Санкт-Петербургский Государственный Политехнический Университет
кафедра телематики

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

ПаВТ-2011

Актуальность

Современной тенденцией в мире информационных технологий является переход к новой парадигме -

Вычислительная услуга в виде сервиса.

Актуальной проблемой является задача обеспечения информационной безопасности систем такого типа.

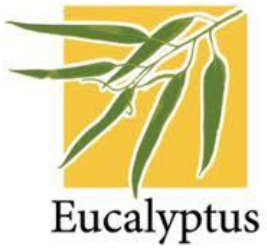
Гетерогенная вычислительная среда

Гетерогенная вычислительная среда (ГВС) – сервис, предоставляющий вычислительные ресурсы разных типов.

Аппаратные средства (CPU, GPU)

Системное ПО (Windows, Linux, FreeBSD, ...)

Прикладное ПО (Ansys, Adams, Pro Engineer, web platform, DB, ...)



Проблемы информационной безопасности

Особенности

- Виртуализация вычислительных ресурсов;
- Новые объекты защиты – гипервизоры, средства управления вычислительными ресурсами;
- Хранение данных;
- Контроль трафика в виртуальных сетях;
- Передача образов по сети;

Угрозы

- Атака на средства управления вычислительными ресурсами
- Неавторизованный доступ к гипервизору;
- Невозможность контроля виртуального трафика традиционными средствами РД;
- Отсутствие «периметра безопасности».

Цель и задачи исследования

Цель

Обеспечить «прозрачное» разграничение доступа в распределенной вычислительной среде.

Задачи

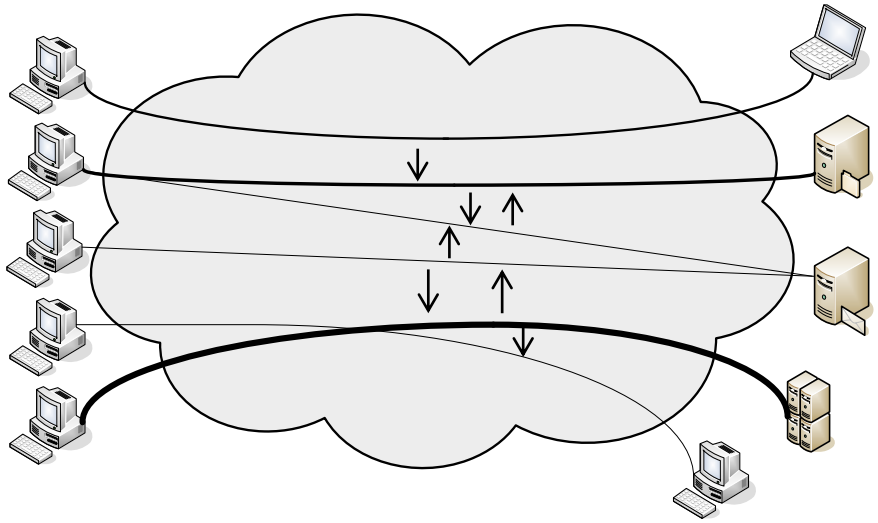
- контроль трафика между вычислительными ресурсами
- защита гипервизора
- защита компонентов управления
- решение задач РД в реальном времени с использованием высокоскоростных сетей (до 10Гб/с)
- согласование политик между узлами вычислительной среды

Формализация предлагаемого подхода к РД

Компьютерная сеть - это совокупность виртуальных соединений (ВС)

Виртуальное соединение — одно или двунаправленный поток пакетов и метаданные, связанные с окружением.

TCP-соединение, UDP обмен видео данными, DNS request-response



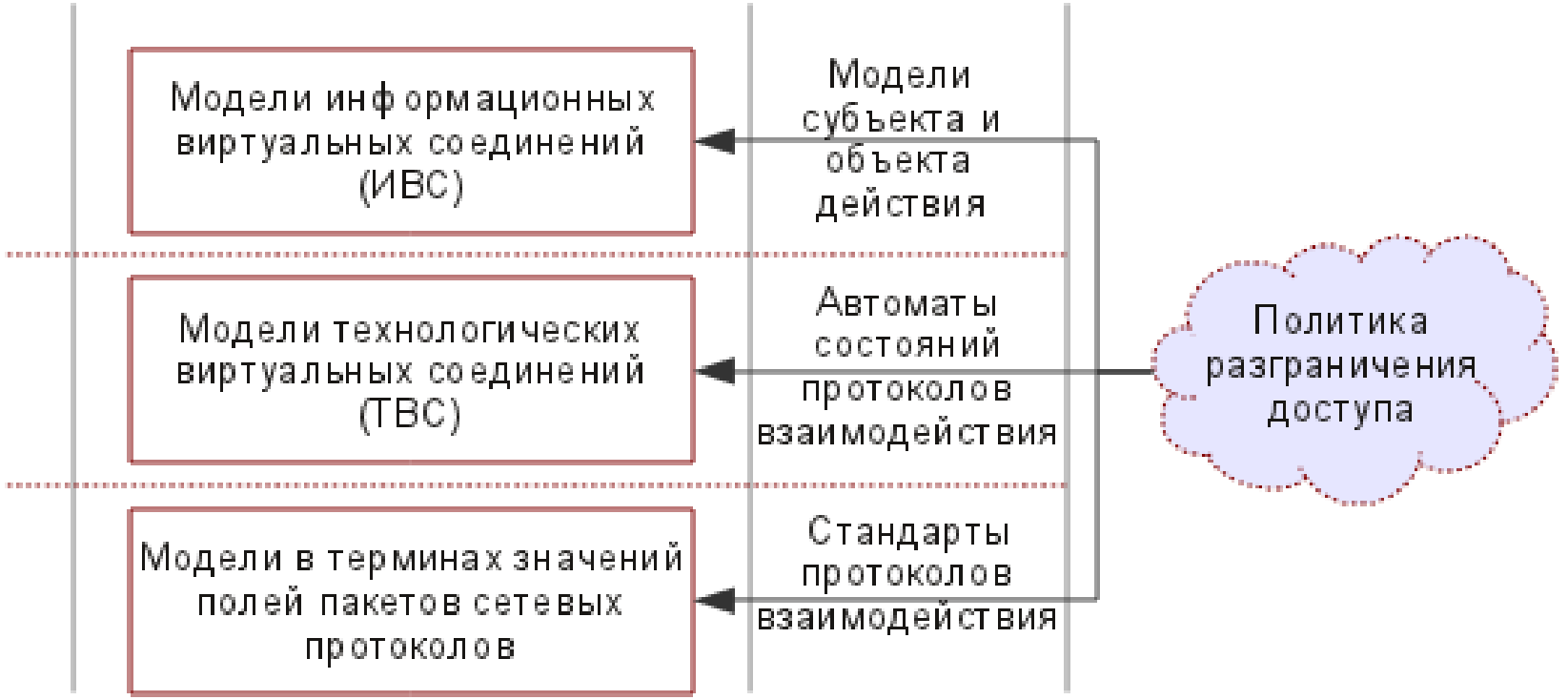
Контроль виртуального соединения - это вычислительный процесс:

Виртуальное соединение имеет контекст – вектор *Y*.

$$F(Y) = \bigwedge_{i=0}^{n} F_i(Y)$$

$$F(Y) = \begin{cases} 1\,\text{ВС разрешено} \\ 0\,\text{ВС запрещено} \\ *\,\text{В данный момент состояние ВС не определено} \end{cases}$$

Классификация уровней систем РД



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

$$IBC = \{TBC_i\},\ i = \overline{1,N} \subset (IMC \times IMD \times IMO)$$

Виртуальный межсетевой экран ССПТ

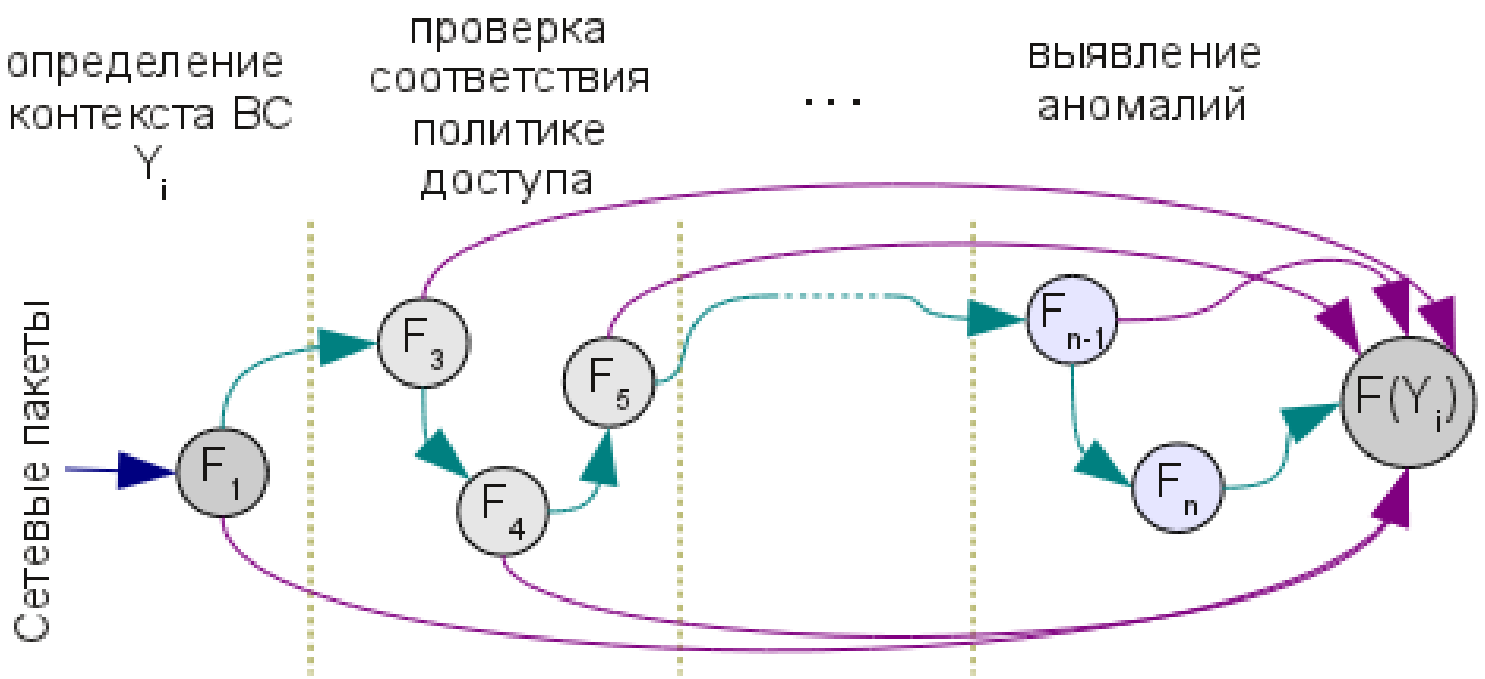
Программно аппаратный МЭ

Функционирование в VMWare ESXi

МЭ в «облаке»

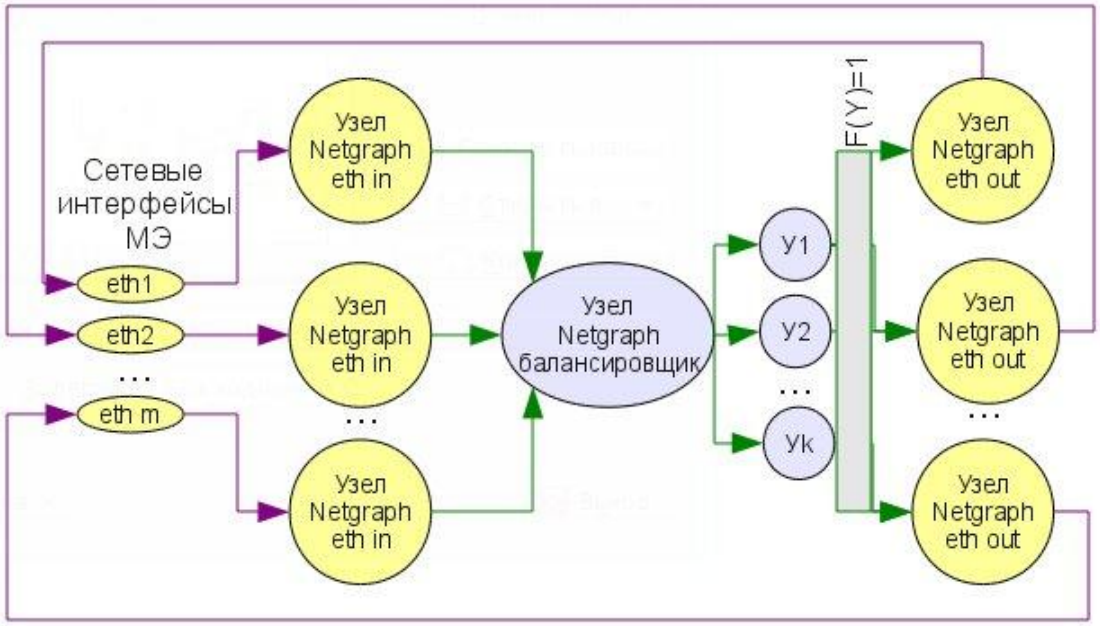
- ССПТ – семейство высокопроизводительных межсетевых экранов (МЭ), работающих в скрытном режиме;
- Анализ трафика и разграничение доступа, контроль ВС;
- Функционирование в виртуальной среде гипервизора.

Параллельная обработка ВС



1. Декомпозиция индикаторной функции F – $\{F_i\}$;
2. Построения графа контроля ВС – G(Q,X);
3. Разбиение на подграфы – конвейеры и параллельные модули обработки ВС;
4. Агрегация результатов вычисления компонент функции F.

Сетевая подсистема Netgraph



Модульная сетевая подсистема;

Топология графа.

- Узлы графа — это вычислительные модули
- Ребра — это соединения, по которым следуют пакеты ;

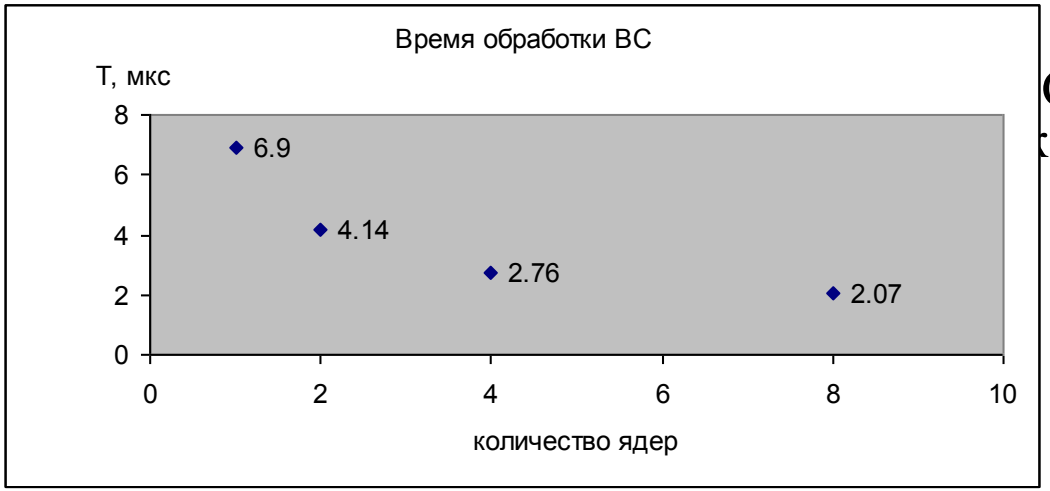
Программный интерфейс для работы с сетевым трафиком;

Обработка данных внутри ядра ОС;

«Ядерные» потоки обработки.

Сетевая подсистема **Netgraph** позволяет организовать **параллельную** обработку виртуальных соединений в контексте ядра ОС.

Оценка эффективности



Среднее время обработки одного кадра:

- Фильтр Netgraph
  T=6,9 мкс
- Фильтра BPF
  T=17,8мкс

Виртуальный ССПТ функционирует в:

1. XEN
2. ESX

Пропускная способность (стенд 10Гбит Ethernet):

- 2.3 Гбит/с - BPF
- 9.2 Гбит/с - Netgraph

Распределенная вычислительная среда университета

Кафедра телематики СПбГПУ:

1. Исследовательский стенд
   2 узла виртуализации
   Узел хранилища
   Узел управления
2. Платформа Eucalyptus-spbstu
3. Поддержка Linux, Windows
4. Бета-тестирование инженерных пакетов сотрудниками ЦНИИ РТК
5. Подготовка образов ВМ

ИТК СПбГПУ:

1. Высокопроизводительные вычислительные ресурсы
2. Поставка нового оборудования в рамках НИУ

Распределенная вычислительная среда университета

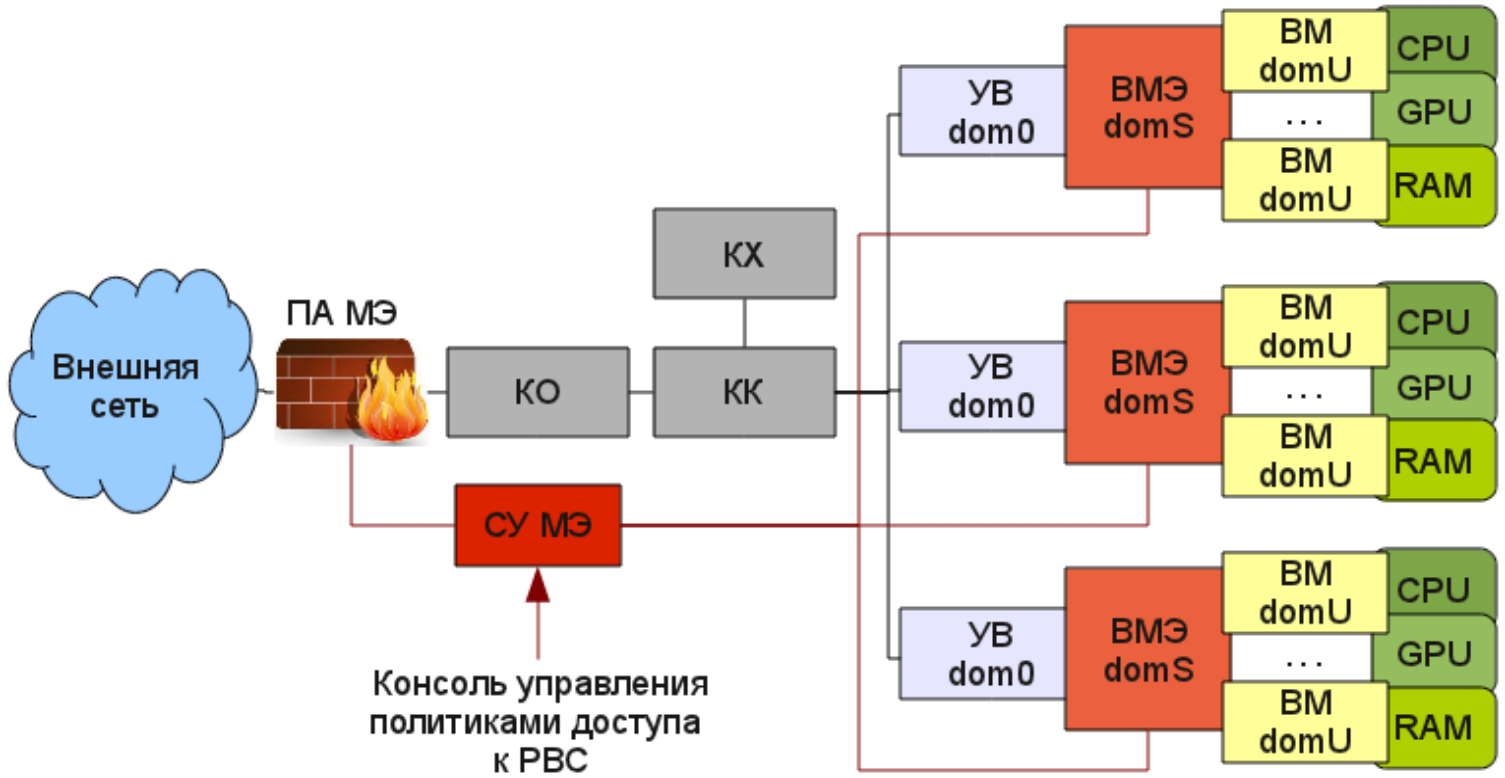
Распределенная вычислительная среда для решения научно-технических задач представляет собой разнородное множество вычислительных ресурсов в виде виртуальных машин и имеет следующие особенности:

1. Широкий круг пользователей и задачи разных классов;
2. Виртуальные машины разных групп пользователей могут функционировать в рамках одного гипервизора;
3. Используется широкий спектр программных компонентов и ОС;
4. Различные аппаратные конфигурации вычислительных ресурсов.

Требования к внедряемой системе защиты:

1. Прозрачная интеграция;
2. Высокая производительность;
3. Согласование политик безопасности;
4. Реконфигурируемость;
5. Масштабируемость.

Архитектура защищенной вычислительной среды



- 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.

Наши дальнейшие планы

1. Разработка МЭ, осуществляющих РД в существующих облачных средах;
2. Интеграция разработанных средств в вычислительную среду СПбГПУ;
3. Развитие открытых «облачных» программных продуктов (Eucalyptus, …);
4. Разработка и исследования методов согласования политик безопасности в распределенной системе защиты;
5. Поддержка GPU в виртуальной инфраструктуре;
6. Разработка методических материалов для внедрения исследуемых технологий в образовательный процесс СПбГПУ.

https://github.com/1ukash/eucalyptus-fork-2.0

https://cloudlet.stu.neva.ru:8443

Заключение

- Предложенные подходы и методы позволяют реализовать высокопроизводительную систему разграничения доступа в распределенной вычислительной среде;
- Благодаря использованию «невидимых» межсетевых экранов, контроль соединений остается прозрачным для компонент вычислительной среды;
- Использование централизованной системы управления МЭ позволяет оперативно согласовывать политики безопасности между компонентами защиты.

СПАСИБО ЗА ВНИМАНИЕ