Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056.5

Пархомик
Сергей Юрьевич

Обеспечение безопасности в виртуальных сетях «Nework as a Service»

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии

по специальности 1-45 81 01 Инфокоммуникационные системы и сети

Научный руководитель
Селезнев Игорь Львович
к.т.н., доцент

Минск 2018

ВВЕДЕНИЕ

В настоящее время наблюдается рост интереса к технологии виртуализации, а именно к облачным вычисления. Вычислительная мощь современных процессоров быстро растет. Возможности современных многоядерных систем, лучше позволяют реализовать богатейший потенциал идей виртуализации операционных систем и приложений, выводя удобство пользования компьютером на качественно новый уровень. Технологии виртуализации становятся одним из ключевых компонентов в самых новых процессорах Intel и AMD, в операционных системах от Microsoft и ряда других компаний. Смысл виртуализации в вычислительной технике – «виртуальные» объекты означают некие абстрактные интерфейсы, за которыми скрывается реальное оборудование. В основе виртуализации лежит возможность одного компьютера выполнять работу нескольких компьютеров благодаря распределению его ресурсов по нескольким средам. С помощью виртуальных серверов можно разместить несколько операционных систем и несколько приложений в едином местоположении, в том числе удаленно. Таким образом, физические и географические ограничения перестают иметь какое-либо значение. Помимо энергосбережения и сокращения расходов, благодаря более эффективному использованию аппаратных ресурсов, виртуальная инфраструктура обеспечивает высокий уровень доступности ресурсов, более эффективную систему управления сервером, повышенную безопасность и усовершенствованную систему восстановления в критических ситуациях.

Если же говорить об обеспечении доступа к услугам, которые появляются благодаря возможностям виртуализации, необходимо обеспечить безопасный доступ к ним из любой точки мира без необходимости покупки выделенного канала связи, что привело бы к росту затрат.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель диссертационной работы заключается в разработке системы обеспечения безопасного подключения поверх сети общего пользования с использованием группы протоколов IPsec.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1 Изучить особенности и основные задачи, решаемые при использовании технологии виртуализации.

2 Провести анализ существующих сервисов, в основе которых лежат облачные вычисления

3 Проанализировать основные типы сетевых атак, их воздействие на сеть и возможные последствия.

4 Проанализировать методы и средства защиты хостов сети от существующих типов атак.

5 Обеспечить безопасность передаваемых данных в виртуальных сетях NaaS.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 статья в сборниках материалов конференций.

Структура и объем диссертации

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, четырех глав и заключения, и библиографического списка. Общий объем диссертации – 71 страниц, работа содержит 25 рисунков, библиографический список включает 29 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено состояние проблематики использования и распределения вычислительных ресурсов. Предложено использование виртуализации в качестве одного из возможных решений данной проблемы. Показана важность совершенствования методов и средств предоставления услуг в области информационных технологий.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с современными задачами в области виртуализации ресурсов и предоставления услуг.

В первой главе рассматривается понятие виртуализации, ее основные виды, преимущества и недостатки, а также основные направления ее применения в современном мире. Приводится сравнение и анализ современных платформ виртуализации, результаты которого выведены в итоговую таблицу.

Во второй главе рассматриваются облачные вычисления, их архитектура, достоинства и недостатки каждой из разновидностей облачных вычислений. Представлен анализ облачных сервисов, их основных достоинств и недостатков. Приведен краткий обзор каждого из сервисов. Для каждого сервиса указана сфера применения и преимущества по сравнению с остальными сервисами.

В третей главе представлен анализ особенностей обеспечения безопасности сети, были приведены основные модели обеспечения безопасности сети, их достоинства и недостатки. Рассмотрены основные типы атак на сеть и методы борьбы с ними. В конце главы рассмотрен набор протоколов защиты данных IPsec, его архитектура, а также принцип построения шифрованных каналов связи. В конце приведен список преимуществ и недостатков по сравнению с другими технологиями обеспечения безопасности сети

В четвертой главе представлен результат организации IPsec туннеля с использованием оборудования S Terra. Приведены настройки устройств шифрования, а также программного обеспечения Bel VPN Client.

ЗАКЛЮЧЕНИЕ

1 Проведена систематизация знаний для понимания термина «виртуализация», особенностей применения данной технологии, ее основных преимуществ и недостатков. Проведено сравнение и анализ основных платформ, представленных на рынке на сегодняшний день.

2 Проведено исследование технических аспектов облачных технологий: изучена архитектура облачных вычислений, особенности частного, публичного и гибридного облаков, применение облачных вычислений в сфере оказания услуг и разновидность облачных сервисов в зависимости от степени оказания поддержки.

3 Изучены особенности обеспечения сетевой безопасности, основные типы атак, их особенности и область воздействия. Рассмотрены возможные меры и комплекс мероприятий для борьбы с данными типами атак. Представлена архитектура IPsec, стадии установления соединения

4 По результатам проведенных исследований произведен выбор оборудования для организации безопасного подключения с использованием IPsec. Представлены основные настройки данного оборудования и способы его взаимодействия.

5 Рассмотрен вариант использования дополнительного программного обеспечения для организации защищенного соединения для отдельных устройств, при организации подключения поверх сети интернет. Продемонстрирован результат проведенных настроек.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Пархомик, С.Ю. Автоматизация и масштабирование локальных вычислительных сетей с использование SDN / С.Ю. Пархомик, А.Д. Семак, И.Л. Селезнев// Алгебраическое кодирование и безопасность данных. – 2017 – С. 56-62.