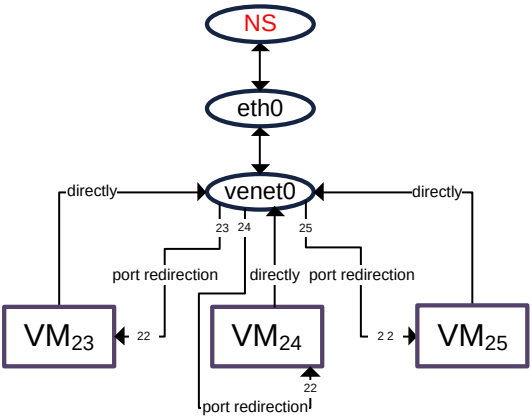


Рис. 2. Схема функционирования доступа к виртуальным машинам

но и не позволяет получить доступ к виртуальной машине извне иначе как через один, заранее определенный порт, что повышает защищенность от сетевых атак.

## 3. Возможные направления сетевых атак

Рассмотрим далее возможные направления сетевых атак:

(1) Атаки на управляющую машину, имеющую выход в интернет:
   (a) атаки извне удаленным злоумышленником;
   (b) атаки изнутри злоумышленником, имеющим доступ к запущенным виртуальным машинам.

(2) Атака на виртуальную машину (несколько машин):
   (a) с другой виртуальной машины (нескольких машин) облака
      (i) в пределах одного вычислительного узла;
      (ii) на другом вычислительном узле по отношению к атакующим машинам (атака возможна при определенных настройках внутренней сети облака).
   (b) извне при наличии доступа к виртуальным машинам;

(3) Атака на вычислительные узлы (как на сами узлы, так и на имеющееся на нем программное обеспечение - гипервизор, контроллер узла и виртуальные машины в случае видимости вычислительных узлов):
   (a) атаки извне удаленным злоумышленником;
   (b) атака из виртуальной машины (либо на этом же вычислительном узле, либо с соседнего).

Таким образом, методика обнаружения и предотвращения сетевых атак на системы облачных вычислений должна учитывать указанные потенциальные источники сетевых атак. Специфика защиты обусловлена прежде всего выбранной системой для организации облачных вычислений, а так же операционной системой и гипервизором. Для защиты от атак класса (1) на управляющей машине необходимо установить компоненты защиты (IDS) как от внешних, так и внутренних атак. Для определения и предотвращения распределенных атак классов (2.a) требуется взаимодействие между IDS на различных узлах (виртуальных машинах). Атаки класса (2.a.i) можно определить и остановить различными способами:

- установить IDS на сами виртуальные машины;
- установить IDS на узлы кластера для защиты соединения типа мост (bridge), через которое производятся сетевые обмены работающих виртуальных машин;
- установить IDS на узлы кластера, организовав доступ к необходимым лог-файлам виртуальных машин;
- установить IDS на узлы кластера и разместить в виртуальных машинах модуль, который будет производить сброс информации о сетевых пакетах IDS на узле (данный вариант имеет место, если по каким-то причинам нет возможности анализировать сетевой трафик моста или обмен между виртуальными машинами производится не через мост).

Последний вариант требует доступа из виртуальной машины к узлу кластера, что повышает уровень риска и расширяет спектр возможных атак и целей для них. Атаки класса (2.a.ii) можно отсечь либо упомянутым способом, либо запретить общаться виртуальным машинам на разных вычислительных узлах с помощью соответствующих сетевых настроек. Атаки класса (2.b) можно выявлять как на управляющей машине, так и на узлах кластера, но предотвращать лучше

на управляющем узле кластера путем оповещения IDS, находящейся на нем. Атаки класса (3.a) можно выявлять как на управляющей машине, так и на IDS, установленной непосредственно на вычислительных узлах. Атаки класса (3.b) отражаются только защитой на уровне соединений типа мост, они возможны только в случае видимости узлов кластера для виртуальных машин. Наилучшей защитой будет отделение адресного пространства узлов кластера от виртуальных машин. Указанные места внедрения системы защиты показаны на рис. 3, где NS — сетевой сенсор, AM — модули анализа и реакции, CM — управление компонентами и SM — модуль хранения.

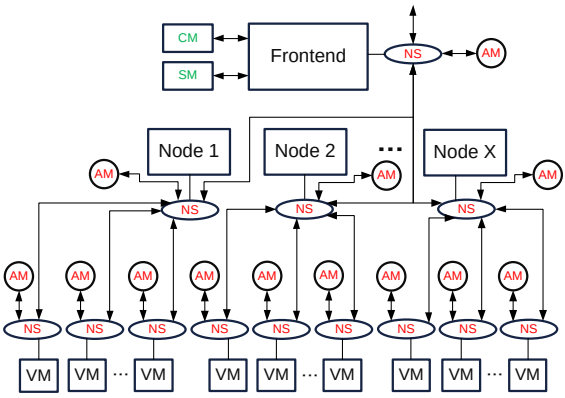


Рис. 3. Схема размещения подсистем сетевой защиты

## 4. Эксперименты по обнаружению атак на системы облачных вычислений

Для определения эффективности предложенной методики обнаружения сетевых атак на системы облачных вычислений был проведен ряд сетевых атак на экспериментальный стенд. Всего было проведено шесть сетевых атак, направленных на нарушение информационной безопасности как управляющей машины (УМ) облака, так виртуальных машин (ВМ) в ее составе. Основным направлением (способом) воздействия являлось сканирование портов, для чего использовалась утилита nmap версии 5.21. Частота обращения к портам в

случае атак внутри облака была ограничена с помощью параметра max-rate до 4000 в секунду. Данное ограничение вызвано снижением эффективности анализатора трафика при большей частоте появления пакетов, что потенциально может приводить к неправильной интерпретации ситуации или к потере данных. Дополнительно была проведена атака типа DDoS на 139-ый сетевой порт с помощью программы TCP/IP DOS Attacker. Управляющей машине был присвоен приватный IP-адрес 192.168.71.88 и внутренний IP-адрес, доступный для виртуальных машин — 10.0.0.1, которым были присвоены адреса 10.0.0.2, 10.0.0.3 и 10.0.0.4 соответственно.

**Атака из внешнего мира на УМ**

Сканирование портов управляющей машины проводилось с компьютера, расположенного вне защитного периметра. Были выполнены следующие команды:

nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.71.88,

nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.71.88.

В результате 1653 пакета было распознано как норма, к сканированию портов отнесено 66448 пакетов, не распознан 281 пакет. К атаке типа DDoS ни один из сетевых пакетов отнесен не был. Производился мониторинг интерфейса eth0.

**Атака с УМ на ВМ**

Сканирование портов одной из виртуальных машин проводилось с управляющей машины. Были выполнены следующие команды:

nmap -sT -T4 -v -P0 10.0.0.2 --max-rate 4000,

nmap -sT -p 1-65535 -T4 -v -P0 10.0.0.2 --max-rate 4000.

В результате 70 пакетов было распознано как норма, к сканированию портов отнесено 66213 пакетов, не распознано 4 пакета. К атаке типа DDoS ни один из сетевых пакетов отнесен не был. Производился мониторинг интерфейса venet0.

**Атаки с ВМ на УМ**

Сканирование портов управляющей машины (сетевая атака по IP-адресу 192.168.71.88) было произведено с одной из виртуальных машин. Были выполнены следующие команды:

nmap -sT -T4 -v -P0 192.168.71.88 --max-rate 4000,

nmap -sT -p 1-65535 -T4 -v -P0 192.168.71.88 --max-rate 4000.

В результате 157 пакетов было распознано как норма, к сканированию портов отнесено 62601 пакетов, не распознано 14 пакетов.

К атаке типа DDoS ни один из сетевых пакетов отнесен не был. Производился мониторинг интерфейса venet0.

Сканирование портов управляющей машины (атака на IP-адрес 10.0.0.1) было произведено с одной из виртуальных машин. Были выполнены следующие команды:

nmap -sT -T4 -v -P0 10.0.0.1 --max-rate 4000,

nmap -sT -p 1-65535 -T4 -v -P0 10.0.0.1 --max-rate 4000.

В результате 199 пакетов было распознано как норма, к сканированию портов отнесено 124068 пакетов, к неизвестным атакам отнесены 383 пакета, не распознано 2208 пакетов. К атаке типа DDoS ни один из сетевых пакетов отнесен не был. Производился мониторинг интерфейса venet0.

### Атака с ВМ на ВМ

На одной из виртуальных машин было выполнено сканирование портов другой виртуальной машины. Были выполнены следующие команды:

nmap -sT -T4 -v -P0 10.0.0.2 --max-rate 4000,

nmap -sT -p 1-65535 -T4 -v -P0 10.0.0.2 --max-rate 4000.

В результате 90 пакетов было распознано как норма, к сканированию портов отнесено 66461 пакетов, не распознано 4 пакета. К атаке типа DDoS ни один из сетевых пакетов отнесен не был. Производился мониторинг интерфейса venet0.

### Атака типа DDoS на УМ

Графический интерфейс использующегося для распределенных сетевых атак программного средства приведен на рис 4. Для участия в

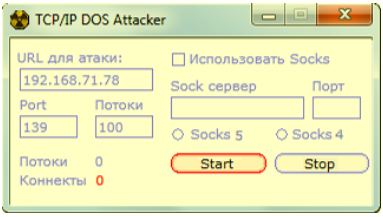


Рис. 4. Интерфейс программы TCP/IP DOS Attacker

атаке на 139-ый порт защищаемой облачной системы была использована сеть из 10 компьютеров. В результате мониторинга интерфейса

eth0 было выявлено 570 пакетов, отнесенных к норме, 48665 к DDoS и нераспознано 190 пакетов.

## 5. Заключение

Результаты, полученные в ходе экспериментов, доказывают правильность размещения сетевых сенсоров и эффективность предложенной модели защиты системы облачных вычислений. В то же время эксперимент выявил недостаточную эффективность указанных сенсоров в плане применения их для анализа трафика между виртуальными машинами в пределах одного узла (по причине отсутствия сетевых задержек внутри облака). Это говорит о необходимости снижения числа одновременно отслеживаемых сетевых сессий. Исследования проводятся в рамках работ по Государственному контракту № 07.514.11.4048 по теме «Разработка интеллектуальных методов автоматизированного обнаружения и предотвращения распределенных сетевых атак и их реализация в современных системах облачных вычислений» (шифр заявки «2011–1.4–514–017–004»).

## Список литературы

[1] Емельянова Ю. Г., Талалаев А. А., Тищенко И. П., Фраленко В. П. *Нейросетевая технология обнаружения сетевых атак на информационные ресурсы* // Программные системы: теория и приложения, 2011. **2**, № 3(7), с. 3–15, URL: http://psta.psiras.ru/read/psta2011_3_3-15.pdf ↑[]

[2] Талалаев А. А., Тищенко И. П., Хачумов В. М., Фраленко В. П. *Разработка нейросетевого модуля мониторинга аномальной сетевой активности* // Нейрокомпьютеры: разработка и применение, 2011, № 7, с. 32–38 ↑

[3] Фраленко В. П. *Нейросетевая технология обнаружения сетевых атак на информационные ресурсы* // III Всероссийская научно-техническая конференция «Актуальные проблемы ракетно-космического приборостроения и информационных технологий». — М. : Изд-во Радиотехника, 2011 ISBN 978–5–88070–299–2, с. 479–488 ↑

[4] Емельянова Ю. Г., Фраленко В. П. *Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления* // Программные системы: теория и приложения, 2011. **2**, № 4(8), с. 17–31, URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf ↑[]

[5] Свидетельство о государственной регистрации программы для ЭВМ №2010610208, Программный комплекс «ППС ИНС». ↑2

[6] Свидетельство о государственной регистрации программы для ЭВМ №2011611277, Модуль мониторинга аномальной сетевой активности на основе искусственных нейронных сетей — «Эгида-НС». ↑1

[7] OpenVZ Wiki, URL:
http://wiki.openvz.org/Main_Page. ↑2

A. A. Kondratyev, I. P. Tishchenko, V. P. Fralenko. *Development of a distributed system security for cloud computing.*

Abstract. The problems of a research stand for network-based attacks on cloud systems organization constructing are disclosed. The concept of a distributed protection system using long-term monitoring module of abnormal network activity takes into account the main lines of attack suggested.

*Key Words and Phrases:* stand, network attack, cloud computing, protection concept, security.

*Образец ссылки на статью:*

А. А. Кондратьев, И. П. Тищенко, В. П. Фраленко. *Разработка распределенной системы защиты облачных вычислений* // Программные системы: теория и приложения : электрон. научн. журн. 2011. № 4(8), с. 61–70. URL: http://psta.psiras.ru/read/psta2011_4_61-70.pdf