SI3000 BGW Пограничный шлюз 3.0

Руководство администратора

АО «Искра Технологии», апрель 2023 г.

Если используется копия, необходимо проверить ее соответствие последней версии документа в определенном для этого официальном месте.

Документ выпущен компанией

АО «Искра Технологии»

РФ, 620066 Екатеринбург, ул. Комвузовская, 9-а

Т +7 343 210 69 51
Ф +7 343 341 52 40

РФ, 105264 Москва, ул. 9-я Парковая, 37

Т +7 495 727 08 50
Ф +7 495 727 08 78

iut@iskratechno.ru
www.iskratechno.ru

Оглавление

Список рисунков

Список таблиц

1. О документе

1.1. Назначение

В этом документе описываются процедуры настройки продукта «SI3000 BGW Пограничный шлюз 3.0» (далее – BGW) в интерфейсе командной строки (BGW CLI).

1.2. Целевая аудитория

Настоящий документ предназначен для системных администраторов и технических специалистов, выполняющих конфигурирование пограничного шлюза BGW.

1.3. Структура документа

Табл. 1.1. Структура документа

Глава	Описывает
«Основной режим работы»	вход в основной режим интерфейса BGW CLI, список и описание доступных команд в основном режиме.
«Режим конфигурирования»	вход в режим конфигурирования в интерфейсе BGW CLI, вход в режим работы с профилем, список и описание доступных команд в режиме конфигурирования.
«Процедуры настройки пограничного шлюза»	процедуры, которые нужно выполнить для конфигурирования и обеспечения корректной работы пограничного шлюза BGW.

1.4. Сопутствующая документация

Табл. 1.2. Сопутствующая документация

Код	Название
KSS883800-	Справочное руководство – HMR

1.5. Условные обозначения

1.5.1. Дополнительная маркировка текста

Табл. 1.3. Условные обозначения для маркировки текста

Знак	Текст	Описание
	Предупреждение!	Этот знак обозначает текст, который следует прочитать и принять к сведению для недопущения опасных последствий.
	Примечание.	Этот знак обозначает дополнительное пояснение.
	Пример.	Этот знак обозначает иллюстративную информацию.

1.5.2. Интерфейс пользователя

Табл. 1.4. Условные обозначения для описания интерфейса

Формат	Описание
Полужирный шрифт	Элементы в интерфейсе пользователя (названия меню, параметров, профилей) и выбираемые или вводимые команды.
`Моноширинный шрифт`	Выбираемое или вводимое значение.
>	Знак указывает на последовательность выбора пунктов меню или опций, например: **configure** > **dos_profile**.

1.6. Сокращения

Табл. 1.5. Сокращения на русском языке

Сокращение	Значение
СЛ	соединительная линия

Табл. 1.6. Сокращения на английском языке

Сокращение	Расшифровка	Значение
ACD	Average Call Duration	средняя продолжительность телефонного разговора
ASR	Answer-Seizure Ratio	коэффициент занятости линии связи
BGW	Border Gateway	пограничный шлюз
CAC	Call Admission Control	контроль приема и передачи вызовов
CDR	Call Detail Record	запись подробностей о вызове
CLI	Command Line Interface	интерфейс командной строки
DNS	Domain Name Server	сервер доменных имен
DOS	Denial of Service	отказ в обслуживании
DTMF	Dual Tone Multi Frequency	двухтональный многочастотный набор телефонного номера
FTP	File Transfer Protocol	протокол передачи файлов
HMR	Header Manipulation Rules	правила обработки заголовков
IMS	IP Multimedia Subsystem	подсистема IP-мультимедиа
IP	Internet Protocol	Интернет-протокол
NAT	Network Address Translation	трансляция сетевых адресов
NGN	Next Generation Network	сеть следующего поколения
PDD	Post Dial Delay	задержка после набора номера
RTCP	Real-Time Transport Control Protocol	протокол управления передачей в реальном времени
RTP	Real-time Transport Protocol	протокол транспорта в реальном времени
SDP	Session Description Protocol	протокол описания сеанса связи
SFTP	Secure File Transfer Protocol	защищенный протокол передачи файлов
SIP	Session Initiation Protocol	протокол инициирования сеанса связи

Сокращение	Расшифровка	Значение
SRTP	Secure Real-time Transport Protocol	защищенный протокол транспорта в реальном времени
TCP	Transmission Control Protocol	протокол управления передачей
UDP	User Datagram Protocol	протокол пользовательских дейтаграмм
URI	Uniform Resource Identifier	унифицированный идентификатор ресурса
VoIP	Voice over IP	голос поверх IP

2. Основной режим работы

Доступ к интерфейсу BGW CLI осуществляется с помощью соединения по протоколу TELNET или SSH.

При запуске интерфейса BGW CLI на экран терминала выводится краткая информация:

- текущее имя пользователя внутри кавычек;
- текущие дата и время входа в интерфейс BGW CLI;
- строка приглашения к вводу пользовательских команд в основном режиме, которая содержит сетевое имя в квадратных скобках:

```
fuko@SKTestVM:~$ bgw_cli
BGW Command Line Interface
Welcome “fuko” 31.05.2022 07:12
[SKTestVM] BGW>
```

Список доступных команд в данном режиме выводится по двойному нажатию клавиши <TAB>:

```
[SKTestVM] BGW>
EOF                  configure            exit                 reset_unactivated_config  save_config          sip
activate_config      dos                  help                 restore_saved_config      show
```

Рис. 2.1. BGW CLI – основной режим

Табл. 2.1. Команды в основном режиме

Команда	Описание
EOF	Выход из режима; если это основной режим, то выход из интерфейса BGW CLI (logout)
configure	Переход в режим конфигурирования BGW
exit	Аналогично команде **EOF**
reset_unactivated_config	Сброс текущей конфигурации, которая была изменена, но не была активирована
save_config	Сохранение текущей конфигурации (как долговременной), которая будет основной после перезапуска BGW
sip	Команда, которая обрабатывает подкоманды (**show registrations**) и выводит список зарегистрированных абонентов через данный BGW. Команда **sip show registrations** получит возможность ввода аргументов, по которым будет возможно фильтровать вывод списка зарегистрированных абонентов по пользовательскому фильтру (еще не реализовано)
activate_config	Активация конфигурации, в которую внесены изменения (в текущей сессии BGW CLI), но только если не осуществлялось выхода (logout) из интерфейса BGW CLI
dos	Команда, которая работает аналогично команде **sip** и содержит подкоманды **show** и **unblock**: ◆ **dos show**: содержит подкоманду **blocked-ips**, которая выводит список заблокированных IP-адресов. В целом команда имеет вид: **dos show blocked-ips**. По мере продвижения от команды к подкомандам доступно автодополнение подкоманды по нажатию клавиши <TAB>. ◆ **dos unblock**: содержит подкоманды: • **<IP_address>**: разблокировка конкретного, введенного пользователем IP-адреса заблокированного абонента,

Команда	Описание
	• **all**: разблокировка IP-адресов всех заблокированных абонентов.
help	Вывод примера использования интересующей команды. Например: **help dos** <Enter> выведет: `Usage: dos {show|unblock}`
restore_saved_config	Восстановление сохраненной ранее конфигурации
show	Команда, которая содержит подкоманды: ◆ **hwid**: вывод строки, необходимой для генерации лицензии. ◆ **running-config**: вывод на экран актуальной конфигурации, согласно которой работает приложение BGW на текущий момент. ◆ **saved-config**: вывод на экран конфигурации, которая находится в базе данных. При перезагрузке приложения именно данная конфигурация станет актуальной (рабочей).

3. Режим конфигурирования

Для входа в режим конфигурирования нужно в строке-приглашении ввести команду **configure** и нажать клавишу <Enter>.

```
[SKTestVM] BGW> configure
```

В результате строка-приглашение изменит свой вид и в скобках будет указан текущий режим:

```
[SKTestVM] BGW(configure)>
```

В режиме редактирования по двойному нажатию клавиши <TAB> выводятся имена профилей, доступных для конфигурирования, и доступные команды:

```
[SKTestVM] BGW(configure)>
EOF                    cdr_storage           exit                hmr_action          log_params          rtp_profile          validate
app_metrics_collector  codec                 float_ip_addr       hmr_matcher         media_proxy_server  show                 work_db_conn
cac_profile            cookie_profile        help                hmr_set             routing_rule        sip_interface
cdr_gen_params         dos_profile           hmr                 hmr_set_rules       rtp_interface       sip_remote_side
[SKTestVM] BGW(configure)>
```

Рис. 3.1. Режим редактирования – профили и команды

Дополнительные команды в этом режиме следующие:

- **EOF** и **exit**: выход из режима конфигурирования;
- **show**: вывод на экран текущей конфигурации;
- **validate**: проверка конфигурации на корректность введенных пользователем данных, соответствие данных необходимому типу.

Остальные команды соответствуют профилям конфигурации.

3.1. Режим работы с профилем

Для перехода в соответствующий профиль нужно ввести имя профиля. При наборе можно использовать функцию автодополнения команд по нажатию клавиши <TAB>. Данная функция реализована во всех режимах.

При вводе имени профиля и нажатии клавиши <Enter> пользователь переходит в режим работы с данным профилем, где по двойному нажатию клавиши <TAB> выводится список команд, доступных для данного профиля, а также изменит вид строка-приглашение:

```
[SKTestVM] BGW(configure)>
EOF                    cdr_storage           exit                hmr_action          log_params          rtp_profile          validate
app_metrics_collector  codec                 float_ip_addr       hmr_matcher         media_proxy_server  show                 work_db_conn
cac_profile            cookie_profile        help                hmr_set             routing_rule        sip_interface
cdr_gen_params         dos_profile           hmr                 hmr_set_rules       rtp_interface       sip_remote_side
[SKTestVM] BGW(configure)>dos_profile
[SKTestVM] BGW(configure)[dos_profile]>
EOF       create    delete    edit      exit      help      show      validate
[SKTestVM] BGW(configure)[dos_profile]>
```

Рис. 3.2. Режим работы с профилем

На рисунке выше показан пример режима конфигурирования (**configure**) профиля (**dos_profile**), а также команды, доступные для манипуляции выбранным профилем.

3.1.1. Режим работы с профилем с одним экземпляром

Если профиль может содержать несколько своих экземпляров, то по двойному нажатию клавиши <TAB> выведется только список команд, как показано выше, а если профиль может иметь только единичный экземпляр в конфигурации, то двойное нажатие клавиши <TAB> выведет сразу список полей для заполнения, как показано на рисунке ниже.

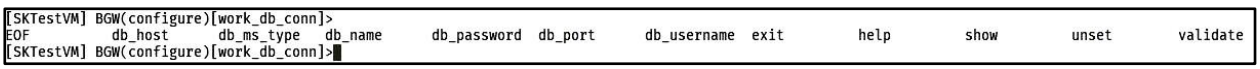

Рис. 3.3. Режим работы с профилем с одним экземпляром

Наряду с полями для заполнения, выводятся дополнительные команды: **EOF**, **exit**, **help**, **show**, **validate**. Данные команды описаны выше.

- **unset**: сброс поле в значение `null`. Т.е. в строке-приглашении нужно набрать **unset**<пробел>**имя_поля**. При наборе доступно автодополнение команды. Пример выполнения команды приведен на рисунке ниже, где **db_name** – имя поля, значение которого станет `null`:

```
[SKTestVM] BGW(configure)[work_db_conn]>unset db_name
```

3.1.2. Режим работы с профилем с несколькими экземплярами

Профили, допускающие множество своих экземпляров в конфигурации при переходе в режим их конфигурирования, имеют следующие не описанные выше команды:

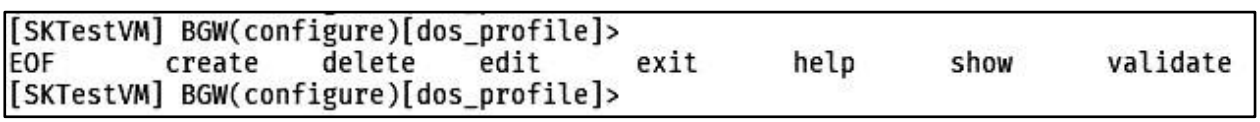

Рис. 3.4. Режим работы с профилем с несколькими экземплярами

- **create**: создание еще одного экземпляра текущего профиля. Ожидает ввода целого числа, где число выступает идентификатором профиля.

Пример.

Команда **create 3** создаст профиль с полем **profile_id 3**. При этом строка-приглашение примет вид режима редактирования вновь созданного профиля, где поля профиля, за исключением **profile_id** примут значение `null`.

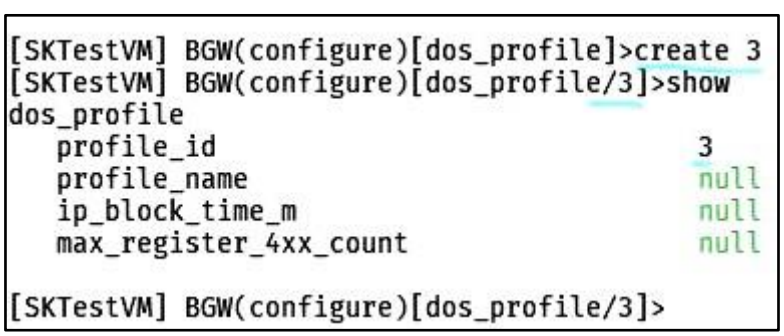

Рис. 3.5. Режим работы с профилем – создание профиля

В этом режиме по двойному нажатию клавиши <TAB> доступен список полей для заполнения в данном профиле, а также дополнительные команды:

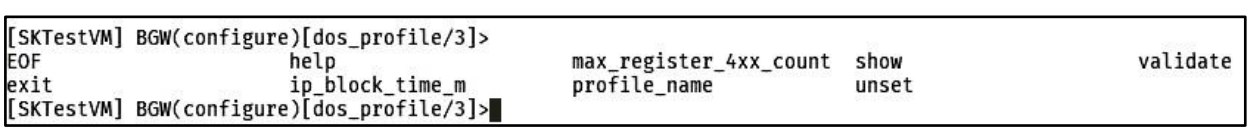

Рис. 3.6. Режим работы с профилем – доступные поля и команды

- **delete**: удаление экземпляра профиля. Ожидает ввода идентификатора экземпляра профиля для удаления в форме целого числа, например, **delete 3**. При этом экземпляр профиля с таким идентификатором должен существовать в конфигурации.

```
[SKTestVM] BGW(configure)[dos_profile]>delete 3
```

- **edit**: редактирование существующего экземпляра профиля. Ожидает ввода идентификатора существующего экземпляра. Например, **edit 2**. При вводе данной команды с идентификатором, строка-приглашение также изменит вид, показывая, что пользователь находится в режиме редактирования профиля с введённым номером идентификатора.

```
[SKTestVM] BGW(configure)[dos_profile]>edit 2
[SKTestVM] BGW(configure)[dos_profile/2]>
```

4. Процедуры настройки пограничного шлюза

4.1. Сбор метрик

В этом разделе описывается, как настроить систему сбора метрик.

Метрики, которые может рассчитывать BGW:

- Answer-Seizure Ratio (ASR) – высчитывается, как процентное отношение числа отвеченных вызовов к общему количеству попыток вызовов по интерфейсам SIP в отдельности. Так как такие ситуации, как занятость абонента и другие ситуации, когда отвергается вызов, считаются как неудачные попытки вызовов, расчетное значение параметра ASR может меняться в зависимости от поведения вызываемого абонента или пиринга партнера. Данная метрика может косвенно свидетельствовать о проблемах на определенном направлении.
- Average Call Duration (ACD) – средняя продолжительность вызова на интерфейсе SIP. Данная метрика может использоваться для оценки спроса на различные направления.
- Post Dial Delay (PDD) – это интервал времени между отправкой начального сообщения INVITE клиентом и приемом (одним и тем же клиентом) сигналов прохождения вызова (например, 18X или 200 OK). Метрика PDD подразделяется на два вида:
  - Successful PDD – это интервал времени между отправкой начального сообщения INVITE клиентом и приемом первого предварительного ответа (кроме 100), указывающего звуковое или визуальное состояние запрос на первоначальную настройку сеанса.

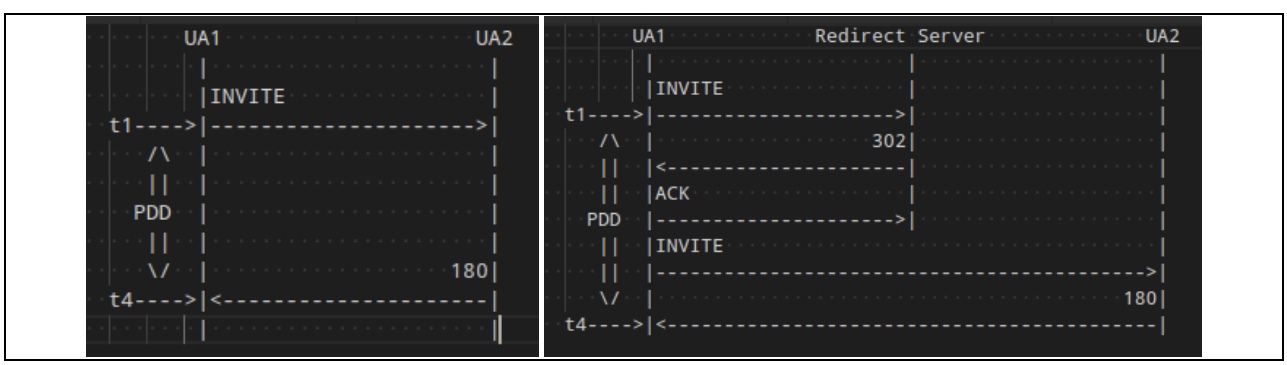

Рис. 4.1. Метрика Successful PDD

  - Failed PDD – это интервал времени между отправкой начального сообщения INVITE клиентом и приемом первого предварительного ответа с указанием сбоя. Ответ на сбой описывается как сообщение 4XX (исключая коды ответа на отказ 401, 402 и 407), 5XX или возможное сообщение 6XX.

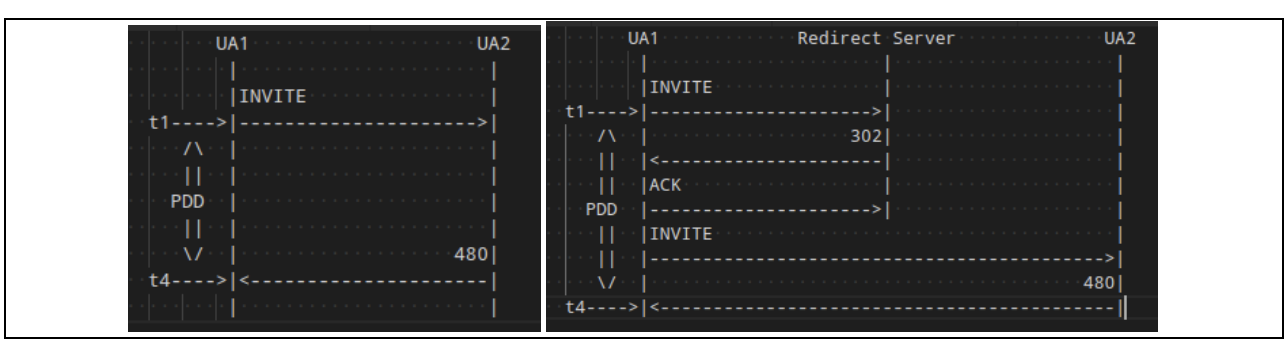

Рис. 4.2. Метрика Failed PDD

- RTP Packet Loss – считается как процентное отношение числа потерянных пакетов RTP к числу отправленных. Данная метрика может показать избыточную загруженность сети, обслуживающей трафик RTP или проблемы на сетевом оборудовании, размещенном на пути следования пакетов RTP по различным транковым направлениям.

4.1.1. Настройка сбора метрик

Все метрики усредняются за период (конфигурируемый для каждой метрики отдельно), так как вывод моментального значение данных метрик не будет являться информативным, для чего и реализован подход усреднения значений за интервал времени.

Чтобы настроить расчет метрик:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **app_metrics_collector** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>app_metrics_collector
[bgw-admin] BGW(configure)>[app_metrics_collector]>
```

4. Введите имя параметра и через пробел значение этого параметра и нажмите клавишу <Enter>.
   - **asr_period_m**: период усреднения Answer-Seizure Ratio, измеряется в минутах. Диапазон значений: от `1` до `1440` минут, значение по умолчанию – `15` минут. Если значение данного параметра не задано, будет использовано значение по умолчанию.
   - **acd_period_m**: период усреднения Average Call Duration, измеряется в минутах. Диапазон значений: от `1` до `1440` минут, значение по умолчанию – `30` минут. Если значение данного параметра не задано, будет использовано значение по умолчанию.
   - **pdd_period_m**: период усреднения Post Dial Delay (Successful и Failed), измеряется в минутах. Диапазон значений: от `1` до `1440` минут, значение по умолчанию – `15` минут. Если значение данного параметра не задано, будет использовано значение по умолчанию.
   - **rtp_loss_period_m**: период усреднения RTP Packet Loss, измеряется в минутах. Диапазон значений: от `1` до `1440` минут, значение по умолчанию – `15` минут. Если значение данного параметра не задано, будет использовано значение по умолчанию.
5. Сохраните внесенные изменения, вернувшись в корень BGW CLI командой **exit**.
6. Введите команды **activate_config** и **save_config**.

```
[bgw-admin] BGW(configure)>[app_metrics_collector]>exit
[bgw-admin] BGW(configure)> exit
[bgw-admin] BGW> activate_config
[bgw-admin] BGW> save_config
[bgw-admin] BGW>
```

4.1.2. Пример настройки сбора метрик

Необходимо сконфигурировать сбор метрик следующим образом:

- усреднение Answer-Seizure Ratio – 10 минут,
- усреднение Average Call Duration – 60 минут,
- усреднение Post Dial Delay – 10 минут,
- усреднение RTP Packet Loss – 30 минут.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>app_metrics_collector
[bgw-admin] BGW(configure)>[app_metrics_collector]>asr_period_m 10
[bgw-admin] BGW(configure)>[app_metrics_collector]>acd_period_m 60
```

```
[bgw-admin] BGW(configure)>[app_metrics_collector]>pdd_period_m 10
[bgw-admin] BGW(configure)>[app_metrics_collector]>rtp_loss_period_m 30
```

Результат настройки можно посмотреть командой **show**:

```
[bgw-admin] BGW(configure)[app_metrics_collector]>show
app_metrics_collector
     asr_period_m                  10
     acd_period_m                  60
     pdd_period_m                  10
     rtp_loss_period_m             30
```

4.1.3. Отчет статистики трафика

Вся статистика и отчет по собранным метрикам находится в файле bgw_metrics, расположенном в директории /var/log/bgwng. К данным из файла можно получить доступ посредством протокола HTTP на порте 8081.

В качестве формата выходных данных используется формат Prometheus.

4.2. Журналирование вызовов (CDR)

В этом разделе описывается, как настроить журналирование вызовов.

В пограничном шлюзе BGW предусмотрена возможность записи файлов Call Detail Record (CDR). Файлы CDR хранятся в дисковом буфере, сконфигурированном администратором. Если настроено внешнее хранилище, то после передачи на него файлов CDR по протоколу FTP/SFTP они удаляются из локального дискового буфера.

4.2.1. Настройка журналирования вызовов

4.2.1.1. Настройка генерации файлов CDR

Чтобы настроить генерацию файлов CDR:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **cdr_gen_params** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>cdr_gen_params
[bgw-admin] BGW(configure)[cdr_gen_params]>
```

4. Введите имя параметра и через пробел значение этого параметра и нажмите клавишу <Enter>.
   - **cdr_gen_enabled**: включение или отключение генерации файлов CDR с детализацией вызовов. Если установлено значение `true`, то файлы CDR будут создаваться. Если установлено значение `false`, то файлы детализации вызовов создаваться не будут. Обязательный параметр. Если значение данного параметра не задано, то будет использовано значение по умолчанию, эквивалентное `false`.
   - **cdr_gen_mode**: параметр для выбора, какие вызовы следует детализировать и регистрировать в файлы CDR, имеет следующие значения:
     - `NO_CDR`: не генерировать файлы CDR.
     - `ANSWERED`: детализируются успешно отвеченные вызовы.
     - `REJECTED_BY_REMOTE_SIDE`: детализируются вызовы, которые были отклонены удаленной стороной (remote_side).

- REJECTED_BY_BGW: детализируются вызовы, которые были отклонены самим BGW по различным причинам (например, не был найден маршрут или недоступно направление, в котором нужно было его передать).

Обязательный параметр. Если значение данного параметра не задано, то будет использовано значение по умолчанию, эквивалентное ANSWERED. Если необходимо генерировать вызовы для различных типов вызовов, то необходимо ввести нужные значения через запятую. Например, чтобы генерировать файлы CDR для успешно отвеченных вызовов и отклоненных удаленной стороной, нужно ввести следующие значения:

```
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_gen_mode ANSWERED,
REJECTED_BY_REMOTE_SIDE
```

cdr_buffer_path: путь до локального дискового буфера, где будут храниться файлы CDR до отправки их во внешнее хранилище. Обязательный параметр. Если значение данного параметра не задано, то будет использовано значение по умолчанию, эквивалентное /opt/si2000/charging.

- **cdr_accml_time_sec**: временной интервал в секундах, указывающий периодичность генерации файлов CDR. В случае если за заданный интервал времени не было вызовов, подлежащих журналированию, то файл за данный промежуток времени генерироваться не будет.

  cdr_file_format: формат, в котором будут формироваться файлы CDR. На данный момент доступен один формат: Si2000. Обязательный параметр. Если значение данного параметра не задано, то будет использовано значение по умолчанию, эквивалентное Si2000.
- **cdr_storage_id**: параметр для выбора идентификатора постоянного внешнего хранилища. Данный параметр ссылается на таблицу **cdr_storage**, поэтому указанный идентификатор должен быть создан в **cdr_storage** заранее.

  Необязательный параметр. Если значение данного параметра не задано, то сгенерированные файлы CDR будут сохраняться только в локальном дисковом буфере и не будут отправляться во внешнее хранилище.

5. Сохраните конфигурацию.

4.2.1.2. Настройка внешнего хранилища

В пограничном шлюзе BGW предусмотрена возможность описать конфигурацию нескольких внешних хранилищ файлов CDR и выбирать при необходимости нужное хранилище.

Чтобы настроить внешнее хранилище:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **cdr_storage** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>cdr_storage
[bgw-admin] BGW(configure)[cdr_storage]>
```

4. Введите **create** и через пробел введите уникальный числовой идентификатор для нового внешнего хранилища, а затем нажмите клавишу <Enter>.
5. Введите имя параметра и через пробел значение этого параметра и нажмите клавишу <Enter>.
   - **storage_type**: тип удаленного хранилища. Определяет, какой протокол будет использоваться для передач файлов CDR. Обязательный параметр. Возможные значения: FTP, SFTP.
   - **storage_ip_addr**: IP-адрес постоянного хранилища, на который можно отправлять файлы CDR. Обязательный параметр.

- **storage_port**: порт постоянного хранилища, на который можно отправлять файлы CDR. Диапазон значений: от `1` до `65535`. Обязательный параметр.
- **storage_login**: логин для авторизации на внешнем хранилище при отправке файлов CDR. Обязательный параметр.
- **storage_password**: пароль для авторизации на внешнем хранилище при отправке файлов CDR. Обязательный параметр.
- **storage_target_dir**: путь до директории на внешнем хранилище, куда будут сохраняться отправленные файлы CDR. Обязательный параметр.
- **storage_keep_alive_s**: время в секундах через которое будет происходить опрос постоянного хранилища для целей мониторинга его доступности, в случае обнаружения недоступности генерируется соответствующий аварийный сигнал. Диапазон значений: от `1` до `3600`. Необязательный параметр. Если значение данного параметра не задано, то опрос не происходит.
- **ftp_transfer_mode**: режим работы по протоколу FTP. Данный параметр является обязательным если в качестве протокола для передачи файлов CDR выбран `FTP` (параметр **storage_type**), в противном случае данный параметр – необязательный. Возможные значения: `ACTIVE`, `PASSIVE`. Режим работы нужно выбрать в соответствии с настройками использующегося сервера FTP (удаленного хранилища).

6. Сохраните конфигурацию.

4.2.2. Пример настройки журналирования вызовов

Требования к конфигурации:

- Запись файлов CDR должна осуществляться для вызовов:
  - на которые был ответ,
  - которые были отклонены удаленной стороной и
  - которые были отклонены самим BGW.
- Файлы CDR должны отправлять во внешнее хранилище по протоколу FTP.
- Сервер FTP работает в режиме passive.
- Настроен мониторинг доступности сервера FTP с проверкой каждые 5 секунд.

4.2.2.1. Пример настройки постоянного хранилища

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>cdr_storage
[bgw-admin] BGW(configure)[cdr_storage]>create 1
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_type FTP
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_ip_addr 192.168.122.64
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_port 21
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_login sysadmin
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_password [password]
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_target_dir /FTP/CDR
[bgw-admin] BGW(configure)[cdr_storage/1]>storage_keep_alive_s 5
[bgw-admin] BGW(configure)[cdr_storage/1]>ftp_transfer_mode PASSIVE
```

Результат настройки:

```
cdr_storage
     storage_id                    1
     storage_type                  FTP
     storage_ip_addr               192.168.122.64
     storage_port                  21
     storage_login                 sysadmin
     storage_password              [password]
     storage_target_dir            /FTP/CDR
```

```
     storage_keep_alive_s          5
     ftp_transfer_mode             PASSIVE
```

4.2.2.2. Пример настройки генерации файлов CDR

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>cdr_gen_params
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_gen_enabled true
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_gen_mode ANSWERED,
REJECTED_BY_REMOTE_SIDE, REJECTED_BY_BGW
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_buffer_path /opt/CDR
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_accml_time_sec 5
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_file_format SI2000
[bgw-admin] BGW(configure)[cdr_gen_params]>cdr_storage_id 1
```

Результат настройки:

```
[bgw-admin] BGW(configure)[cdr_gen_params]>show
cdr_gen_params
     cdr_gen_enabled               true
     cdr_gen_mode                  ANSWERED, REJECTED_BY_REMOTE_SIDE,
REJECTED_BY_BGW
     cdr_buffer_path               /opt/CDR
     cdr_accml_time_sec            5
     cdr_file_format               SI2000
     cdr_storage_id                1
```

4.3. Контроль приема и передачи вызовов (Call Admission Control)

В этом разделе описывается, как настроить различные возможные ограничения при обработке вызовов и регистраций.

BGW предоставляет возможность вводить ограничения по:

- количеству одновременно установленных вызовов,
- скорости попыток их установки (кол-во новых попыток установки вызовов за секунду),
- скорости обработки новых регистраций (кол-во новых регистраций за секунду),
- продолжительности вызова, находящегося в разговорной фазе (после принятия вызова вызываемого абонента),
- разрешенной продолжительности отсутствия голосового потока в вызове, при превышении которой вызов будет корректно завершен самим шлюзом BGW.

Профиль CAC может быть применен как к интерфейсу SIP, так и к удаленному агенту или группе агентов.

4.3.1. Ограничение установки вызовов

Когда на BGW поступает запрос создания нового вызова (SIP INVITE), происходит сравнение количества уже установленных вызовов, находящихся в разговорной фазе, и скорости поступления попыток установки новых вызовов на интерфейсах SIP, через которые вызов должен будет установиться, с заданными лимитами CAC. Если ни один лимит CAC не превышен, то происходит дальнейшая обработка SIP INVITE, в противном случае вызов отклоняется самим BGW с кодом ошибки (503 Service Unavailable).

При установке нового вызова могут проверяться, например, четыре профиля CAC, где:

- профиль 1 назначен на удаленном агенте, который инициирует попытку установки вызова,
- профиль 2 назначен на интерфейсе SIP, который обеспечивает прием данного трафика,

- профиль 3 задан на интерфейсе SIP выхода из BGW после процедуры нахождения маршрута для данного вызова и
- профиль 4 может быть задан на удаленном агенте, куда требуется направить данный вызов.

Если лимит одновременных вызовов (CC) и лимит установки вызовов в секунду (CPS) не заданы, то проверка считается пройденной, соответственно, никаких ограничений по данным параметрам накладываться не будет.

4.3.2. Ограничение регистраций

Когда на BGW приходит запрос на регистрацию (SIP REGISTR) от абонента, происходит сравнение скорости обработанных регистраций на интерфейсе SIP (входном и выходном) с заданными лимитами в CAC. Если лимит не превышен, то происходит дальнейшая обработка запроса SIP REGISTR, в противном случае запрос будет «отброшен» с кодом ошибки (503 Service Unavailable). Если запрос на регистрацию получил ответ 401 Unauthorized, то последующий запрос SIP REGISTR с авторизационными данными не проходит данной проверки, так как он уже включен в рассчитанную скорость.

Если лимит не задан, то проверка считается пройденной, соответственно, никаких ограничений не накладывается.

Рекомендуется настраивать данный параметр на интерфейсе SIP доступа (отвечающим за работу с оконечным клиентским терминальным оборудованием).

Данный алгоритм выполняется и для удаленной стороны SIP (remote side).

4.3.3. Ограничение продолжительности разговора

Когда на BGW устанавливается вызов, происходит проверка наличия для входного и выходного направления (под направлением подразумевается удаленная сторона SIP, если она есть на интерфейсе SIP) заданных ограничений по продолжительности разговора. Если таковые есть, то выбирается наименьшее найденное значение в профилях CAC. По достижении заданного лимита продолжительности разговора на обе стороны вызова отправляется сообщение SIP BYE для его корректного завершения. Для каждой стороны это выглядит так, как если бы вызов был разорван удаленной стороной.

Если ограничения не заданы, то продолжительность разговора не ограничивается.

4.3.4. Контроль отсутствия голосового потока

В пограничном шлюзе BGW предусмотрена возможность осуществлять контроль за наличием голосового потока в установленных вызовах. Контроль осуществляется только за входящим потоком от оконечного оборудования. Например, есть установленный вызов между интерфейсами SIP A и B, на которых назначены CAC профили CAC_A и CAC_B, на профиле CAC_A настроен контроль отсутствия голосового потока, на профиле CAC_B данный параметр не задан. От абонента B пропадает голосовой поток и это не приведет к завершению вызова т.к. на интерфейсе SIP B отсутствует контроль входящего потока, а для интерфейса SIP A данный поток, который бы приходил от абонента B является исходящим. В случае отсутствия голосового потока от абонента A вызов уже будет завершаться аналогичным механизмом как при ограничении продолжительности вызова.

Если таймер контроля отсутствия голосового потока не задан, то данный функционал не работает.

4.3.5. Настройка профилей CAC

В пограничном шлюзе BGW предусмотрена возможность создания нескольких профилей CAC, каждый профиль можно использовать для нескольких интерфейсов SIP и/или для нескольких удаленных сторон SIP. Однако такой подход не рекомендуется ввиду того что, если будут изменены настройки одного профиля CAC – эти изменения затронут сразу несколько интерфейсов SIP и удаленных направлений.

Чтобы создать и настроить конфигурацию профиля CAC:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **cac_profile** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>cac_profile
[bgw-admin] BGW(configure)[cac_profile]>
```

4. Введите **create** и через пробел введите уникальный числовой идентификатор профиля CAC, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[cac_profile]>create 1
[bgw-admin] BGW(configure)[cac_profile/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **profile_name**: наименование профиля CAC. Обязательный параметр. Значение по умолчанию – `default`. Если не конфигурировать данный параметр, будет использовано значение по умолчанию.
   - **max_cc**: ограничение максимального кол-во одновременно установленных вызовов. Диапазон значений: от `0` до `100000`. Необязательный параметр. Если значение данного параметра не задано, то кол-во одновременно установленных вызовов будет не ограничено.
   - **max_cps**: ограничение максимальной скорости создания новых вызовов. Диапазон значений: от `1` до `5000` вызовов за секунду. Необязательный параметр. Если значение данного параметра не задано, то скорость создания новых вызовов будет не ограничена.
   - **max_rps**: ограничение максимальной скорости обработки новых регистраций. Диапазон значений: от `1` до `5000` вызовов за секунду. Необязательный параметр. Если значение данного параметра не задано, то скорость обработки новых регистраций будет не ограничена.
   - **max_call_duration_s**: ограничение максимальной продолжительности разговора измеряется в секундах. Диапазон значений: от `5` до `10800` секунд (3 часа), значение по умолчанию – `1800` секунд (30 минут). Если значение данного параметра не задано, будет использовано значение по умолчанию. Необязательный параметр. Если не конфигурировать данный параметр, то продолжительность разговора будет не ограничена.
   - **rtp_inactivity_timeout_s**: интервал в секундах, который начинает работать, когда пропадает входящий голосовой поток от удаленной стороны. По истечении таймера вызов корректно завершается. Необязательный параметр. Если значение данного параметра не задано, то вызовы по причине отсутствия голосовых потоков завершаться не будут.
6. Сохраните конфигурацию.

4.3.6. Пример настройки профилей CAC

Необходимо сконфигурировать ограничения CAC следующим образом:

- максимальное кол-во одновременно установленных вызовов – 5000,

- максимальная скорость создания новых вызовов – 500 в секунду,
- максимальная скорость обработки новых регистраций – 500 в секунду,
- максимальная продолжительность разговора – не ограничена.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>cac_profile
[bgw-admin] BGW(configure)[cac_profile]>create 1
[bgw-admin] BGW(configure)[cac_profile/1]>max_cc 5000
[bgw-admin] BGW(configure)[cac_profile/1]>max_cps 500
[bgw-admin] BGW(configure)[cac_profile/1]>max_rps 500
[bgw-admin] BGW(configure)[cac_profile/1]>unset max_call_duration_s
```

Результат настройки:

```
[bgw-admin] BGW(configure)[cac_profile/1]>show
cac_profile
     profile_id                    1
     profile_name                  default
     max_cc                        5000
     max_cps                       500
     max_rps                       500
     max_call_duration_s           null
```

4.4. Система защиты сети VoIP

В этом разделе описан принцип и настройка защиты сети VoIP.

В пограничном шлюзе BGW предусмотрены следующие возможности для защиты сети VoIP:

- Все сообщения, не использующие протокол SIP – игнорируются, данная функциональность работает всегда.
- Можно включить защиту сети от перебора учетных записей абонентов. Для этого нужно задать ограничение на количество неудачных попыток регистрации абонента. Если превышен указанный в конфигурации лимит, IP-адрес устройства, с которого приходили запросы, попадает в список заблокированных, на заданное в конфигурации время, и все последующие сообщения SIP с данного IP-адреса игнорируются. Попытки считаются в диапазоне одного часа после первой неудачной регистрации, по истечении данного времени значение попыток обнуляется.

4.4.1. Настройка системы защиты сети VoIP

В пограничном шлюзе BGW предусмотрена возможность создания нескольких профилей DOS для защиты сети VoIP, каждый профиль можно использовать для нескольких интерфейсов SIP (см. раздел 4.11).

Чтобы создать и настроить конфигурацию профиля защиты сети VoIP:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **dos_profile** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>dos_profile
[bgw-admin] BGW(configure)[dos_profile]>
```

4. Введите **create** и через пробел введите уникальный идентификатор профиля, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[dos_profile]>create 1
[bgw-admin] BGW(configure)[dos_profile/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.

- **profile_name**: наименование профиля защиты. Обязательный параметр. Значение по умолчанию – `default`. Если не конфигурировать данный параметр, будет использовано значение по умолчанию.
- **ip_block_time_m**: время в минутах, на которое IP-адрес попадает в список заблокированных. Диапазон значений: от `1` до `7200`, значение по умолчанию – 30 минут. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию.
- **max_register_4xx_count**: максимальное количество допустимых попыток регистрации, на которые получен ответ со значением в диапазоне то `400` до `500` (значение `500` не включено в диапазон). Диапазон значений: от `0` до `2147483647`. Необязательный параметр. Если значение данного параметра не задано, то проверка неудачных попыток регистраций не происходит.

6. Сохраните конфигурацию.

4.4.2. Пример настройки системы защиты сети VoIP

Необходимо сконфигурировать профиль защиты сети VoIP следующим образом: блокировать на 2 часа IP-адреса устройств, у которых было 15 неудачных попыток регистрации в течении часа.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>dos_profile
[bgw-admin] BGW(configure)[dos_profile]>create 1
[bgw-admin] BGW(configure)[dos_profile/1]>ip_block_time_m 120
[bgw-admin] BGW(configure)[dos_profile/1]>max_register_4xx_count 15
```

Результат настройки:

```
[bgw-admin] BGW(configure)[dos_profile/1]>show
dos_profile
     profile_id                    1
     profile_name                  Default
     ip_block_time_m               30
     max_register_4xx_count        10
```

4.5. Система cookie

В этом разделе описывается, как настроить систему дополнительной защиты аккаунтов SIP-абонентов от использования их злоумышленниками для совершения вызовов.

В пограничном шлюзе BGW предусмотрена возможность защитить аккаунты SIP-абонентов.

Когда на BGW приходит запрос на регистрацию (SIP REGISTR) от абонента, на входном и/или выходном интерфейсе происходит расчет уникального значения cookie из полей и/или сетевых реквизитов абонента. Данное значение будет добавлено к идентификатору URI в поле Contact при отправке запроса регистратору. При успешной регистрации абонента данное значение сохраняется в базу данных.

Когда на BGW поступает запрос создания нового вызова (SIP INVITE), происходит расчет уникального значения cookie из полей и/или сетевых реквизитов абонента. Полученное значение сравнивается со значением cookie из регистрации абонента. Если значения совпадают, то происходит дальнейшая обработка SIP INVITE, иначе запрос будет «отброшен» с кодом ошибки 403 Forbidden.

Описание полей и/или сетевых реквизитов абонента (профиль cookie), из которых будет рассчитано cookie, может быть указано на входном и/или выходном интерфейсе. Приоритет выбора, какой профиль cookie будет использоваться, следующий:

- если на обоих интерфейсах задан профиль cookie, будет использоваться тот, что находится на интерфейсе доступа (Access);
- если профиль cookie задан только на одном интерфейсе, он и будет использоваться.

4.5.1. Настройка профилей cookie

В пограничном шлюзе BGW предусмотрена возможность создания нескольких профилей cookie, каждый профиль можно использовать для нескольких интерфейсов SIP (см. раздел 4.11).

Чтобы создать и настроить конфигурацию профиля cookie:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **cookie_profile** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>cookie_profile
[bgw-admin] BGW(configure)[cookie_profile]>
```

4. Введите **create** и через пробел введите уникальный идентификатор профиля cookie, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[cookie_profile]>create 1
[bgw-admin] BGW(configure)[cookie_profile/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **profile_name**: наименование профиля cookie. Обязательный параметр. Значение по умолчанию – `default`. Если не конфигурировать данный параметр, будет использовано значение по умолчанию.
   - **cookie_fields**: выбор, из каких данных будет рассчитываться значение cookie. Формат записи: цифры (соответствующие данным) через запятую. Список возможных данных для расчета cookie:
     - **UserAgent**: поле user-agent сообщения SIP, обозначается цифрой `1`.
     - **PhoneNr**: номер или имя абонента, указанное в идентификаторе URI поля Contact сообщения SIP, обозначается цифрой `2`.
     - **SrcHP**: IP-адрес и порт, с которых получено сообщение SIP, обозначается цифрой `3`.

     Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: **UserAgent** и **SrcHP** (`2`, `3`).
6. Сохраните конфигурацию

4.5.2. Пример настройки профилей cookie

Необходимо сконфигурировать профиль cookie таким образом, чтобы для расчета значения cookie использовать:

- данные из поля user-agent сообщения SIP,
- номер или имя абонента из идентификатора URI поля Contact сообщения SIP и
- IP-адрес и порт с которых получено SIP сообщение.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>cookie_profile
[bgw-admin] BGW(configure)[cookie_profile]>create 1
[bgw-admin] BGW(configure)[cookie_profile/1]>cookie_fields 1, 2, 3
```

Результат настройки:

```
[bgw-admin] BGW(configure)[cookie_profile/1]>show
cookie_profile
     profile_id                1
```

```
    profile_name              default
    cookie_fields             [1, 2, 3]
```

4.6. Список кодеков

В этом разделе описывается, как сконфигурировать список кодеков, с которыми работает BGW.

После инсталляции шлюза BGW основные кодеки уже включены в список в конфигурации, они включают следующие:

- аудиокодеки: G.711-a, G.711-u, G.729, G.722, opus, iLBC, G726-16, G726-24, G726-32, G726-40, telephone-event/8000;
- видеокодеки: H263, H264, VP8.

4.6.1. Настройка списка кодеков

В пограничном шлюзе BGW предусмотрена возможность создания списка с описанием кодеков, каждый кодек можно использовать для нескольких профилей RTP (см. раздел 4.7).

Чтобы создать описание кодека:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **codec** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>codec
[bgw-admin] BGW(configure)[codec]>
```

4. Введите **create** и через пробел введите уникальный идентификатор описания кодека, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[codec]>create 15
[bgw-admin] BGW(configure)[codec/15]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **codec_name**: наименование кодека профиля. Обязательный параметр.
   - **codec_rtpmap_name**: имя кодека/тактовая частота, указываемые в SDP.
   - **codec_payload_type**: тип полезной нагрузки.
6. Сохраните конфигурацию.

4.7. Профиль RTP

В этом разделе описывается, как настроить профили RTP.

В пограничном шлюзе BGW предусмотрены следующие возможности настройки профиля RTP:

- разрешить только определенные кодеки,
- включить или запретить транскодирование,
- разрешить или запретить передачу пакетов RTCP,
- разрешить DTMF только определенного формата,
- изменять порядок кодеков в SDP на интерфейсе SIP (см. раздел 4.11).

4.7.1. Разрешение только определенных кодеков и транскодирование

На BGW для поступающих сообщений SIP, содержащих SDP, происходит сравнение разрешенных на интерфейсе SIP (входном и выходном) кодеков. Если кодек запрещен, то он удаляется из описания медиапотока, указанного в SDP, в противном случае – сохраняется.

Если в профиле RTP для интерфейса SIP не задан список разрешенных кодеков, все кодеки запрещены.

Если для интерфейса SIP не задан профиль RTP, то все кодеки разрешены.

4.7.2. Разрешение передачи пакетов RTCP

Когда в вызове согласована передача трафика RTP, на BGW выполняется проверка разрешения или запрета передачи пакетов RTCP. Если передача RTCP разрешена, BGW будет проксировать приходящие пакеты RTCP. В противном случае приходящие пакеты RTCP не будут передаваться дальше. Данная проверка выполняется для входного и выводного интерфейса SIP.

Если для интерфейса SIP не задан профиль RTP, то приходящие пакеты RTCP не будут передаваться дальше.

4.7.3. Изменение порядка кодеков в SDP

Когда BGW отправляет сообщения SIP, содержащие SDP, и на выходном интерфейсе SIP разрешено изменение порядка кодеков для аудио- и видеопотоков, то BGW меняет порядок кодеков в соответствии с указанным в конфигурации для медиапотока порядком (параметры **audio_codecs** и **video_codecs**, см. раздел 4.7.4).

Если для медиапотока не указаны кодеки, то изменение порядка кодеков не происходит.

Если для интерфейса SIP не задан профиль RTP, то изменение порядка кодеков не происходит.

4.7.4. Настройка профиля RTP

В пограничном шлюзе BGW предусмотрена возможность создания нескольких профилей RTP, каждый профиль можно использовать для нескольких интерфейсов SIP (см. раздел 4.11).

Чтобы создать и настроить конфигурацию профиля RTP:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **rtp_profile** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>rtp_profile
[bgw-admin] BGW(configure)[rtp_profile]>
```

4. Введите **create** и через пробел введите уникальный идентификатор профиля, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[rtp_profile]>create 1
[bgw-admin] BGW(configure)[rtp_profile/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **profile_name**: наименование профиля RTP. Обязательный параметр. Значение по умолчанию – `default`. Если не конфигурировать данный параметр, будет использовано значение по умолчанию.
   - **audio_codecs**: список разрешенных аудиокодеков. Через запятую указываются уникальные идентификаторы кодеков из таблицы codec (см. раздел 4.11), разрешен формат ввода `<идентификатор кодека>:<имя кодека>`. Обязательный параметр. В качестве значения можно не указывать ни одного кодека, тогда все аудиокодеки запрещены.

- **video_codecs**: список разрешенных видеокодеков. Через запятую указывается уникальные идентификаторы кодеков из таблицы codec (см. раздел 4.11), разрешен формат ввода `<идентификатор кодека>:<имя кодека>`. Обязательный параметр. В качестве значения можно не указывать ни одного кодека, тогда все видеокодеки запрещены.
- **transcoding_allowed**: разрешение транскодирования. Если параметр установлен в значение `true`, то транскодирование разрешено, если установлено `false`, то транскодирование запрещено. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `false`.
- **rtcp_allowed**: разрешение проксирования пакетов RTCP. Если параметр установлен в значение `true` – то пакеты RTCP будут проксироваться, если установлено `false` – то проксирование пакетов RTCP не произойдет. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `false`.
- **dtmf_mode**: разрешенный формат DTMF:
  - `ANY`: разрешен любой формат DTMF, если установлен данный параметр, то DTMF просто проксируется.
  - `INBAND`: разрешен DTMF в формате Inband, данный формат может транскодироваться в формат SIP INFO.
  - `RFC2833`: разрешен в DTMF формате RFC-2833 (telephone-event), данный формат может транскодироваться в формат SIP INFO.
  - `SIP_INFO`: разрешен в DTMF формате SIP INFO, данный формат может транскодироваться в формат Inband и RFC-2833.

  Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `ANY`.
- **reorder_codecs**: изменение порядка кодеков. Если параметр установлен в значение `true`, то порядок кодеков в описании медиапотока (аудио- и/или видеопотока), указанного в SDP, будет изменяться в соответствии с указанным в параметрах **audio_codecs**, **video_codecs**. Если параметр установлен в значение `false`, то порядок кодеков не изменяется. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `false`.

6. Сохраните конфигурацию.

4.7.5. Пример настройки профиля RTP

Необходимо сконфигурировать профиль RTP следующим образом:

- разрешены аудиокодеки PCMA/8000, PCMU/8000;
- запрещены все видеокодеки;
- траскодинг запрещен;
- проксирование RTCP разрешено;
- разрешенный формат DTMF – RFC-2833;
- изменение порядка кодеков включено.

Ввод данных:

```
[bgw-admin] BGW(configure)[rtp_profile]>create 1
[bgw-admin] BGW(configure)[rtp_profile/1]>profile_name onlyPcmaAndPcmu
[bgw-admin] BGW(configure)[rtp_profile/1]>audio_codecs 1:G.711-a, 2:G.711-u
[bgw-admin] BGW(configure)[rtp_profile/1]>video_codecs
[bgw-admin] BGW(configure)[rtp_profile/1]>transcoding_allowed false
[bgw-admin] BGW(configure)[rtp_profile/1]>rtcp_allowed true
[bgw-admin] BGW(configure)[rtp_profile/1]>dtmf_mode RFC2833
[bgw-admin] BGW(configure)[rtp_profile/1]>reorder_codecs true
```

Результат настройки:

```
[bgw-admin] BGW(configure)[rtp_profile/1]>show
rtp_profile
     profile_id                1
     profile_name              onlyPcmaAndPcmu
     audio_codecs              ['1:G.711-a', '2:G.711-u']
     video_codecs              []
     transcoding_allowed       False
     rtcp_allowed              True
     dtmf_mode                 RFC2833
     reorder_codecs            True
```

4.8. Интерфейс RTP

В этом разделе описывается, как сконфигурировать интерфейсы RTP.

В пограничном шлюзе BGW предусмотрена возможность описать интерфейсы RTP, через которые будет передаваться трафик RTP.

4.8.1. Настройка интерфейса RTP

В пограничном шлюзе BGW предусмотрена возможность создания нескольких интерфейсов RTP, каждый интерфейс RTP можно использовать для нескольких интерфейсов SIP (см. раздел 4.11).

Чтобы создать и настроить интерфейс RTP:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите configure и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **rtp_interface** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>rtp_interface
[bgw-admin] BGW(configure)[rtp_interface]>
```

4. Введите **create** и через пробел введите уникальный идентификатор интерфейса RTP, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[rtp_interface]>create 1
[bgw-admin] BGW(configure)[rtp_interface/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **rtp_interface_name**: наименование интерфейса RTP. Обязательный параметр.
   - **local_ip_addr**: IP-адрес, который будет использоваться шлюзом BGW для передачи трафика RTP. Обязательный параметр.
   - **public_ip_addr**: IP-адрес, который будет подставлен в SDP при модифицировании сообщений SIP при отправке. В общем случае значение данного параметра будет совпадать с **local_ip_addr**, кроме случаев, когда при отправке сообщения с BGW происходит трансляция сетевых адресов (NAT). Необязательный параметр. Если параметр не конфигурировать, то будет использоваться значение из поля **local_ip_addr**.
   - **rtp_low_port**: начальное значение диапазона потов, из которого будут выбираться порты при создании канала RTP. Обязательный параметр. Диапазон значений: от `1` до `65535`, значение по умолчанию – `10000`.
   - **rtp_high_port**: конечное значение диапазона потов из которого будут выбираться порты при создании канала RTP. Обязательный параметре. Диапазон значений: от `1` до `65535`, значение по умолчанию – `40000`.

Предупреждение!

Связка **local_ip_addr** и **rtp_low_port** : **rtp_high_port** должна быть уникальной для каждой конфигурации интерфейса RTP.

6. Сохраните конфигурацию.

4.8.2. Пример настройки интерфейса RTP

Необходимо сконфигурировать интерфейс RTP следующим образом:

- IP-адрес, который будет использоваться BGW для передачи трафика RTP: 192.168.0.156;
- IP-адрес, который будет подставлен в SDP: 5.140.161.5 (перед BGW стоит NAT);
- диапазон портов, из которого будут выбираться порты при создании канала RTP: от 40000 до 60000.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>rtp_interface
[bgw-admin] BGW(configure)[rtp_interface]>create 1
[bgw-admin] BGW(configure)[rtp_interface/1]>rtp_interface_name Access
[bgw-admin] BGW(configure)[rtp_interface/1]>local_ip_addr 192.168.0.156
[bgw-admin] BGW(configure)[rtp_interface/1]>public_ip_addr 5.140.161.5
[bgw-admin] BGW(configure)[rtp_interface/1]>rtp_low_port 40000
[bgw-admin] BGW(configure)[rtp_interface/1]>rtp_high_port 60000
```

Результат настройки:

```
[bgw-admin] BGW(configure)[rtp_interface/1]>show
rtp_interface
     rtp_interface_id                  1
     rtp_interface_name                Access
     local_ip_addr                     192.168.0.156
     public_ip_addr                    5.140.161.5
     rtp_low_port                      20000
     rtp_high_port                     40000
```

4.9. DNS-резолвер

В этом разделе описывается, как настроить сервера DNS, к которым будут выполняться запросы DNS.

В пограничном шлюзе BGW предусмотрена возможность выполнять запросы DNS (получения записей A, SRV и NAPTR) для определения сетевых реквизитов конечных точек. Запросы могут выполняться к нескольким серверам DNS (если один сервер не отвечает, то выполняется запрос к следующему).

4.9.1. Настройка DNS-резолвера

В пограничном шлюзе BGW предусмотрена возможность описать DNS-резолвер, который будет содержать информацию об одном или нескольких серверах DNS. DNS-резолвер используется интерфейсом SIP (см. раздел 4.11), для каждого интерфейса SIP должен быть создан уникальный DNS-резолвер, но сервера DNS в них могут быть одинаковыми.

Чтобы создать и настроить конфигурацию DNS-резолвера:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **dns-resolver** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>dns_resolver
[bgw-admin] BGW(configure)[dns_resolver]>
```

4. Введите **create** и через пробел введите уникальный идентификатор конфигурации DNS-резолвера, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[dns_resolver]>create 1
[bgw-admin] BGW(configure)[dns_resolver/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **dns_resolver_name**: наименование конфигурации DNS-резолвера. Обязательный параметр.
   - **local_ip_addr**: IP-адрес, с которого BGW будет отправлять запросы DNS. Обязательный параметр.
   - **local_port**: порт, с которого BGW будет отправлять запросы DNS. Обязательный параметр. Обязательный параметр. Диапазон значений: от `1` до `65535`.

Предупреждение!

Связка **local_ip_addr** и **local_port** должна быть уникальной для каждой конфигурации DNS-резолвера.

   - **dns_servers**: список IP-адресов серверов DNS. Формат: IP-адреса вводятся через запятую. Обязательный параметр. В качестве значения можно не указывать ни одного IP-адреса, тогда запросы DNS не будут отправляться.

6. Сохраните конфигурацию.

4.9.2. Пример настройки DNS-резолвера

Необходимо сконфигурировать DNS-резолвер следующим образом:

- IP-адрес, с которого BGW будет отправлять запросы DNS: 192.168.0.156;
- порт, с которого BGW будет отправлять запросы DNS: 5003;
- список серверов DNS: 192.168.122.90, 192.168.143.22.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>dns_resolver
[bgw-admin] BGW(configure)[dns_resolver]>create 1
[bgw-admin] BGW(configure)[dns_resolver/1]>dns_resolver_name ims.ru
[bgw-admin] BGW(configure)[dns_resolver/1]>local_ip_addr 192.168.0.156
[bgw-admin] BGW(configure)[dns_resolver/1]>local_port 5003
[bgw-admin] BGW(configure)[dns_resolver/1]>dns_servers 192.168.122.90, 192.168.143.22
```

Результат настройки:

```
[bgw-admin] BGW(configure)[dns_resolver/1]>show
dns_resolver
     dns_resolver_id                 1
     dns_resolver_name               ims.ru
     local_ip_addr                   192.168.0.156
     local_port                      5003
     dns_servers                     ['192.168.122.90', '192.168.143.22']
```

4.10. Профиль SIP

В этом разделе описывается, как настроить профиль SIP.

В пограничном шлюзе BGW предусмотрены следующие возможности настройки профиля SIP:

- настройка политики работы с трафиком SRTP,
- настройка политики работы с абонентами с трансляцией сетевых адресов (абоненты за NAT),
- включение или выключение системы Cookie,

- разрешение или запрет реройтинга.

4.10.1. Политика работы с трафиком SRTP

Когда на BGW приходит сообщение SIP, содержащее SDP, происходит проверка политики SRTP, установленной на входном и/или выходном интерфейсе SIP. Если установлена политика:

- **FORBIDDEN** – из SDP будут удалены все атрибуты для создания потока STRP.
- **ALLOWED** – в SDP не произойдет изменений, связанных с атрибутами для создания потока STRP.
- **PREFERRED** – BGW генерирует атрибуты для создания STRP, далее, если в исходном SDP уже были атрибуты STRP, они заменяются на сгенерированные, если атрибутов не было, то они добавляются для каждого медиапотока.

Поскольку для входного и выходного интерфейсов SIP могут быть установлены разные политики работы с трафиком SRTP, чтобы решить проблему, когда абоненты на входном интерфейсе обязательно требуют передачу медиапотоков через SRTP, а конечная точка на выходном интерфейсе не поддерживает или запрещает SRTP, нужно выполнить следующие действия:

1. на входном интерфейсе установить политику **PREFERRED**,
2. на выходном интерфейсе установить политику **FORBIDDEN**.

4.10.2. Политика работы с абонентами с NAT

На BGW есть возможность запрещать или разрешать регистрацию абонентов с трансляцией сетевых адресов (NAT). Также предусмотрены механизмы решения проблем, возникающих при работе с абонентами NAT (препятствия для прохождения голосовых пакетов, а также инициализации соединений).

4.10.3. Настройка профиля SIP

В пограничном шлюзе BGW предусмотрена возможность создания нескольких профилей SIP, каждый профиль можно использовать для нескольких интерфейсов SIP (см. раздел 4.11).

Чтобы создать и настроить конфигурацию профиля SIP:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_profile** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>sip_profile
[bgw-admin] BGW(configure)[sip_profile]>
```

4. Введите **create** и через пробел введите уникальный идентификатор профиля SIP, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[sip_profile]>create 1
[bgw-admin] BGW(configure)[sip_profile/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **profile_name**: наименование профиля SIP. Обязательный параметр. Значение по умолчанию – `default`. Если не конфигурировать данный параметр, будет использовано значение по умолчанию.
   - **srtp_policy**: политика трафика SRTP. Обязательный параметр. Возможные значения: `FORBIDDEN`, `ALLOWED`, `PREFERRED`. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `ALLOWED`.

- **nat_subscribers_allowed**: регистрация абонентов с NAT. Если установлено значение `true`, то регистрация абонентов с NAT разрешена. Если установлено значение `false`, то регистрация NAT абонентов запрещена. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `true`.
- **nat_keep_alive_s**: интервал в секундах, через который абонентам NAT будут отправляться SIP OPTIONS. Диапазон значений: от `10` до `300`. Необязательный параметр. Если значение данного параметра не задано, то сообщение SIP OPTIONS отправляться не будет.
- **cookie_profile_id**: уникальный идентификатор профиля cookie. Профиль с данным идентификатором должен быть заранее создан в таблице **cookie_profile** (см. раздел 4.5). Необязательный параметр.
- **reroute_mode**: данный параметр позволяет указать, в каких случаях разрешено изменение маршрута или вовсе запрещено:
  - `NO_REROUTE`: изменение маршрута запрещено.
  - `REROUTE_ON_REMOTE_SIDE_OOS`: изменение маршрута разрешено для случаев, когда направление выбранного маршрута недоступно по какой-то причине, в этом случае будет произведен поиск следующего маршрута с меньшим приоритетом.
  - `REROUTE_ON_3XX`: разрешить перемаршрутизацию сообщений SIP с кодами ответов от 300 до 400 (400 в диапазон не попадает). Если не конфигурировать данный параметр, будет использовано значение по умолчанию:

  Если необходимо разрешить перемаршрутизацию для разных случаев, то нужно ввести нужные значения через запятую. Например, чтобы настроить перемаршрутизацию по недоступности направления и перемаршрутизацию сообщений SIP с кодами ответов от 300 до 400, введите следующее:

```
[bgw-admin] BGW(configure)[sip_profile/1]>reroute_mode REROUTE_ON_REMOTE_SIDE_OOS,
REROUTE_ON_3XX
```

6. Сохраните конфигурацию.

4.10.4. Пример настройки профиля SIP

Необходимо сконфигурировать профиль SIP следующим образом:

- запретить SRTP,
- разрешить регистрацию абонентов NAT,
- установить интервал отправки абонентам NAT сообщений SIP OPTIONS, равный 15 секундам,
- запретить перемаршрутизацию.

Ввод данных:

```
[bgw-admin] BGW(configure)[sip_profile]>create 1
[bgw-admin] BGW(configure)[sip_profile/1]>srtp_policy FORBIDDEN
[bgw-admin] BGW(configure)[sip_profile/1]>nat_keep_alive_s 15
[bgw-admin] BGW(configure)[sip_profile/1]>reroute_mode NO_REROUTE
```

Результат настройки:

```
[bgw-admin] BGW(configure)[sip_profile/1]>show
sip_profile
     profile_id                    1
     profile_name                  default
     srtp_policy                   FORBIDDEN
     nat_subscribers_allowed       True
     nat_keep_alive_s              15
     cookie_profile_id             null
     reroute_mode                  NO_REROUTE
```

4.11. Интерфейс SIP

В этом разделе описывается, как настроить интерфейсы SIP.

В пограничном шлюзе BGW предусмотрена возможность создания и настройки интерфейсов SIP, через которые будет передаваться трафик, содержащий сообщения SIP.

4.11.1. Настройка интерфейса SIP

Чтобы создать конфигурацию интерфейса SIP:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_interface** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>sip_interface
[bgw-admin] BGW(configure)[sip_interface]>
```

4. Введите **create** и через пробел введите уникальный идентификатор интерфейса SIP, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[sip_interface]>create 1
[bgw-admin] BGW(configure)[sip_interface/1]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **sip_interface_name**: наименование интерфейса SIP. Обязательный параметр.
   - **sip_interface_type**: тип интерфейса SIP:
     - `ACCESS`: интерфейс данного типа используется для взаимодействия с абонентскими устройствами из внешней незащищенной сети.
     - `TRUNK`: интерфейс данного типа используется для взаимодействия с конечными устройствами из доверенной сети. Обязательный параметр.
   - **local_ip_addr**: IP-адрес, который будет использоваться шлюзом BGW для передачи сообщений SIP. Обязательный параметр.
   - **public_ip_addr**: IP-адрес, который будет подставлен в поля сообщения SIP при модифицировании перед отправкой. В общем случае значение данного параметра будет совпадать с **local_ip_addr**, кроме случаев, когда при отправке сообщения со шлюза BGW происходит трансляция сетевых адресов (NAT). Необязательный параметр. Если поле не конфигурировать, то будет использоваться значение из поля **local_ip_addr**.
   - **udp_enabled**: если установлено значение `true`, то на интерфейсе SIP разрешено получать и отправлять сообщения SIP по протоколу UDP. Если установлено значение `false`, то это запрещено. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `true`.
   - **udp_local_port**: номер порта для получения и отправки сообщений SIP по протоколу UDP. Диапазон значений: от `1` до `65535`. Необязательный параметр. Если значение данного параметра не задано, будет использовано значение по умолчанию: `5060`. Если не конфигурировать данный параметр, то передача данных по протоколу UDP невозможна.
   - **tls_enabled**: если установлено значение `true`, то на интерфейсе SIP разрешено получать и отправлять сообщения SIP по протоколу TLS. Если установлено значение `false`, то это запрещено. Обязательный параметр. Если значение данного параметра не задано, будет использовано значение по умолчанию: `false`.
   - **tls_local_port**: номер порта для получения и отправки сообщений SIP по протоколу TLS. Диапазон значений: от `1` до `65535`. Необязательный параметр. Если значение данного параметра не задано, то передача данных по протоколу TLS невозможна.

- **tls_certificate_path**: полный путь, указывающий, где на файловой системе расположен сертификат TLS. Необязательный параметр. Если значение данного параметра не задано, то передача данных по протоколу TLS невозможна.
- **tls_private_key_path**: полный путь, указывающий, где на файловой системе расположен приватный ключ для TLS. Необязательный параметр. Если значение данного параметра не задано, то передача данных по протоколу TLS невозможна.
- **tcp_enabled**: если установлено значение `true`, то на интерфейсе SIP разрешено получать и отправлять сообщения по протоколу TLS. Если установлено значение `false`, то это запрещено. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: `false`.
- **tcp_local_port**: номер порта для получения и отправки сообщений SIP по протоколу TCP. Диапазон значений: от `1` до `65535`. Необязательный параметр. Если значение данного параметра не задано, то передача данных по протоколу TCP невозможна.
- **rtp_interface_ids**: уникальные идентификаторы конфигурации интерфейсов RTP, указываются через запятую (конфигурация интерфейса RTP должна быть заранее создана в таблице **rtp_interface** (см. раздел 4.8), разрешен формат ввода `<идентификатор>:<имя>`. Обязательный параметр. В качестве значения можно не указывать ни одного интерфейса RTP, тогда на этом интерфейсе невозможно будет создать вызов.
- **cac_profile_id**: уникальный идентификатор профиля CAC. Профиль с данным идентификатором должен быть заранее создан в таблице **cac_profile** (см. раздел 4.3). Обязательный параметр.
- **dos_profile_id**: уникальный идентификатор профиля защиты сети VoIP. Профиль с данным идентификатором должен быть заранее создан в таблице **dos_profile** (см. раздел 4.4). Необязательный параметр.
- **in_hmr_set_id**: уникальный идентификатор списка HMR. Список правил HMR с данным идентификатором должен быть заранее создан в таблице **hmr_set** (см. документ «Справочное руководство – HMR»). Правила HMR из списка будут применяться только к входящим сообщениям SIP. Необязательный параметр.
- **out_hmr_set_id**: уникальный идентификатор списка HMR. Список правил HMR с данным идентификатором должен быть заранее создан в таблице **hmr_set** («Справочное руководство – HMR»). Правила HMR из списка будут применяться только к исходящим сообщениям SIP. Необязательный параметр.
- **rtp_profile_id**: уникальный идентификатор профиля RTP. Профиль с данным идентификатором должен быть заранее создан в таблице **rtp_profile** (см. раздел 4.7). Необязательный параметр.
- **dns_resolver_id**: через запятую указывается уникальные идентификаторы конфигурации DNS-resolver. Конфигурация DNS-resolver должна быть заранее создана в таблице **dns-resolver** (см. раздел 4.9), разрешен формат ввода `<идентификатор>:<имя>`. Обязательный параметр. В качестве значения можно не указывать ни одного DNS-resolver, тогда невозможно будет определение сетевых реквизитов конечных точек, если они заранее неизвестны.
- **trusted**: если установлено значение `true`, то на интерфейсе типа TRUNK разрешено получение сообщений SIP от любых конечных точек и разрешено изменение сетевых реквизитов конечной точки во время установленного вызова. Если установлено значение `false`, то на интересе типа TRUNK разрешено получать сообщения SIP только от конечных точек, связанных с данным интерфейсом SIP. Обязательный параметр. Если значение данного параметра не задано, будет использовано значение по умолчанию: `false`.

- **sip_profile_id**: уникальный идентификатор профиля SIP. Профиль с данным идентификатором должен быть заранее создан в таблице **sip_profile** (см. раздел 4.10). Обязательный параметр.

6. Сохраните конфигурацию.

4.11.2. Пример настройки интерфейса SIP

Необходимо сконфигурировать два интерфейса SIP следующим образом:

1. Интерфейс SIP для взаимодействия с абонентскими устройствами только по протоколу TCP. IP-адрес и порт, которые будут использоваться шлюзом BGW для получения и отправки сообщений SIP: 192.168.0.156:5070. В качестве профиля SIP будет использоваться заранее сконфигурированный профиль (см. раздел 4.10) с идентификатором 1.
2. Интерфейс SIP для взаимодействия с программным коммутатором по протоколу UDP. IP-адрес и порт, которые будут использоваться шлюзом BGW для получения и отправки сообщений SIP: 192.168.10.156:5060. В качестве профиля SIP будет использоваться заранее сконфигурированный профиль (см. раздел 4.10) с идентификатором 1.

Ввод данных:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>sip_interface
[bgw-admin] BGW(configure)[sip_interface]>create 1
[bgw-admin] BGW(configure)[sip_interface/1]>sip_interface_name Public
[bgw-admin] BGW(configure)[sip_interface/1]>sip_interface_type ACCESS
[bgw-admin] BGW(configure)[sip_interface/1]>local_ip_addr 192.168.0.156
[bgw-admin] BGW(configure)[sip_interface/1]>udp_enabled false
[bgw-admin] BGW(configure)[sip_interface/1]>tcp_enabled true
[bgw-admin] BGW(configure)[sip_interface/1]>tcp_local_port 5070
[bgw-admin] BGW(configure)[sip_interface/1]>sip_profile_id 1
```

Для завершения настройки интерфейса SIP 1 нужно нажать комбинацию клавиш <Ctrl+D>.

```
[bgw-admin] BGW(configure)[sip_interface]>create 2
[bgw-admin] BGW(configure)[sip_interface/2]>sip_interface_name Core
[bgw-admin] BGW(configure)[sip_interface/2]>sip_interface_type TRUNK
[bgw-admin] BGW(configure)[sip_interface/2]>local_ip_addr 192.168.10.156
[bgw-admin] BGW(configure)[sip_interface/2]>udp_local_port 5060
[bgw-admin] BGW(configure)[sip_interface/2]>sip_profile_id 1
```

Результат настройки:

```
sip_interface
     sip_interface_id                  1
     sip_interface_name                Public
     sip_interface_type                ACCESS
     local_ip_addr                     192.168.0.156
     public_ip_addr                    null
     udp_enabled                       False
     udp_local_port                    5060
     tls_enabled                       False
     tls_local_port                    null
     tls_certificate_path              null
     tls_private_key_path              null
     tcp_enabled                       True
     tcp_local_port                    5070
     rtp_interface_ids                 null
     cac_profile_id                    null
     dos_profile_id                    null
     in_hmr_set_id                     null
     out_hmr_set_id                    null
     rtp_profile_id                    null
     dns_resolver_id                   null
     trusted                           False
     sip_profile_id                    1
```

```
sip_interface
     sip_interface_id                  2
     sip_interface_name                Core
     sip_interface_type                TRUNK
     local_ip_addr                     192.168.10.156
     public_ip_addr                    null
     udp_enabled                       True
     udp_local_port                    5060
     tls_enabled                       False
     tls_local_port                    null
     tls_certificate_path              null
     tls_private_key_path              null
     tcp_enabled                       False
     tcp_local_port                    null
     rtp_interface_ids                 null
     cac_profile_id                    null
     dos_profile_id                    null
     in_hmr_set_id                     null
     out_hmr_set_id                    null
     rtp_profile_id                    null
     dns_resolver_id                   null
     trusted                           False
     sip_profile_id                    1
```

4.12. Удаленная сторона SIP

В этом разделе описывается как описать удаленную конечную точку, с которой будет происходить взаимодействие через интерфейс SIP типа TRUNK.

В пограничном шлюзе BGW предусмотрена возможность создания и настройки конечных точек для двух типов сетей: NGN или IMS. Конечные точки могут быть объединены в группу с одной из возможных политик балансировки (Round Robin, Hunt, Minimum Active Session, Active Standby). Группы также могу быть объединены в другие группы, которые в свою очередь тоже можно объединить в группы и т.д., вложенность групп ограничена значением 3.

4.12.1. Настройка удаленной стороны SIP

В пограничном шлюзе BGW предусмотрена возможность описания множества конечных точек.

Описание конечной точки разбито на два этапа:

1. Создание конфигурации для конечной точки с уникальным идентификатором, где указан ее тип и общие для конечных точек всех типов данные. Как только будет указан тип, в таблице с конфигурацией для удаленной стороны данного типа будет создана пустая запись с таким же уникальным идентификатором.
2. Редактирование конфигурации для конечной точки по ранее указанному типу, где указываются данные, свойственные только для конечной точки определенного типа.

Если был выполнен только один этап, то конфигурация конечной точки считается неконсистентной и взаимодействие с такой конечной точкой не будет происходить.

4.12.1.1. Создание конфигурации конечной точки

Чтобы создать конфигурацию конечной точки:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_remote_side** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>sip_remote_side
[bgw-admin] BGW(configure)[sip_remote_side]>
```

4. Введите **create** и через пробел введите уникальный идентификатор конфигурации конечной точки, нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[sip_remote_side]>create 1
[bgw-admin] BGW(configure)[sip_remote_side/1]>
```

5. Введите имя параметра и через пробел значение этого параметра, нажмите клавишу <Enter>.
   - **sip_remote_side_name**: наименование конечной точки. Обязательный параметр.
   - **sip_remote_side_type**: тип конечной точки. Обязательный параметр.
     - `NGN`: конечная точка расположена в сети типа NGN. Примером такой конечной точки является программный коммутатор.
     - `IMS`: конечная точка расположена в сети типа IMS. При работе с такой конечной точкой шлюз BGW выполняет роль функции PCSCF.
     - `GROUP`: группа конечных точек.
   - **cac_profile_id**: уникальный идентификатор профиля CAC. Профиль с данным идентификатором должен быть заранее создан в таблице **cac_profile** (см. раздел 4.3). Необязательный параметр.
6. Сохраните конфигурацию.

4.12.1.2. Создание конфигурации конечной точки типа NGN

Чтобы создать конфигурацию конечной точки типа NGN:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_remote_side_ngn** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>sip_remote_side_ngn
[bgw-admin] BGW(configure)[sip_remote_side_ngn]>
```

4. Введите **create** и через пробел введите уникальный идентификатор ранее созданной в таблице **sip_remote_side** конечной точки типа NGN, затем нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[sip_remote_side_ngn]>create 1
[bgw-admin] BGW(configure)[sip_remote_side_ngn/1]>
```

5. Введите имя параметра и через пробел значение этого параметра, нажмите клавишу <Enter>.
   - **remote_host**: IP-адрес или домен для связи с удаленной точки. Обязательный параметр.
   - **remote_port**: порт для связи с конечной точкой. Необязательный параметр. Если значение для данного параметра не задано и для параметра **remote_host** указан IP-адрес, то в зависимости от транспортного протокола, используемого для передачи сообщений SIP, будет использоваться порт по умолчанию:
     - для UDP и TCP – будет использоваться порт 5060,
     - для TLS – будет использоваться порт 5061.
   - **transport_mode**: тип транспортного протокола, используемого для передачи сообщений SIP. Возможные варианты: `UDP`, `TCP`. Обязательный параметр. Если значение данного параметра не задано, будет использовано значение по умолчанию: `UDP`.
   - **options_ping_period_s**: интервал, с которым BGW будет проверять состояние конечной точки, посылая сообщение SIP OPTIONS на нее, и анализировать ответ. Диапазон значений: от `1` до `65535`. Необязательный параметр. Если значение для данного параметра не задано, то BGW не будет проверять состояние конечной точки и будет считать, что она всегда доступна.
6. Сохраните конфигурацию.

4.12.1.3. Создание конфигурации конечной точки типа IMS

Чтобы создать конфигурацию конечной точки типа IMS:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_remote_side_ims** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>sip_remote_side_ims
[bgw-admin] BGW(configure)[sip_remote_side_ims]>
```

4. Введите **create** и через пробел введите уникальный идентификатор ранее созданной в таблице **sip_remote_side** конечной точки типа IMS, затем нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[sip_remote_side_ims]>create 2
[bgw-admin] BGW(configure)[sip_remote_side_ims/2]>
```

5. Введите имя параметра и через пробел значение этого параметра, нажмите клавишу <Enter>.
   - **ims_domain**: домен для связи с удаленной точкой. Обязательный параметр.
6. Сохраните конфигурацию.

4.12.1.4. Создание конфигурации группы конечных точек

Чтобы создать конфигурацию группы конечных точек:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_remote_side_group** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)>sip_remote_side_group
[bgw-admin] BGW(configure)[sip_remote_side_group]>
```

4. Введите **create** и через пробел введите уникальный идентификатор ранее созданной в таблице **sip_remote_side** конечной точки типа GROUP, затем нажмите клавишу <Enter>.

```
[bgw-admin] BGW(configure)[sip_remote_side_group]>create 3
[bgw-admin] BGW(configure)[sip_remote_side_group/3]>
```

5. Введите имя параметра и через пробел значение этого параметра, нажмите клавишу <Enter>.
   - **balancing_policy**: алгоритм балансировки. Обязательный параметр. Если не конфигурировать данный параметр, будет использовано значение по умолчанию: ROUND_ROBIN.
     - ROUND_ROBIN: каждый новый приходящий вызов в группу маршрутизируется сначала в первую, затем во вторую, …, и в последнюю конечную точку из списка данной группы, затем вызовы начинают снова маршрутизироваться на 1-ую конечную точку из списка и так далее.
     - HUNT: при данном алгоритме балансировки выбирается первая доступная из списка конечная точка, у которой не исчерпан параметр CC из CAC.
     - MINIMUM_ACTIVE_SESSION: при данном алгоритме балансировки выбирается первая доступная из списка конечная точка, у которой наименьшее значение по CC из CAC.
     - ACTIVE_STANDBY: при данном алгоритме балансировки выбирается первая доступная из списка конечная точка, учитывается только состояние конечной точки – ее сетевая доступность.

- **group_member_ids**: через запятую указываются уникальные идентификаторы конечной точки (конечная точка должна быть заранее создана в таблице **sip_remote_side** (см. раздел 4.12.1.1)), разрешен формат ввода `<идентификатор>:<имя>`. Обязательный параметр. В качестве значения можно не указывать ни одной конечной точки, группа считается пустой, и она недоступна для создания на ней вызовов.

  В списке **group_member_ids** разрешено повторять уникальные идентификаторы, это полезно, если политика балансировки указана как `ROUND_ROBIN`, тогда за счет повторения становится возможно пропорционально распределять нагрузку на конечной точке, например: **group_member_ids** содержит следующий список: `[1, 1, 1, 2, 2, 3]`, в результате на 1-ю конечную точку будет 60% нагрузки, на 2-ю – 40%, на 3-ю – 20%

4.12.2. Пример настройки удаленной стороны SIP

4.12.2.1. Пример настройки удаленной стороны SIP в сети NGN

Необходимо описать конфигурацию двух удаленных точек в сети NGN и объединить их в группу с политикой балансировки Active Standby.

- Обе удаленные точки необходимо опрашивать на предмет доступности с интервалом в 15 секунд.
- Сетевые реквизиты первой удаленной точки: IP 192.168.104.40, порт 5060.
- Сетевые реквизиты второй удаленной точки: IP 192.168.104.41, порт 5061.
- Транспортный протокол для взаимодействия с удаленными точками: UDP.
- Для удаленных точек NGN качестве профиля CAC будет использоваться заранее сконфигурированный профиль (см. раздел 4.3) с идентификатором 1.
- На группу отдельно профиль CAC не будет установлен.

Процедура настройки

1. Создайте базовые конфигурации удаленных сторон:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>sip_remote_side
[bgw-admin] BGW(configure)[sip_remote_side]>create 111
[bgw-admin] BGW(configure)[sip_remote_side/111]>sip_remote_side_name cs_1.1
[bgw-admin] BGW(configure)[sip_remote_side/111]>sip_remote_side_type NGN
[bgw-admin] BGW(configure)[sip_remote_side/111]>cac_profile_id 1
```

2. Завершите настройку удаленной стороны 111, нажав комбинацию клавиш <Ctrl+D>.

```
[bgw-admin] BGW(configure)[sip_remote_side]>create 112
[bgw-admin] BGW(configure)[sip_remote_side/112]>sip_remote_side_name cs_1.2
[bgw-admin] BGW(configure)[sip_remote_side/112]>sip_remote_side_type NGN
[bgw-admin] BGW(configure)[sip_remote_side/112]>cac_profile_id 1
```

3. Завершите настройку удаленной стороны 112, нажав комбинацию клавиш <Ctrl+D>.

```
 [bgw-admin] BGW(configure)[sip_remote_side]>create 113
[bgw-admin] BGW(configure)[sip_remote_side/113]>sip_remote_side_name group_cs_1
[bgw-admin] BGW(configure)[sip_remote_side/113]>sip_remote_side_type GROUP
```

Результат настройки:

```
[bgw-admin] BGW(configure)[sip_remote_side]>show
sip_remote_side
     sip_remote_side_id                  111
     sip_remote_side_name                cs_1.1
     sip_remote_side_type                NGN
     cac_profile_id                      1

sip_remote_side
     sip_remote_side_id                  112
```

```
      sip_remote_side_name                cs_1.2
      sip_remote_side_type                NGN
      cac_profile_id                      1

sip_remote_side
      sip_remote_side_id                  113
      sip_remote_side_name                group_cs_1
      sip_remote_side_type                GROUP
      cac_profile_id                      null
```

Далее необходимо указать конфигурацию удаленной точки согласно ее типу. Для этого нужно вернуться в меню **configure** и перейти в соответствующие разделы.

4. Настройте удаленные стороны NGN, введя данные:

```
[bgw-admin] BGW(configure)>sip_remote_side_ngn
[bgw-admin] BGW(configure)[sip_remote_side_ngn]>edit 111
[bgw-admin] BGW(configure)[sip_remote_side_ngn/111]>remote_host 192.168.104.40
[bgw-admin] BGW(configure)[sip_remote_side_ngn/111]>options_ping_period_s 15
```

5. Завершите настройку удаленной стороны 111, нажав комбинацию клавиш <Ctrl+D>.

```
 [bgw-admin] BGW(configure)[sip_remote_side_ngn]>edit 112
[bgw-admin] BGW(configure)[sip_remote_side_ngn/112]>remote_host 192.168.104.41
[bgw-admin] BGW(configure)[sip_remote_side_ngn/112]>remote_port 5061
[bgw-admin] BGW(configure)[sip_remote_side_ngn/112]>options_ping_period_s 15
```

Результат настройки:

```
[bgw-admin] BGW(configure)[sip_remote_side_ngn]>show
sip_remote_side_ngn
      sip_remote_side_id                  111
      remote_host                         192.168.104.40
      remote_port                         null <– будет использован 5060
      transport_mode                      UDP
      options_ping_period_s               15

sip_remote_side_ngn
      sip_remote_side_id                  112
      remote_host                         192.168.104.41
      remote_port                         5061
      transport_mode                      UDP
      options_ping_period_s               15
```

6. Настройте группу удаленных сторон, введя данные:

```
[bgw-admin] BGW(configure)>sip_remote_side_group
[bgw-admin] BGW(configure)[sip_remote_side_group]>edit 113
[bgw-admin] BGW(configure)[sip_remote_side_group/113]>balancing_policy ACTIVE_STANDBY
[bgw-admin] BGW(configure)[sip_remote_side_group/113]>group_member_ids 111:cs_1.1,
112:cs_1.2.
```

Результат настройки:

```
[bgw-admin] BGW(configure)[sip_remote_side_group/113]>show
sip_remote_side_group
      sip_remote_side_id                  113
      balancing_policy                    ACTIVE_STANDBY
      group_member_ids                    ['111:cs_1.1', '112:cs_1.2']
```

4.12.2.2. Пример настройки удаленной стороны SIP в сети IMS

Необходимо описать конфигурацию удаленной точки в сети IMS с доменом ims.ekb.ru.

- Данная удаленная точка представляет собой I-CSCF.
- BGW будет выступать в роли P-CSCF.
- Транспортный протокол для взаимодействия: UDP.
- Ограничения CAC – нет.

Процедура настройки

- Создайте базовую конфигурацию удаленной стороны, введя данные:

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>sip_remote_side
[bgw-admin] BGW(configure)[sip_remote_side]>create 200
[bgw-admin] BGW(configure)[sip_remote_side/200]>sip_remote_side_name ims_core_ekb
[bgw-admin] BGW(configure)[sip_remote_side/200]>sip_remote_side_type IMS
```

Результат настройки:

```
[bgw-admin] BGW(configure)[sip_remote_side/200]>show
sip_remote_side
     sip_remote_side_id                  200
     sip_remote_side_name                ims_core_ekb
     sip_remote_side_type                IMS
     cac_profile_id                      null
```

Далее необходимо указать конфигурацию удаленной точки согласно ее типу. Для этого нужно вернуться в меню **configure** и перейти в соответствующие разделы.

Ввод данных:

```
[bgw-admin] BGW(configure)>sip_remote_side_ims
[bgw-admin] BGW(configure)[sip_remote_side_ims]>edit 200
[bgw-admin] BGW(configure)[sip_remote_side_ims/200]>ims_domain ims.ekb.ru
```

Результат настройки:

```
[bgw-admin] BGW(configure)[sip_remote_side_ims/200]>show
sip_remote_side_ims
     sip_remote_side_id                  200
     ims_domain                          ims.ekb.ru
```

4.13. Связка интерфейса SIP с удаленной стороной

В этом разделе описывается, как в конфигурации настроить, с какими удаленными сторонами (см. раздел 4.12) работает интерфейс SIP (см. раздел 4.11) типа TRUNK.

После настройки интерфейсов SIP типа TRUNK и удаленных сторон необходимо указать, с какими удаленными сторонами работает интерфейс SIP.

Если интерфейс SIP типа TRUNK не связан с удаленной стороной, то с интерфейса SIP невозможно отправить сообщение SIP на удаленную сторону (так как неизвестны реквизиты удаленной стороны), а также принять сообщение от этой удаленной стороны.

В пограничном шлюзе BGW предусмотрена возможность указать одну или множество удаленных сторон для одного интерфейса SIP. Каждая удаленная сторона также может быть указана для разных интерфейсов SIP.

4.13.1. Настройка связки интерфейса SIP с удаленной стороной

Чтобы создать и настроить удаленную сторону для интерфейса типа TRUNK:

1. Запустите интерфейс BGW CLI пользователем с правами администратора BGW.
2. Введите **configure** и нажмите клавишу <Enter>.

```
[bgw-admin] BGW> configure
[bgw-admin] BGW(configure)>
```

3. Введите **sip_interface_remote_sides** и нажмите клавишу <Enter>.

```
[israfilov] BGW(configure)>sip_interface_remote_sides
[israfilov] BGW(configure)[sip_interface_remote_sides]>
```

4. Введите **create** и через пробел введите уникальный идентификатор ранее созданного интерфейса SIP, нажмите клавишу <Enter>.

```
[israfilov] BGW(configure)[sip_interface_remote_sides]>create 2
```

```
[israfilov] BGW(configure)[sip_interface_remote_sides/2]>
```

5. Введите имя параметра и через пробел значение этого поля и нажмите клавишу <Enter>.
   - **sip_remote_side_ids**: уникальные идентификаторы удаленной стороны, указываются через запятую (удаленная сторона должна быть заранее создана в таблице **sip_remote_side** (см. раздел 4.12.1.1)), разрешен формат ввода `<идентификатор>:<имя>`. Необязательный параметр.
6. Сохраните конфигурацию