УДК 004.738.2

ПОСТРОЕНИЕ ГИБРИДНОЙ ОТКАЗОУСТОЙЧИВОЙ КОРПОРАТИВНОЙ ТЕЛЕФОННОЙ СЕТИ

Н.А. УЧАЕВ, С.Н. ПЕТРОВ, С.В. ВЛАСЮК*, Т.А. ПУЛКО

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

**Институт информационных технологий*
Козлова, 28, Минск, 220037, Беларусь

Поступила в редакцию 29 октября 2016

Обоснована актуальность внедрения гибридных корпоративных телефонных сетей, включающих аналоговые системы и системы IP-телефонии, на примере коммуникационной платформы Asterisk. Проведен анализ вопросов экономической эффективности, обеспечения приемлемого качества связи, а также надежности и безопасности предоставляемых услуг.

Ключевые слова: интернет-телефония, кластеризация сервисов, IP-АТС Asterisk, SIP-трафик, RTP-поток, протокол TLS, протокол ZRTP.

Введение

В случае развертывания телефонной сети на предприятии, выбор в пользу IP-решений очевиден: достаточно учесть отсутствие необходимости прокладки дополнительной линий связи. Однако чаще организации и предприятия уже имеют определенный набор сконфигурированного оборудования, линии связи и устоявшиеся практики совершения вызовов. В таком случае возможна миграция инфраструктуры с сохранением ключевых узлов (IP-телефония только для новых абонентов и связи между существующими АТС), линий связи и конечного оборудования (ядро телефонной сети переходит на IP-телефонию, часть абонентов используют аналоговые линии).

Для связи аналоговых линий с IP-сетью применяются FXS-шлюзы. Стандартная телекоммуникационная стойка на 18U позволяет подключить около 430 абонентов (с использованием шести универсальных абонентских шлюзов Eltex TAU-72.IP и патч-панелей для подключения абонентов). При необходимости обеспечения большей плотности подключения и аппаратного резервирования можно использовать специализированные решения, например, интегрированную платформу MSAN MC1000-PX. В базовом варианте указанное выше оборудование может быть подключено к IP-АТС в той же стойке, в результате чего формируется конвергентное решение для задач корпоративной телефонии.

Система, построенная на основе IP-АТС Asterisk, позволяет решать вопросы масштабирования без существенных финансовых затрат. Аналогичное же решение, реализованное средствами аналоговой телефонии, обойдется большими денежными затратами, обладая при этом определенными аппаратно-программными ограничениями (ограниченное количество слотов для плат расширения, необходимость приобретения лицензий и т.п.). В случае с подключением внешних линий, стоимость IP-решений также оказывается ниже стоимости настройки аналоговых АТС, с учетом необходимости оплаты лицензий и стоимости работ квалифицированного инженера.

Помимо стандартных PRI-каналов и GSM-линий, для IP-АТС возможно использование SIP-линий операторов IP-телефонии, что актуально с учетом внедрения Белтелекомом плат-

Библиотека БГУИР

формы передачи мультимедийного содержимого на основе протокола IP (IP Multimedia Subsystem, IMS). Для создания бюджетных VoIP GSM-шлюзов может использоваться решение на основе USB 3G-модемов.

В современных реализациях аппаратных АТС уже присутствуют функциональные возможности, позволяющие подключить SIP-транки [1], что требует приобретения лицензий или плат расширения [2], а сама настройка является сложной задачей [3].

Итоговое решение позволяет снизить практически до нуля стоимость подключения новых абонентов, позволяет отказаться от использования корпоративной мобильной связи, посредством использования личных смартфонов сотрудников, и использовать автоматическую маршрутизацию по наиболее дешевому маршруту. Хотя стоимость решений для подключения внешних линий к IP-АТС и дает выигрыш в сравнении с решениями для аналоговых АТС, необходимость приобретения аппаратной платформы для запуска программной АТС может привести к большим расходам (например, при закупке выделенных серверов). Для снижения затрат можно рассматривать решения на основе десктопных комплектующих, в ряде случаев используя уже имеющийся компьютерный парк организации. Подобная схема приводит лишь к увеличению числа точек отказа. Вопросы обеспечения надежности спроектированной подобным образом системы выходят на передний план.

Обеспечение отказоустойчивости систем на основе сетевых АТС

Традиционно отказоустойчивость повышают путем дублирования шлюзов и увеличения числа внешних каналов. Локальные сети, интернет-каналы и системы питания также резервируются или дублируются. Для этого существует масса методик и готовых решений. Однако при переходе к системам IP-телефонии, единой точкой отказа зачастую становится именно сам сервер Asterisk. Само ПО Asterisk, в особенности LTS-ветки, работает достаточно стабильно. Отказ систем приходится на утрату работоспособности аппаратных компонентов. Для решения этой проблемы предлагается использовать кластеризацию.

Кластеризация может быть выполнена различными способами и применяться с различными целями. В контексте задачи повышения надежности системы, применение кластеризации обусловлено низкой надежностью аппаратных компонентов. По умолчанию, Asterisk не содержит средств для кластеризации, схема дублирования сервиса должна быть реализована инженером самостоятельно. Достаточно популярным решением для таких случаев является использование программного продукта для виртуализации VmWare ESXi в качестве гипервизоров. Устанавливается и настраивается Fault-tolerance кластер с общим хранилищем, которое также можно сделать распределенным, используя средства свободной программной объектной сети хранения Ceph (рис. 1).

Рис. 1. Схема кластеризации системы виртуализации

Библиотека БГУИР

В случае падения одного из гипервизоров сервис продолжит работу. Даже не касаясь вопроса стоимости лицензий (которая в несколько раз превышает стоимость оборудования), старый парк персональных компьютеров не будет удовлетворять минимальным требованиям для организации подобной схемы работы. Решения на базе гипервизоров KVM (например, несколько хостов Proxmox и несколько хостов в качестве программно-определяемого хранилища) позволяют организовывать виртуализацию на основе ПК под управлением ОС Linux, однако использование любых технологий полной виртуализации влечет за собой излишние накладные расходы, что критично сказывается на кластере, ноды которого могут располагать по 512-1024 Мб устаревшей оперативной памяти типа DDR или DDR2. Под нодой в данном случае понимается рабочая единица в составе кластера, единичный сервер.

Для кластеризации сервисов на нодах, располагающих небольшим объемом ресурсов и высокой вероятностью отказа, стоит рассмотреть системы паравиртуализации. Популярным примером подобной системы является ПО для автоматизации развертывания и управления приложениями в среде виртуализации на уровне операционной системы Docker, которая позволяет создавать контейнеры с пользовательскими приложениями и гибко управлять ими, работая поверх операционной системы, лишь предлагая слой абстракции, изолируя пользовательские сервисы. Если рассматривать его в качестве платформы для создания кластера, то стоит обратить внимание на систему под названием Docker Swarm. Данный продукт позволяет управлять группой хостов docker-machine, быстро создавать необходимое количество экземпляров сервисов и поддерживать его на заданном уровне при внезапном падении отдельных нод (рис. 2).

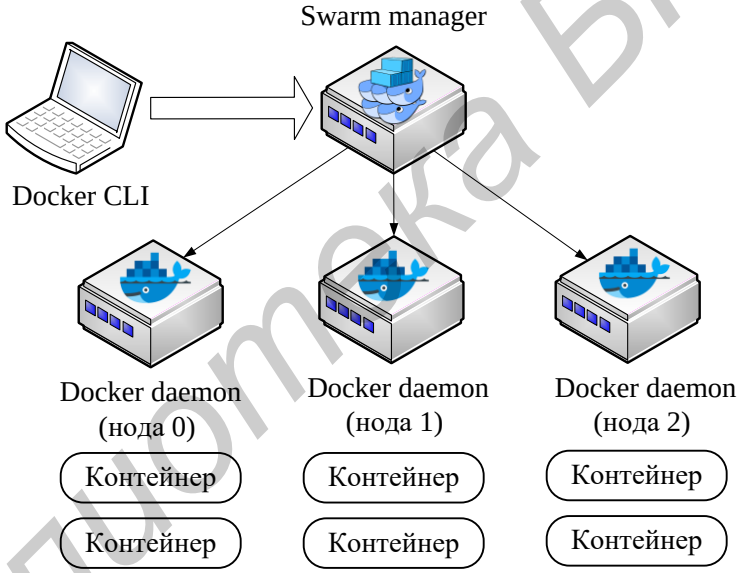

Рис. 2. Общая схема Docker-кластера

Так как в конечной системе будет использоваться ряд контейнеров, содержащих образ IP-АТС Asterisk, необходимо реализовать сервис-посредник, который займется проксированием SIP-трафика до конечных клиентов. В качестве устоявшегося решения, для этих целей применяется программный продукт Kamailio. В конечной схеме он выступит центральным сервисом, к которому будут обращаться клиенты для регистрации. Также этот сервис позволит интегрировать систему аутентификации с корпоративным Radius-сервером или LDAP-базой. Недостаток такой схемы в том, что формируется единая точка отказа в виде данного контроллера сеансов. Для решения проблемы используется программный продукт Keepalived, реализующий протокол VRRP под ОС Linux (сетевой протокол, предназначенный для увеличения доступности маршрутизаторов выполняющих роль шлюза по умолчанию), и позволяющий создавать виртуальный IP-адрес сервиса, который, в свою очередь, будет прослушивать пара нод Kamailio. Результатом будет кластеризация нод контроллера сеансов.

Для того, чтобы ноды Kamailio корректно работали в паре и распределяли нагрузку между Asterisk-нодами, необходимо использовать программное приложение kamailio-etcd-dispatcher. Это готовый преднастроенный образ Docker с etcd хранилищем (распределенным

Библиотека БГУИР

Key-Value хранилищем, которое запускается на каждой машине кластера и обеспечивает общий доступ практически ко всем данным в масштабе всего кластера), преднастроенный для кластеризации связки контейнеров Kamailio и Asterisk (рис. 3).

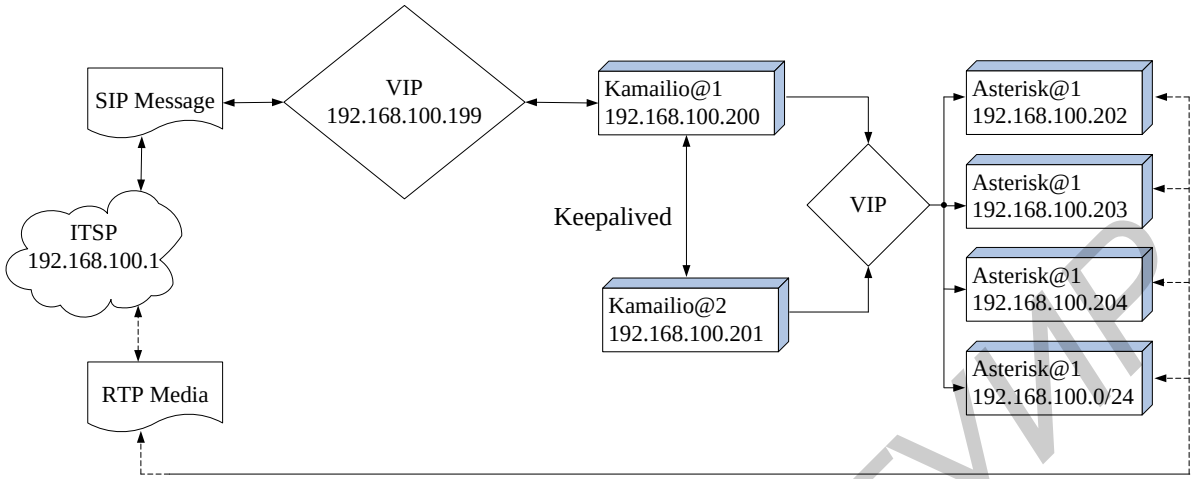

Рис. 3. Диаграмма обслуживания вызовов в кластере телефонии

Кластеризация сервисов позволит повысить надежность аппаратно-программных составляющих, и предоставит гибкие возможности для последующего масштабирования системы или, к примеру, свободного переноса контейнеров в ЦОД хостинг-провайдера.

Качество связи

Преимущественно, на качество передачи голоса влияет качество канала связи и используемый кодек (если не затрагивать вопрос конечных абонентских устройств). Для борьбы с большими задержками звука и замираниями необходимо настроить параметр QoS (качество обслуживания) для VoIP-трафика. На сегодняшний день, даже бытовые реализации сетевого оборудования располагают всем необходимым для приоретизации трафика телефонии. При выборе кодека стоит учитывать доступную ширину канала и особенности различных реализаций. В пределах кластера, для регистрации шлюзов можно использовать широкополосный кодек G.711, который имеет наивысшую оценку MOS (субъективной оценки качества передачи в телефонных сетях). Однако использование этого кодека конечными абонентами негативно скажется на полосе пропускания и для удаленных офисов, использующих ADSL-линии, настройка параметров QoS может быть малоэффективна. Решением может стать переход на использование кодека G.729. В отличии от кодека G.711, он занимает в 8 раз меньшую полосу (с учетом всех накладных расходов почти в три раза) при достойном уровне MOS. Недостатком этого решения является повышенная нагрузка на сервер Asterisk.

В предложенной схеме Asterisk сервера кластеризованы, следовательно, даже с учетом потенциально слабой конфигурации нод, дополнительная нагрузка не окажет существенного влияния на производительности всей системы.

Для мобильных абонентов, использующих сети Wi-Fi и 3G, можно рекомендовать кодек Opus, который специально разрабатывался для сред с изменяющейся полосой пропускания и качество которого зависит от ширины канала. На сегодняшний день он применяется в Skype и ряде иных решений для IP-телефонии. Также можно воспользоваться кодеком GSM. При достаточно низком показателе MOS, GSM-кодек прост в реализации и имеет низкие требования к полосе пропускания. Помимо указанных выше кодеков, инженер может воспользоваться любым из десятка прочих, свободно доступных для использования.

Безопасность

Архитектура систем IP-телефонии не содержит обязательных механизмов защиты. Сигнальный трафик и SIP-трафик передаются по сетям в открытом виде. Простые снифферы поз-

Библиотека БГУИР

воляют собрать и проанализировать данные, получить данные учетных записей пользователей и адреса ключевых сервисов. Аналогичная ситуация с медиа и RTP-потоками, перехватив которые можно прослушать разговор абонентов. Воспользовавшись простыми программными преобразователями текста в речь (Speech to Text) и поиском по ключевым словам, злоумышленник может в короткие сроки получить широкий спектр персональных данных пользователя.

Для VoIP решений существует ряд механизмов, повышающих защищенность конечного решения с помощью криптографических протоколов. Наиболее распространена комбинация протоколов является SIP/TLS (для обеспечения аутентификации) плюс SRTP (для обеспечения шифрования медиапотока и проверки подлинности). В таком случае, SIP-сессия инкапсулируется в SSL-поток, в процессе установления соединения происходит обмен ключами для последующего шифрования RTP-потока. Протокол ZRTP (менее распространен) позволяет обмениваться ключами в начале RTP сессии. Подобный механизм позволяет устанавливать прямые шифрованные каналы связи между абонентами, гарантируя безопасность передаваемых данных. Схема возможного подключения SIP-клиентов приведена на рис. 4.

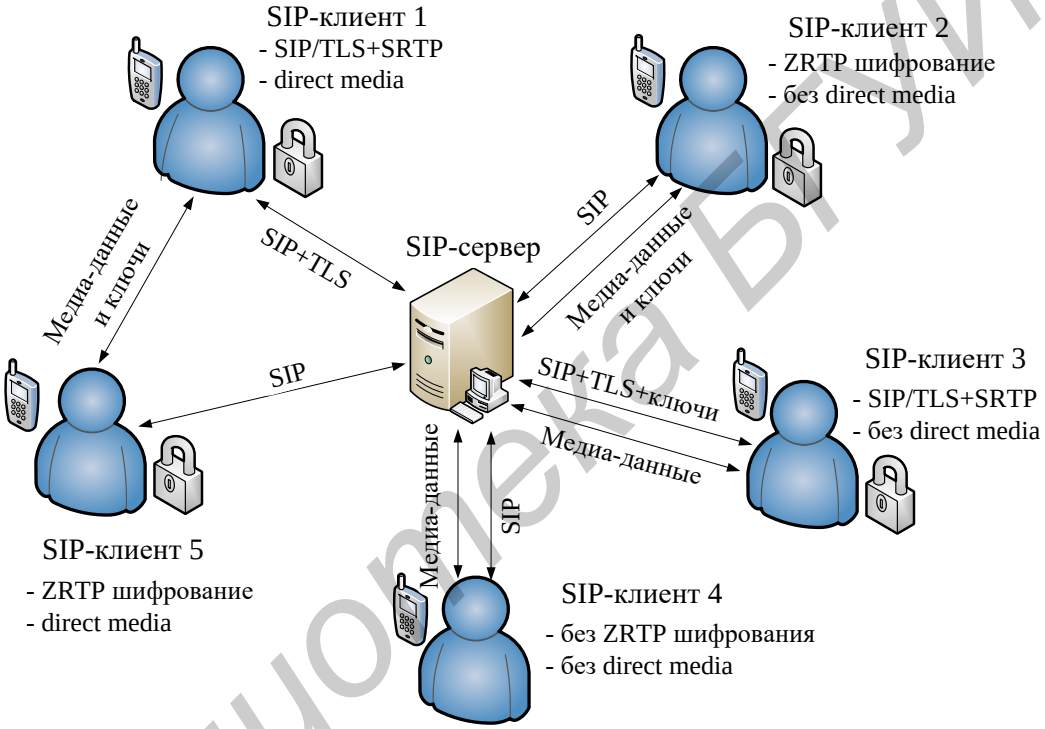

Рис. 4. Схема подключения SIP-клиентов

Предложенная схема организации связи обладает совокупностью уязвимостей, присущих каждому отдельному звену, Однако все применяемые механизмы (вплоть до используемых речевых кодеков) являются продуктами с открытыми исходными кодами, а значит организация, внедряющая у себя такие решения, может провести проверку исходного кода на наличие закладок и уязвимостей. Найденные уязвимости могут быть оперативно исправлены как разработчиками, так и пользователями. Сами средства используют безопасные механизмы обмена трафиком, например, Swarm передает данные только поверх протокола TLS.

Использование Linux-сред позволяет использовать широкий спектр средств для организации защиты сервисов. В их числе правила для корректной настройки межсетевых экранов (iptables, ufw) и блокировки подозрительной активности (fail2ban), системы мониторинга и оповещений об изменениях файлов начального уровня (Tripwire), а также общие системы мониторинга и оповещений (Zabbix). В связке с сервисами телефонии и системами предотвращения утечки информации можно реализовать оповещение ответственных лиц об инцидентах информационной безопасности в автоматическом режиме, посредством голосового вызова на личные мобильные телефоны.

Библиотека БГУИР

Заключение

Современные системы IP-телефонии и сопутствующие сервисы позволяют строить отказоустойчивые системы, покрывающие любые потребности предприятий, при этом не требуя серьезных финансовых вложений. Ввиду открытости применяемых программных решений, защищенность конечной схемы многократно возрастает, в сравнении с закрытыми решениями вендоров.

FAULT-TOLERANT CONSTRUCTION OF HYBRID CORPORATE TELEPHONE NETWORK

N.A. UCHAEV, S.N. PETROV, S.V. VLASYUK, T.A. PULKO

Abstract

The method of constructing a hybrid telephone network i. e. a network where modern telephony IP-systems works together with analog systems and communication lines is described. The analysis of the economic advisability of switching to digital communication lines, ensuring an acceptable quality of communication, also reliability and security is carried out. The software implementation Asterisk can be used as the core of a hybrid Private Branch eXchange.

Keywords: IP-telephony, clustering services, Asterisk IP-PBX, SIP traffic, RTP media, TLS, ZRTP.

Список литературы

1. Реализация Voip в системах Samsung OfficeServ. [Электронный ресурс]. Режим доступа: http://www.slideshare.net/tech99/voip-samsung-officeserv.
2. Лицензия для использования 1 IP-системного телефона или 1 IP Softphone. [Электронный ресурс]. Режим доступа: http://www.proftelecom.by/litsenziya_IP_panasonic_KX-NCS4201XJ_IP_Softphone.htm.
3. Настройка SIP линии на Panasonic TDE-100. [Электронный ресурс]. Режим доступа: http://ilyait.blogspot.com.by/2015/11/sip-panasonic-tde-100.html.

Библиотека БГУИР