ГАРДА

Модуль Сетевой экран

Руководство пользователя

gardatech.ru

2023

Тип документа:	Руководство пользователя
Дата выпуска:	09.10.2023
Статус документа:	Released
Версия:	5.0.0

ООО "Гарда Технологии"
Все права сохраняются за правообладателем.

ООО "Гарда Технологии" оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО "Гарда Технологии". Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким- либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО "Гарда Технологии". Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство пользователя к программному модулю "Сетевой экран", входящему в состав программного обеспечения "Гарда БД" (далее Система, Комплекс).

1.2 Типографические соглашения

Обозначения и типографические соглашения, использованные в данном документе, приведены ниже.

Пример	Обозначение
***Примечание**: текст*	Важная информация, требующая особого внимания
См. Руководство администратора	Ссылка на документ
Войти	Названия вкладок, кнопок и конфигурационных параметров в веб-интерфейсе
http://www.example.com/	Гиперссылки

1.3 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

Гарда Технологии (входит в ГК Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту

цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

1.5 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по московскому времени).
- Email: gbd.support@gardatech.ru.

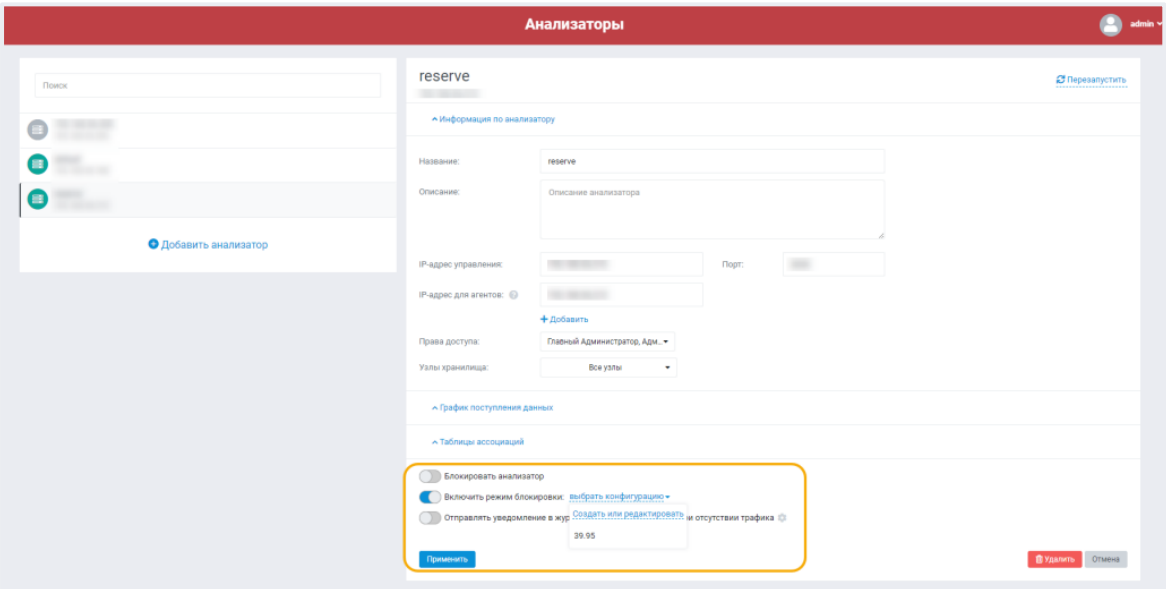
2 Назначение модуля

Модуль "Сетевой экран" (далее Модуль) предназначен для блокировки пользовательских запросов к СУБД/серверам приложений в режиме реального времени с помощью политик блокировки.

3 Настройка режима блокировки

Для того чтобы настроить режим блокировки, выполните следующие действия:

1. При установке Модуля выберите пункт `Включить сетевой экран`. Подробнее об установке и настройке модуля см. *Руководство администратора раздел Установка сетевого экрана*.
2. На сервере "Гарда БД" в разделе `/opt/web_pu` откройте файл `appsettings.json` и в строке `Firewall` установите значение `true`.
3. Подключитесь к серверу "Гарда БД" через ssh-консоль и введите команду:
   `service web_pu restart`
4. Зайдите в веб-интерфейс Гарда БД и выберите раздел **Настройки** → **Анализаторы**.
5. Выберите анализатор, активируйте переключатель **Включить режим блокировки**.
6. Добавьте новую конфигурацию для режима блокировки. Для этого выполните следующие действия:
   6.1. Нажмите **выбрать конфигурацию** → **Создать или редактировать**.



   6.2. На странице **Конфигурации режима блокировки** нажмите **Добавить новую конфигурацию**.

   6.3. Введите название конфигурации.

6.4. В поле **Конфигурация** задайте конфигурацию в Json-формате. Используйте кнопку **Загрузить пример настроек** для быстрого заполнения поля стандартными параметрами. В конфигурации должны быть настроены следующие параметры:

- `bind_port` - указывает, на каком TCP-порте анализатор ожидает подключения (например, `"1234"`).
- `bind_address` - указывает, на каком IP-адресе анализатор ожидает подключения (например, `"0.0.0.0"`). Все дополнительные IP-адреса необходимо настроить средствами Linux.
- `bind_ssl` - включает/выключает дешифровку SSL-трафика между клиентом и анализатором. Принимает значения `true` или `false`.
- `bind_crt_file` - имя файла в формате PEM, содержащего сертификат и приватный ключ (например, `"mysni.local.pem"`).
- `server_address` - IP-адрес сервера БД (например, `"1.1.1.1"`).
- `server_port` - TCP-порт сервера БД (например, `"5678"`).
- `server_ssl` - включает/выключает дешифровку SSL-трафика между анализатором и сервером БД. Принимает значения `true` или `false`.

При необходимости помимо стандартных параметров могут быть заданы следующие параметры:

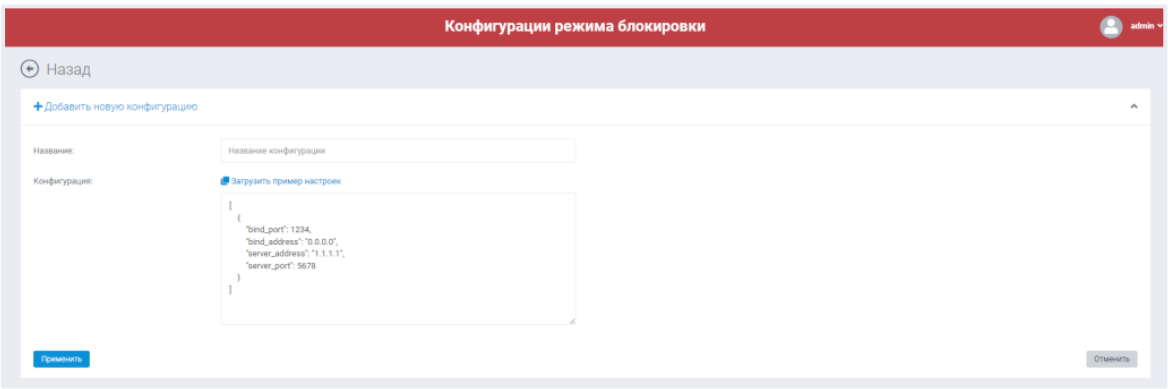
- `disabled` - прекращение приема новых соединений от клиентов. Текущие соединения не разрываются. По умолчанию имеет значение `false`.
- `server_source` - используемый IP-адрес для исходящих соединений к БД (например, `"5.6.7.8"`). Для корректной работы может потребоваться настройка маршрутизации и настройка протокола ARP.
- `server_interface` - сетевой интерфейс для исходящих соединений (например, `"eth1"`).

- `block_on_decoder_rejected` - если установить данный параметр в значение `true`, то при шифрованном соединении, нехватке памяти и других ситуациях весь трафик будет блокироваться. По умолчанию имеет значение `false`.

***Примечание**: Если контролируемых БД несколько, то для каждой из них пользователь может задать параметры с различными портами (`bind_port`) в рамках одной конфигурации.*

7. Нажмите **Применить**.
8. Перейдите обратно в раздел Анализаторы при помощи кнопки **Назад**.
9. Выберите созданную конфигурацию из раскрывающегося списка **выбрать конфигурацию**.

После включения режима блокировки все соединения на любой IP-адрес сетевого экрана по указанному в конфигурации порту будут перенаправляться на сервер БД.



4 Политики

4.1 О политиках

Перехват действий пользователей в БД/веб-приложениях и выявление подозрительных операций осуществляется на основании специальных правил (политик). Настройки политик находятся на странице **Политики**. В левой области страницы находится список политик. Напротив названия каждой политики отображается специальный счетчик, показывающий количество событий, перехваченных по политике. Возможен поиск политик по названию, сортировка по дате создания и алфавиту, фильтрация по статусу политики и используемым в политике параметрам. Блок фильтрации расположен в верхней части страницы. Для поиска политики с помощью фильтрации выберите из соответствующего раскрывающегося списка необходимый статус или параметр:

Статус:

- **Все**;
- **Запущенные**;
- **Остановленные**;

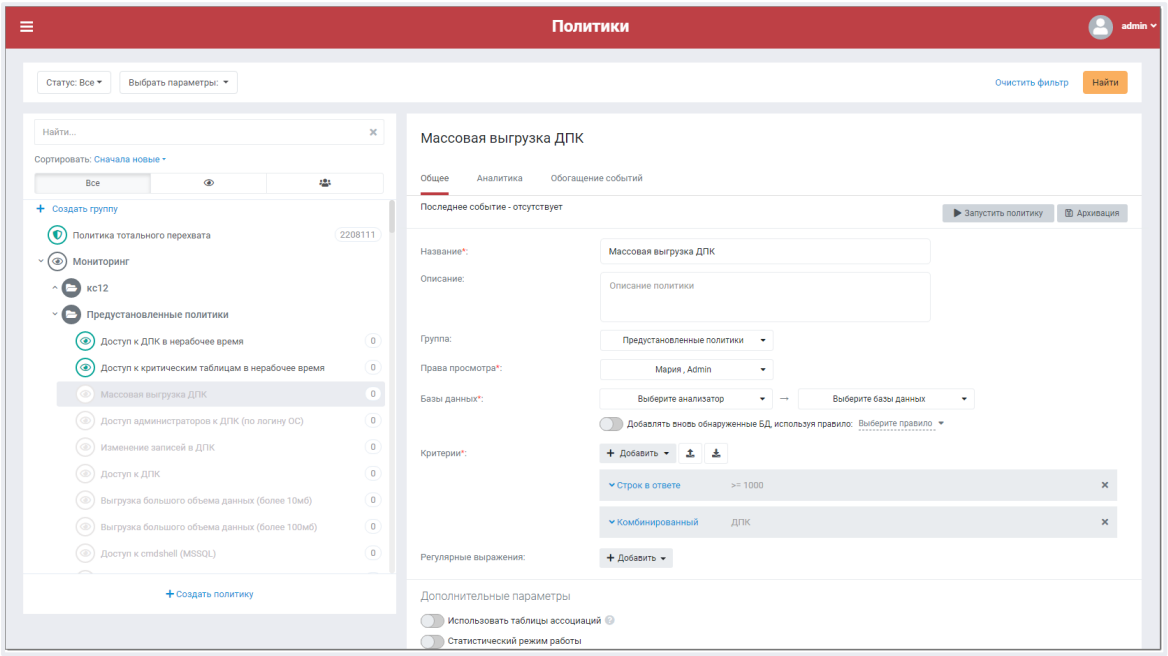
Параметры:

- **Обогащение событий**;
- **Автодобавление**;
- **Таблицы ассоциаций**;
- **Статистический режим**;
- **Экспорт в SIEM**;
- **Email оповещения**;
- **Аналитика**:
  - **Обучение**;
  - **Выявление отклонений**;
  - **Выявление аномалий**;

- **Экспорт в SIEM аномалий**;
- **Email оповещения аномалий**;
- **Аномалии за интервал**;

- **Архивация**.

При выборе политики из списка в правой области страницы появятся параметры политики.



4.2 Политики блокировки

Политики блокировки предназначены для блокировки действий пользователей в БД. Политика блокировки может быть создана как с чистого листа, так и на основе уже созданной политики.

Создание политики профилирования на основе другой

Чтобы создать политику на основе другой (т.е. с уже заполненными параметрами), выполните следующие действия:

1. Нажмите напротив нужной политики в списке или на вкладке **Общее**. Таким образом будет создана пока еще несохраненная копия политики. Проверить, что копия создалась, можно по окончанию **copy**, добавленному к названию копии.

2. При необходимости отредактируйте политику.
3. Сохраните политику.

Создание политики профилирования с чистого листа

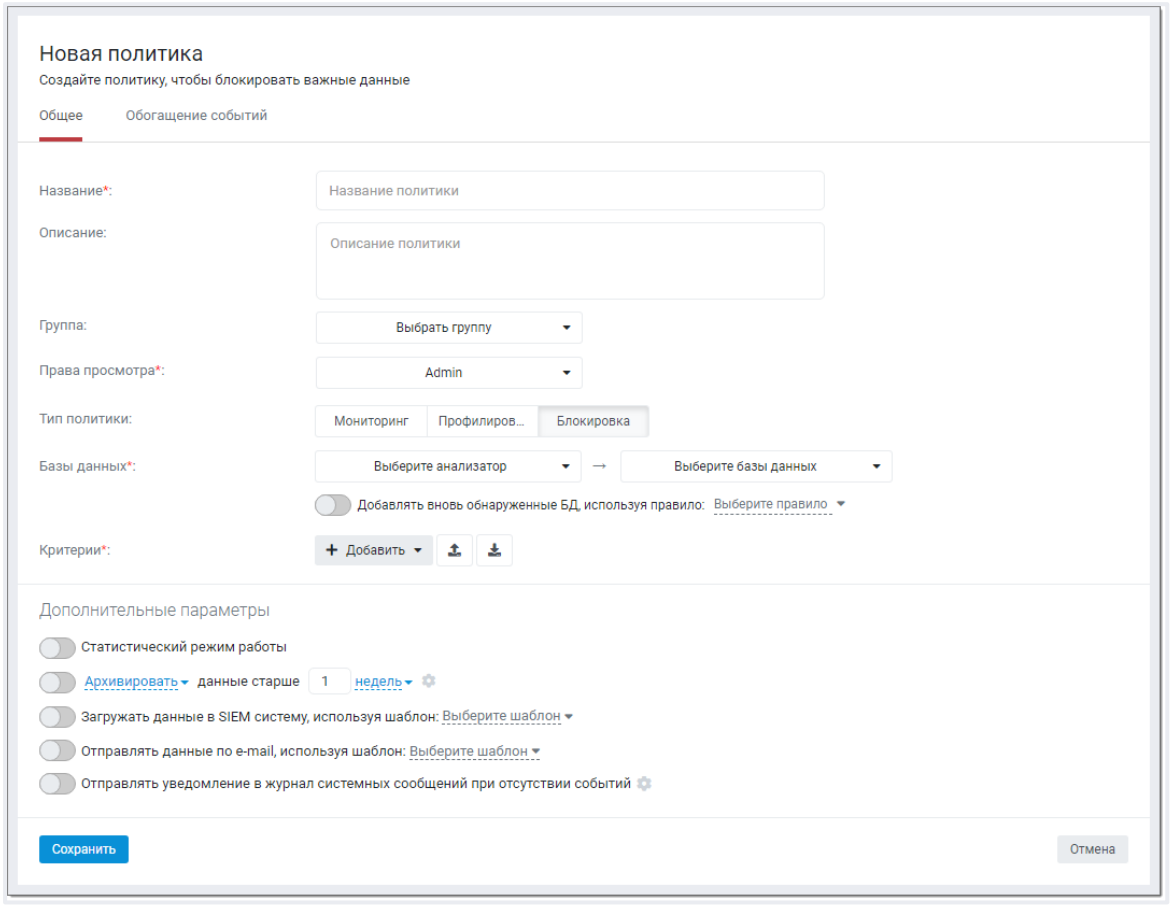
Чтобы создать политику блокировки с чистого листа, выполните следующее:

1. Находясь на странице **Политики**, нажмите **Добавить политику**, расположенную под списком политик.
2. В открывшемся окне **Новая политика** задайте параметры новой политики:
   2.1. Заполните поля **Название** и **Описание**. Название политики не может совпадать с названием другой политики или архивной папки.
   2.2. В раскрывающемся списке **Права доступа** необходимо задать права доступа к политике. При необходимости выдать право доступа пользователю раскройте роль и установите флажки напротив отдельных пользователей. При необходимости выдать права доступа целой роли установите флажок напротив роли. Однако, необходимо иметь в виду, что при выдаче прав доступа целой роли новые пользователи с данной ролью также будут иметь доступ к данной политике. У пользователей с ролями **Администратор** и **Главный администратор** доступ к политике есть всегда. У создателя политики доступ есть только до тех пор, пока не будет отозван.
   2.3. В поле **Тип политики** выберите **Блокировка**.
   2.4. В поле **Базы данных** выберите анализаторы и подлежащие контролю БД, установив соответствующие флажки. При необходимости автоматического добавления определенных баз данных в политику активируйте переключатель **Добавлять вновь обнаруженные БД, используя правило:** и выберите или создайте новое правило, по которому БД будут добавляться в политику.
   2.5. **Критерии** - задайте критерии, по которым будут перехватываться обращения к БД, при помощи кнопки **Добавить** либо путем импорта критериев из файла.

2.6. Задайте **Дополнительные параметры политики мониторинга**.

3. При необходимости пополнения событий вспомогательными данными из внутренних и внешних источников (поля запросов/ответов/переменных/веб-форм, сервер LDAP, словари) произведите настройки на вкладке **Обогащение событий**.

4. Нажмите **Сохранить**.



Примечание: *Если на агенте настроено игнорирование/блокировка по SQL-операциям или SQL-таблице, будет исключена/блокирована вся сессия полностью, начиная с запроса, на котором критерий сработал.*