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

УДК 004.725.5

Коротченя
Олеся Николаевна

Обеспечение безопасности и качества обслуживания мультисервисной сети

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологии
по специальности 1–45–81–01 «Инфокоммуникационные системы и сети»

Научный руководитель
Королев Алексей Иванович
канд. техн. наук, доцент

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

При разработке современных крупных сетей городского масштаба необходимо решать ряд задач, сложность и характер которых зависит от требований к функциональному назначению сети. Основная масса постоянно обновляющихся требований, предъявляемых, в настоящее время, к технологиям глобальных (магистральных) сетей операторов связи, исходит от растущего спроса клиентов на дополнительные услуги.

При разработке современных крупных сетей передачи данных, отвечающих таким требованиям, выбираются такие технологии и стандарты, которые позволяют в конечном итоге получить сеть, отвечающую требованиям и характеристикам мультисервисной сети.

Мультисервисные сети должны отвечать жестким требованиям безопасности, обладать высокими показателями живучести и обеспечивать необходимое качество предоставления сервисов.

Обеспечить безопасность сети возможно за счет объединения сервисов в виртуальные частные сети, гибкая настройка списков контроля доступа ограничит доступность этих сетей для пользователей. Живучесть СПД достигается за счет резервирования оборудования и каналов связи, мониторинга узлов и трактов, использования протоколов динамической маршрутизации.

Мультисервисная сеть – это сеть, которая образует единую информационно–телекоммуникационную структуру, которая поддерживает все виды трафика (данные, голос, видео) и предоставляет все виды услуг (традиционные и новые, базовые и дополнительные) в любой точке, в любое время, в любом наборе и объеме, с дифференцированным гарантированным качеством и по стоимости, удовлетворяющей различные категории пользователей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа выполнялась по теме «Обеспечение безопасности и качества обслуживания мультисервисной сети».

Проведённая работа по диссертационной тематике соответствует мировым тенденциям в сфере телекоммуникаций. Рассмотренные технологии настройки и обслуживания сетей передачи данных отражают современные тенденции в области проектирования и построения крупных сетей передачи данных (провайдерских сетей).

Целью данной работы является выбор оптимальных решений для обеспечения таких важных вопросов в сети передачи данных, как безопасность, живучесть и качество сервисов.

Для достижения цели необходимо решить следующие задачи:

– рассмотреть возможные угрозы и уязвимости в сетях;

– проанализировать возможные и выбрать варианты обеспечения безопасности в СПД;

– рассмотреть вопрос обеспечения живучести сети передачи данных;

– оценить и выбрать оптимальные решения для обеспечения живучести в сети;

– проработать вопрос обеспечения качества сервисов в городских сетях передачи данных.

Актуальность проблемы обеспечения безопасности и качества сервисов в городских сетях передачи данных обусловлена сильным ростом за последнее время ростом количества абонентов в сети, а также увеличением количества предоставляемых услуг для пользователей.

КРАТКОЕ СОДЕРЖАНИЕ

Безопасность крупной сети передачи данных является одним из наиболее важных моментов. Для возможности обеспечения безопасности сеть построена с применением технологии VPN.

Данная технология позволяет создавать закрытые от посторонних каналов обмена информацией. Т.к. в сети предоставляются такие сервисы как IMS-телефония, IP-телевидение, виртуальные частные сети для корпоративных пользователей, то использование данной технологии получило свое широкое применение, за счет объединения сервисов в закрытые VPN сети. Так в рассматриваемой сети созданы отдельные VPN сети для IP-телефонии, IPTV, услуги доступа в сеть интернет. Так же создана отдельная сеть для управления и мониторинга узлами СПД. Согласно политике безопасности, сеть является закрытой для доступа из вне. Однако, при для удаленного управления сетью установлен межсетевой экран Cisco ASA 5515-X, который позволяет получить доступ к сети авторизованным пользователям через VPN туннель посредствам Cisco VPN Client

Простейшим способом ограничения доступа в сетях передачи данных является использование Access Control List – список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом. Гибкая настройка списков контроля доступа и применение их на интерфейсы позволяет закрыть доступ нежелательным пользователям к виртуальным частным сетям.

Опорные маршрутизаторы включаются в ядро сети посредствам линейного резервирования. Ядро сети реализовано на оборудовании Cisco ASR 1009-X. К ядру с обратной стороны подключены IMS и IPTV платформы, доступ в сеть интернет. Линии связи оптические, все физические линии в процессе модернизации сети собраны в агрегированные каналы. Это позволяет не только повысить пропускную способность канала, но и обеспечить резерв на случай выхода из строя одного из каналов связи.

Расширение канала так же возможно без его отключения. В одном кольце включено по возможности 2-3 маршрутизатора.

Включение колец из опорных маршрутизаторов происходит одновременно в два коммутатора ASR 1009-X. Тем самым достигается резервирование самого ядра.

В опорные маршрутизаторы включается оборудование ZTE C 320. Подобное оборудование позволяет подключать пользователей по технологиям PON, VDSL. Включение в опорные маршрутизаторы выполняется посредствам нескольких волокон. На управляющей плате имеется несколько up-link портов. Допускается агрегирование портов (Link aggregation). Это позволяет в случае повреждения одного из волокон бесперебойно предоставлять услуги пользователям. Включение в опорные маршрутизаторы выполняется в разные управляющие платы, что позволяет увеличить живучесть узла.

Маршрутизация в сети динамическая и основана на протоколе OSPF. В случае выхода из строя опорных маршрутизаторов или линий связи происходит быстрое обновление таблицы маршрутизации. Это позволяет практически без сбоев предоставлять услуги пользователям.

Обеспечение быстродействия протокола OSPF в сети достигнуто за счет деления сегментов сети на области. При такой конфигурации маршрутизаторам нет необходимости обновлять всю таблицу маршрутизации.

Обновление таблицы маршрутизации при разделении на области на практике происходит за 5-10 секунд. Без разграничения на области это занимало до 10 минут.

Для отслеживания состояния сети применяется система мониторинга Zabbix. В данной сети мониторингу подвергается состояние линий связи, их загруженность, состояние маршрутизаторов (загруженность процессора, температурные показатели, состояние портов), доступность узлов, которые находятся за пределами сети, контролируется подача электропитания на станционное оборудование.

Ведется постоянная статистика данных параметров, которую наглядно можно оценивать в графиках помимо статистики ведется журнал событий. Данные инструменты позволяют значительно сократить время на локализацию и устранение аварийной ситуации на сети передачи данных города.

Даная сеть является мультисервисной. Количество предоставляемых услуг постоянно растет, так же растет и количество пользователей. В первую очередь QoS необходим для потоков трафика мультимедийных приложений, VoIP и видеоконференций в сетях. Контроль таких параметров, как полоса пропускания (Bandwidth), задержка при передаче пакета (Delay), колебания (дрожание) задержки при передаче пакетов – джиттер, потеря пакетов (Packet loss), позволяет добиться необходимого уровня качества сервисов в сети передачи данных.

ЗАКЛЮЧЕНИЕ

Крупные сети передачи данных более подвержены вторжениям, чем локальные сети меньшего масштаба или централизованные информационные системы предприятия. Реализация сети по технологии VPN позволяет максимально обеспечить ее безопасность. Гибким инструментом для для ограничения доступа является применение Access Control List.

Для обеспечения живучести сети имеет место применение механизмов резервирования и мониторинга сети. Объектами резервирования являются линии связи и узловые маршрутизаторы. Такие решения, как Zabbix, при квалифицированной настройке позволяют производить постоянный мониторинг и аудит сети передачи данных, а также сокращать время простоя сети в случае аварийных ситуаций за счет сокращения времени устранении аварии.

Решение задачи обеспечения требуемого качества обслуживания в сетях IP, безусловно, может быть достигнуто прямым путем – на основе предоставления гарантированной полосы пропускания, повышения производительности сетевых устройств – маршрутизаторов и шлюзов, использовании магистралей с высокими пропускными способностями.

Наиболее целесообразным представляется применение гибких методов, которые обеспечивают требуемые показатели качества обслуживания при эффективном использовании ресурсов сети для большого набора различных приложений, включая и наиболее критичные аудио- и видео-приложения реального времени.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Коротченя О.Н. Разработка комплекса мероприятий для обеспечения защиты SSL–сервера / А.С. Зайцев, О.Н. Коротченя, В.Ю. Цветков // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. науч.–техн. семинара, Минск / БГУИР. – Минск, 2017. – С. 31– 32.

2–А. Коротченя О.Н. Агрегирование каналов связи / К.А. Волков, О.Н. Коротченя // Сборник материалов 54-й СНТК за 2018 г.: 54-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», Минск / БГУИР. – Минск, 2018. – С. 25.

«Магистерская диссертация выполнена самостоятельно, проверена в системе «Антиплагиат». Процент оригинальности составляет 89,38%. Цитирования обозначены ссылками на публикации, указанные в «Списке литературы»