Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений

В.С. Заборовский, А.А. Лукашин, С.В. Купреенко, В.А. Мулюха

Санкт-Петербургский государственный политехнический университет

В статье представлена модель разграничения доступа на основе контроля виртуальных соединений. Предложена идея осуществлять обработку виртуальных соединений при помощи скрытой фильтрации. Отмечен новый уровень сложности задач защиты информации при обеспечении информационной безопасности в распределенных виртуализированных вычислительных средах. Рассмотрена архитектура разработанной защищенной гетерогенной распределенной вычислительной среды для решения научно-технических задач. Предложено использование специализированных межсетевых экранов для разграничения доступа между вычислительными ресурсами, как в рамках гипервизора, так и в рамках вычислительной среды в целом.

1. Введение

Виртуализация распределенных вычислительных ресурсов и формирование гетерогенных сред виртуальных вычислительных машин является перспективным направлением развития информационных технологий. В настоящее время различные компоненты данного направления принято объединять термином «облачные вычисления» (cloud computing), которые развиваются как технология, предоставляющая вычислительную услугу в виде сервиса. Обеспечение информационной безопасности (ИБ) таких вычислительных сред является важнейшей задачей. В статье вводится понятие виртуального соединения как эмерджентной сущности, на основе анализа которой осуществляется разграничение доступа. Сетевой трафик рассматривается как совокупность виртуальных соединений. Благодаря тому, что распределенная виртуализированная среда предоставляет гетерогенные вычислительные ресурсы, целесообразно использовать их для обеспечения её информационной безопасности. Так как виртуальные соединения функционируют независимо друг от друга, можно организовать параллельную обработку сетевого трафика при помощи организации «домена безопасности», функционирующего в рамках гипервизора и использующего то количество ресурсов (ядра, память), которое требуется для решения текущих задач ИБ.

2. Специфика обеспечения ИБ в виртуализированных средах

На сегодняшний день многие компании переводят вычислительные ресурсы в виртуальную инфраструктуру, в том числе и ведущие университеты России, используя для этого как открытые системы (Eucalyptus, OpenNebula), так и коммерческие решения (VmWare, Citrix, IBM). В связи с этим, остро встает проблема обеспечения информационной безопасности в виртуальных вычислительных системах такого рода [1]. Такая виртуальная среда обладает определенными специфическими особенностями, хотя многие ее характеристики аналогичны тем, которые встречаются в сетях распределенных вычислительных ресурсов и ГРИД приложениях. Среди важных отличий можно выделить следующие:

1. Обработка информации происходит в виртуальных машинах, которые находятся под полным контролем гипервизора, способного контролировать все данные, обрабатываемые виртуальными вычислительными ресурсами;
2. Средства управления виртуальной инфраструктурой (например, Eucalyptus) осуществляют распределение нагрузки между гипервизорами и являются новой сущностью в информационной среде, требующей защиты;

3. Традиционные средства защиты информации, такие как программно-аппаратные межсетевые экраны не могут контролировать трафик внутри узла виртуализации, таким образом, сетевое взаимодействие между виртуальными машинами в рамках одного гипервизора оказывается вне контроля;
4. В виртуальной среде в качестве устройств хранения данных выступают файлы, которые размещаются в сетевых хранилищах, а не аппаратные жесткие диски;
5. При миграции виртуальных машин между гипервизорами возникает передача фрагментов оперативной памяти, которая может содержать конфиденциальную информацию.

Таким образом, благодаря вышеперечисленным особенностям, возникают новые угрозы информационной безопасности, среди которых:

1. Атака на средства управления виртуальными машинами, контроллеры вычислительной среды (контроллер облака), кластера и на хранилище данных, на котором располагаются виртуальные образы машин и пользовательские данные;
2. Неавторизованный доступ к узлу виртуализации;
3. Использование виртуальной сети для передачи данных, не предусмотренных политикой информационной безопасности.

Важной особенностью виртуальной инфраструктуры является то, что атака или неавторизованный доступ могут быть произведены из виртуальной сети, где отсутствуют такие устройства как коммутаторы, аппаратные межсетевые экраны и физические линии связи, что существенно затрудняет применение существующих методов и средств защиты информации в компьютерных сетях и ГРИД системах.

Распределенные и виртуальные вычислительные среды в настоящее время не имеют эффективных средств защиты информации. Одна из проблем заключается в отсутствии межсетевых экранов, способных функционировать в среде виртуальных машин так же эффективно, как существующие на рынке программно-аппаратные средства защиты информационных ресурсов и отражения компьютерных атак. Отсутствие межсетевых экранов, сертифицированных по требованиям РД ФСТЭК, сдерживает применение новых технологий облачных вычислений в государственных учреждениях, научных и образовательных центрах [2]. Для ряда решений, например, свободно распространяемой и открытой облачной среды Eucalyptus, построенной на гипервизорах XEN или KVM, отсутствуют эффективные решения по защите виртуальных машин, несмотря на быстро растущую популярность данной среды, которая обеспечивается благодаря совместимости с интерфейсами продуктов от компании Amazon (Amazon EC2, Amazon S3).

3. Разграничение доступа как задача обработки виртуальных соединений

Виртуального соединение (ВС) [3] **–** это любой логически упорядоченный обмен сообщениями между узлами сети. Компьютерная сеть – это совокупность виртуальных соединений. Виртуальные соединения классифицируются на два уровня – технологические виртуальные соединения (ТВС) и информационные виртуальные соединения (ИВС) (рис. 1). Для реализации политики разграничения доступа правила фильтрации, которые могут быть заданы для различных уровней описания потоков данных, основанных на полях и заголовках канальных, транспортных и прикладных протоколов декомпозируются в форму ИВС и ТВС. В терминах разграничения доступа модель ТВС можно определить как поток пакетов, формируемый сетевыми приложениями в рамках информационного взаимодействия. Модель ТВС представлена в виде потенциально счетного подмножества декартова произведения множества пакетов P и временных меток T:

$$TBC = \{ p_{ti} \}, i = \overline{1, N}, N \in [1, \infty) \subset P \times T .$$

Представленная модель характеризуется конечным набором параметров, характеризующих субъект и объект доступа, а также действие в форме потока пакетов между ними в рамках межсетевого взаимодействия. Параметрами модели являются идентификаторы субъекта и объекта, такие как адреса, порты, и другие характеристики сетевых протоколов. Для оперативной классификации трафика, наряду с моделью ТВС, используется модель ИВС для описания взаимо-

действие между объектом и субъектом на уровне прикладных сервисов. Модель ИВС представляет собой совокупность ТВС, число и характеристики которой определяются декартовым произведением информационных моделей взаимодействия (ИМД), субъекта (ИМС) и объекта (ИМО) доступа:

$$ИВС = \{ТВС_i\}, i = \overline{1, N} \subset (ИМС \times ИМД \times ИМО).$$

Представленная формализация позволяет представить ИМС доступа как конечное подмножество, объем которого определяется на основе описания разрешенных субъектов межсетевого взаимодействия в рамках заданной политики разграничения доступа. ИМО характеризуется конечным подмножеством информационно-сетевых ресурсов, доступ к которым разрешен в соответствии с политикой РД. ИМД характеризует операции, совершаемые субъектом в рамках ИМО.

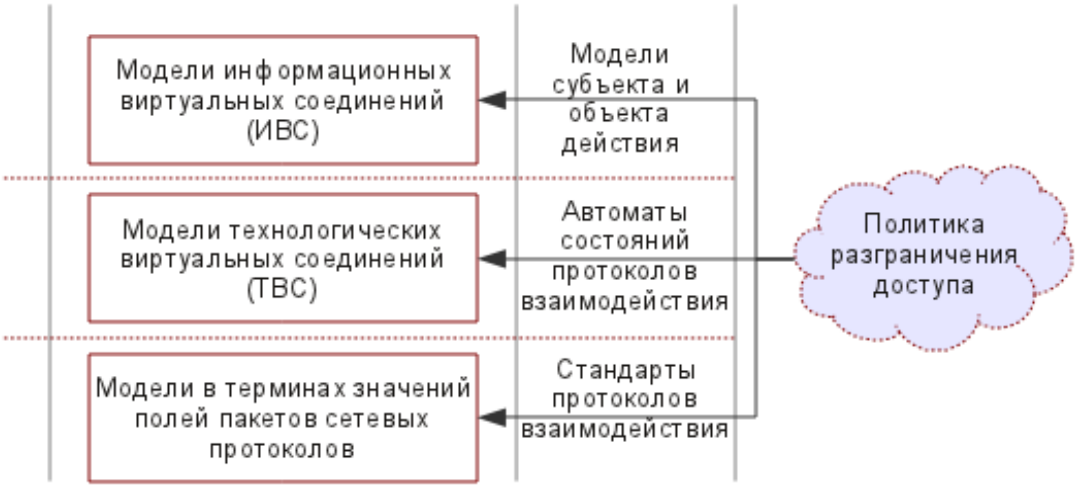

Рис. 1. Иерархическая структура формирования требований РД при использовании моделей ИВС и ТВС

4. Параллельная обработка ВС разных классов

Виртуальное соединение, как некоторая абстракция, существует параллельно и независимо от других виртуальных соединений, при этом виртуальные соединения не имеют между собой разделяемых ресурсов, что позволяет осуществлять их параллельную обработку [4]. Предложенный подход к фильтрации сетевого трафика, построенный на понятии виртуального соединения, позволяет выделить контекст соединения, который можно представить в виде вектора Y_i, описывающего его параметры, например, такие как порты и адреса источника и приемника, состояние соединения (на примере протокола TCP). Контроль виртуального соединения есть вычисление индикаторной функции *F*, для выполнения которого требуются такие ресурсы, как вычислительные процессоры и оперативная память: $F(Y_i\} = \{1,0,*\}$. Индикаторная функция F принимает значения: 1 – если ВС разрешено, 0 – если ВС запрещено, * - если на текущий момент невозможно однозначно определить запрещенное оно или нет, решение откладывается и ВС временно разрешается.

Вычислительные задачи можно разбить на две группы. Задачи первой группы носят потоковый характер и могут быть вычислены с помощью SIMD вычислителей (например, используя графические процессоры и технологию CUDA). Задачи второй группы решаются на стандартных многоядерных вычислителях MIMD. Так как описываемая распределенная среда является гетерогенной по отношению к доступным вычислителям, то в задачах межсетевого экранирования могут быть задействованы как потоковые SIMD вычислители, так и классические многоядерные MIMD процессоры. Благодаря тому, что межсетевые экраны, обеспечивающие защиту гипервизора, функционируют в виртуализированной среде, можно менять конфигурацию (вычислительные ядра, память, потоковые вычислители) устройства защиты в зависимости от параметров загрузки, политик доступа и количества имеющихся ресурсов.

Вычисление индикаторной функции F декомпозируется на множество вычислительных процессов – $\{F_i\}$. В таком случае, задачу контроля ВС можно описать в форме графа G(Q,X), называемого информационным графом контроля ВС (графовое описание потоковых задач подробно представлено в [5]). Граф контроля ВС состоит из множества вершин $F_i \in Q$, каждой из которых приписана операция F_i. Дуги $x(f_i, f_{i+1}) \in X$ определяют последовательность операций, приписанных вершинам графа G(Q,X), причем если две вершины q_i и q_{i+1} соединены дугой, то это означает, что результат операции F_i является входным для операции F_{i+1}. Каждый узел имеет дугу $x(f_i, F) \in X$, которая характеризует ситуацию, когда $F_i = 0$. В этом случае ВС считается запрещенным и дальнейший анализ не производится.

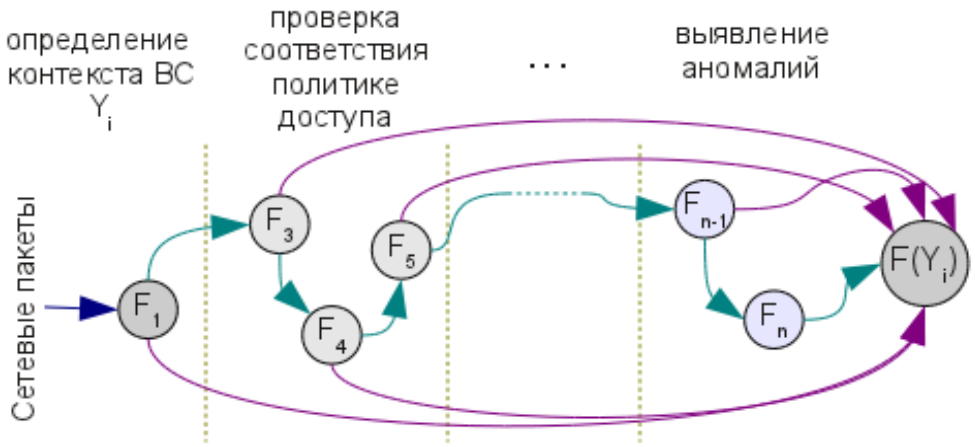

Рис. 2. Информационный граф контроля ВС с использованием вычислителей разных типов

Многопроцессорную вычислительную систему, решающую задачи межсетевого экранирования можно также представить в виде полносвязного графа $G^*(Q_m^*, Q_s^*)$, вершинами которого являются MIMD вычислители q_{mi}^* и потоковые вычислители q_{si}^*. Граф является полносвязным, так как коммуникации между вычислителями обеспечиваются аппаратными средствами и операционной системой и нет заранее заданного пути между вычислителями, данные могут попасть напрямую с одного узла на другой. Обычно граф вычислительной системы и информационный графы не соответствуют друг другу в силу того, что количество вычислительных ресурсов ограничено и меньше количества вычислительных процессов.

Граф контроля ВС можно разбить на N непересекающихся подграфов и построить конвейер обработки ВС, а также благодаря тому, что виртуальные соединения существуют независимо друг от друга возможна их параллельная обработка. При наличии C вычислителей MIMD типа время обработки ВС будет ограничено соотношением:

$$T_{BC} \le \frac{\max(z(f_i)) \cdot \max(\tau_j)}{C},$$

$z(f_i)$ - количество тактов требуемых для вычисления f_i, τ_j - продолжительность такта. Неравенство возникает благодаря тому что решение о классификации ВС может быть принято до окончания прохода всех узлов графа.

Благодаря гетерогенности и реконфигурируемости вычислительной среды в ряде случаев можно адаптировать конфигурацию межсетевого экрана под решаемые в данный момент задачи разграничения доступа. Достичь этого можно при помощи графовых моделей обработки сетевого трафика и использования технологии Netgraph[6], позволяющей организовать обработку сетевого трафика в контексте ядра операционной системы [4]. На рис. 2 представлен пример информационного графа контроля виртуальных соединений с декомпозицией индикаторной функции контроля на составляющие. Представленный подход вместе с использованием технологии виртуализации ресурсов позволяет повысить производительность контроля сетевого трафика и использовать только те вычислительные компоненты, которые нужны для решения текущих задач разграничения доступа.

5. Архитектура защищенной гетерогенной вычислительной среды

Распределенная вычислительная среда для решения научно-технических задач представляет разнородное множество вычислительных ресурсов в виде виртуальных машин и имеет следующие особенности [7]:

1. Среду используют широкий круг пользователей, решающих задачи разных классов;
2. Виртуальные машины разных групп пользователей могут функционировать в рамках одного гипервизора;
3. Используется широкий спектр программных компонентов (CAD/CAE приложения, средства разработки) и операционных систем (Linux, Windows);
4. Различные аппаратные конфигурации, в том числе виртуальные многоядерные вычислительные машины и виртуальные машины, позволяющие проводить потоковые вычисления с использованием технологии CUDA.

Гипервизор вычислительной среды является мощным многоядерным узлом, на котором функционирует домен уровня 0 (dom0 в терминах гипервизора XEN или сервисная консоль в терминах других гипервизоров) и виртуальные вычислительные машины (домен уровня U, domU). Для обеспечения информационной безопасности и разграничения доступа (РД) между виртуальными машинами, функционирующими в рамках одного гипервизора необходимо осуществлять контроль внутреннего («виртуального» трафика) и внешнего (поступающего с других гипервизоров и из внешних сетей). Решить задачу разграничения доступа можно путем интеграции в гипервизор виртуального межсетевого экрана, функционирующего в рамках гипервизора, но отдельно от пользовательских виртуальных машин. Домен виртуального межсетевого экрана можно определить как «домен безопасности» (security domain, domS). Важным аспектом при осуществлении контроля сетевого трафика является скрытое функционирование средства фильтрации, межсетевой экран не должен изменять топологию сетевой подсистемы гипервизора. Достичь этого можно путем использования технологии «Стелс» – осуществления невидимого для других сетевых компонентов контроля пакетного трафика [8].

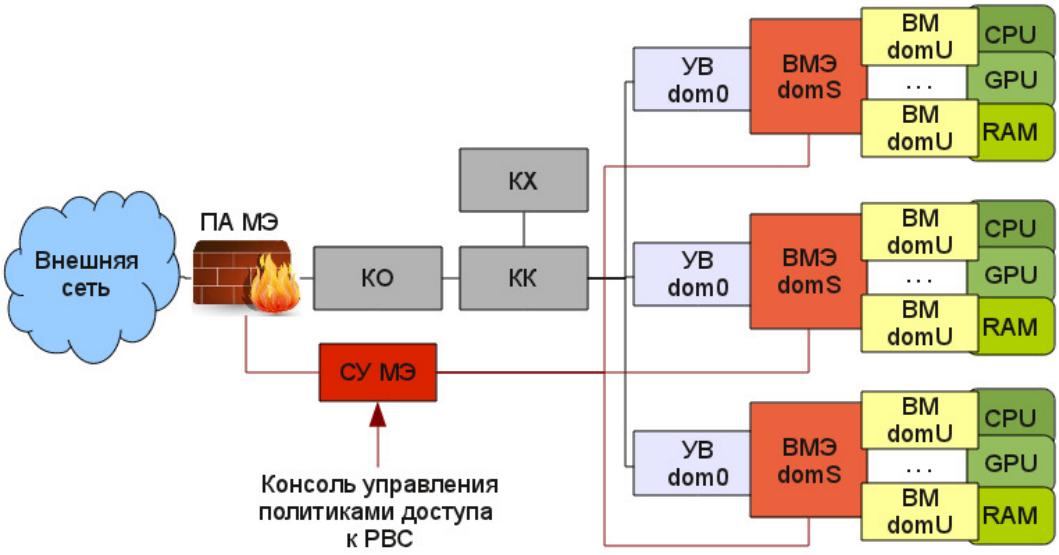

Рис. 3. Архитектура защищенной вычислительной среды

На рис 3. представлена обобщенная архитектура распределенной вычислительной среды с внедренными средствами разграничения доступа. Используются следующие сокращения: ПА МЭ – программно-аппаратный межсетевой экран, ВМЭ – виртуальный межсетевой экран, СУ МЭ – система управления межсетевыми экранами, ВМ – виртуальная машина, КО – контроллер облака, КК – контроллер кластера, КХ – контроллер хранилища. СУ МЭ решает задачи синхронизации и согласования политик безопасности между компонентами средств защиты информации (ПА МЭ, ВМЭ). При изменении политики доступа, новые правила реплицируются на все компоненты защиты РВС. Предложенный подход позволяет защитить распределенную вычислительную среду как от внешних так и от внутренних угроз. Внедрение прозрачного домена

безопасности domS изолирует гипервизор от виртуальных вычислительных машин, что исключает возможность атаки гипервизора из внутренней сети.

6. Заключение

Представленная архитектура распределенной гетерогенной вычислительной среды предоставляет вычислительные ресурсы разных конфигураций, что позволяет организовать в ней средства защиты в виде выделенного домена безопасности (domS), обладающего свойством реконфигурирумости. Реконфигурация средств защиты происходит в соответствии с решаемой в данный момент задачей, таким образом вычислительная среда защищает сама себя и адаптируется под текущую ситуацию. Проведенные исследования зависимости времени обработки ВС от количества доступных ядер показали линейную масшабируемость до восьми вычислителей включительно. На базе кафедры телематики СПбГПУ разработан и функционирует прототип вычислительной среды [7], предоставляющий гетерогенные вычислительные ресурсы, что позволяет проводить дальнейшие исследования и разработки в области обеспечения информационной безопасности распределенных вычислительных сред.

Литература

1. Cloud Security Alliance, Top Threats to Cloud Computing, Март 2010. [Электронный ресурс]. URL: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (дата обращения: 5.11.2010).
2. В.Мулюха, А.Г.Новопашенный, Ю.Е. Подгурский, В.С. Заборовский Методы и средства защиты компьютерной информации. Межсетевое экранирование. Издательство СПб Государственный политехнический университет, СПб, 2010, 90 с.
3. Силиненко А.В. Разграничение доступа в IP-сетях на основе моделей состояния виртуальных соединений: дис. канд. тех. Наук : 05.13.19: / Силиненко Александр Витальевич. – СПб, 2010. – 144 с.
4. Заборовский В.С., Лукашин А.А., Купреенко С.В. Многоядерная вычислительная платформа для высокопроизводительных межсетевых экранов. Высокопроизводительные вычислительные системы // Материалы Седьмой Международной научной молодежной школы. – Таганрог: Изд-во ТТИ ЮФУ, 2010. - 336 с.
5. Каляев И.А., Левин И.И., Семерников Е.А., Шмойлов В.И. Реконфигурируемые мультиконвейерные вычислительные структуры. - Ростов-на-Дону: Изд-во ЮНЦ РАН, 2008. - 320 с.
6. Cobbs A. All about Netgraph. [Электронный ресурс]. URL: http://www.daemonnews.org/200003/netgraph.html (дата обращения: 5.11.2010).
7. Лукашин А.А. Рощупкин И.А. Методы и средства построения распределенной вычислительной среды для решения наукоемких задач // XXXIX неделя науки СПбГПУ, Материалы Всероссийской межвузовской научно-технической конференции студентов и аспирантов, 6 - 11 декабря 2010 года, Часть XV, факультет при ЦНИИ робототехники и технической кибернетики. – СПб.: Изд-во Политехнического университета. – 2010. – с. 13-15
8. V. Zaborovsky, A. Titov. Specialized Solutions for Improvement of Firewall Performance and Conformity to Security Policy. Proceedings of the 2009 International Conference on Security & Management. v. 2. p. 603-608. July 13-16, 2009.