



ГАРДА



Модуль Сетевой экран

Руководство администратора

gardatech.ru

2023



Тип документа: Руководство администратора
Дата выпуска: 05.10.2023
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	4
1.1 Аннотация.....	4
1.2 Типографические соглашения.....	4
1.3 Использование имен, номеров телефонов, сетевых адресов.....	4
1.4 О компании.....	4
1.5 Техническая поддержка.....	5
2 Назначение Модуля	6
3 Установка и настройка Модуля	7
4 Диагностика работы Модуля	11

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора 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
<i>См. Руководство администратора</i>	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 Установка и настройка Модуля

Установка сетевого экрана

Для установки сетевого экрана:

1. Установить rpm пакет командой: `rpm -ivh sniffer.DBS.el7.x86_64.rpm`.
2. Выбрать соответствующий пункт меню. Для этого ввести цифру, соответствующую опции **Включить сетевой экран**.

```
Вычисляем конфигурацию
-----
hp_per_node_limit=1
hp_mem_pools_per_node=70462156
hp_mem_per_sniff=700000000
sniff_per_node_hp_limit=1
common_cpus_nr=3
balancer_node=0
reserved_cpus_per_node=5
sniff_per_node_cpu_limit=3
sniff_per_node_limit=16
sniff_per_node=1
hp_per_node=1

Конфигурация
-----
Тип установки: анализатор + хранилище
Тип лицензии: сервер лицензий на 192.168.239.24
Агенты БД: нет
Агенты pcap: нет
Сетевой экран: нет

Устройства захвата:
  dpdk: 0000:00:13.0 Ethernet controller [0200]: Intel Corporation 82540EM Gigabit Ethernet Controller [8086:100e] (rev 03)
        numa_node=0 mtu=1700 fc=0 elem_size=2048 elem_count=32767 sp=0 sc=0

CPUs:
  master 0
  balancer 1
  sniff 2
  spool 3
  aaa_proc 3
  reserved 4 5 6 7
hugepagesz 2M
hugepages 512

Что делать дальше?
-----
y - Начать установку
1 - Изменить тип установки
2 - Изменить тип лицензии
3 - Добавить устройство захвата
4 - Удалить устройство захвата
5 - Включить/выключить агенты БД
6 - Включить/выключить сетевой экран
7 - Показать конфигурацию
8 - Выполнить автонастройку
9 - Показать информацию о системе
q - Выход
```

Отображение настройки сетевого экрана в веб-интерфейсе

Для того, чтобы в веб-интерфейсе появилась возможность настройки Модуля:

1. Отредактировать конфигурационный файл `/opt/web_pu/appsettings.json`:
 - Найти строку `Firewall: false`, изменить `false` на `true`.

2. Перезапустить сервис web_pu командой `service web_pu restart`.

Использование анализатора в режиме съема трафика и сетевого экрана одновременно

Если анализатор будет использоваться одновременно в режиме съема трафика (выбраны устройства захвата) и в режиме сетевого экрана (включен сетевой экран), то необходимо выполнить ручную донастройку анализатора:

1. Отредактировать в `probe.cfg` устройства.
 - Заменить часть `device: tcp_proxy` на `device: dpdk:rngX`.
Соотношение устройств должно соответствовать соотношению объема обрабатываемого трафика сетевым экраном и трафиком поступающим со SPAN и с агентов. Общее количество не должно изменяться.

Например:

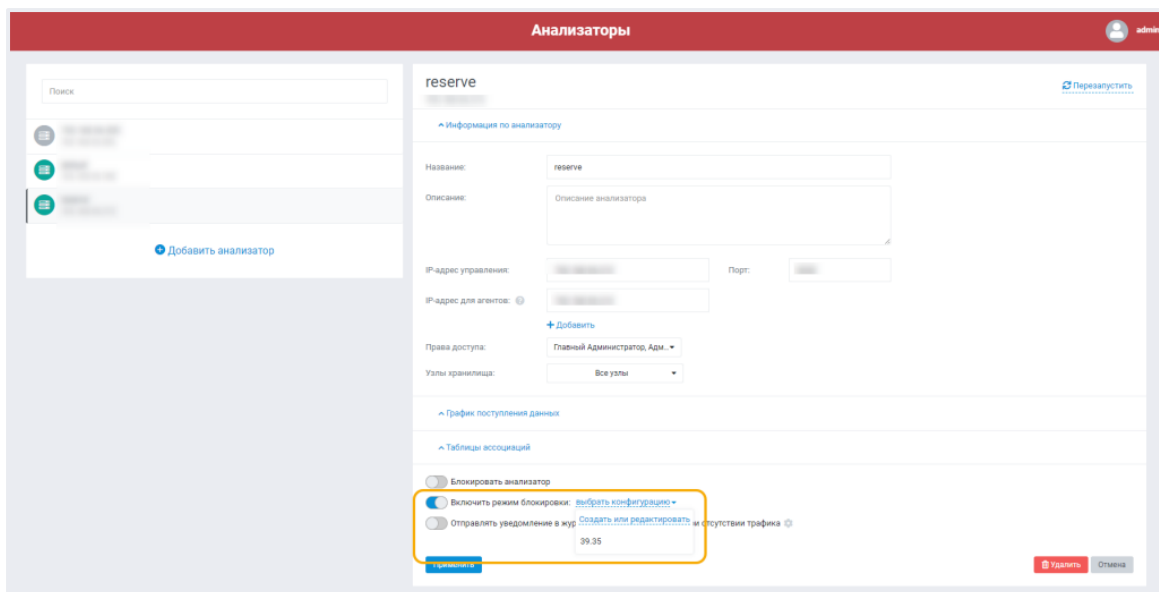
```
device: dpdk:rng1
device: dpdk:rng2
...
device: dpdk:rngN
device: tcp_proxy
...
device: tcp_proxy
```

2. Отредактировать в `meteor.conf` раздел `jobs/bs0/ports/lp1/out`.
Количество `rngX` должно совпадать с указанными в `probe.cfg`.

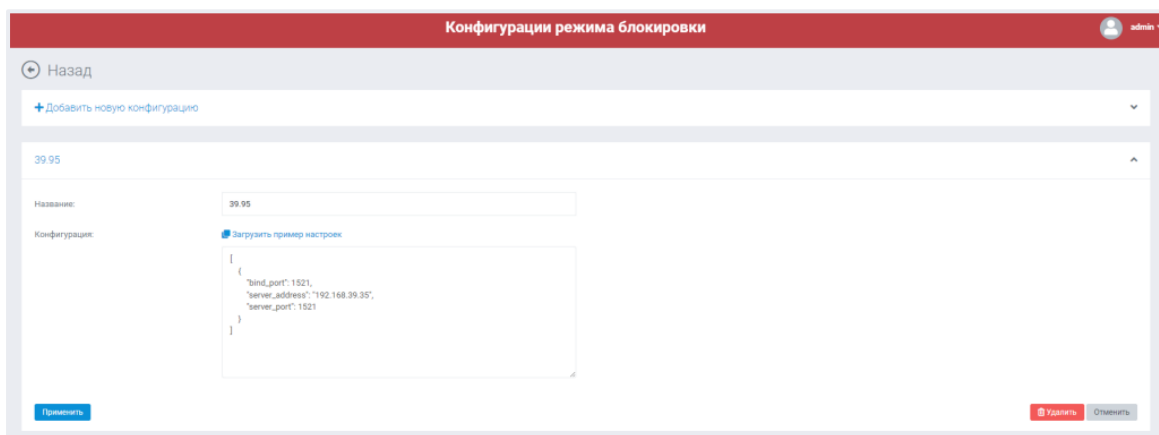
Конфигурирование сетевого экрана в веб-интерфейсе

Для конфигурирования сетевого экрана:

1. Открыть раздел **Настройки** → **Анализаторы**.
2. Выбрать анализатор и включить режим блокировки.



3. Создать новую конфигурацию сетевого экрана выбрав **Создать или редактировать** в выпадающем меню **Выбрать конфигурацию**.
4. На странице создания конфигурации необходимо указать название конфигурации и заполнить поле **Конфигурация**. Для удобства можно воспользоваться [примером настроек](#).



5. После первого обращения к базе данных, она будет автоматически обнаружена анализатором. Её можно будет поставить на контроль на странице Базы данных.
6. В клиенте подключения к БД необходимо изменить IP-адрес и порт подключения к БД на IP-адрес сетевого экрана и порт, указанные при настройке ранее.

Пример конфигурации сетевого экрана:

```
[
{
  "bind_port": 1234,
  "bind_address": "0.0.0.0",
  "server_address": "192.168.0.2",
  "server_port": 5678
}
]
```

Настройки конфигурации имеют следующие параметры:

- `bind_port` - порт на котором ожидаются подключения от клиента.
- `bind_address` - явно указывает на каком IP-адресе анализатор ожидает подключение, все дополнительные IP-адреса нужно настроить средствами Linux. Если указан IP 0.0.0.0 то соединения ожидаются на всех IP адресах.
- `server_address` - IP-адрес сервера базы данных.
- `server_port` - порт сервера базы данных.
- `disabled` - прекращение приема новых соединений от клиентов, текущие соединения не разрываются. По умолчанию имеет значение `false`.
- `source` - используемый IP-адрес для исходящих соединений к БД, для корректной работы возможно потребуется настройка маршрутизации и протокола ARP (например, `"192.168.0.3"`).
- `interface` - сетевой интерфейс для исходящих соединений (например, `"eth1"`).

4 Диагностика работы Модуля

Для проверки работы выполните команду: `test_sniff -q all/proxy.`

Пример результата приведен ниже.

```
===== НАЧАЛО КОМБИНИРОВАННОГО ТЕСТИРОВАНИЯ СНИФФЕРА =====
all/proxy
192.168.239.83:81=192.168.239.105:80 :
conn_active : 0
conn_active_closing : 0
conn_active_decode : 0
conn_active_initial : 0
conn_active_max : 0
conn_active_pending : 0
conn_active_proxy : 0
conn_active_tasting : 0
conn_closed : 0
conn_closed_blocked : 0
conn_closed_connect_server_error : 0
conn_closed_connect_server_timeout : 0
conn_closed_disabled : 0
conn_closed_fin_timeout : 0
conn_closed_idle_decode_timeout : 0
conn_closed_idle_proxy_timeout : 0
conn_closed_io_error : 0
conn_closed_no_mem : 0
conn_closed_normal : 0
conn_closed_not_tasted : 0
conn_closed_taste_timeout : 0
conn_closed_unk_error : 0
conn_closed_wrong_proto : 0
conn_created : 0
conn_proxy_decoder_overflow : 0
conn_proxy_decoder_rejected : 0
conn_proxy_decoder_stall : 0
conn_proxy_no_mem : 0
conn_proxy_not_tasted : 0
conn_proxy_taste_timeout : 0
conn_proxy_wrong_proto : 0
conn_tasted : 0
data_client_read :
  bytes : 0 бит/сек
  packets : 0 объектов/сек
=====
data_client_write :
  bytes : 0 бит/сек
  packets : 0 объектов/сек
=====
data_server_read :
  bytes : 0 бит/сек
  packets : 0 объектов/сек
=====
data_server_write :
  bytes : 0 бит/сек
  packets : 0 объектов/сек
=====
disabled : 0
=====
conn_deferred : 0
conn_deferred_max : 0
=====СНИФФЕР 0, ААА PROC 1===== КОНЕЦ КОМБИНИРОВАННОГО ТЕСТИРОВАНИЯ СНИФФЕРА =====
```