УДК 004.732

ОПТИМИЗАЦИЯ РАБОТЫ ЗАЩИЩЕННОЙ МУЛЬТИСЕРВИСНОЙ СЕТИ

С.Ю. ЛОСКОТ, А.В. МУРАШКО, О.А. ХАЦКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 10 ноября 2018

Аннотация. Предложен метод оптимизации работы и повышения информационной безопасности корпоративной мультисервисной сети связи при помощи использования межсетевого экрана. Представлена подробная классификация межсетевых экранов. Выполнена оценка эффективности работы защищенной мультисервисной сети.

Ключевые слова: межсетевой экран, мультисервисная сеть, базы данных, WAN-соединение.

Введение

Для эффективной разработки и внедрения в эксплуатацию мультисервисных сетей связи необходимо предусмотреть своевременную защиту программ и баз данных, средств хранения, обработки и передачи информации. Основные требования, предъявляемые к мультисервисной сети связи, заключаются в следующем: высокий уровень информационной безопасности; организация четкой аутентификации и идентификации всех пользователей автоматизированной информационной системы; организация системы централизованного управления и др. [1].

Классификация межсетевых экранов

Межсетевой экран, сетевой экран – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа, реализуемого с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами. Помимо защитной функции, межсетевые экраны позволяют отфильтровывать нежелательный трафик и блокировать его попадание в сеть или в отдельно взятые ее сегменты [2].

Имеется множество классификаций и вариантов реализации межсетевых экранов. К основным можно отнести реализации, предложенные компанией Cisco [3].

1. *Прокси-сервер*. Прокси-сервер служит шлюзом между сетями для конкретного приложения. Прокси-серверы могут выполнять дополнительные функции, например, кэширование и защиту контента, а также препятствовать прямым подключениям из-за пределов сети. Однако это может отрицательно сказаться на пропускной способности и производительности поддерживаемых приложений.

2. *Межсетевой экран с контролем состояния сеансов*. Он пропускает или блокирует трафик с учетом состояния, порта и протокола, а также осуществляет мониторинг всей активности с момента открытия соединения и до его закрытия. Решения о фильтрации принимаются на основании правил, определяемых администратором, а также контекста. Под контекстом понимается информация, полученная из предыдущих соединений и пакетов, принадлежащих данному соединению.

3. *Межсетевой экран UTM (unified threat management)*. Сочетает такие функции, как контроль состояния сеансов, предотвращение вторжений и антивирусное сканирование. Также оно может включать в себя дополнительные службы, а зачастую – и управление облаком. Основные достоинства UTM – простота и удобство эксплуатации.

4. *Межсетевой экран нового поколения (Next-Generation Firewall).* Современные межсетевые экраны не ограничиваются фильтрацией пакетов и контролем состояния сеансов. Большинство компаний внедряет межсетевые экраны нового поколения, чтобы противостоять современным угрозам, таким как сложное вредоносное ПО и атаки на уровне приложений. Эти экраны должны включать в себя такие функции как контроль состояния сеансов; система предотвращения вторжений; учет и контроль особенностей приложений, позволяющих распознавать и блокировать приложения, предотвращения вторжений; функции учета и контроля особенностей приложений, позволяющие распознавать и блокировать приложения, представляющие опасность; схема обновления, позволяющая учитывать будущие каналы информации; технологии защиты от постоянно меняющихся и усложняющихся угроз безопасности.

5. *NGFW (Next-Generation Firewall) с активной защитой от угроз.* Эти экраны обеспечивают защиту от угроз путем интеллектуальной автоматизации безопасности в динамическом режиме. Обладают такими функциями, как определение ресурсов, наиболее подверженых риску; быстрое реагирование на атаки, благодаря интеллектуальной автоматизации безопасности, которая устанавливает политики и регулирует защиту в динамическом режиме; выявление отвлекающей и подозрительной деятельности путем применения корреляции событий в сети и на оконечных устройствах; использование ретроспективных средств обеспечения безопасности, которые осуществляют непрерывный мониторинг на предмет подозрительной деятельности и поведения даже после первоначальной проверки; применение унифицированных политик, обеспечивающих защиту на протяжении всего жизненного цикла атаки.

Для проведения исследования в рамках настоящей работе был выбран межсетевой экран с контролем состояния сеансов.

Описание разработанной модели. Результаты исследования.

В качестве объекта исследования была выбрана сеть ЗАО «Технопром». Организация имеет два офиса. Каждый офис имеет собственную локальную сеть. Суммарное количество рабочих станций в двух локальных сетях – 500. Пользователи имеют доступ к серверу базы данных, где хранится информация о клиентах, а также к электронной почте и HTTP-серверу. Некоторые сотрудники компании загружают мультимедиа контент, замедляя доступ к сети Интернет другим сотрудникам. В целях обеспечения необходимо уровня безопасности и оптимизации работы мультисервисной сети организацией используется брандмауэр.

Моделирование мультисервисной сети выполнено в программе Riverbed Modeler 17.5. Она представляет собой объектно-ориентированный инструмент моделирования сетей связи, который располагает обширным пакетом различных моделей сетевых элементов, библиотеками протоколов сетей связи. Кроме того, с помощью этой программы можно выполнять расчет основных характеристик с учетом параметров QoS для различных типов трафика [4]. Результаты моделирования представлены в виде графиков, которые отражают процент загрузки WAN-соединения, время отклика базы данных и время отклика Web-страницы.

Были смоделированы два случая работы сети: без установки брандмауэра и с установкой брандмауэра. При моделировании в первом случае были получены следующие данные: время отклика базы данных составляет более 1 с (рис. 1); время отклика Web-страницы – более 3 с (рис. 2); процент загрузки WAN-соединения равен в среднем 80 (рис. 3), что приводит к некорректной работе приложений в сети.

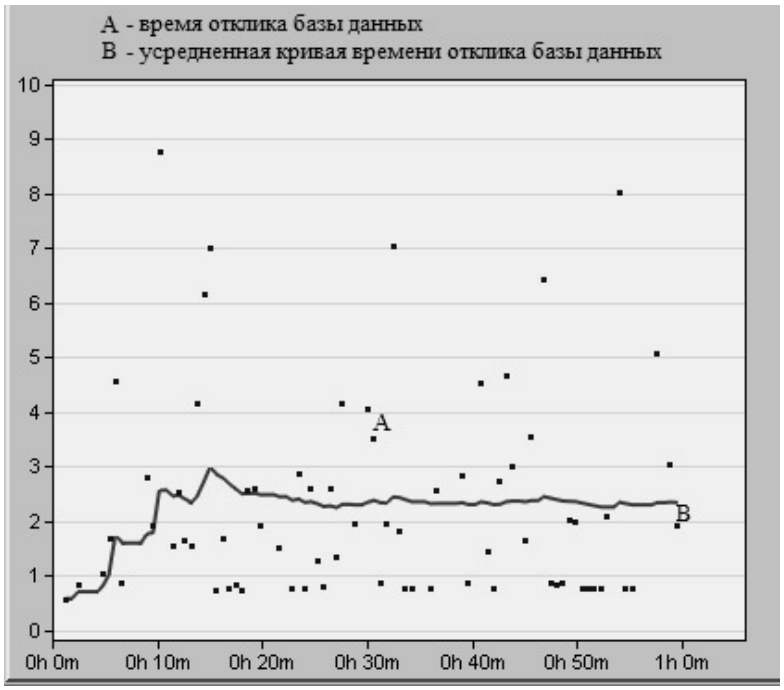

Рис. 1. График отклика баз данных без использования брандмауэра

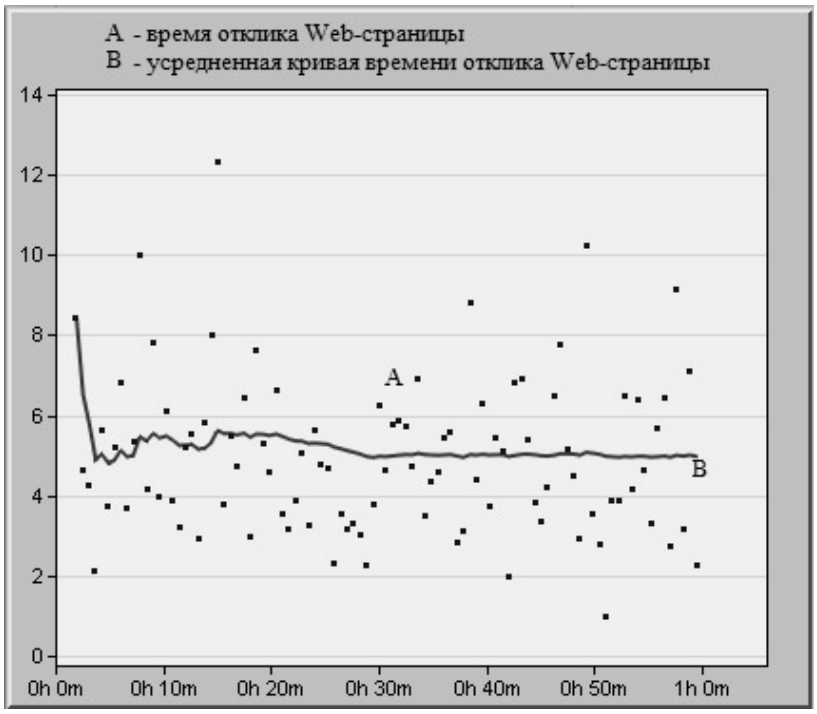

Рис. 2. График отклика Web-страниц без использования брандмауэра

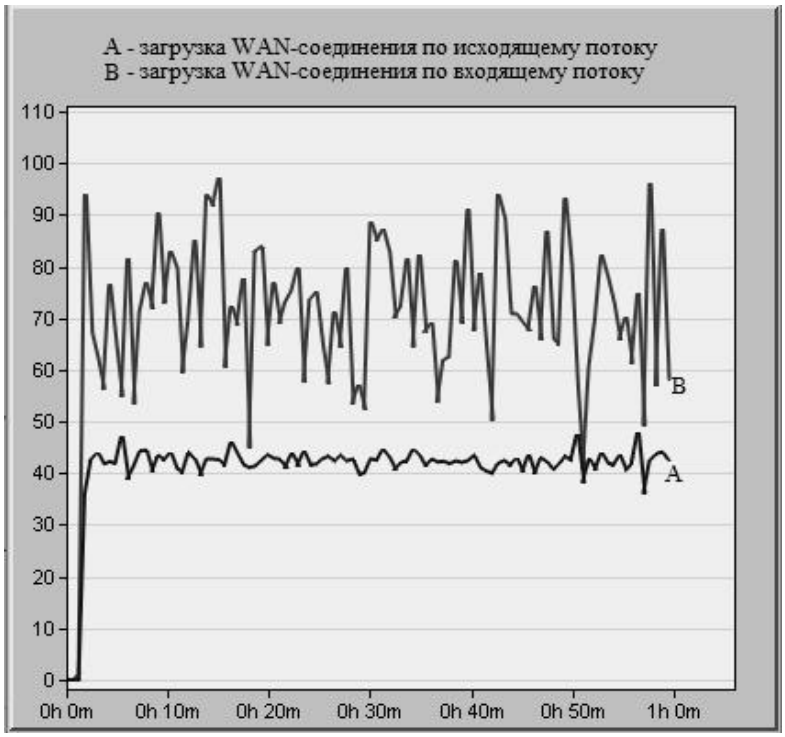

Рис. 3. Графики загрузки общего WAN-соединения без использования брандмауэра

При моделировании во втором случае были получены следующие данные: время отклика базы данных составляет 1 с (рис. 4); время отклика Web-страницы – 3 с (рис. 5); процент загрузки WAN-соединения уменьшился с 80 до 40 %(рис. 6).

Рис. 4. Графики сравнения отклика баз данных без использования и с использованием брандмауэра

Рис. 5. Графики сравнения отклика Web-страниц без использования и с использованием брандмауэра

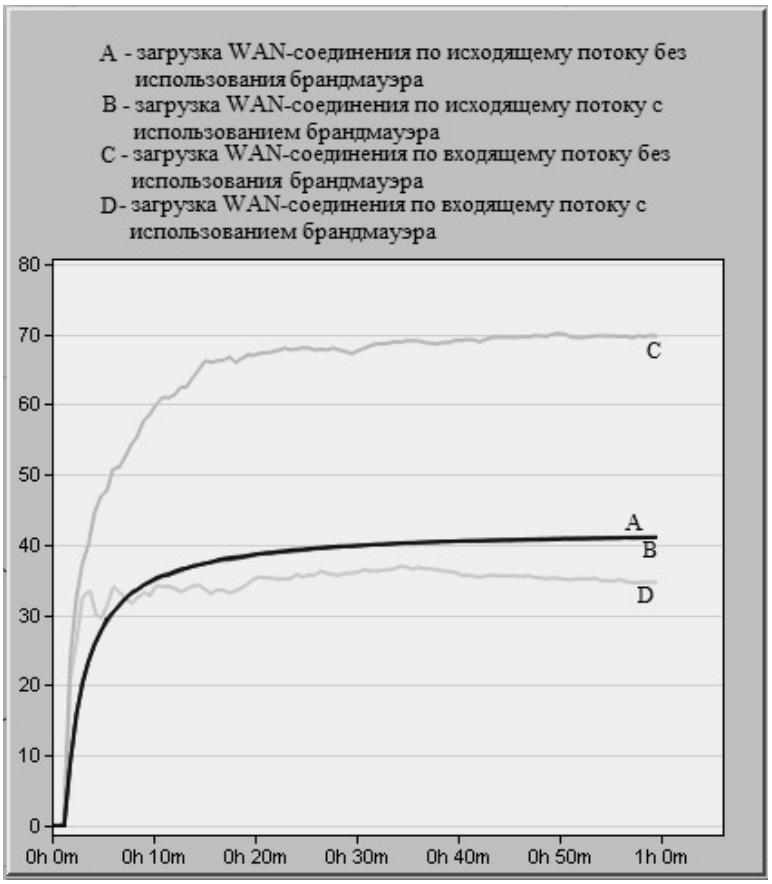

Рис. 6. Графики сравнения загрузки общего WAN-соединения без использования и с использованием брандмауэра

Заключение

Предложенный в работе метод моделирования мультисервисной сети позволил наглядно проиллюстрировать способ оптимизации ее работы и повышения ее информационной безопасности с помощью межсетевого экрана.

В результате моделирования доказана возможность снижения времени отклика базы данных и времени отклика Web-страницы с 3 до 1 с и с 5 до 3 с соответственно, а также возможность уменьшения процента загрузки WAN-соединения с 80 до 40 %.

Проведенные исследования показывают, что при использовании в сети устройства защиты от несанкционированного доступа и его правильной конфигурации можно оптимизировать работу мультисервисной сети, улучшить ее производительность и обеспечить необходимый уровень безопасности.

OPTIMIZATION OF WORK OF PROTECTED MULTISERVICE NETWORK

S.Yu. LOSKOT, A.V. MURASHKO, O.A. KHATSKEVICH

Abstract. A method of optimizing the work and increasing the information security of a corporate multiservice communication network by using the firewall is proposed. Detailed classification the firewalls is submitted. Efficiency of secure multiservice network is evaluated.

Keywords: firewall, multiservice network, database, WAN-connection.

Список литературы

1. Мультисервисные сети следующего поколения. [Электронный ресурс]. URL: http://www.iksmedia.ru/articles/718285-Multiservisnye-seti-sleduyushhego.html (дата доступа: 10.11.2018)
2. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. МГТУ им. Н. Э. Баумана, 2002.
3. Типы межсетевых экранов [Электронный ресурс]. URL: http://www.cisco.com/c/ru_ru/products/security/firewalls/what-is-a-firewall.html (дата доступа: 10.11.2018)
4. Тарасов В.Н. [и др.] Проектирование и моделирование сетей связи в системе Riverbed Modeler. Самара, 2016.