Agat SBC. Ключевые возможности.

Содержит детальное описание основных функциональных возможностей Agat SBC.

Version 2.2.4-a17, июль 2023

Содержание

1. Ключевые функции SBC

1. Георасределенная, катастрофоустойчивая единая SBC предприятия
    a. Единый мониторинг доступности и нагрузки
    b. Централизованное разграниченное по правам управление всеми элементами
    c. Общие распределяемые лицензии
    d. Открытый REST API для интеграций
2. Обеспечение функций безопасности обслуживания
    a. внешних голосовых транков к операторам связи
    b. подключения внешних (аутсорсинговых) сотрудников
    c. внутренних транков от корпоративных IP-АТС
    d. подключения внутренних сотрудников по SIP-устройствам и WebRTC приложениям
3. Транскодирование и шифрование медиа трафика
    a. Поддержка RTP и SRTP как на внешних и внутренних линиях
    b. Прозрачная работа механизма транскодирования без доп. Лицензирования
    c. Обработка видео потоков
4. Удаленное подключение сотрудников организации
    a. через SIP-устройства
    b. через Web-приложение и WebRTC телефон
    c. через SIP-телефон на Android, iOS с едиными правилами работы внутри и вне офиса
5. Единые правила обслуживания входящих вызовов от клиентов
    a. Единое приветствие
    b. Единые правила распределения вызовов между корпоративными IP-АТС
6. Обеспечение безопасности не голосовых WebService каналов
    a. WebHook по http/https и WebSocket по ws/wss
    b. Поддержка языков xml, json, soap, plain text
    c. Поддержка аутентификации ldap/AD, sso, soap, otp

2. Георазпределенная, катастрофоустойчивая единая SBC предприятия

Agat SBC представляет собой единое георазпределенное решение по обеспечению отказоустойчивости и защиты периметра телефонной SIP сети предприятия. Сервера SBC могут располагаться в необходимом количестве узлов периметра сети, работать как единое целое, обеспечивать высокую доступность (HA), балансировку нагрузки и динамическое перетекание в случае сбоев. Добавление нового сервера не приводит к прерыванию обслуживания и необходимости перезагрузки уже запущенных узлов.

Все модули Agat SBC работают в режиме `active-active`, обеспечивая необходимый уровень катастрофоустойчивости и защищенности периметра сети с возможностью балансировки, перетекания и динамического распределения нагрузки по внешним транков и внутренним узлам защищаемой сети.

Лицензионная политика не ограничивает количество и георазпределенность узлов SBC, обеспечивает возможность горячего перераспределения между элементами единой системы, включая дублирование и перетекание каналов связи.

Централизованный мониторинг и управление позволяет выполнять регламентные действия и изменения настроек из любой точки развернутой системы Agat SBC. Распределение измененных настроек происходит автоматически по всем узлам без прерывания обслуживания в считанные секунды. Система логирования позволяет проанализировать кто, когда и что изменил с возможностью отката на предыдущие настройки.

Agat SBC имеет открытые интерфейсы взаимодействия с другими Информационными Системами в рамках единого IT пространства предприятия по открытым протоколам:

- REST API (с поддержкой языков `xml` и `json`),
- ldap (с поддержкой `Active Directory`),
- SQL (нативная поддержка `PostgreSQL` с возможностью подключиться к любым СУБД через `ODBC`),
- nfs, (s)ftp и S3 для доступа к файлам.

Интеграция с системами централизованного мониторинга (например `Zabbix` или `Splunk`) позволяет автоматизировать анализ доступности узлов, достаточности ресурсов для обслуживания всех звонков, а также иметь исторические отчеты распределения нагрузки и количества обслуживаемых звонков.

3. Обеспечение функций безопасности обслуживания

Agat SBC обеспечивает защиту периметра телефонной сети предприятия от различных попыток несанкционированного доступа, взлома, осуществления запрещенных вызовов. Защита работает на всех интерфейсах системы — внешних и внутренних.

Архитектурно Agat SBC разрывает SIP-диалоги между любыми участниками через внутреннее безопасное замыкание через себя, включая возможность георасределенного использования (когда один участник разговора подключен к одному серверу SBC, а второй участник к другому серверу SBC в другой области единой системы). Такой подход позволяет полностью скрыть топологию защищаемых телефонных сетей, гарантировать отсутствие атак из-вне на корпоративную телефонию. Встроенная логика анализа и контроля двухуровневой маршрутизации гарантирует только разрешенные звонки в любом направлении, с возможностью применения единых корпоративных политик безопасности и доступа из учетной системы.

Контроль доступа и защита осуществляется для

- внешних линий (SIP-транков), подключенных к операторам SIP телефонии,
- внутренних линий (SIP-транков), подключенных к защищаемых IP-АТС предприятия,
- подключений удаленных сотрудников через публичные сети через SIP-аппараты и WebRTC клиенты,
- прямого подключения сотрудников через SIP-аппараты и WebRTC клиенты.

В рамках единой георасределенной системы Agat SBC в режиме `active-active` возможно обеспечить достаточный уровень доступности корпоративной телефонии в условиях `DoS/DDoS` атак. Один кластер SBC позволяет обрабатывать до 300 cps (звонков в секунду) длительной нагрузки и до 600 cps краткосрочной нагрузки, при этом блокировка злоумышленников происходит за первые несколько секунд ненормального поведения и далее не утилизирует пропускную способность кластера.

Встроенный `Web-портал` позволяет подключаться удаленным сотрудникам к корпоративной телефонной сети через нативное Web-приложение `Point` (Рабочее место сотрудника) или разрешенные SIP-устройства (аппаратные и программные). Web-приложение `Point` использует технологию `WebRTC`, имеет открытую архитектуру и может быть интегрировано в единую систему аутентификацию - LDAP/AD, SSO, двухфакторное подтверждение через SMS/e-mail или другими способами. Web-портал построен на web-server `cowboy`, позволяющий выдерживать большую нагрузку и дополнительно создана обвязка безопасности от попыток взлома, переборов паролей и перехвата трафика.

При необходимости Agat SBC может защищать не только SIP/RTP трафик, но и неголосовые WebService каналы предоставления ограниченной корпоративной информации внешним сервисам по протоколам `http(s)`, `ws(s)` через распределенные REST `endpoint`.

4. Транскодирование и шифрование медиа трафика

Agat SBC поддерживает различные аудио (pcmu, pcma, g.722, gsm, g.729, speex 8000/16000/32000, g.726-16/24/32/40, iLBC, opus mono/stereo) и видео (h.263, h.263-1998, h.264, vp.8, vp.9) кодеки.

При обработке голосового трафика система автоматически выбирает наиболее подходящие кодеки с каждой стороны диалога, при необходимости использует транскодирование, переключается между режимами работы. Все изменения SDP-диалога происходят на лету без прерывания голосового потока с единой сквозной записью разговора. Использование режима транскодирования является базовой не лицензируемой функцией системы.

Поддержка протокола SRTP позволяет включить дополнительную защиту от прослушивания трафика как на внутренних линиях, так и для внешних подключений.

При обработке видео потоков, по-умолчанию SBC выбирает кодеки для работы в скозном режиме (режим pass-through). При необходимости можно включить режим транскодирования видео потоков.

Для обработки передачи изображений (факсов) в SBC реализованы протоколы t.30, t.38, g.711 fax pass-through. Передача факсов может осуществляться между оконечными устройствами через SBC или терминироваться на встроенном факс-сервере с последующей передачей адресату в виде e-mail или ссылки на файл.

5. Удаленное подключение сотрудников организации

Удаленные сотрудники могут подключаться к ресурсам корпоративной телефонии через Agat SBC. При этом номер сотрудника может сохраняться или отличаться, удаленное подключение может работать паралельно с внутренним номером, вместо внутреннего номера или полностью независимо.

Удаленные сотрудники могут использовать разрешенные политиками безопасности SIP-аппараты, SIP-программные клиенты (включая ПО под Android, iOS), а также WebRTC решения.

Agat SBC имеет в поставке web-приложение Point, которое является полноценным телефоном сотрудника, со справочником телефонов, возможностью видео-звонков и трансляции экрана, многосторонних конференций, получения доступа к статистики и записям разговоров. Также приложение Point или отдельно WebRTC телефон могут быть встроены в сторонние решения или быть интегрированы в единое рабочее пространство сотрудника.

При подключении удаленного сотрудника Agat SBC может работать в двух режимах:

- для каждой регистрации удаленного сотрудника пробрасывать зеркальную регистрацию в корпоративную АТС (каскадный режим работы)
- все регистрации удаленных сотрудников обслуживать в рамках единых подключений к корпоративной АТС

За счет удаленного подключения сотрудников можно реализовать функцию роуминга для сотрудников, работающих в разных офисах. Также можно реализовать функционал, когда все сотрудники работают с корпоративной телефонией с приложений на своих мобильных телефонах вне зависимости от своего местоположения.

Дополнительную безопасность подключения удаленных сотрудников может обеспечить:

- Интеграция с AD по групповым политикам и проверки что сотрудник работает в компании
- Дополнительная проверка через одноразовые пароли, отправляемые на корпоративную почту
- Уведомления ответственным о превышении порогов активности удаленным подключением.

6. Единые правила обслуживания входящих вызовов от клиентов

В геораспределенной инфраструктуре поддерживать единые IVR обслуживания входящих звонков от клиентов бывает затруднительной задачей, особенно при необходимости менять алгоритмы обработки. Agat SBC может обеспечить обработку входящих звонков через IVR сценарии, а механизм синхронизации настроек в считанные секунды синхронизирует любые изменения между всеми узлами.

Подсистема IVR позволяет выстраивать многоуровневые голосовые меню, интегрироваться с сервисами ASR и TTS от Яндекс, получать информацию от внутренних информационных систем и выстраивать персонализированное обслуживание для каждого звонка, включая индивидуальное приветствие, проигрывание индивидуальных предложений или предположений о наиболее вероятных запросах клиента.

Результатом выполнения IVR может стать переключение в Контактный центр (наиболее подходящий по метрикам реального времени для обслуживания этого запроса), на групповые номера или на персонального менеджера. А если, например, у клиента в CRM системе установлен признак «не соединять с сотрудниками», то клиента можно отправить на голосовую почту или записать обращение и отправить в e-mail секретарю.

Данный функционал позволяет объединить все подразделения в единые правила обслуживания, выделить отдельные линии / номера / клиентов в приоритетное обслуживание и расширить функционал части устаревших АТС.

Функционал является отдельно лицензируемым параметром в рамках всей системы - ограничивается максимальное количество создаваемых IVR-сценариев, но не ограничивается его использование.

Создается сценарий в web-приложении Редактор сценариев, который представляет собой no-code/low-code визуальный интерфейс. При сохранении измененного сценария система автоматически сохраняет предыдущую копию для возможности откатиться назад.

7. Обеспечение безопасности не голосовых WebService каналов

В корпаративной IT инфраструктуре SBC защищает не только голосовой трафик, но и WebService внешние взаимодействия.

Agat SBC обеспечивает защиту неголосовых WebService каналов предоставления информации внешним системам по `REST API` запросам. Данный функционал работает в георасределенной среде с возможностью быстрого применения изменений на всех серверах системы, логирования успешных изменений настроек с возможностью быстрого отката назад.

Защищаемые сервисы могут работать по протоколам `http/https` и `ws/wss`. При получении запроса происходит следующая его обработка

- проверка на безопасность инициатора запроса
- проверка на безопасность данных (например на `otp` пароль или `OAuth2`, предотвращающий возможность влинивания в диалог третьей стороны)
- логирование запроса и инциатора
- получение данных из внутренней информационной системы от имени одного из SBC серверов
- модификация данных перед отправкой (фильтрация, изменение формата, транслитерация и т.д.) и их нормализация
- возможно дополнительная безопасность в виде шифрование данных, hash-подпись для гарантии неизменности ответа и генерация `otp` для следующего обращения
- логирование подготовленного ответа
- отправка ответа на запрос, обычно используются форматы `json`, `xml`, `plain text`.

При необходимости можно обеспечить агрегацию данных для ответа из различных внутренних информационных систем, ldap/AD каталогов, файлов.

Пропускная способность подсистемы — до 300 запросов в секунду на один узел и до 10'000 запрос в секунду на один кластер (сервера в рамках одного ЦОД). Фактическая максимальная нагрузка зависит от сложности обработки и нормализации ответа.

Защита от несанкционированного доступа, DoS/DDoS атак обеспечивается внутренними средствами Agat SBC с возможностью отслеживать попытки взлома в единой системе мониторинга.

8. Пропускная способность SBC

1. На одном сервере (4*vCPU 2,5GHz, 6GB RAM, 40Gb HDD)
    a. до 250 единовременных разговоров без транскодинга
    b. до 200 единовременных разговоров с транскодингом
2. В одном кластере (сайте)
    a. до 32 серверов
    b. до 30'000 регистраций внешних сотрудников на одном кластере
    c. до 300 cps (call per seconds) на одном кластере (в пике до 600 cps)
3. В единой системе
    a. до 96 кластеров (сайтов)
    b. до 5000 доменов

9. Основные функции.

9.1. Функции платформы

1. Отказоустойчивость
    a. Объединение нескольких серверов ЦОД в единый функциональный кластер на уровне приложения (Сайт)
    b. Отсутствие единой точки отказа
    c. Дублирование всех ресурсов
    d. Все элементы системы работают в режиме active-active или в горячем резервировании
2. Георасределенность
    a. Необходимое количество сайтов в разных ЦОД
    b. Взаимодействие Сайтов по выделенным или публичным каналам связи (требуется канал 1Мбит/с)
3. Масштабирование
    a. увеличение вычислительных ресурсов в кластере без прерывания обслуживания
    b. увеличение количества кластеров без прерывания обслуживания
4. Централизованное управление
    a. Изменения автоматически растекаются по всем необходимым узлам без прерывания обслуживания
    b. Единое администрирование всех георасределнных точек
5. Многодоменность
    a. Множество различных доменов (instance) на единых кластерах
    b. Функциональное разделение между доменами
    c. Различное администрирование в рамках домена
    d. Каждый домен может обслуживаться на одном или нескольких Сайтах
6. Безопасность
    a. Логирование всех успешных изменений с возможностью отката
    b. Различные Пользователи по разным Доменам
    c. Логирование всех активностей по каналам связи

9.2. Функции SBC

1. Обеспечение безопасности
    a. сокрытие топологии внутренней сети

   b. предотвращение DoS и DDoS атак на внутренние сегменты
   c. разрыв трафика
      i. сигнального трафика SIP, SIPS
      ii. голосового трафика RTP, sRTP
      iii. контроля каналов RTCP
      iv. WebService каналов http(s), ws(s)
2. Согласование голосовых кодеков (транскодирование RTP трафика)
3. Подключение удаленных сотрудников
   a. SIP-аппараты
   b. Рабочее место сотрудника на web-портале (WebRTC браузерный клиент)
      i. Внутренняя база аутентификации
      ii. Интеграция с AD/LDAP или внешними системами аутентификации
      iii. Двухфакторная аутентификация
   c. Предотвращение атак перебора паролей
4. Единое управление внешними транками
   a. Динамические правила распределения вызовов
   b. Балансировка нагрузки транков
   c. Объединение транков в единый пул
   d. Перетекания в реальном времени без прерывания обслуживания
5. Предотвращение несанкционированных звонков
   a. Интеграция с AD/LDAP/учетными системами
   b. Учет рабочего времени сотрудников
   c. Доступ к направлениям по персональным пин-кодам
6. Единая система приветствия и распределения звонков по ресурсам обслуживания
   a. Распределение между
      i. внутренними КЦ
      ii. внешними КЦ
      iii. внутренними очередями (персональными и общими, например группа секретарей)
      iv. внутренними групповыми номерами
      v. персональными сотрудниками
   b. Входной IVR для отдельных или всех внешних номеров / направлений
   c. Единые правила отсеивания нежелательных звонков blacklist
   d. Динамическое распределение звонков по внутренним ресурсам

e. Обратные звонки для нагруженных линий (например при прогнозируемом долгом ожидании)

7. Интеграция с CRM
    a. Управление звонками из CRM
    b. Отображение звонков в CRM
    c. Информация и записи разговоров в CRM
8. Управление не голосовыми WebService каналами
    a. Поддержка различных протоколов и их согласование / транскодирование
    b. json, xml, plain text, ldap
    c. rest, soap, iam, crud
    d. Безопасность публичных endpoint предоставления данных (например интеграция с корпоративной 1С для партнеров)
    e. Фильтрация предоставляемых данных
    f. Агрегация предоставляемых данных из различных источников

9.3. Сетевая архитектура

- Единый сетевой интерфейс под все коммуникации
- Разделение на LAN/WAN сегмент
- Разделение на LAN/DMZ/WAN сегменты
- Разделение на большее число сегментов с выделением отдельных сетевых интерфейсов под разных операторов связи