УДК 004

М.Цішевський, магістр гр. КН-23М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АНАЛІЗУ ТА КОНСОЛІДАЦІЇ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЇ ВІРТУАЛІЗОВАНИХ ОБ'ЄДНАНИХ КОМУНІКАЦІЙ У МЕРЕЖІ

У статті розроблено програмне забезпечення, яке призначено для системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі. Метою розробки є дослідження та програмна реалізація системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі. Об'єктом дослідження є процес аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі. Предметом дослідження є методи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі. Методи дослідження базуються на методах аналізу та консолідації розподіленої інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Віртуалізовані рішення для реалізації об'єднаних комунікацій уже широко поширені на підприємствах, однак медіашлюзи – спеціалізовані апаратні пристрої, що виконують роль посередників між різними комунікаційними технологіями, – дотепер залишалися осторонь. Тепер і в цьому сегменті спостерігається тенденція до переходу на програмні засоби, а виходить, і до віртуалізації.

Крім скорочення витрат на апаратне забезпечення, віртуалізація володіє рядом інших переваг: насамперед це значне поліпшення доступності систем. Сучасні рішення для резервування й аварійного відновлення після збоїв (Backup/Disaster Recovery) при необхідності забезпечують безперебійний перехід на резервні системи й дозволяють скоротити час простою до мізерно малих значень – одне з найважливіших вимог для телефонії. Однак використання виділених апаратних пристроїв зв'язку нівелює вигоду, одержувану від високої доступності віртуальних телекомунікаційних рішень.

Тільки віртуалізовані медіашлюзи дозволяють успішно завершити реалізацію об'єднаних комунікацій (Unified Communications, UC) за допомогою програмних засобів, а виходить, створити повністю віртуалізовану інфраструктуру.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі.

– Дослідження системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі.

– Програмна реалізація системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

Об’єктом дослідження є процес аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

Предметом дослідження є методи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

Методи дослідження базуються на методах аналізу та консолідації розподіленої інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Віртуальні шлюзи підтримують функції гнучкого масштабування за рахунок виділення відповідних ресурсів. Від числа виділених процесорних ядер залежить продуктивність шлюзу, а виходить, і кількість паралельно використовуваних каналів. Якщо паралельних з'єднань більше ста, їх бажано розподілити між декількома системами. Для успішної передачі голосових даних за допомогою протоколу RTP потрібно забезпечити тверді параметри передачі даних у реальному часі, тому необхідно стежити за тим, щоб паралельно функціонуючі системи не гальмували роботу віртуальної машини, на якій виконується шлюз.

Сучасні середовища віртуалізації пропонують для цих цілей цілий ряд налаштувань, за допомогою яких можна здійснити необхідне тонке налагодження систем. У виняткових випадках, коли це неможливо або вимоги до якості роботи паралельних з'єднань особливо високі, цей же програмний шлюз можна встановлювати на фізичні серверні системи й експлуатувати без віртуалізації.

Віртуальні шлюзи дуже прості в установці – досить завантажити відповідний інсталяційний образ, і вже через десять хвилин шлюз готовий до первинного налаштування. Потім треба виконати резервне копіювання віртуальної машини, щоб у випадку відмови хост-системи її можна було швидко активувати на іншому хості. Тим самим підтримується високий рівень доступності, що традиційні апаратні комунікаційні контролери забезпечити не здатні. Використовуючи віртуальні телекомунікаційні сервіси для підтримки ключових бізнес-процесів, підприємства хочуть бути впевнені в їхній якості, масштабованості й надійності. Проект інтелектуальної мультисервісної мережі й голосової платформи націлений на створення для цього необхідних умов.

Широко обговорювані в останні роки хмарні комунікаційні сервіси стають реальністю. Їхнє застосування дозволяє підвищити ефективність бізнес-процесів по обслуговуванню клієнтів і збільшити продажі, що, поряд із гнучкістю й зручністю, є стимулом для переходу до нової моделі. Однак щоб бути визнаними замовниками, вони повинні ґрунтуватися на надійній операторській інфраструктурі. Насамперед, це стосується хмарних сервісів з інтегрованою телефонією, від якої традиційно очікують високого рівня доступності.

Складні послуги, попит на які росте, знаходять застосування при рішенні таких завдань, як розширення вирви продажів, підвищення якості обслуговування, лояльності й задоволеності клієнтів. Наприклад, підключившись до хмарного ЦОВ, територіально розподілені компанії одержують нові можливості для більше продуктивної роботи з потоками дзвінків, поліпшення різних параметрів бізнесу, обслуговування клієнтів і використання ресурсів.

Для обслуговування зростаючої клієнтської бази розгорнута масштабна інтелектуальна мультисервісная мережа (ІМС) і впроваджена вдосконалена система моніторингу. Завдяки наявному резерву продуктивності інтелектуальної голосової й хмарної платформи, пропоновані сервіси можуть бути адаптовані для компанії будь-якого розміру, що дозволить підтримувати високу якість сервісу при швидкому росту числа користувачів і збільшенні обсягу послуг, а також допоможе справлятися з піковими навантаженнями.

На базі вдосконаленої ІМС надається широкий спектр послуг зв'язку: віртуальна IP-АТМ, ЦОВ, багатоканальні телефонні номери, номери «8-800», телефонізація офісів і об'єднання філій під одним номером, послуги місцевого, міжміського й міжнародного

зв'язку – однак для їхнього використання потрібно організувати взаємодію з телефонними мережами загального користування (ТфОП). Внутрікорпоративні комунікації реалізуються переважно за допомогою SIP, а з'єднання із ТфОП задіються лише при обробці вхідних і вихідних місцевих, міжміських і міжнародних дзвінків.

Однак через збільшення кількості дзвінків з SIP-телефонів і шлюзів треба було збільшити число сполучних ліній із ТфОП у сегменті мережі – до 120 потоків E1. Цифрові потоки E1 використовуються для організації високоякісних голосових каналів, взаємодії систем VoIP з телефонними мережами операторів традиційного фіксованого й мобільного зв'язку. VoIP-шлюзи й SIP-телефони для SMB вибираються з урахуванням вимог до числа портів і схеми організації зв'язку в клієнта.

Віртуальна АТМ – це георозподілений кластер, доповнений кластером автентифікації й сигнальними серверами.

У частині телефонії SIP це вісім розподілених комутаторів SoftSwitch, що працюють як єдина система. Якщо один з комутаторів виходить із ладу або стає недоступним, забезпечувані ним з'єднання губляться, але кожної з абонентів може миттєво ініціювати повторний виклик. ВАТМ реалізована на платформі OpenSIPS і підтримує СОРМ власної реалізації, що повністю враховує специфіку хмарних телекомунікаційних сервісів

Для забезпечення безперервності бізнесу необхідне резервування компонентів інфраструктури. Це дозволило перетворити центральний технічний вузол у єдиний комплекс, розподілений по трьох площадках ЦОД з повним взаємним резервуванням всіх ключових підсистем, і забезпечити резервування каналів зв'язку між окремими елементами цього вузла, а також між центральним і регіональним вузлами.

За рахунок територіального рознесення вузлів зв'язку й організації дубльованих з'єднань між ними підвищила пропускну здатність, керованість, масштабованість і катастрофостійкість інфраструктури. Крім того, була розширена функціональність хмарної платформи, що підтримує телефонію (SIP-кластер), і поліпшені Web-Інтерфейс особистого кабінету з керуванням налаштуваннями послуг, мережа передачі даних і транспортне приєднання до операторів.

Всі системи в ЦОД функціонують у режимі повного взаємного резервування, для них реалізовані гаряче резервування конфігурацій і плани аварійного відновлення. Аварії й збої на одному з компонентів інфраструктури опорно-транспортної мережі не позначаються на її функціонуванні й не впливають на працездатність мережі в цілому. Наприклад, компоненти кластера АТМ (географічно розподілені комутатори SoftSwitch) і сигнальні сервери ОКС-7 перебувають на різних площадках ЦОД і працюють у режимі автоматичного взаємного резервування. Якщо один з комутаторів цієї єдиної АТМ виходить із ладу, дзвінки перерозподіляються між що залишилися. Відмова кожного із сигнальних серверів теж не впливає на якість сервісів – логіка спрацьовується на іншому сервері.

Типове рішення являє собою три площадки. Між трьома площадками – офісом компанії й двома географічно розподіленими ЦОД – створене відказостійке кільце SDH і організоване з'єднання «кожний з кожним» (full mesh), тобто перший вузол з'єднується із третім через другий без його участі, що ще більше підвищує катастрофостійкість. Рівень надійності орендованих площадок у ЦОД, де перебувають 60-70 серверів оператора, відповідає, відповідно до заяви оператора, Tier III.

У центральному офісі розташоване некритичне для бізнесу встаткування, а також розгорнуті тестового середовища для розробки й перевірки нового функціонала. Основну частину серверного парку становить устаткування SuperMicro – багатопроцесорні (2 і більше) сервери в корпусі 2U+. Для рішення деяких завдань застосовуються сервери HP. До складу встаткування входять, крім іншого, багатодискові системи зберігання даних.

На перерахованих площадках виконані пірінгові приєднання до мереж операторів зв'язку й провайдерам послуг передачі даних. Триває співробітництво з операторами зв'язку по резервуванню сигнальних каналів і їхньому підключенню до географічно розподіленого встаткування SDH. Таке резервування підвищує надійність сервісу й дозволяє територіально

розподіленим компаніям, що пред'являють високі вимоги до безперервності бізнесу, задіяти сервіси оператора в ключових бізнес-процесах.

Для підвищення надійності сервісів використовується повноцінна кластеризація з безліччю вузлів і балансуванням навантаження – програмної (засобами OpenSIPS і Web-додатків) і апаратної (на рівні SDH, компонентів мереж передачі даних, серверів і комутаторів). Бази даних, у яких утримуються налаштування BATM, файли CDR, статистика, журнали, дані для біллінгу й автентифікації абонентів, функціонують у режимі реплікації, а навантаження на них розподіляється виходячи із критичності додатків.

Розробка структурної схеми

Система централізованого моніторингу й керування територіально розподіленою мережею контролює роботу кластера АТМ, сервера конфігурацій, інтегрованої системи запобігання шахрайства (антифрод) і системи інтелектуального керування маршрутизацією трафіку. Кореляція інформації системи моніторингу з даними від бізнес-додатків (BATM, CRM і ЦОВ), використовуваних оператором у власних бізнес-процесах, наприклад з довжиною черги звернень користувачів, дозволяє виявляти аномалії у функціонуванні мережі й оперативно реагувати на них.

Програмно-апаратні комплекси й телекомунікаційна інфраструктура, використовувані для надання послуг, створювалися з метою забезпечення безперервності зв'язку й відказостійкості сервісів при різному навантаженні, у тому числі при відновленні сервісів і проведенні планових регламентних робіт. У цьому випадку робота більшої частини простих сервісів (дзвінки, комутація) не зупиняється. Підприємства, для яких безперервність бізнесу життєво важлива, одержали адекватне технічне рішення.

У якості одного з інструментів використовується система моніторингу й відстеження статусів різноманітних сервісів комп'ютерної мережі, серверів і мережного встаткування, що може перевіряти доступність стандартних сервісів без установки якого-небудь програмного забезпечення на хост-системі, а встановлювані програмні агенти дозволяють одержувати розширені дані – про завантаження процесора, використанні мережі, дисковому просторі й т.д. Крім того, програма підтримує моніторинг через SNMP.

Для спостереження й контролю за станом обчислювальних вузлів і служб застосовується також програма для моніторингу функціонування комп'ютерних систем і мереж з відкритим кодом. Вона сповіщає адміністратора, якщо якісь служби припиняють роботу. Для моніторингу BATM у регіонах використовуються їхні власні тригери.

За допомогою бізнес-правил, що налаштовуються, утиліта дозволяє програмувати різні дії для тих або інших ситуацій, аж до блокування окремих користувачів/абонентів при сплесках трафіку (система антифрод) з повідомленням системного адміністратора по різними каналами зв'язку, у тому числі й через SMS-шлюз.

Захист від DDoS реалізована на рівні компонентів мереж передачі даних: інформація про IP-адреси зловмисників регулярно обновляється за допомогою автоматизованих сценаріїв на підставі даних, одержуваних із загальнодоступних джерел.

З певною періодичністю плани аварійного відновлення (DR) мережі перевіряються на придатність і актуальність після внесення змін в архітектуру мережі, збільшення її масштабів і появи нових компонентів інформаційних систем. Перевірка плану по відновленню критичних систем проводиться в годинники найменшого навантаження. Резервне копіювання здійснюється залежно від типів даних і вимог до їхньої цілісності.

Канали для передачі голосової інформації у всіх містах присутності оператора резервуються, що дозволяє перенаправляти трафік у випадку аварії по іншому маршруті. Вузол кожної філії має не менш двох крапок приєднання до місцевих мереж телефонії. Крім того, для збільшення пропускної здатності мережі передачі даних при обробці внутрімережних потоків даних і поліпшення взаємодії з іншими операторами зв'язку були замінені мережні комутатори й граничні маршрутизатори.

Обробку всіх додаткових видів послуг п'ятого класу здійснює центральний комутатор, взаємодіючий з регіональними комутаторами четвертого класу й мультиплексорами.

Сигнальний трафік ОКС-7 управляється кластером з лінк-серверів. Централізована й база даних біллингу, що забезпечує миттєвий доступ до інформації про всі зроблені дзвінки.

Віртуальна АТМ

Принцип функціонування хмарної АТМ, що є одним з передових рішень у рамках IP-телефонії, проста: компанія використовує віртуальну телефонну станцію, «розміщену» на сервері провайдеру, причому функціонал АТМ можна настроїти під потреби свого бізнесу. Передача даних здійснюється за допомогою SIP- і VoIP-протоколів. Перші потрібні для передачі мультимедіа (відео), а другі – для голосового зв'язку. Всі дані зберігаються на хмарному сервері організації, що надає послугу.

Із цього випливають особливості підключення послуги: не потрібно прокладати додаткові проведення й здобувати складне дороге встаткування, досить лише стабільного доступу до Мережі. Таким чином, за невелику плату організація одержує всі можливості офісної міні-АТМ, а витрати на послуги зв'язку, тим часом, скорочуються в рази.

Можливості хмарної телефонії

Сучасний офіс бідує не тільки в якісному телефонному зв'язку, але й у додаткових функціях, які надає хмарна АТМ:

– Багатоканальний номер дозволяє приймати необмежене число дзвінків одночасно. Якщо всі оператори зайняті, клієнт «займає місце» у віртуальній черзі.

– Додаткові номери для всіх співробітників – простий і зручний спосіб зв'язку усередині компанії.

– Голосове меню дозволяє істотно знизити навантаження на секретаря або операторів. Клієнт одержує можливість набору додаткового номера й самостійно попадає до потрібного фахівця.

– Інтелектуальна переадресація – це не тільки звичайні функції перенапрямку дзвінків у випадках, «якщо зайнято» або «якщо немає відповіді», але й налаштування алгоритмів з'єднання залежно від часу доби, дня тижня й інших факторів.

– Інтеграція із сайтом, у першу чергу, містить у собі популярний сервіс «зворотний дзвінок», що дозволяє користувачам зв'язуватися з операторами прямо зі сторінок онлайн-ресурсу натисканням однієї клавіші.

– Складання деталізованих звітів про кількість і тривалість розмов.

– Відеодзвінки для багатьох стають заміною «живому» спілкуванню з колегами при географічній далекості філій або співробітників.

– Конференцзв’язок – зручне проведення групових переговорів і нарад на будь-яких відстанях.

– Голосова пошта дозволяє клієнтам залишати звукові повідомлення, які потім приходять на e-mail організації у вигляді аудіофайлу.

– Запис телефонних розмов, як показує практика, – необхідний сервіс для компаній, що займаються продажами, обслуговуванням і роботою із клієнтами. Це й постійний контроль над якістю виконання своїх обов'язків операторами, і можливість швидкого рішення проблем у випадку конфліктів і претензій.

– Електронний факс приймає повідомлення й документи так само, як і звичайний. Єдине розходження – вони надходять на e-mail у вигляді файлу й при необхідності друкуються на принтері.

– «Чорний список» обмежує небажані дзвінки.

Переваги віртуальної АТМ

Хмарна телефонна станція, крім зручності у використанні, має й інші, не менш важливі переваги. У першу чергу, ця висока якість IP-телефонії, значно перевищуючі показники стільникового зв'язка й аналогових каналів.

Але, мабуть, найважливішим для більшості є економічна перевага хмарних АТМ: поза залежністю від розміру компанії їхня організація не вимагає більших витрат. Не потрібні проведення й дороге встаткування, монтаж і технічна підтримка системи, спрощується процедура одержання прямого міського номера. Налаштування віртуальної АТМ із нуля

займають 5-30 хвилин часу й не вимагає спеціальних пізнань. Витрати на дзвінки теж істотно зменшуються – приміром, міжміський зв'язок обходиться до 70% дешевше, міжнародна – до 80%, а внутрішні дзвінки й зовсім стають безкоштовні.

Хмарна АТМ популярна серед компаній всіх розмірів і форматів. Індивідуальних підприємців і маленьких колективів залучає можливість швидко почати роботу. При цьому співробітники можуть виконувати свої обов'язки в будь-якій крапці земної кулі. У розпорядженні компанії буде прямий міський номер, що викликає довіра клієнтів і цілодобово доступний для дзвінків і повідомлень. При необхідності можна обійтися й без реального офісу – фактичне місце розташування фірми з віртуальної АТМ надійно приховано від що дзвонять.

При розширенні організації стають помітні й інші достоїнства IP-АТМ: наприклад, легке збільшення числа каналів виклику й внутрішніх номерів. Кілька філій легко поєднуються в мережу із загальним номером і зручною переадресацією до співробітника з будь-якого регіону.

Великі компанії за допомогою хмарної АТМ одержують можливість створення повноцінного call-центра при невеликих витратах, з повним контролем статистики дзвінків, легенею зміною налаштувань і записом всіх розмов.

Вибір постачальника будь-якої послуги вкрай важливий, а тим більше, коли мова йде про провайдер телефонного зв'язку. Підключення до IP-телефонії й установка віртуальної АТМ – справа нескладний і недовге, а от підбор оператора, що пропонує умови, що влаштовують, може затягтися. Приведемо кілька критеріїв для вибору хмарної станції.

В Інтернеті чимало відкликань від уже використовують послугу хмарної телефонної станції, тому, якщо у вас ще немає досвіду подібної діяльності, прочитайте уважно про всі сильні й слабкі сторони продукції тих або інших провайдерів.

Звичайно, у кожної компанії своя сфера діяльності й своїх вимог до провайдеру і його послуг, тому сліпо опиратися на чийсь досвід використання тої або інший хмарної АТМ не можна. Потрібно, виходячи із цілей вашої конкретної організації, вибрати саме той спектр послуг, які будуть необхідні вам. Інші можуть бути більш-менш корисним доповненням, але «базовий» пакет потрібно відбирати найбільше ретельно.

Для рекламних, юридичних або ріелторських агентств, навіть невеликих, украй важлива послуга «віртуальний секретар», у великій компанії, де офіси найчастіше перебувають у різних містах, а те й країнах, не обійтися без внутрішньої корпоративної мережі. Власники інтернет-магазинів повинні задуматися про організацію call-центра, а банкам і медичним центрам буде корисно підключення послуги «гарячої лінії».

Отже, після того, як ви визначилися із провайдером і вибрали потрібний пакет послуг, залишається ще одна немаловажна процедура – підключення до того або іншого тарифу. У кожного постачальника є тариф-«база», що містить у собі, крім прямого багатоканального міського номера, інтелектуальне голосове меню й голосову пошту, можливість занесення в «чорний список», кілька внутрішніх ліній, сховище для записів розмов. Базовий тариф може бути розширений у будь-який момент. Деякі компанії пропонують можливість налаштування індивідуального тарифу, адаптованого під всі ваші вимоги, однак така послуга, як ви розумієте, буде не з дешевих.

Багато які аналітики ринку послуг зв'язки сходяться в тому, що IP-телефонія поступово витісняє аналогову й через кілька років майже не залишиться компаній, що не використовують віртуальні АТМ. Це пояснюється тим, що подібні рішення дозволяють легко управляти вхідними й вихідними дзвінками, організовувати call-центри й скорочувати витрати на зв'язок як великим організаціям, так малому й середньому бізнесу. Спробуйте самі й переконаєтеся в тому, що хмарні АТМ набагато вигідніше й простіше у використанні, ніж застаріваючі аналогові системи.

Розглянемо структурну схему системи. Почнемо з розгляду пристроїв складових системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

Гібридні мережні пристрої. Як правило, використовують маршрутизатори, які містять як порти для передачі даних (Ethernet), так і голосові порти (FXS або FXO) – фактично вони є гібридом маршрутизатора й адаптера або шлюзу. Гібридний мережний пристрій може застосовуватися для створення корпоративної системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі, з'єднуючи офісні УПАТМ через мережу Інтернет.

При такій схемі організації прийдеться мати втрати на придбання шлюзів, а також на створення служб експлуатації. При цьому звичайний провайдер послуг мережі Інтернет не зможе гарантувати надання необхідної смуги пропущення, тому що по каналу передаються й дані, і мова. Щоб уникнути подібних проблем доцільніше скористатися послугами ITSP-провайдеру. Провайдери системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі гарантують не тільки доступ до шлюзового встаткування, але й необхідну смугу пропущення.

ITSP надають можливості для викликів наступних типів сценаріїв:

– "Від телефону до телефону". Виклик іде зі звичайного телефонного апарата до комплекту встаткування ITSP і через мережу Інтернет доходить до іншого ITSP, що здійснює зворотні перетворення.

– "Від телефону до комп'ютера". Для організації переважніше встановити на кожне автоматизоване робоче місце локальної мережі програмне забезпечення системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі й мікрофон (більшість сучасних ПК уже мають звукові адаптери й акустичні системи) і підключити локальну мережу до ITSP.

– "Від комп'ютера до телефону". Шлюз в IP-системі виконує значне функціональне навантаження. Шлюз призначений для перетворення аналогових мовних і службових сигналів у цифрову послідовність, організації із цієї послідовності пакетів глобальної мережі Інтернет і передачі її в мережу, прийому пакетів і відновлення кодової послідовності цифрових, мовних і службових сигналів і їхнього перетворення в аналогову форму, а також рішення інших завдань, пов'язаних з організацією інтерфейсів, генеруванням і детектуванням сигналів абонентської сигналізації, керуванням режимами телефонних переговорів і деяких інших.

Шлюзи можуть установлюватися на серверах інтернет-провайдерів, міських телефонних станціях, АТМ для установ, серверах локальних обчислювальних мереж, веб-серверах компаній, що потребують в організації голосових гарячих ліній, служб технічної підтримки, діалогових довідкових служб і т.д. Також шлюзи можуть входити до складу маршрутизаторів.

Залежно від схеми організації зв'язку архітектура шлюзу може мінятися, можуть додаватися й інтегруватися деякі функції, виконувані шлюзом, додаватися або мінятися інтерфейси. Однак головні завдання шлюзу – забезпечення якісного дуплексного телефонного спілкування абонентів у режимі пакетної передачі й комутації цифрових сигналів – зберігаються поза залежністю від варіанта.

Варто помітити, що розглянуті вище базові схеми можуть комбінуватися. Можливі різноманітні способи організації IP-телефонного зв'язку з використанням шлюзів, розміщених у функціонально різних точках мережі. Однак у кожному разі шлюз у кожному з варіантів з'єднання буде ключовим елементом.

Рисунок 1 – Структурна схема системи

Крім терміналів користувачів, які підключаються до мереж аналогової телефонії, існують також і сервери керування. До серверів керування відносяться:

– SIP-сервер (він же SIP-Proxy). Веде список підключених до нього й зареєстрованих клієнтів для того, щоб брати участь у пошуку абонента для з'єднання й керування сеансом з'єднання.

– Проксі для вихідних з'єднань (outbound proxy). Потрібний для обходу клієнтом обмежень, що накладаються використанням трансляції адрес (NAT).

– STUN-сервер. Спеціальний сервер, що дозволяє клієнтові визначити використовуваний тип трансляції адрес для того, щоб спробувати обійти його обмеження без використання проксі для вихідних з'єднань.

– DNS (Domain Name Service). Відомий протокол, що в SIP застосовується для знаходження SIP-сервера для заданого домену шляхом публікації спеціальних DNS-записів у зоні цього домену.

Окремим типом сервера є SIP-агент. Це програма, що безпосередньо займається прийомом і здійсненням дзвінків. Вона містить у собі кодеки й взаємодіє з кінцевим користувачем. SIP-агент убудований у кожний SIP-термінал – будь то програмний телефон, шлюз або апаратний VoIP-телефон. SIP-агенти взаємодіють між собою прямо (у випадку використання технології SIP Peer to Peer) або через SIP-сервери й проксі для вихідних з'єднань.

Помітимо, що сам протокол SIP голос не передає. Але він використовується для установки сеансу зв'язку й керування ім. Самі голосові дані передає протокол RTP. Причому працюють вони паралельно, але по різних портах: SIP координує сесію, а RTP передає голос.

Без використання RTP SIP не може "передавати" голос, а без SIP – RTP не зможе встановити сеанс зв'язку.

Типи погроз у мережах системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі

Існує кілька основних типів погроз, що представляють небезпеку в мережах системи аналізу та консолідації розподіленої інформації віртуалізованих об'єднаних комунікацій у мережі:

– Прослуховування. У момент передачі конфіденційної інформації про користувачів (ідентифікаторів, паролів) або конфіденційних даних по незахищених каналах існує можливість прослуховування й зловживання ними в корисливих цілях зловмисником.

– Маніпулювання даними. Дані, які передаються по каналах зв'язку, у принципі можна змінити.

– Підміна даних про користувача відбувається у випадку спроби видачі одного користувача мережі за інший. При цьому виникає ймовірність несанкціонованого доступу до важливих функцій системи.

– Відмова в обслуговуванні (denial of service – DoS) є одніє. з різновидів атак порушників, у результаті якої відбувається вивід з ладу деяких вузлів або всієї мережі. Вона

здійснюється шляхом переповнення системи непотрібним трафіком, на обробку якого йдуть всі системні ресурси. Для запобігання даної погрози необхідно використовувати засіб для розпізнавання подібних атак і обмеження їхнього впливу на мережу.

Базовими елементами в області безпеки є:

– автентифікація;
– цілісність;
– активна перевірка.

Застосування розширених засобів автентифікації допомагає зберегти в недоторканності вашу ідентифікаційну інформацію й дані. Такі засоби можуть ґрунтуватися на інформації, що користувач знає (пароль).

Цілісність інформації – це здатність засобу обчислювальної техніки або автоматизованої системи забезпечувати незмінність інформації в умовах випадкового й (або) навмисного перекручування (руйнування). Під погрозою порушення цілісності розуміється будь-яка навмисна зміна інформації, що зберігається в обчислювальній системі або передаваємій з однієї системи в іншу. Коли зловмисники навмисно змінюють інформацію, говориться, що цілісність інформації порушена. Цілісність також буде порушена, якщо до несанкціонованої зміни приводить випадкова помилка програмного або апаратного забезпечення.

І, нарешті, активна перевірка означає перевірку правильності реалізації елементів технології безпеки й допомагає виявляти несанкціоноване проникнення в мережу й атаки типу DoS. Активна перевірка даних діє як система раннього оповіщення про різні типи неполадок і, отже, дозволяє вжити попереджуючі заходи, поки не нанесений серйозний збиток.

Особливості системи безпеки в системі аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі

У системі аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі повинні забезпечуватися два рівні безпеки: системний і викличний.

Для забезпечення системної безпеки використовуються наступні функції:

– Запобігання неавторизованого доступу до мережі шляхом застосування поділюваного кодового слова. Кодове слово одночасно обчислюється по стандартних алгоритмах на ініціюючій і кінцевій системах, і отримані результати порівнюються. При встановленні з'єднання кожна із двох систем системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі спочатку ідентифікує іншу систему; у випадку принаймні одного негативного результату зв'язок переривається.

– Списки доступу, у які вносяться всі відомі шлюзи системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

– Запис відмов у доступі.

– Функції безпеки інтерфейсу доступу, включаючи перевірку ідентифікатора й пароля користувача з обмеженням доступу по читанню/запису, перевірку прав доступу до спеціального WEB-серверу для адміністрування.

– Функції забезпечення безпеки виклику, включаючи перевірку ідентифікатора й пароля користувача (необов'язково), статус користувача, профіль абонента.

При встановленні зв'язку шлюзу з іншим шлюзом своєї зони виробляється необов'язкова перевірка ідентифікатора й пароля користувача. Користувач у будь-який час може бути позбавлений права доступу.

Дійсно, при розробці протоколу IP не приділялося належної уваги питанням інформаційної безпеки, однак згодом ситуація мінялася, і сучасні додатки, що базуються на IP, містять досить захисних механізмів. А рішення в області системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі не можуть існувати без реалізації стандартних технологій автентифікації й авторизації, контролю цілісності й шифрування й т.д. Для наочності розглянемо ці механізми в міру того, як вони

задіються на різних стадіях організації телефонної розмови, починаючи з підняття слухавки й закінчуючи сигналом відбою:

– Телефонний апарат. В системі аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі, перш ніж телефон пошле сигнал на встановлення з'єднання, абонент повинен увести свій ідентифікатор і пароль на доступ до апарата і його функцій. Така автентифікація дозволяє блокувати будь-які дії сторонніх і не турбуватися, що чужі користувачі будуть дзвонити в інше місто або країну за ваш рахунок.

– Установлення з'єднання. Після набору номера сигнал на встановлення з'єднання надходить на відповідний сервер керування дзвінками, де здійснюється цілий ряд перевірок з погляду безпеки. У першу чергу засвідчує дійсність самого телефону – як шляхом використання протоколу 802.1x, так і за допомогою сертифікатів на базі відкритих ключів, інтегрованих в інфраструктуру системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі. Така перевірка дозволяє ізолювати несанкціоновано встановлені в мережі IP-телефони, особливо в мережі з динамічною адресацією. Однак автентифікацією телефону справа не обмежується – необхідно з'ясувати, чи надано абонентові право дзвонити по набраному їм номеру. Це не стільки механізм захисту, скільки міра запобігання шахрайства. Якщо інженерові організації не можна користуватися міжміським зв'язком, то відповідне правило відразу записується в систему керування дзвінками, і з якого би телефону не здійснювалася така спроба, вона буде негайно припинена. Крім того, можна вказувати маски або діапазони телефонних номерів, на які має право дзвонити той або інший користувач. У випадку ж з IP-телефонією проблеми зі зв'язком, подібні до перевантажень ліній в аналоговій телефонії, неможливі: при грамотному проектуванні мережі з резервними з'єднаннями або дублюванням сервера керування дзвінками відмова елементів інфраструктури системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі або їхнє перевантаження не робить негативного впливу на функціонування мережі.

– Телефонна розмова. В системі аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі рішення проблеми захисту від прослуховування передбачалося із самого початку. Високий рівень конфіденційності телефонного зв'язку забезпечують перевірені алгоритми й протоколи (DES, 3DES, AES, IPSec і т.п.) при практично повній відсутності витрат на організацію такого захисту – всі необхідні механізми (шифрування, контролю цілісності, хешування, обміну ключами й ін.) уже реалізовані в інфраструктурних елементах, починаючи від IP-телефону й закінчуючи системою керування дзвінками. При цьому захист може з однаковим успіхом застосовуватися як для внутрішніх переговорів, так і для зовнішніх (в останньому випадку всі абоненти повинні користуватися IP-телефонами). Однак із шифруванням зв'язаний ряд моментів, про які необхідно пам'ятати, впроваджуючи інфраструктуру VoIP. По-перше, з'являється додаткова затримка внаслідок шифрування/дешифрування, а по-друге, ростуть накладні витрати в результаті збільшення довжини переданих пакетів.

– Невидимий функціонал. Дотепер ми розглядали тільки ті небезпеки, яким піддана традиційна телефонія і які можуть бути усунуті впровадженням системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі. Але перехід на протокол IP несе із собою ряд нових погроз, які не можна не враховувати. На щастя, для захисту від цих погроз уже існують рішення, технології й підходи, які добре зарекомендували себе. Більшість із них не вимагає ніяких фінансових інвестицій, будучи вже реалізованими в мережному встаткуванні, що і лежить в основі будь-якої інфраструктури системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі. Найпростіше, що можна зробити для підвищення захищеності телефонних переговорів, коли вони передаються по тій же кабельній системі, що й звичайні дані, – це сегментувати мережу за допомогою технології VLAN для усунення можливості прослуховування переговорів звичайними користувачами. Гарні результати дає використання для сегментів системі аналізу та консолідації розподіленої інформації

віртуалізованих об’єднаних комунікацій у мережі окремого адресного простору. І, звичайно ж, не варто скидати з рахунків правила контролю доступу на маршрутизаторах (Access Control List, ACL) або міжмережних екранах (firewall), застосування яких ускладнює зловмисникам завдання підключення до голосових сегментів.

– Спілкування із зовнішнім миром. Якої би переваги IP-телефонія не надавала в рамках внутрішньої мережі, вони будуть неповними без можливості здійснення й прийому дзвінків на міські номери. При цьому, як правило, виникає завдання конвертації IP-трафіка в сигнал, переданий по телефонній мережі загального користування (ТфОП). Вона вирішується за рахунок застосування спеціальних голосових шлюзів (voice gateway), що реалізують і деякі захисні функції, а сама головна з них – блокування всіх протоколів системі аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі (H.323, SIP і ін.), якщо їхнього повідомлення надходять із неголосового сегмента. Для захисту елементів голосової інфраструктури від можливих несанкціонованих впливів можуть застосовуватися спеціалізовані рішення – міжмережні екрани (MME), шлюзи прикладного рівня (Application Layer Gateway, ALG) і прикордонні контролери сеансів (Session Border Controller). Зокрема, протокол RTP використовує динамічні порти UDP, відкриття яких на міжмережному екрані приводить до появи зяючої діри в захисті. Отже, міжмережний екран повинен динамічно визначати використовувані для зв'язку порти, відкривати їх у момент з'єднання й закривати по його завершенню. Інша особливість полягає в тому, що ряд протоколів, наприклад, SIP, інформацію про параметри з'єднання розміщає не в заголовку пакета, а в тілі даних. Тому пристрій захисту повинне бути здатне аналізувати не тільки заголовок, але й тіло даних пакета, отримуючи з нього всі необхідні для організації голосового з'єднання відомості. Ще одним обмеженням є складність спільного застосування динамічних портів і NAT.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

– Досліджена система аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

– На основі отриманих результатів досліджень створена програмна реалізація системи аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання аналізу та консолідації розподіленої інформації віртуалізованих об’єднаних комунікацій у мережі. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
2. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
3. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w
4. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.

5. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) – 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
6. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
10. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
11. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
12. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
13. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
14. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
15. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
16. Zhurakovskyi, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
17. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
18. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
19. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.517-522.
20. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
21. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
22. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
23. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
24. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.