

SI3000 BGW

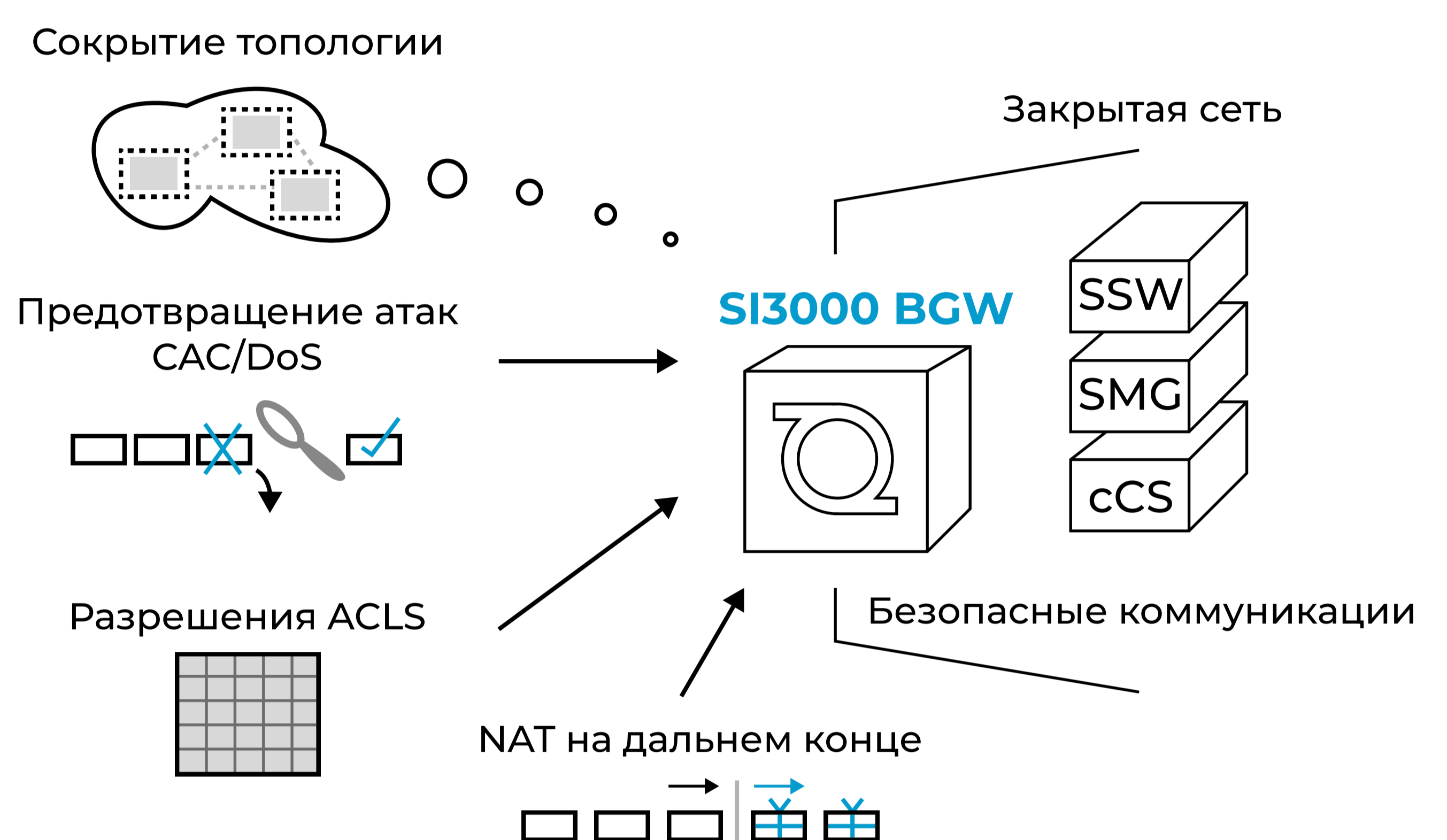
Пограничный шлюз BGW 3.0

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

SI3000 BGW Пограничный шлюз BGW 3.0 (далее – SI3000 BGW) – это сетевой элемент, который находится на границе сети для обеспечения безопасного предоставления сервисов телефонии и выполняет контроль SLA. Он дополняет портфель Искра Технологии в качестве пограничного контроллера сессий, который может использоваться во всех сценариях в сетях NGN, IMS и 4/5G.

SI3000 BGW – это пограничный контроллер сессий для межстанционного взаимодействия по протоколу SIP в сценариях «доступ» или «транк», которые используются, в том числе в проектах с реализацией функций «Универсальные коммуникации» и IMS/vIMS. Как правило, **SI3000 BGW** разворачивается на границе сетей Enterprise/NGN/IMS/vIMS/4G/5G и обеспечивает безопасное соединение для сервисов SIP, деление нагрузки трафика, а также позволяет отслеживать и контролировать качество обслуживания.

SI3000 BGW представляет собой экономичный способ реализации необходимых функций для обеспечения безопасности протокола SIP и устраняет проблемы с подключением к различным IP-сетям. SI3000 BGW помогает подключать разрозненные сети связи в режиме реального времени на основе SIP при одновременном снижении угрозы безопасности, устранении проблем совместимости и обеспечении надежной связи.



Продукт может быть расположен там, где он будет наиболее эффективным и наименее затратным в эксплуатации, что позволяет предприятиям удовлетворять свои возросшие потребности в гибких и динамичных инфраструктурах голосовой связи, видео и унифицированных коммуникациях (UC), а также сокращать капитальные и операционные затраты в рамках сервисной поддержки продуктов SBC.

ОСОБЕННОСТИ ПРОДУКТА:

- регистрация абонентов на станции;
- проксирование медиа (голос, видео, факс);
- прохождение абонентского NAT;
- сокрытие топологии сети;
- межсетевой обмен TCP/UDP;
- шифрование сигнализации и медиа;
- транскодирование;
- контроль установки вызовов;
- динамические и статические списки контроля доступа;
- защита от DoS-атак;
- правила манипуляции с заголовками SIP-сообщений;
- резервирование 1+1;
- контроль SLA;
- маршрутизация SIP;
- балансировка вызовов;
- логирование и аварийные сигналы (FMS).

Реализованный в продукте Rх-интерфейс позволяет использовать **SI3000 BGW** в роли P-CSCF в ядре IMS, предоставляя, таким образом, услугу VoLTE для мобильных абонентов. Функционал транскодирования мобильных кодеков (AMR/AMR-WB) дает возможность объединить в голосовой сети мобильных и фиксированных абонентов. Для операторов связи продукт **SI3000 BGW** также предоставляет функционал суррогатных регистраций (когда SBC самостоятельно иницирует регистрацию в заданный удаленный агент SIP) и регистрации SIP-транка (в случаях, когда сетевые реквизиты удаленного агента SIP неизвестны и SBC ожидает регистрацию с заданными реквизитами для его идентификации).

SI3000 BGW – это продукт, лидирующий на рынке Российской Федерации, сопоставляющий свой функционал и отказоустойчивость с продуктом vSBC от Oracle. Продукт реализован без использования компонентов с открытым исходным кодом и компонентов, разработанных в недружественных странах, и внесен в Единый реестр российского программного обеспечения (запись в реестре №5979 от 19.11.2019). **SI3000 BGW** поддерживает разные операционные системы и базы данных. У продукта есть сертификаты соответствия, заявляющие поддержку работы в среде Astra Linux Special Edition и с СУБД Postgres Pro.

МОДЕЛЬ НАДЕЖНОСТИ И ДОСТУПНОСТИ

SI3000 BGW обеспечивает безопасность, надежность и масштабируемость, на которые полагаются предприятия и контакт-центры при работе в режиме реального времени.

SI3000 BGW может быть развернут малыми и очень крупными предприятиями для разных вариантов использования:

- SIP-транкинг;
- унифицированные коммуникации и совместная работа (UC&C);
- контакт-центры (CC);
- удаленные голосовые сервисы и подключение удаленных сотрудников к общей вычислительной сети предприятия с неограниченным доступом к необходимым вычислительным ресурсам компании.

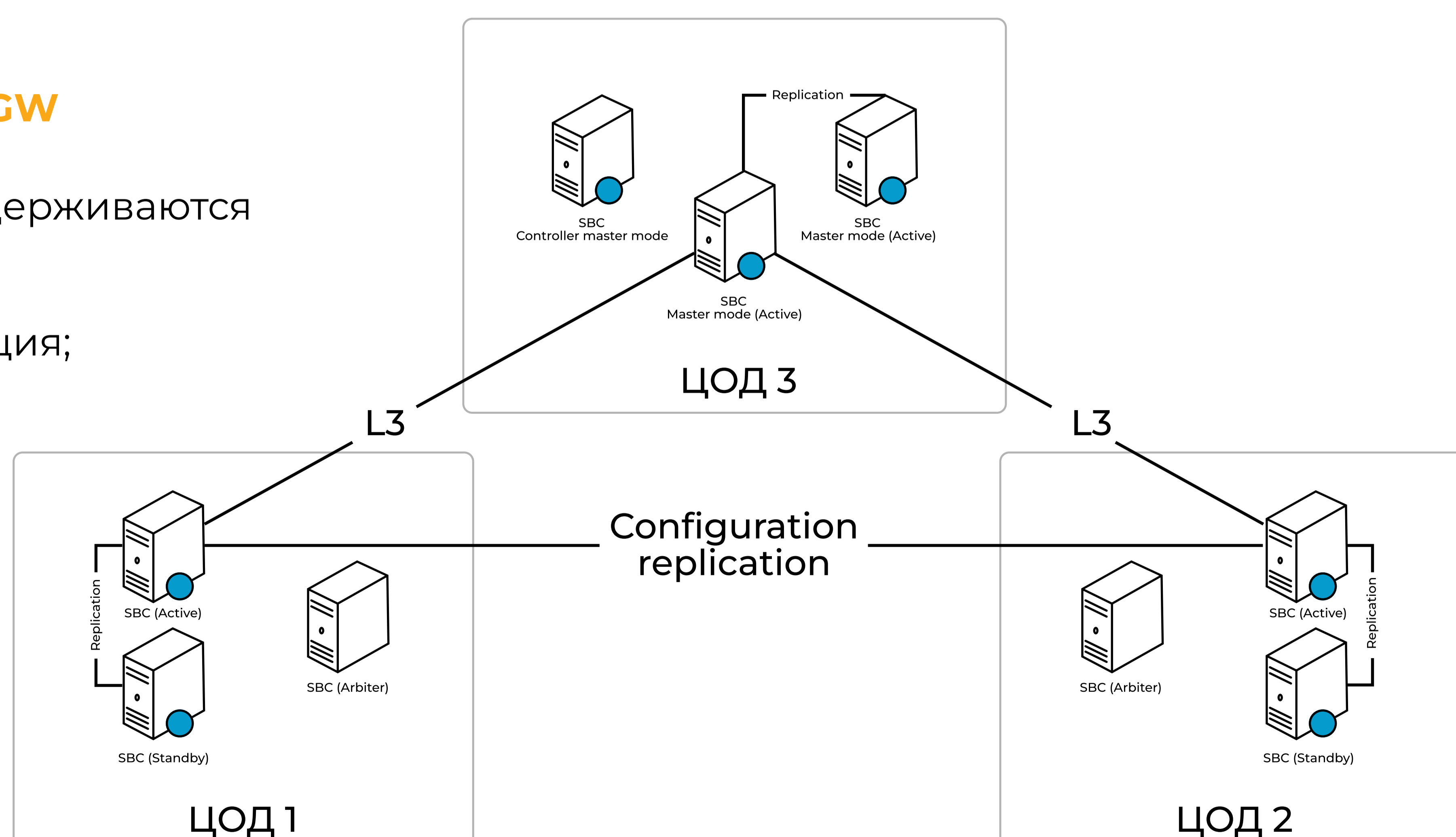
SI3000 BGW может гарантировать доступность сервиса на уровне 99,999% с использованием избыточного оборудования и программных механизмов для обеспечения правильной работы в случае сбоев.

Резервирование может быть достигнуто с включением режима работы «основной-резервный».

АРХИТЕКТУРА ПРОДУКТА SI3000 BGW

В рамках архитектуры продукта поддерживаются три режима работы:

- одиночная (standalone) инсталляция;
- high availability инсталляция (инсталляция в режиме высокой доступности);
- geo-redundancy инсталляция (инсталляция с георезервированием).



Архитектура продукта в рамках high availability инсталляции построена на решении для обеспечения высокой доступности PostgreSQL — Patroni. Для такого подхода требуются два, либо три физических или виртуальных узла. Стабильность работы обеспечивается за счет переключения между активным и резервным модулем. В режиме работы «основной-резервный» (high availability, высокой доступности) обеспечение отказоустойчивости сервиса телефонии происходит за счет использования плавающих IP-адресов, присутствующих на основном в данный момент времени узле. Все оконечное оборудование должно взаимодействовать с BGW по плавающим IP-адресам.

В момент переключения активности все плавающие адреса назначаются на новом основном узле, и в сеть передачи данных отправляются соответствующие уведомления (GARP). При этом существует возможность «автоматического» и «ручного» режима переключения на резервный узел (возможен разрыв проксируемых соединений). Система поддерживает различные конфигурации, например «2+2», когда четыре сервера обеспечивают функции SBC контроллера, объединены в отказоустойчивый кластер «горячего» резервирования: два сервера в режиме active и два сервера в режиме standby.

УПРАВЛЕНИЕ

Управление и мониторинг продукта **SI3000 BGW** осуществляется в интерфейсе командной строки и выполняется независимо от управления и контроля других элементов **SI3000** и без необходимости в центральной системе управления. Для подключения к интерфейсу командной строки используется протокол SSH. Также управление и мониторинг может осуществляться средствами веб-интерфейса, протокола SNMP, через REST API.

РАБОЧАЯ СРЕДА

SI3000 BGW доступен на стандартных аппаратных платформах MEA/MED от Искра Технологии и подразумевает компактную интеграцию с другими продуктами Искра Технологии в той же стойке с оптимизированными по стоимости решениями.

SI3000 BGW масштабируется как по горизонтали, так и по вертикали. В зависимости от требований к емкости и производительности продукта, **SI3000 BGW** может быть развернут на широком спектре гипервизоров (KVM, VMware, ICP (OpenStack)), на публичных облачных сервисах и на аппаратных платформах.

ЭКСПЛУАТАЦИЯ И ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

Все основные текущие диагностические данные и показатели производительности видны через интерфейс командной строки.

Поддерживается возможность мониторинга и оповещения при аварийных ситуациях (Grafana, Zabbix). **SI3000 BGW** можно настроить для отправки диагностических данных на удаленные сервисы: **SI3000 FMS** систему мониторинга неисправностей или любую другую систему мониторинга, использующую SNMP. Узлы BGW можно опрашивать по SNMP или http для получения метрик приложения, которые обновляются каждые 20 секунд.

Метрики, отдаваемые по http, подготовлены в формате для системы мониторинга Prometheus. Метрики формируются как по всей системе, так и по отдельно взятым интерфейсам SIP и по удаленным агентам (транкам).

Для централизованного сбора и хранения логов приложения в продукте предусмотрена поддержка syslog, администратор может указать сразу несколько серверов.

Для централизованного управления доступом предусмотрено использование протоколов LDAP и TACACS+, благодаря которым продукт может быть интегрирован с имеющимися системами AAA.

Консоль управления продуктом **SI3000 BGW** может быть выбрана в качестве оболочки для любых пользователей ОС, закрывая таким образом возможность изменять настройки ОС административному персоналу, но при этом давая наблюдать за предоставлением сервиса телефонии и менять настройки ПО.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Производительность системы	Платформа MEA/MED	Коммерческие серийные аппаратные средства COTS
Аппаратная платформа	Плата CVN/CVP	Virtual machine
Максимальное число абонентов	20.000/50.000	100.000+
Максимальное число параллельных сессий SIP или каналов медиа (G711 ulaw, 20мс)	2.000/2.500	20.000+
Туннели IPSec или VPN (одновременная сумма)	200	1.000+

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Работа с протоколом SIP:

- прокси SIP и агент B2BUA (RFC3261);
- поддержка SIP-методов: REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INVITE, ACK, PRACK, UPDATE, BYE, CANCEL, OPTIONS, INFO, REFER;
- медиация передачи сигналов SIP (Signaling Mediation);
- транзитная регистрация SIP (Upper Registration);
- поддержка SIP-T/I;
- сокрытие топологии сети;
- поддержка cookie;
- правила манипуляции с заголовками;
- IMS (P-CSCF, IBCF);
- поддержка интерфейса Rx;
- локальная обработка сообщений: reINVITE, UPDATE, REFER, PRACK, SIP 3xx Redirect Responses;
- работа в режиме Delayed Offer;
- локальная обработка метода OPTIONS (без дальнейшей трансляции);
- локальная обработка заголовков сообщения: History-Info, Diversion, P-Asserted-Identity, Session-Expires;
- приём и передача сигналов DTMF с использованием методов RFC2833, in band (G.711) и SIP INFO;
- локальная обработка метода PRACK;
- транскодирование payload DTMF RFC 2833;
- транскодирование DTMF RFC 2833 в SIP INFO;
- передача факсимильных сообщений по протоколам T.38 (T.30) и G.711;
- обогащение содержимого SIP-заголовков дополнительной информацией, на основе уникальных правил, закрепленных за источником трафика (IP, Hostname, SIP-Interface): добавление параметров и значений tgrp, trunk-context, добавление заголовков X-<header>;
- анализ доступности удаленной стороны на основе ответа на SIP-сообщения, в том числе использование метода OPTIONS;
- маршрутизация SIP-запросов на основе информации, получаемой от DNS-сервера: A-запись, SRV-запись;
- анализ SDP заголовка для подключения RTP-трафика;
- поддержка SIP-redirect, обработка сообщений согласно RFC 3261: маршрутизация по SIP-ответам 300-multiple choices, 302-moved temporarily;
- локальная обработка SIP REFER;
- суррогатная регистрация;
- регистрация SIP-транка.

Транспортные режимы:

- TLS, включая SIP over TLS;
- UDP, включая SIP over UDP;
- TCP, включая SIP over TCP;
- межсетевой обмен TCP/UDP/TLS, включая SIP через UDP/TCP/TLS;
- поддержка режимов работы:
 - несколько сигнальных и медиа-поточков на одном IP-адресе;
 - несколько сигнальных сообщений и медиа-поточков на разных IP-адресах в одном VLAN;
 - несколько сигнальных сообщений и медиа-поточков на разных IP-адресах в разных VLAN;
 - пересекающиеся IP-адреса на сетевых интерфейсах в пределах одного SBC;
- SCTP;
- IPSec;
- списки контроля доступа;
- IPv4 interworking;
- IPv6;
- межсетевой обмен IPv6/IPv4, IPv4/IPv4, IPv6/IPv6;
- bonding;
- VPN;
- несколько SIP-интерфейсов с одним IP-адресом, но разными IP-портами в рамках одного сетевого интерфейса (VLAN) с независимыми профилями настроек и маршрутизацией для каждого SIP-интерфейса.

Работа с медиаданными:

- проксирование медиаданных;
- управление RTP-сессиями с проксированием и без проксирования;
- прикрепление медиаданных (media anchoring);
- транскодирование;
- транскодирование Embedded Media Transcoding кодеков: G.711 a-law (μ -law), G.722, G.722.2 (AMR-WB), G.723.1, G.729 A, OPUS;
- шифрование медиаданных (SRTP);
- поддержка Hairpinning;
- корректировка и контроль QoS-маркеров (ToS bits, DiffServ) на базе информации о каждой сессии для обеспечения требуемого уровня обслуживания (SLA);
- QoS для трафика управления, мониторинга, сигнальных сообщений и RTP;
- возможность назначения разных меток DSCP на трафик управления, сигнализации, голосовых потоков, видеопотоков, изображений индивидуально по интерфейсам;
- ограничение приема RTP-потоков на основании IP-адреса источника (src ip), IP-адреса SDP (SDP ip), IP-адреса назначения (dst ip);
- выделение пула используемых RTP-портов в рамках сетевого интерфейса (VLAN);
- управление RTP-сессиями для предотвращения несанкционированного использования полосы пропускания, проверка используемого медиакодека на соответствие заявленному в SDP.

Безопасность:

- контроль установки вызовов;
- мониторинг и ограничение продолжительности вызовов;
- предотвращение DoS/DDoS-атак;
- списки контроля доступа;
- обработка экстренных вызовов;
- валидация сигналов и медиаданных;
- access Control List фильтр, основанный на application protocol и на IP-адресах, портах, их диапазонах;
- защита сети от следующих атак, событий:
 - IP Address Spoofing;
 - IP Address Sweeping;
 - Ping of Death Attack;
 - Teardrop Attack;
 - ICMP Fragment;
 - Land Attack;
 - Unknown Protocol;
 - UDP Short Header;
 - UDP spoofed broadcast echo («Fraggle Attack»);
 - UDP attack on diag ports («Pepsi Attack»);
 - SIP request message flood attack;
 - SIP response message flood attack;
 - SIP Invite spoof;
 - SIP Register spoof;
 - SIP Register flood attack;
 - SIP request spoof;
 - SIP response spoof;
 - SIP end-call attack;
- доступ зарегистрированных пользователей, находясь под атакой;
- механизм предохранения CPU от перегрузок;
- сохранение работоспособности при воздействии атак типа SIP registration flooding, при этом экстренные вызовы всегда доступны;
- автоматическая идентификация атакующих UE, основываясь на их поведении;
- автоматическая изоляция атакующих UE, основываясь на их поведении;
- собственная защита и защита ядра от всплеска регистраций;
- SIP Digest аутентификация согласно RFC 3261;
- разъединение вызовов в обоих направлениях при отсутствии трафика RTP;
- ограничение количества одновременных соединений, попыток установления соединений на уровне отдельных сигнальных элементов.

Маршрутизация:

- маршрутизация с наименьшей стоимостью (LCR);
- маршрутизация сессий на основе качества обслуживания;
- маршрутизация сессий на основе нагрузки;
- маршрутизация вызовов в соответствии с локальной таблицей маршрутизации;
- балансировка нагрузки;
- ENUM;
- внутренняя маршрутизация для нормализации номеров;
- маршрутизация конкретного SIP-метода на определенный SIP-транк, группу транков;
- в случае отказа удаленной стороны перемаршрутизация вызовов на альтернативное направление;
- поддержка сценариев альтернативной маршрутизации:
 - в зависимости от кода отбоя, полученного со стороны удаленного SIP-сервера;
 - по недоступности удаленного сервера:
 - при отсутствии ответа на SIP-сообщения;
 - периодические отправки сообщения SIP OPTIONS;
- при достижении пороговых значений по количеству одновременных вызовов в заданном направлении перемаршрутизация вызовов на альтернативное направление;
- маршрутизация сообщения SIP в зависимости от метода сообщений: INVITE, REGISTER, SUBSCRIBE.

Другие функции:

- прохождение NAT на удаленной стороне;
- прохождение NAT на ближнем конце;
- виртуальный MAC-адрес;
- обеспечение работы абонентских SIP-терминалов за NAT-маршрутизаторами и сетевыми экранами клиентов без поддержки SIP ALG (Hosted NAT traversal);
- синхронизация времени с внешними источниками по протоколам NTPv4 (RFC 5905) и SNTP (RFC 4330);
- высокая доступность;
- правила манипуляции с заголовками;
- масштабируемость (повышение производительности);
- детектирование состояний SIP-транка («падение» и «поднятие») на основе сообщений SIP OPTIONS;
- поддержка средствами SBC локального ответа на запрос OPTIONS без трансляции запроса;
- установка в одну стойку с SI3000 SSW, SMG, CCS, xDSL;
- автоматическое переключение на резервный программный коммутатор;
- без дополнительного оборудования для шифрования;
- поддержка передачи и преобразования DTMF (inband/RFC2833/SIP-INFO);
- виртуализация;
- распределенный режим работы;
- виртуальные сетевые функции (VNF);
- шлюз WebRTC;
- рабочие характеристики (46.000 CC и выше);
- мониторинг производительности;
- логирование;
- системный журнал;
- аутентификация и авторизация;
- поддержка авторизации из LDAP;
- аутентификация RADIUS;
- интеграция системы управления неисправностями;
- формирование файлов CDR;
- просмотр файлов CDR;
- сохранение всей информации об осуществленных вызовах (CDR) при работе в отказоустойчивом режиме в случае аварийного переключения между элементами кластера;
- настройка автоматической выгрузки CDR на внешнее хранилище по протоколу SFTP и SSH.

Сетевые интерфейсы

Ethernet 10/100/1000/10000 Мбит/с

Система управления

Протоколы управления SSH, SFTP, Telnet, REST API

Интерфейсы управления

Ethernet 10/100/1000 Мбит/с

Консоль RS232

Типы поддерживаемых ОС и СУБД

Операционные системы (хостовые) для серверных платформ/систем виртуализации*	Astra Linux Special Edition v.1.7 «Орел», Debian 10.3, SP5000 ИскраТехноЛинукс, Ubuntu 22.04
Операционные системы (гостевые) для серверных платформ/систем виртуализации*	Astra Linux Special Edition v.1.7 «Орел», Debian 10.3, SP5000 ИскраТехноЛинукс, Ubuntu 22.04
Операционные системы (хостовые) для HW плат собственного производства*	Wind River Linux 7/10, SP5000 ИскраТехноЛинукс
СУБД	PostgreSQL 11, Postgres Pro Standard 11

Поддерживаемые среды виртуализации и облачные системы

Среда виртуализации	SP5000 ICP «Интеллектуальная облачная платформа» (ICP-VP), VMware ESXi 6.5, ZVIRT, СКАЛА, и др.
Облачные системы	SP5000 ICP «Интеллектуальная облачная платформа»

* ВАЖНО!

Продукт может работать как при установке **напрямую на хостовую ОС, так и при использовании систем виртуализации**. В пункте **«Операционные системы (хостовые/гостевые) для серверных платформ/систем виртуализации»** перечислены ОС, на которых продукт может корректно работать (как при инсталляции на хостовую ОС, так и при инсталляции на платформу виртуализации (в гостевой ОС). В пункте **«Операционные системы (хостовые) для HW плат собственного производства»** перечислены ОС, на которых продукт корректно работает при установке на хостовую ОС на HW платы собственного производства.

ХАРАКТЕРИСТИКИ ВИРТУАЛЬНЫХ МАШИН ДЛЯ ИНСТАЛЛЯЦИИ SI3000 VGW БЕЗ ИСПОЛЬЗОВАНИЯ ФУНКЦИИ DRDK (ДЛЯ НЕБОЛЬШИХ ОБЪЕКТОВ И ИНСТАЛЛЯЦИЙ)

Кол-во одновременных сессий	CPU load	Кол-во одновременных сессий
100	32%	2 vCPU, 4 vGb RAM, 60Gb vHDD (SSD)
200	63%	
300	55%	
400	72%	
500	48%	4 vCPU, 4 vGb RAM, 60Gb vHDD (SSD)
600	60%	
700	71%	
800	80%	

ХАРАКТЕРИСТИКИ ВИРТУАЛЬНЫХ МАШИН ДЛЯ ИНСТАЛЛЯЦИИ SI3000 VGW С ИСПОЛЬЗОВАНИЕМ ФУНКЦИИ DRDK (ДЛЯ НЕБОЛЬШИХ ОБЪЕКТОВ И ИНСТАЛЛЯЦИЙ)

Кол-во одновременных сессий	Кол-во ресурсов	Тип Ethernet Card
801 - 3.000	6 vCPU, 6 Gb vRAM, 60Gb vHDD (SSD)	1 GbE
3.000 - 46.000*		10 GbE

* В момент тестирования **46.000 СС** было использовано **1.555 CPS**

* ВАЖНО!

Характеристики виртуальных машин указаны **без учета функционала транскодирования голосовых сессий**. При необходимости работы функционала транскодирования голосовых сессий необходимо дополнительно **к указанным выше характеристикам** добавлять **0,8 vCPU на 100 одновременных сессий транскодирования**.

ХАРАКТЕРИСТИКИ ВИРТУАЛЬНОЙ МАШИНЫ ДЛЯ СЕРВИСОВ SI3000 BGW (АРБИТР/CONTROLLER MASTER NODE)

Кол-во СС	Кол-во ресурсов	Тип Ethernet Card
Без ограничений	2 vCPU, 2 Gb vRAM, 40 Gb vHDD (HDD)	1 GbE

КОЛИЧЕСТВО ВИРТУАЛЬНЫХ МАШИН СОГЛАСНО ТИПОВ ИНСТАЛЛЯЦИЙ ПРОДУКТА

Топология инсталляции	SI3000 BGW, шт.	SI3000 BGW (Абитр), шт.
Standard (Стандартная конфигурация)	1	
Redundance (Дублированная система) *	2	1*
GeoRedundance (Георезервируемая система)	4	1

* Redundance (Дублированная система) может состоять из 2 (двух) виртуальных машин.

СПИСОК ЛИЦЕНЗИРУЕМЫХ ФУНКЦИОНАЛЬНОСТЕЙ ПРОДУКТА SI3000 BGW ПОГРАНИЧНЫЙ ШЛЮЗ BGW 3.0 (ЗАПИСЬ В РЕЕСТРЕ №5979) ПРИВЕДЕН В ТАБЛИЦЕ НИЖЕ.

Базовый функционал IMS:

- функциональная лицензия BGW (P-CSCF/IBCF), на 1 IMS домен;
- лицензия BGW на 1 SIP сессию, при заказе 1 - 1000 сессий одновременно;
- лицензия BGW на 1 SIP сессию, при заказе 1001 - 5000 сессий одновременно;
- лицензия BGW на 1 SIP сессию, при заказе 5001 - 10000 сессий одновременно;
- лицензия BGW на 1 SIP сессию, при заказе от 10001 сессий одновременно.

Базовый функционал NGN:

- функциональная лицензия BGW, на 1 NGN узел;
- функциональная лицензия BGW для резервирования NGN узла (с переносом сигнальных и разговорных сессий);
- лицензия BGW на 1 SIP сессию, при заказе 1 - 1000 сессий одновременно;
- лицензия BGW на 1 SIP сессию, при заказе 1001 - 5000 сессий одновременно;
- лицензия BGW на 1 SIP сессию, при заказе 5001 - 10000 сессий одновременно;
- лицензия BGW на 1 SIP сессию, при заказе от 10001 сессий одновременно.

Дополнительный функционал NGN:

- лицензия на функцию транскодирования, на 1 сессию;
- лицензия на функционал WebRTC/SIP interworking, на 1 вызов;
- лицензия на функционал SRTP/RTP interworking, на 1 вызов;
- локальная коммутация, на 1 вызов;
- лицензия на генерацию дополнительных метрик для отслеживания качества сервиса в текущем времени;
- генерация CDR-файлов;
- дополнительные правила маршрутизации на 1 SIP интерфейс.