StormWall Sensor Appliance

Руководство пользователя

Введение

StormWall Sensor Appliance представляет собой многопользовательский программный сервис, который взаимодействует с сетевым оборудованием и получает с него информацию о трафике либо сэмплированный трафик. Далее, на основании этой информации, проводится аналитика включающая в себя выявление DDoS-атак, выявление легитимного и нелегитимного трафика с последующим оповещением пользователя о выявлении атак. Сервис отображает все подробности выявленных атак, включая графическое представление. Сервис также определяет время атаки, период ее начала и завершения.

Сервис поддерживает ролевую модель работы пользователей, включающую в себя администраторские и пользовательские роли. Администратор может создавать новых пользователей в рамках выделенных ему прав, выделять им диапазоны IP-адресов и объемы (скопы). Последняя функция позволяет сдавать сервис в субаренду другим заказчикам.

Получение дистрибутива и его установка

Получение

Обратитесь в отдел продаж компании StormWall, заключите Договор и произведите оплату лицензии. Также предусмотрен вариант предварительного тестирования Sensor Appliance перед принятием решения о приобретении лицензии. Получите от менеджера отдела продаж ISO-образ (ссылку для скачивания) дистрибутива Sensor Appliance, ключ активации и инструкцию по установке. ISO-образ содержит специальную версию операционной системы Linux, в которую уже интегрирована система Sensor Appliance. Размер ISO-образа составляет около 1 ГБ.

Технические требования

Для установки системы StormWall Sensor Appliance необходим выделенный сервер. со следующими минимальными характеристиками:

- 8-ми ядерный CPU;
- 16 ГБ RAM;
- 50GB SSD.

В качестве операционной системы на виртуальную машину устанавливается дистрибутив Sensor Appliance. Также возможна установка на “чистое железо” (Bare Metal).

Установка

Установите Sensor Appliance, руководствуясь инструкцией по установке. Введите ключ активации. После активации и завершения процесса установки сервер автоматически перезагрузится, после чего система Sensor Appliance будет готова к работе и регистрации первого пользователя.

Регистрация

Регистрация Администратора

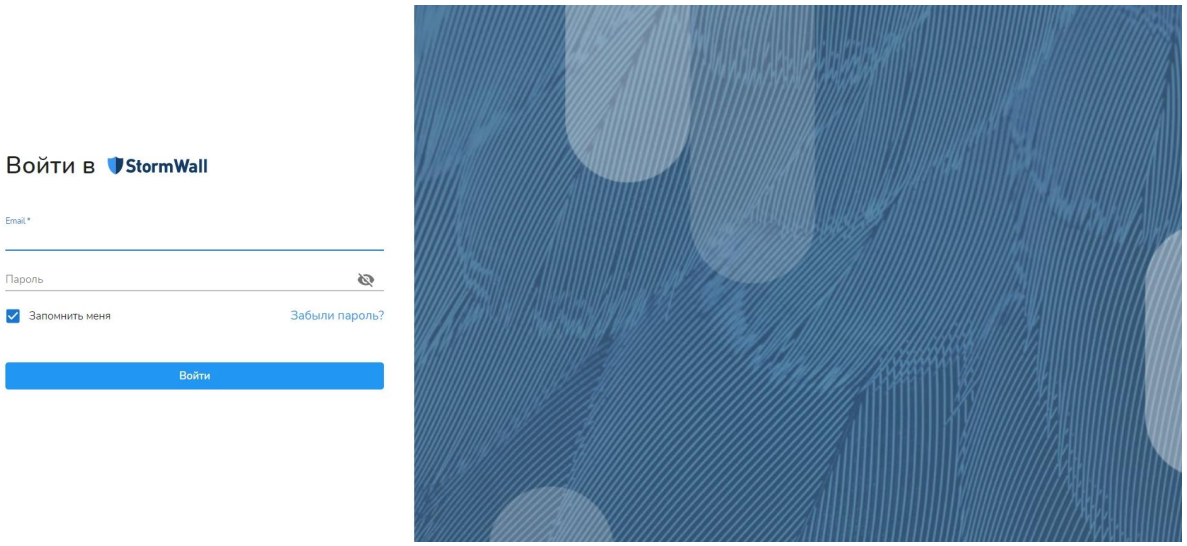
Если осуществляется первый вход в систему, пользователь получит предложение завести аккаунт Администратора. Для этого необходимо указать e-mail и пароль, а затем нажать на кнопку **Register**.

В дальнейшем учетные записи новых пользователей создает Администратор системы.

Создание Пользователя

Для создания нового пользователя выполните следующие действия:

- Авторизуйтесь в системе с правами Администратора;

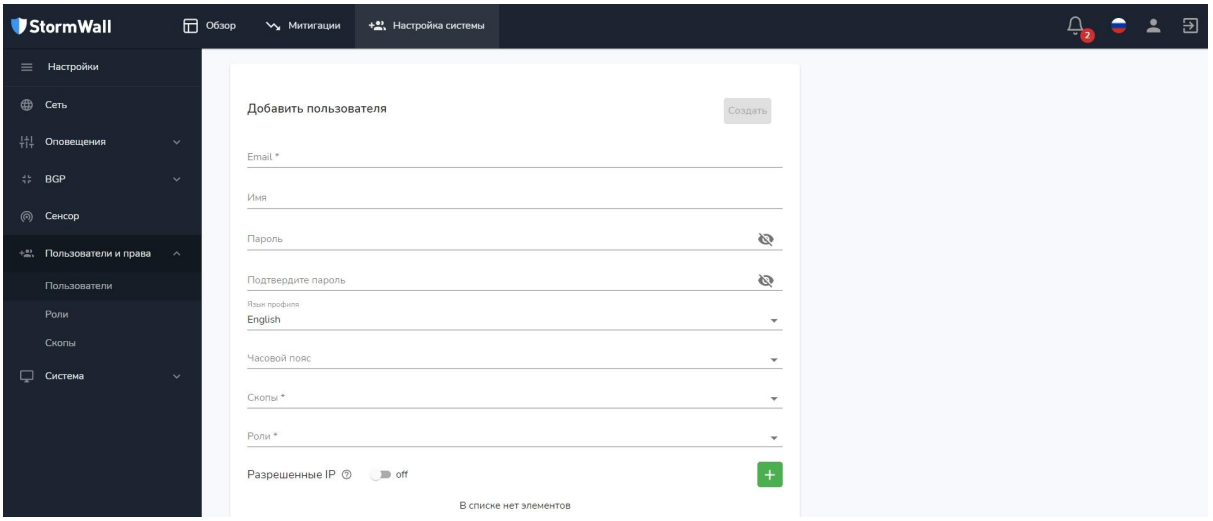


- В главном меню выберите пункт **Настройка системы**;
- В меню **Пользователи и права** → **Пользователи** нажмите на кнопку **Создать пользователя**;
- На открывшейся странице **Добавить пользователя** заполните следующие необходимые параметры:
    - Email;
    - Пароль (должен содержать не менее 8 символов, не менее одной заглавной буквы и не менее одного спецсимвола);
    - Скопы (если они необходимы для данного пользователя);
    - Роли (выберите из списка - Administrator, User).

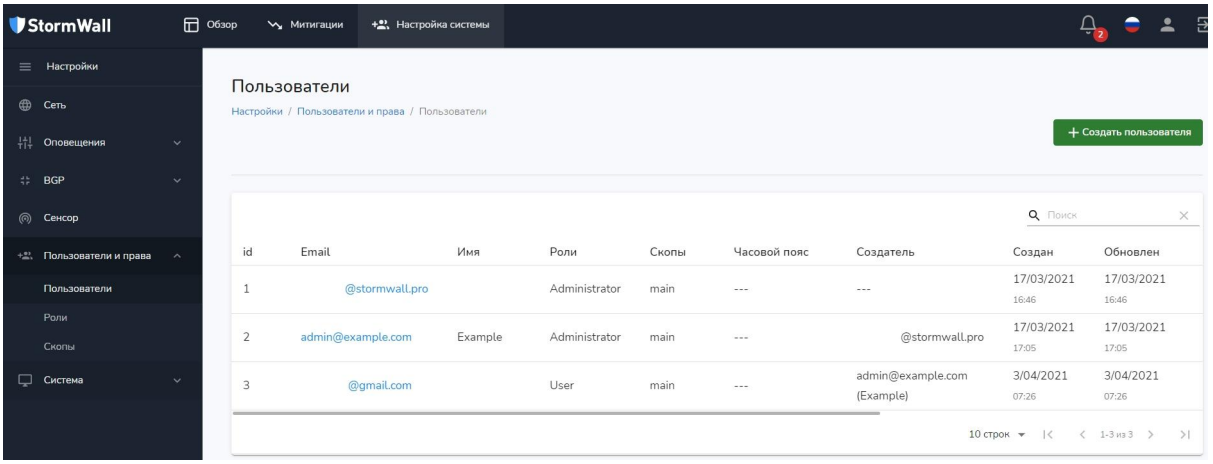
При необходимости также заполните необязательные параметры:

- Язык интерфейса пользовательского профиля (Русский или Английский);
- Часовой пояс;
- Включите диапазон разрешенных IP-адресов, с которых сможет заходить пользователь, если этого требует политика информационной безопасности.

После заполнения нажмите на кнопку **Создать**. Если все параметры заполнены корректно, она будет активной. При наличии ошибок, они будут подсвечены и снабжены подсказками красного цвета.

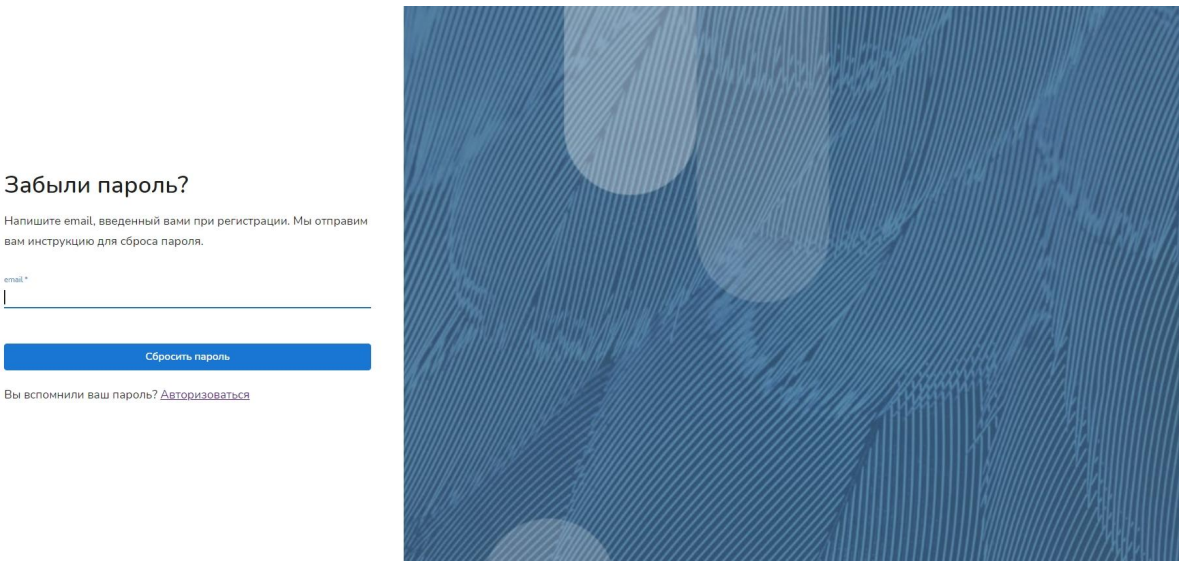


Добавленного пользователя можно найти в списке в меню **Настройки** → **Пользователи и права** → **Пользователи**. Теперь он может авторизоваться в системе, введя свои учетные данные.



Восстановление пароля

Для восстановления утерянного или забытого пароля на странице входа нажмите на ссылку **Забыли пароль?**. На открывшейся странице **Забыли пароль?** введите Email, указанный при регистрации.

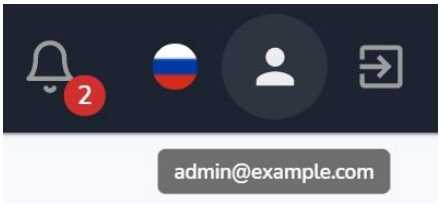


Пользователю будет отправлен проверочный код, который необходимо ввести для создания нового пароля.

Для работоспособности данной функции нужно настроить параметры SMTP-сервера (подробнее см. SMTP) в настройки Sensor Appliance, в противном случае Sensor Appliance не сможет отправить ссылку на восстановление пароля.

Личный кабинет

У каждого пользователя системы StormWall Sensor Appliance имеется **Личный кабинет**. Чтобы войти в него, необходимо авторизоваться в системе, и в правом верхнем углу главного меню нажмите на кнопку с символическим изображением человечка. При наведении на нее курсора мыши всплывает Email пользователя.



В **Личном кабинете** пользователь может добавить или изменить необходимую информацию о себе. В разделе **Общая информация** можно указать:

- Имя;
- Часовой пояс;
- Язык профиля;
- Формат даты;
- Формат времени;
- Скопы (подсети для субарендаторов). Данный параметр предназначен только для чтения и изменять его может только администратор через административный интерфейс (подробнее см. Скопы).

Также в **Личном кабинете** можно сменить адрес Email и пароль. При изменении любого параметра необходимо нажать на кнопку **Сохранить**.

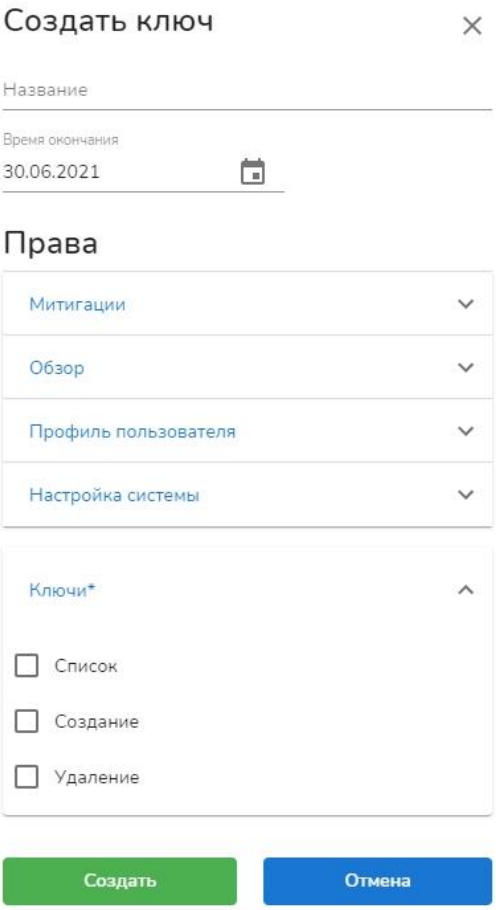
Примечание: в целях безопасности под одной и той же учетной записью может быть выполнен вход только из одного браузера.

Создание API-ключа

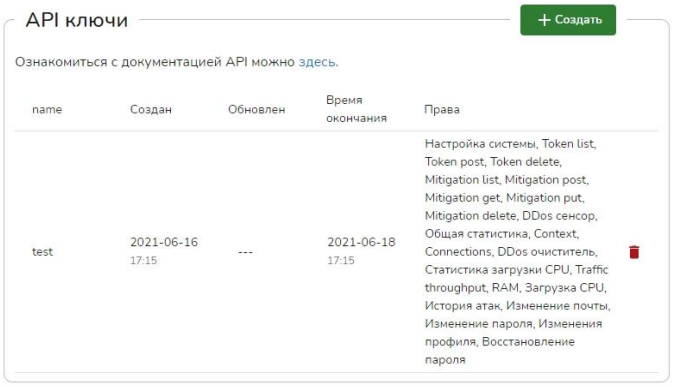
В Личном кабинете можно создать API-ключ для работы с API-запросами. API-запросы используются для взаимодействия с Sensor Appliance с помощью сторонних сервисов и приложений. Подробнее см. API.
Для создания API-ключа выберите в Личном кабинете раздел **API ключи** и нажмите на кнопку **Создать**.
В открывшемся окне **Создать ключ** укажите:

- **Название**;
- **Время окончания** (Дата окончания действия ключа);
- В разделе **Права** настройте права на выполнение различных операций в системе с помощью создаваемого ключа;
    - Митигации;
        - Список;
        - Создание;
        - Чтение;
        - Обновление;
        - Удаление.
    - Обзор;
        - DDoS сенсор;
        - Статистика загрузки CPU;
        - RAM;
        - Загрузка CPU;
        - История атак.
    - Профиль пользователя;
        - Изменение почты;
        - Изменение пароля;
        - Изменения профиля;
        - Восстановление пароля.
    - Настройка системы.
        - Настройка системы.
- Раздел “Ключи”, который позволяет создать ключ, с помощью которого можно производить операции над другими ключами.
    - Список;
    - Создание;
    - Удаление.

Поставьте галочки в нужных пунктах раскрывающегося меню, а затем нажмите на кнопку **Создать**.



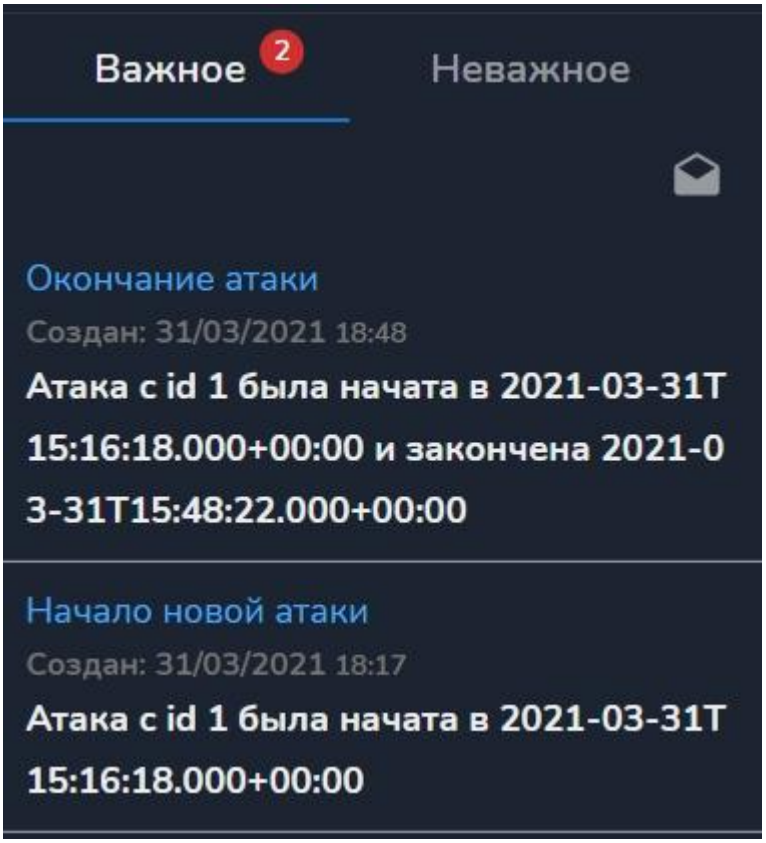
Созданный API-ключ появится в разделе **API ключи** в Личном кабинете.



Оповещения

В процессе работы с системой пользователь получает служебные оповещения о различных событиях и инцидентах, проведении работ и т.д. Их генерирует система. Для просмотра оповещений нажмите на символическое изображение колокольчика, расположенное в правом верхнем углу главного меню. Новые и непрочитанные уведомления обозначаются в виде красного кружочка возле колокольчика. На кружочке находится цифра, которая показывает число непрочитанных уведомлений.

Оповещения разделяются на **Важные** и **Неважные**. В раздел **Важные** попадают сообщения о начале и конце атаки на ресурсы текущего пользователя.



Настройка системы

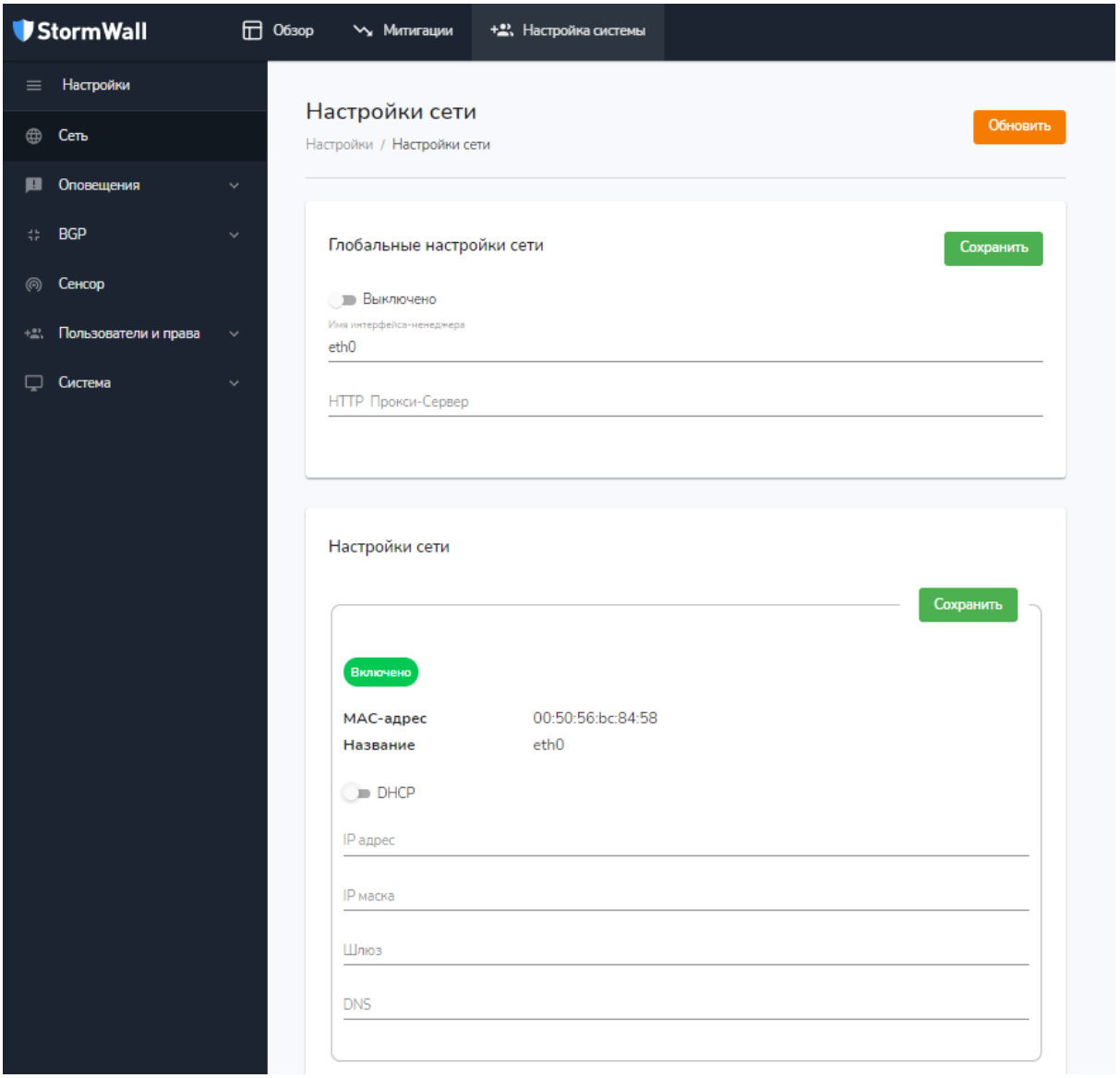
Для настройки системы выберите в главном меню пункт **Настройка системы**. Он доступен только Администратору системы (Administrator) или пользователю, которому было предоставлено разрешение на работу с настройками, подробнее см. Создание роли. По умолчанию открывается страница **Настройка сети**.

Настройка сети

В системе StormWall Sensor Appliance можно подключить несколько сетевых интерфейсов, каждый из которых можно настроить по-отдельности.
Обязательно нужно указать имя интерфейса, у которого есть доступ до ресурса *sb.stormwall.pro*, используемого в служебных целях.
Для настройки сетевого интерфейса виртуальной машины подключите его к StormWall Sensor Appliance, а затем нажмите на кнопку **Обновить**. Настройки нового сетевого интерфейса будут отображены в меню **Настройки** → **Настройки сети**. Это следующие параметры:

- DHCP (включение или выключение);
- IP-адрес;
- IP-маска;
- Шлюз;
- DNS.

После редактирования параметров необходимо нажать на кнопку **Сохранить**.
В разделе Глобальные настройки сети указывается название **Имя интерфейса-менеджера** (название управляющего интерфейса, через который осуществляется работа с системой), а также, при необходимости, адрес **HTTP-Прокси-сервера**.



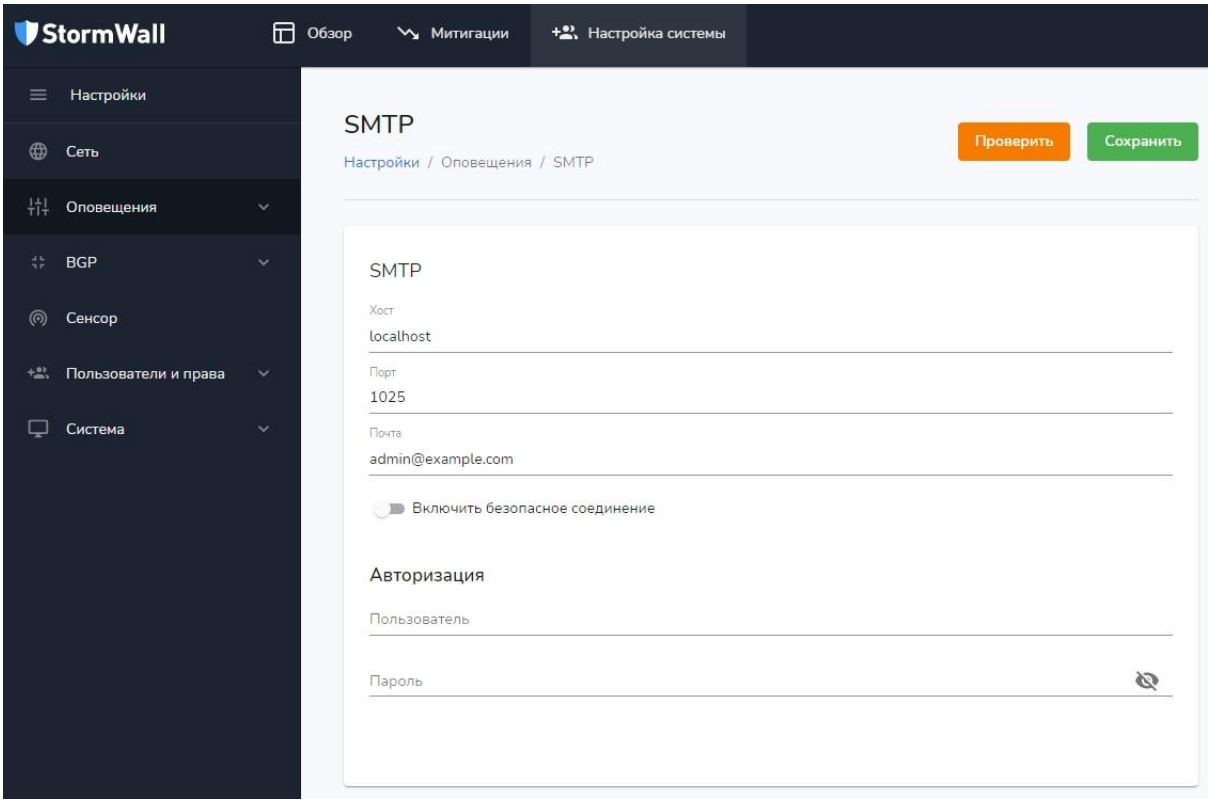
Настройка оповещений

StormWall Sensor Appliance может автоматически отправлять оповещения о события на Email пользователя и в различные сторонние сервисы, например в мессенджеры через webhooks.

SMTP

Чтобы пользователи системы могли получать письма со ссылками на восстановление пароля, а также оповещения о важных событиях, необходимо настроить SMTP-сервер.

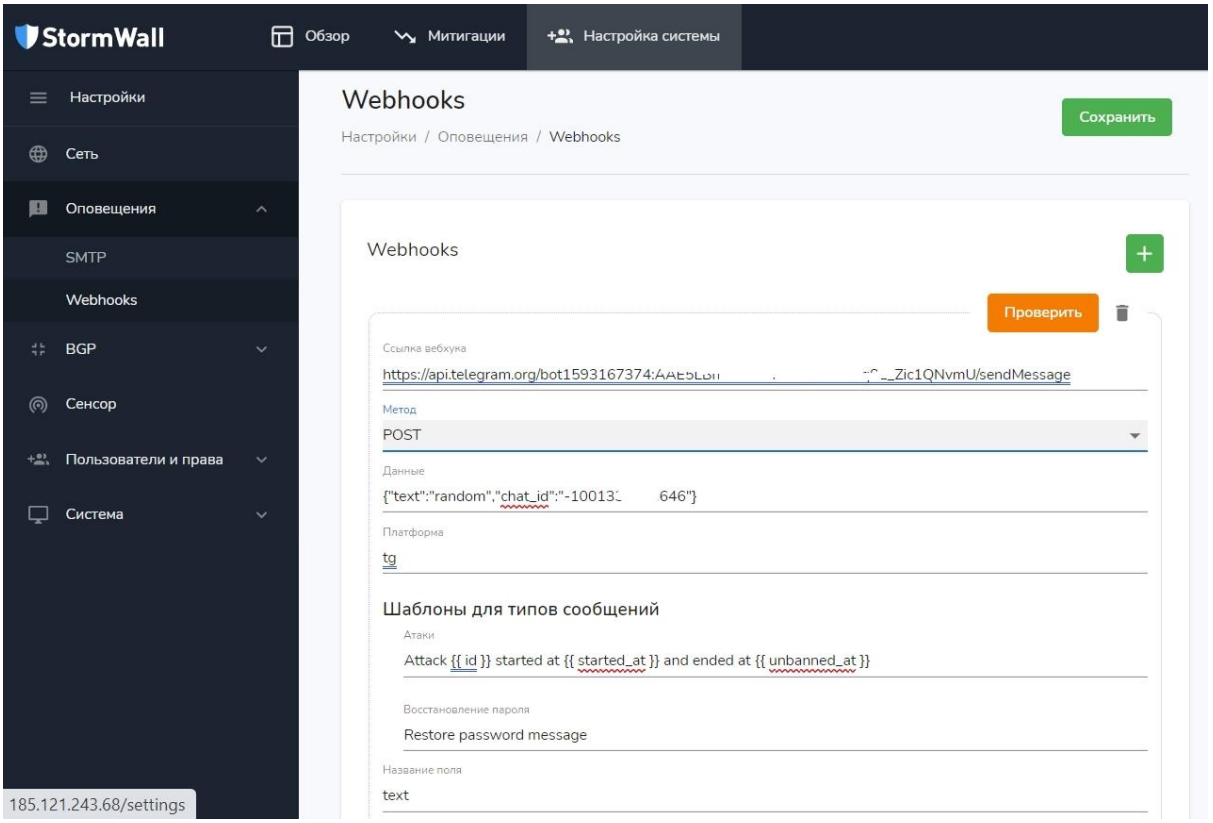
В меню **Настройки** → **Оповещения** → **SMTP** укажите адрес сервера (хост), порт и Email (этот email будет указан в поле **От кого** для каждого письма), а также имя пользователя и пароль для SMTP. Для проверки работоспособности настройки нажмите на кнопку **Проверить**, а для сохранения - на кнопку **Сохранить**.



Webhooks

В меню **Настройки** → **Оповещения** → **Webhooks** вы можете настроить параметры оповещений, поступающих в различные приложения. На скриншоте приведен пример настройки для мессенджера Telegram.

Для проверки работоспособности настроек нажмите на кнопку **Проверить**. Если вы увидите сообщение о том, что проверка прошла успешно, нажмите на кнопку



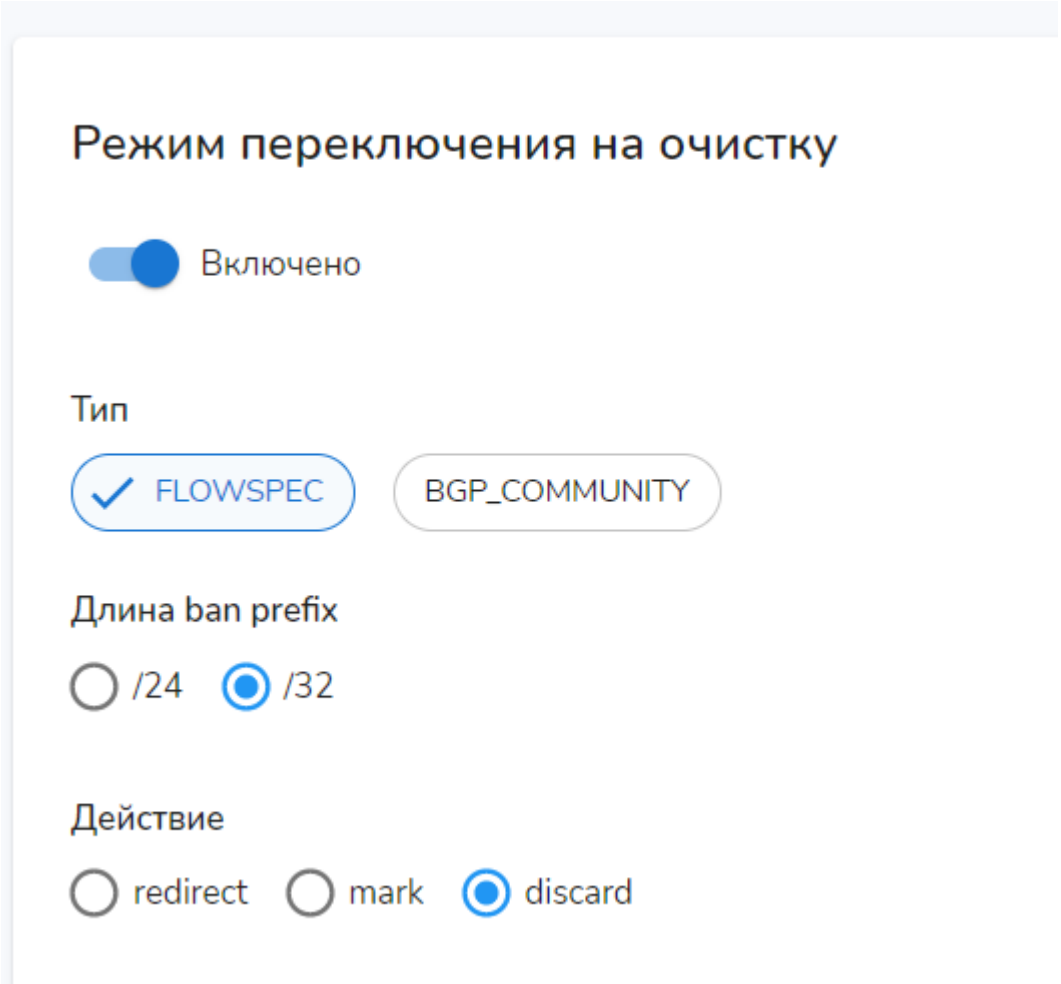
Сохранить. Вы можете создать любое необходимое количество вебхуков. Для создания нового вебхука нажмите на кнопку с изображением плюса, а для удаления ошибочных и более ненужных - на изображение корзины.

Настройка BGP

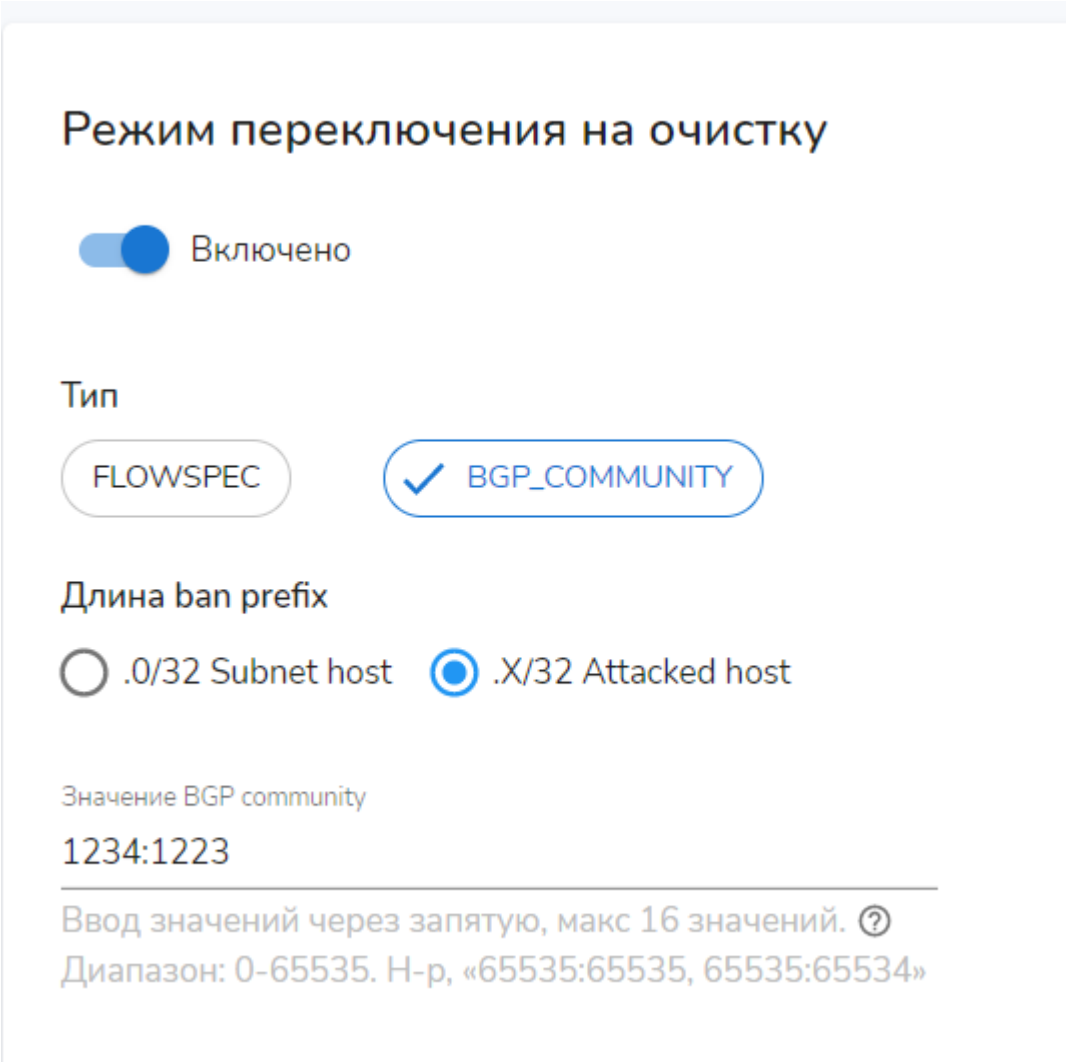
Если вы используете маршрутизацию по BGP-протоколу, настроить ее можно в меню **Настройки → BGP-протокол → Настройки BGP**. Благодаря использованию BGP-маршрутизации, можно настроить очистку трафика. Такая очистка может происходить как на серверах компании StormWall, так и на площадках других компаний, в зависимости от ваших предпочтений. Фактически, благодаря BGP-маршрутизации, нелегитимный трафик может быть отсечен на сетевом уровне. В разделе **Режим переключения на очистку** вы можете выбрать один из двух вариантов, нажав на соответствующую кнопку:

- **FLOWSPEC;**
- **BGP_COMMUNITY.**

При выборе режима **FLOWSPEC** можно указать в качестве длины ban prefix /24 (вся подсеть) или /32 (один атакуемый IP-адрес), а в качестве выбранного действия - **redirect** (перенаправление), **mark** (маркировка) или **discard** (перевод в “blackhole”).



При выборе режима **BGP_COMMUNITY** в качестве длины ban prefix следует указать .0/32 Subnet host или .0/32 Attacked host. В первом случае обрабатывается весь трафик подсети, а во втором - только трафик, идущий на атакуемый адрес. В качестве значения BGP Community по умолчанию установлено 1234:1223. Вы можете ввести любое значение в формате AS:community, например 65535:65535, 65535:65534. Для правильного выбора значений, нужно знать число поддерживаемых community. Обратитесь к производителю или к документации вашего роутера.

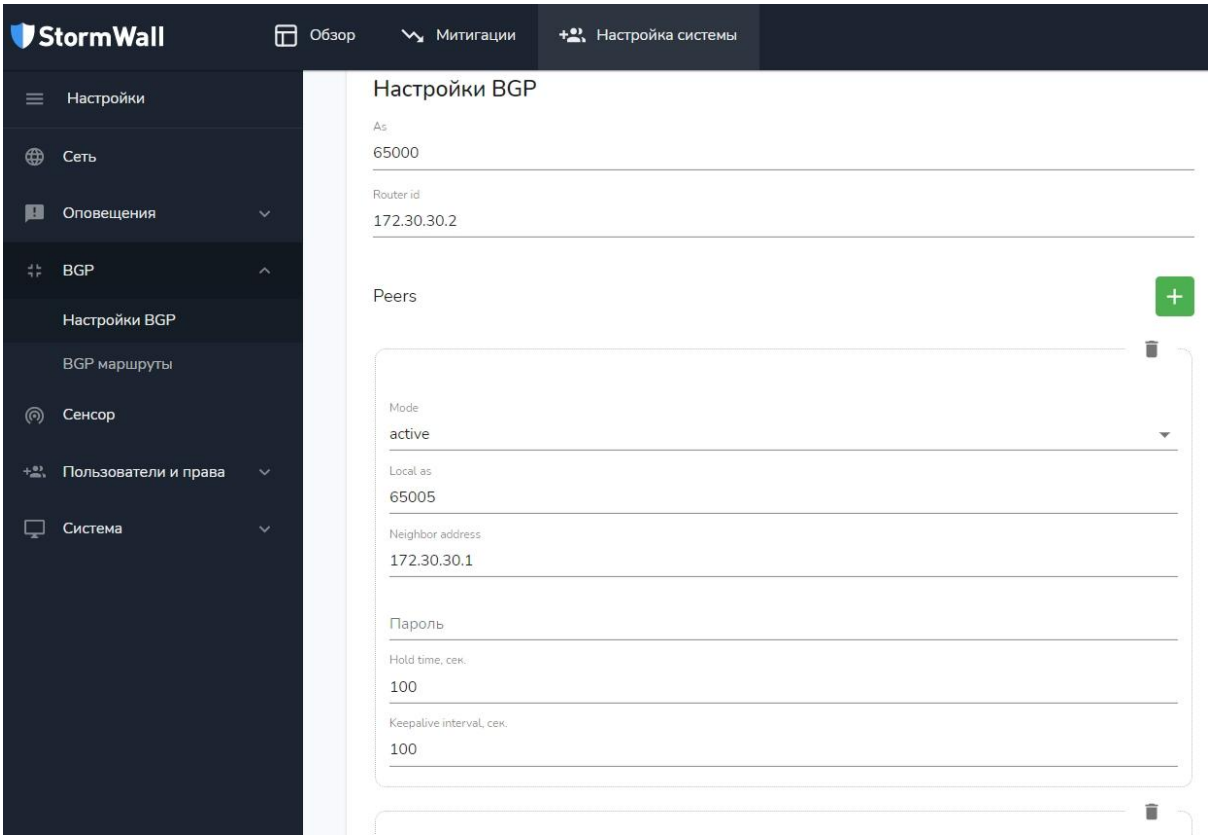


В разделе **Настройки BGP** необходимо настроить следующие параметры:

- **As.** Номер клиентской сети;
- **Router ID**. IP-адрес BGP-маршрутизатора;
- **Peers**. Одноранговые узлы, устанавливаемые между BGP-маршрутизаторами.

В меню настройки **Peers** можно настроить следующие параметры:

- **Mode** (режим). Active или Passive;
- **Local as** (локальный номер клиентской сети);
- **Neighbor address** (локальный IP-адрес);
- **Пароль**;
- **Hold time**;
- **Keepalive interval**.



Просмотр и удаление уже работающих BGP-маршрутов доступны в меню **Настройки → BGP-протокол → BGP маршруты**.

Настройка сенсора

В меню **Общие настройки** укажите следующие параметры:

КАТЕГОРИЯ	ПАРАМЕТР	ОПИСАНИЕ
Общая блокировка трафика	enable_ban disable (switch)	***Срабатывание защиты (вкл/выкл)***
	ban_for_bandwidth enable (switch)	***Срабатывание защиты, при превышении полосы пропускания (вкл/выкл)***
	ban_for_pps enable (switch) threshold_mbps 1000 (threshold_mbps - max 512 Гбит/с)	***Срабатывание защиты, если трафик к хосту превышает значение 1000 Мбит/с или 30 kpps (вкл/выкл)***

	threshold_pps 30000 (threshold_pps - max 512 mpps)	
ICMP	ban_for_icmp_bandwidth enable (switch)	***Срабатывание защиты при превышении порога пропускной способности ICMP (вкл/выкл)***
	threshold_icmp_mbps 15 threshold_icmp_pps 7000	***Срабатывание защиты, если ICMP-трафик к хосту превышает установленное значение Мбит/сек или pps***
TCP	ban_for_tcp_bandwidth enable (switch)	***Срабатывание защиты при достижении порога пропускной способности TCP (вкл/выкл)***
	ban_for_tcp_pps enable (switch) threshold_tcp_mbps 1000 threshold_tcp_pps 25000	***Срабатывание защиты, если TCP-трафик к хосту превышает установленное значение Мбит/сек или pps (вкл/выкл)***
UDP	ban_for_udp_bandwidth enable (switch)	***Срабатывание защиты при достижении порога пропускной способности UDP (вкл/выкл)***
	ban_for_udp_pps enable (switch) threshold_udp_mbps 500 threshold_udp_pps 25000	***Срабатывание защиты, если UDP-трафик к хосту превышает установленное значение 500 Мбит/сек или 25000 pps (вкл/выкл)***

TCP SYN	ban_for_tcp_syn_bandwidth enable (switch)	***Срабатывание защиты при достижении предела пропускной способности TCP SYN (вкл/выкл)***
	ban_for_tcp_syn_pps enable (switch) threshold_tcp_syn_mbps 15 threshold_tcp_syn_pps 5000	***Срабатывание защиты, если TCP SYN-трафик к хосту превышает установленное значение 15 Мбит/сек или 5000 pps (вкл/выкл)***

В меню **Расширенные настройки** можно указать следующие параметры:

ПАРАМЕТР И ЕГО РЕКОМЕНДУЕМОЕ ЗНАЧЕНИЕ	ОПИСАНИЕ
enable_ban_hostgroup: enabled (по умолчанию)	***Детектинг по значениям из митигаций Включение срабатывания защиты для группы хостов (вкл/выкл)***
ban_time: 1900	***Время блокировки IP (значение 0 недопустимо)***
ban_time_total_hostgroup	***Время блокировки группы хостов (значение 0 недопустимо)***: ***1900 - совпадает с ban_time на фронте disabled***
do_not_ban_incoming: disabled	***Не срабатывать на входящий трафик (вкл/выкл)***
do_not_ban_outgoing: enabled	***Не срабатывать на исходящий трафик (вкл/выкл)***
average_calculation_time: 5	***Среднее значение скорости трафика за временной интервал***

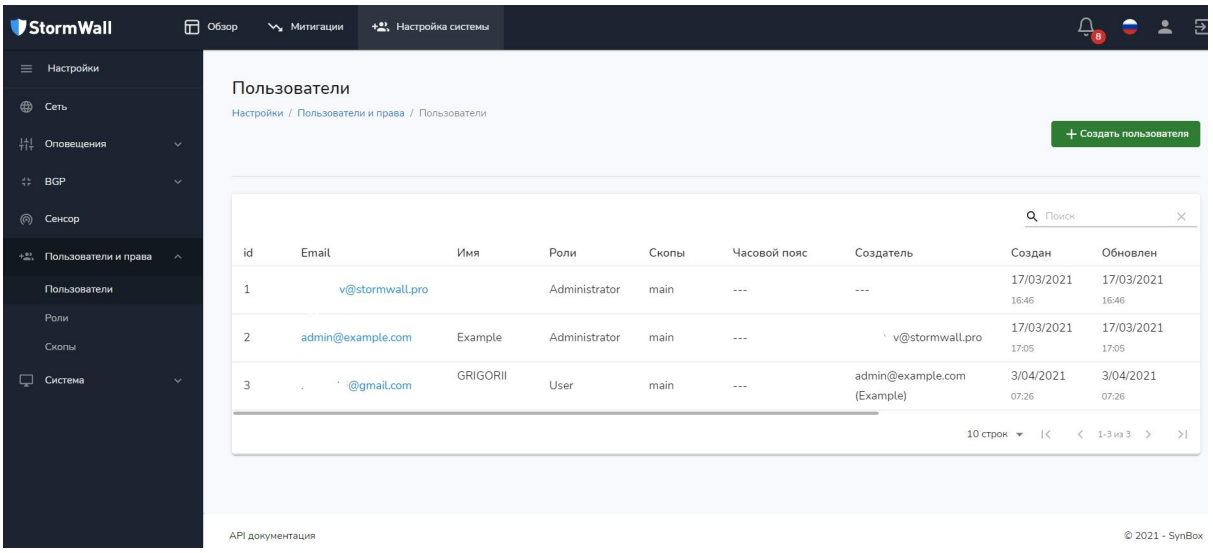
average_calculation_time_for_hostgroups: 5	***Среднее значение скорости трафика за временной интервал для групп хостов***
average_calculation_time_for_subnets: 5	***Среднее значение скорости трафика за временной интервал для подсетей***
speed_calculation_delay: 1	***Частота запуска функции пересчета скорости***
override_internal_traffic_as_incoming: disabled	***Переопределение внутреннего трафика, как входящего (вкл/выкл)***
override_internal_traffic_as_outgoing: disabled	***Переопределение внутреннего трафика, как исходящего (вкл/выкл)***
process_incoming_traffic: enabled	***Обработка входящего трафика (вкл/выкл)***
process_outgoing_traffic: enabled	***Обработка исходящего трафика (вкл/выкл)***
monitor_local_ip_addresses: disabled (enable по умолчанию)	***Мониторинг IP-адресов локальной сети (вкл/выкл)***
netflow: disabled	***Netflow (вкл/выкл)***
netflow_custom_sampling_ratio_enable: disabled	***Расчет коэффициента выборки для агентов Netflow (вкл/выкл)***
netflow_host: 0.0.0.0	***Привязка хоста-сборщика Netflow***
netflow_ignore_long_duration_flow_enable: disabled	***Netflow игнорирует включение длительного потока (вкл/выкл)***

netflow_ignore_sampling_rate_from_device : disabled	***Netflow игнорирует сообщения о частоте дискретизации от устройства (вкл/выкл)***
netflow_long_duration_flow_limit: 1	***Ограничение длительного потока Netflow***
netflow_multi_thread_processing: disabled	***Многопоточная обработка для каждого порта Netflow (вкл/выкл)***
netflow_ports:	***Порты сборщика Netflow (можно указать несколько)***
netflow_sampling_ratio: 1	***Коэффициент выборки для всех агентов Netflow***
netflow_templates_cache: enabled	***Кэширование на диске шаблонов данных Netflow (вкл/выкл)***
netflow_threads_per_port: 1	***Количество потоков на порт Netflow***
sflow: disabled	***sFlow (вкл\выкл)***
sflow_host: 0.0.0.0	***Хост сборщика sFlow (при значении 0.0.0.0 прослушиваются все интерфейсы)***
sflow_ports:	***Порты для сборщика sFlow (можно указать несколько)***
sflow_track_sampling_rate: disabled	***Отслеживание частоты дискретизации sFlow (вкл/выкл)***
sflow_use_new_generation_parser: disabled	***Новый улучшенный парсер пакетов sFlow (вкл/выкл)***
networks_list:	***Список сетей***
networks_whitelist:	***Список dst сетей которые не детектируются (белый список), на которые идет трафик***

networks_whitelist_remote:	***Список src сетей которые не детектируются (белый список), с которых идет трафик)***

Пользователи и их права

StormWall Sensor Appliance является многопользовательским ПО. Список всех пользователей (в том числе обладающих правами администратора) доступен в меню **Настройки → Пользователи и права → Пользователи**.

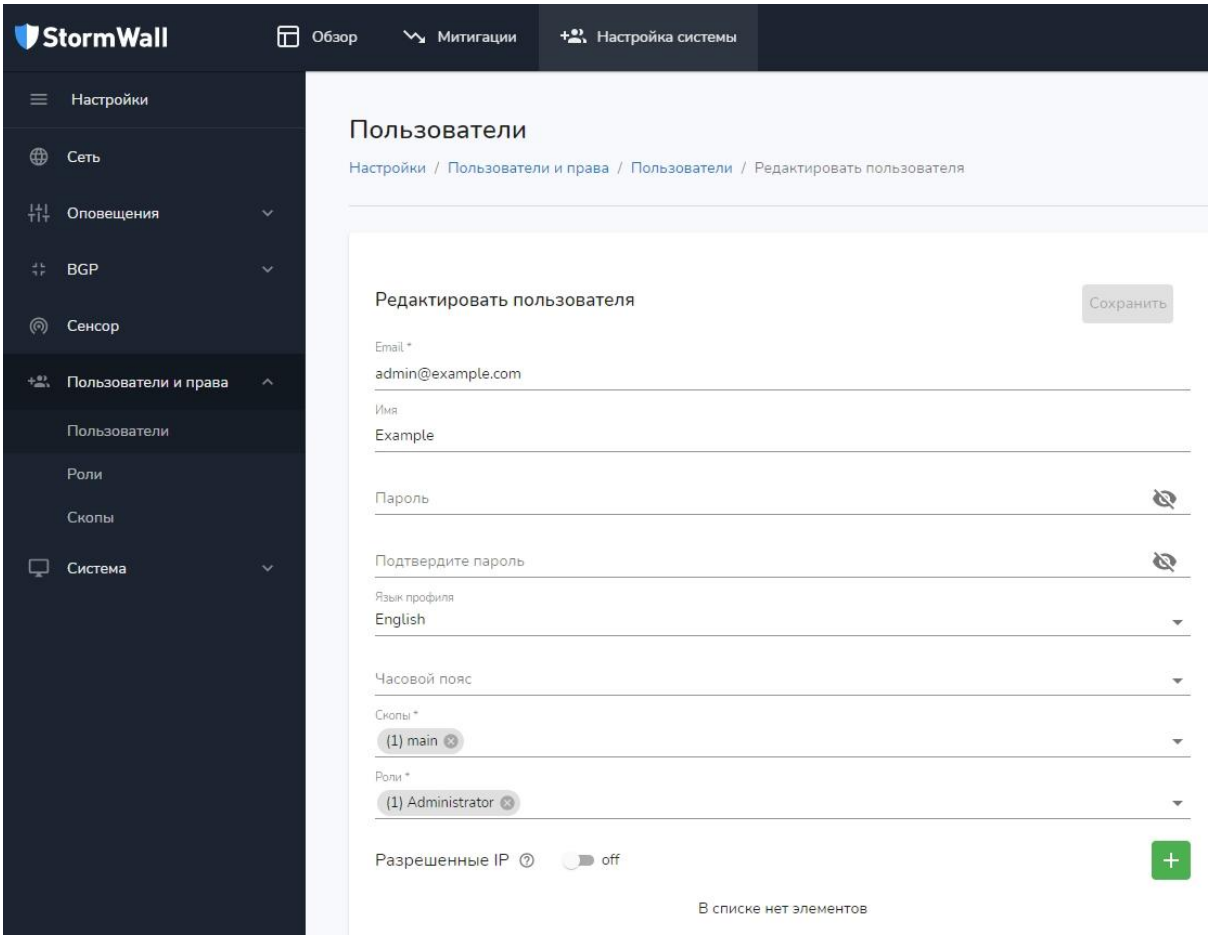


Создание нового Пользователя

По нажатию на кнопку **Создать пользователя** вы можете создать нового пользователя. Подробнее см. Создание Пользователя.

Редактирование Пользователя

Вы можете изменить или отредактировать параметры пользователя, зарегистрированного в системе. Для этого войдите в меню **Настройки → Пользователи и права → Пользователи**. Далее выберите E-mail пользователя, которого вы бы хотели отредактировать.



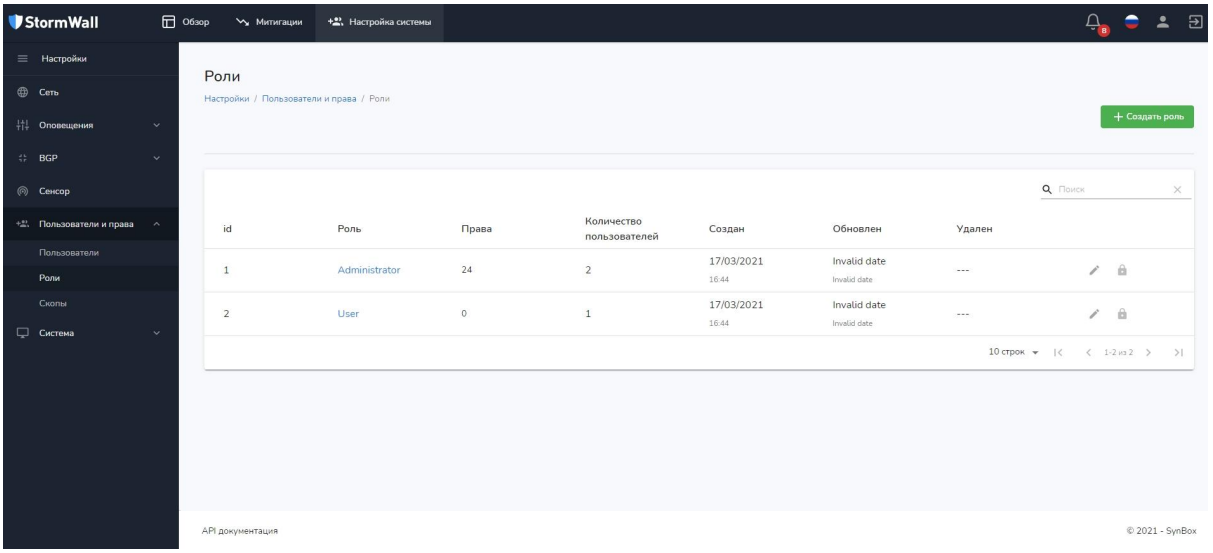
Доступные для редактирования параметры пользователя аналогичны параметрам **Личного кабинета** пользователя. Подробнее см. Личный кабинет. Только Личный кабинет может настроить для себя любой пользователь персонально, а изменение параметров прочих пользователей, напоминаем, доступно только пользователю с правами Администратора.

Роли

По умолчанию в системе доступны две пользовательские роли:

1. **Administrato**r (Администратор).
2. **User** (Пользователь).

Для просмотра, редактирования существующих, а также для создания новых ролей войдите в меню **Настройки** → **Пользователи и права** → **Роли**.



На странице **Роли** отображается информация об имеющихся в системе ролях:

- ID роли;
- Название роли;
- Количество прав;
- Количество пользователей, обладающих данной ролью;
- Дата создания;
- Дата обновления (если роль обновлялась);
- Дата удаления (если роль удалена).

Создание роли

Если существующие роли вам не подходят, вы можете создать абсолютно новую роль. Для этого странице **Роли** нажмите на кнопку **Создать роль**. На открывшейся странице **Добавить роль** введите параметры будущей роли:

- Название роли;
- Описание роли;
- Права на просмотр и изменение различных настроек.

В подпункте **Митигации** вы можете настроить права на работу с митигациями (подробнее см. Митигации):

- Просмотр списка;
- Создание;
- Чтение;
- Обновление;
- Удаление.

В подпункте **Обзор** вы можете настроить права на просмотр работы системы и различной статистики:

- DDoS сенсор;
- Статистика загрузки CPU;
- Загрузка CPU (в реальном времени);
- История атак.

В подпункте **Профиль пользователя** вы можете настроить права на изменения пользовательского профиля в **Личном кабинете**:

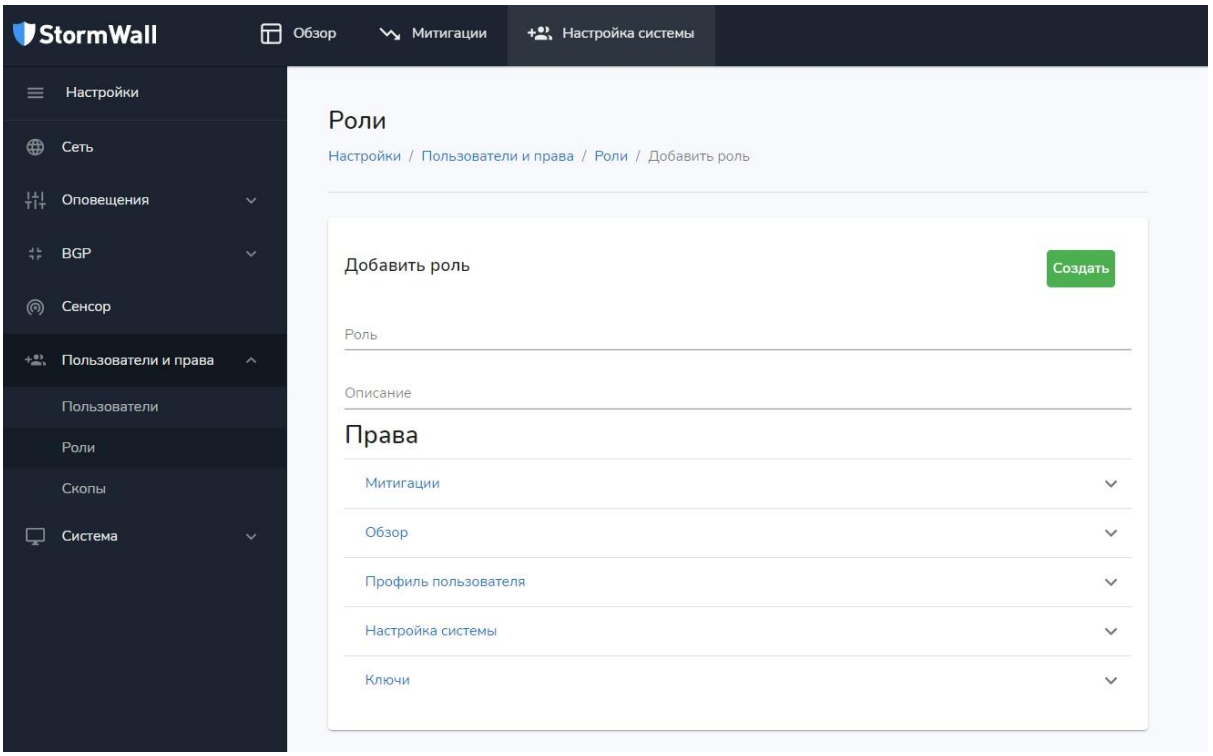
- Изменение почты;
- Изменение пароля;

- Изменение профиля;
- Восстановление пароля.

В подпункте **Настройка системы** вы можете разрешить пользователям с новой ролью просматривать и изменять параметры системы. В случае разрешения, будет доступно все меню **Настройка системы**. В случае запрета, пользователь его просто не увидит.

В подпункте **Ключи** можно настроить работу с API-ключами:

- Просмотр списка ключей;
- Создание;
- Удаление.



После того, как вы включите все нужные параметры, нажмите на кнопку **Создать**. Роль будет создана и появится в списке ролей. Ее состояние будет **Активно**. В отличие от встроенных в систему ролей **User** и **Administrator**, созданную пользователем роль можно активировать (включить) и деактивировать (выключить). Для этого необходимо переключить ползунок, расположенный в правой части строки роли в общем списке. У ролей **User** и **Administrator** такой ползунок отсутствует, и вместо него имеется изображение замочка.

Изменение роли

Вы можете изменить любую роль, как созданную пользователем, так и встроенную в систему. Для этого нажмите на изображение карандаша, расположенное в правой части строки роли в списке **Настройки** → **Пользователи и права** → **Роли**. Изменение роли осуществляется по той же схеме, что и создание новой роли. Подробнее см. Создание роли.

Привязка новой роли к пользователю

Если вы изменили уже существующую в системе роль, дополнительно привязывать ее к пользователю не нужно, если она уже была к нему привязана. Если вы создали новую роль, то для привязки ее к пользователю выполните следующие действия:

- Войдите в меню **Настройки** → **Пользователи и права** → **Пользователи**;
- Нажмите на E-mail пользователя, к которому вы хотите привязать новую роль;
- На странице **Редактировать пользователя** найдите строку **Роли,** и из выпадающего списка выберите новую роль. Уже привязанные роли можно открепить (нажав на крестик).

.

Скопы

Скопы - это способ разделения пользователей и митигаций внутри StormWall Sensor Appliance. С помощью скопов лицензиаты - (интернет-провайдеры, телеком-операторы, владельцы ЦОДов и другие), могут предлагать систему своим клиентам в субаренду. Для этого они могут создать клиентский скоп, ограничив его рамками выделенных IP-префиксов, и в настройках любого пользователя назначить ему только этот, либо несколько скопов. Таким образом пользователь, авторизовавшись в системе, сможет работать только в рамках обозначенных набором выделенных ему скопов, например - сможет управлять митигацией только в рамках набора префиксов обозначенных в скопах, и никак не шире.

Виды скопов

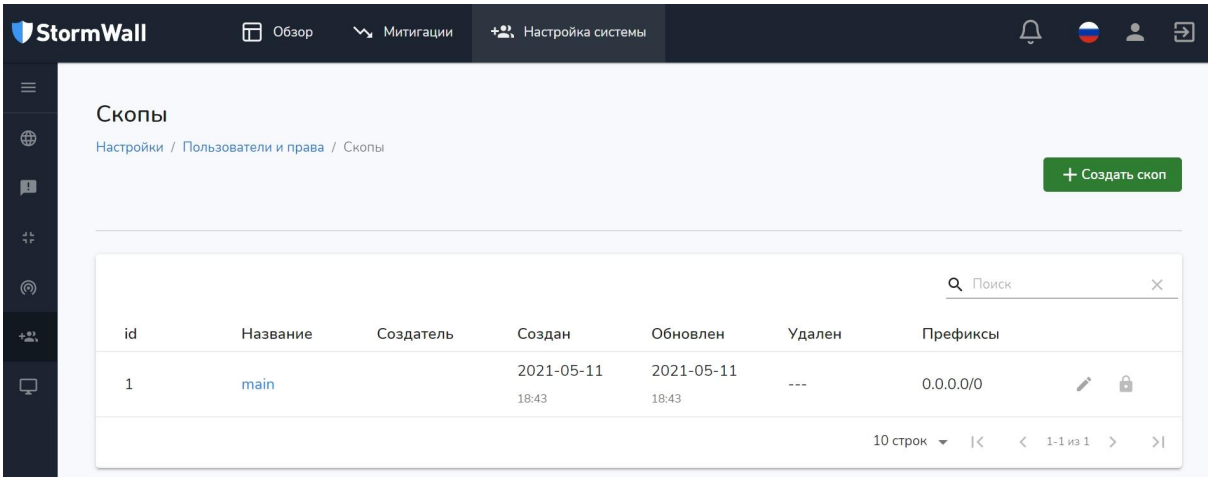
- Администраторский скоп: может осуществлять любые действия, видит все атаки, администрирует любые префиксы;
- Пользовательский скоп: создается администратором для некоторой группы пользователей, имеет ограничения в рамках IP-префикса, видит только атаки в рамках своего скопа.

Пример практического применения скопов

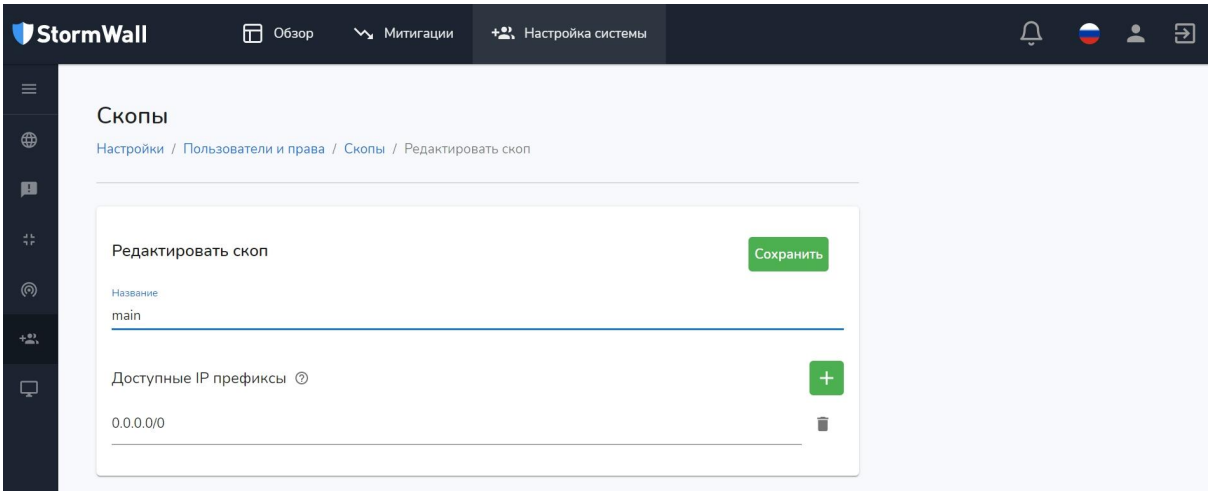
- Интернет провайдер “WebNet” установил Sensor Appliance, ему принадлежит префикс 1.1.1.1/24 (255 адресов);
- Он хочет отдать 1.1.1.1/28 под управление своему клиенту “GameWeb”. Для этого он создает скоп GameWeb с перфиксом 1.1.1.1/28 (15 адресов), добавляет туда пользователей;
- Теперь из скопа GameWeb сможет управлять и видеть статистику только в рамках своего префикса (т.е. эти 15 адресов).

Редактирование скопа

Войдите в меню **Настройки** → **Пользователи и права** → **Скопы**. По умолчанию в системе уже присутствует скоп **main**. Вы можете отредактировать его, нажав на изображение карандаша, расположенной в правой части строки данного скопа. Удалить системный скоп **main** невозможно.



На странице **Редактировать скоп** вы можете поменять его название, а также установить новый диапазон доступных IP префиксов. По умолчанию установлено значение 0.0.0.0/0. Можно задать не один, а несколько диапазонов. Для этого нажмите на кнопку с изображением знака +. Ненужные диапазоны удаляются с помощью кнопки с изображением корзины. После завершения операции редактирования скопа нажмите на кнопку **Сохранить.**



Можно использовать не только установленный по умолчанию в системе, но и собственные скопы. Для этого их нужно создать.

Создание скопа

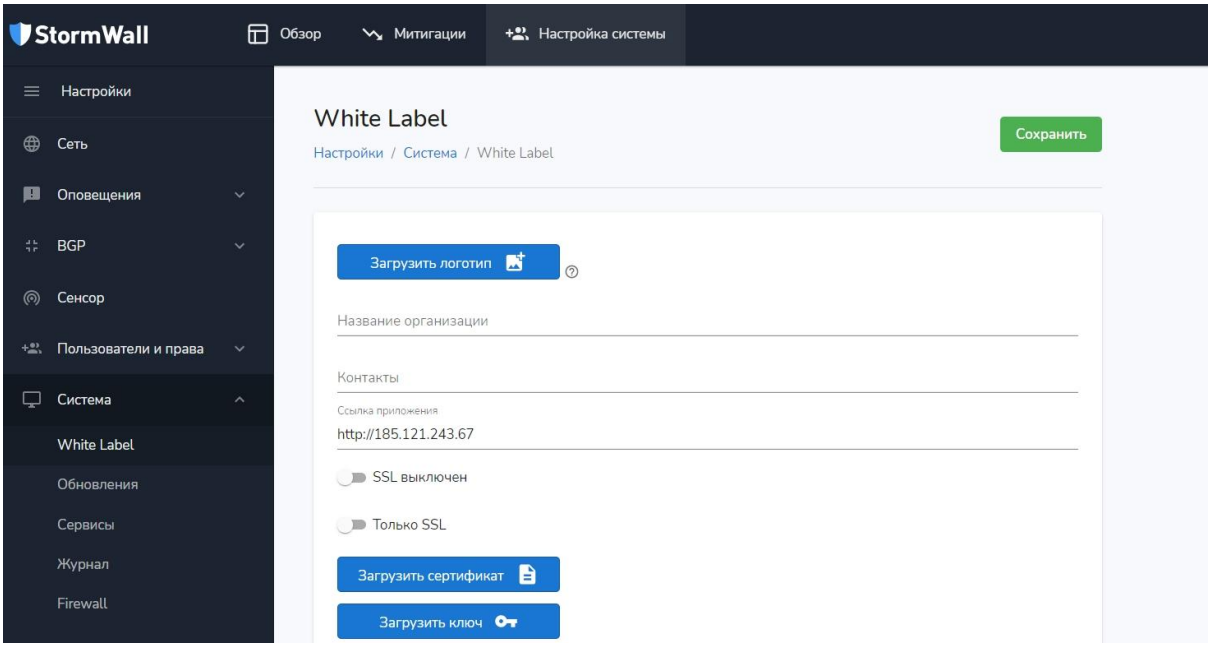
Войдите в меню **Настройки** → **Пользователи и права** → **Скопы** и нажмите на кнопку **Создать скоп**. Процесс создания скопа практически аналогичен процессу редактирования скопа, подробнее см. Редактирование скопа.

Система

В меню **Настройки** → **Система** содержатся различные инструменты для изменения системных параметров, настройки и обновления ПО, средства мониторинга.

White Label

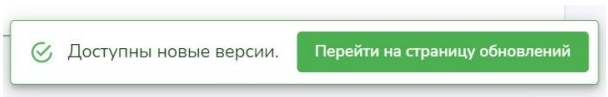
Разработчик предоставляет сервис StormWall Sensor Appliance лицензиарам (ЦОДам, провайдерам, ИБ-интеграторам, телеком-операторам и т.д.) по модели оказания услуги под собственной торговой маркой (White Label). В этом случае последние могут предоставлять его своим клиентом под собственным брендом. Для настройки White Label войдите в меню **Настройки** → **Система** → **White Label**.



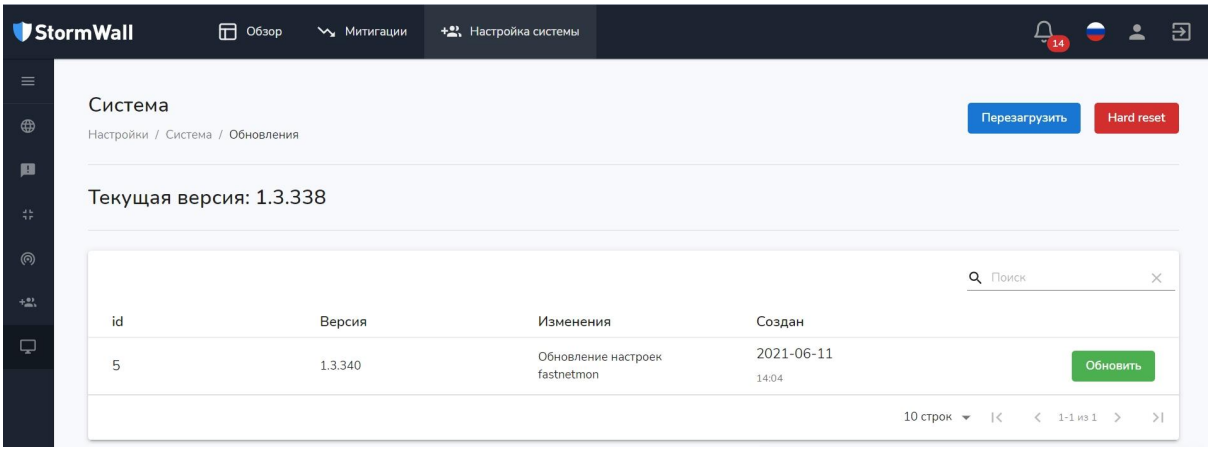
На странице **White Label** можно загрузить логотип компании, указать ее название, указать контакты службы поддержки, IP-адрес или DNS имя, по которому должен быть доступен StormWall Sensor Appliance. Также здесь можно загрузить SSL-сертификат и ключ к нему, включить или отключить поддержку SSL, разрешить доступ только по SSL. По завершении процесса настройки нажмите на кнопку **Сохранить**.

Обновления

В меню **Настройки** → **Система** → **Обновления** отображается текущая версия системы, а также доступные для загрузки обновления. При наличии не установленного обновления пользователь видит специальное окно с оповещением. Оно доступно в любом меню Sensor Appliance.



Также в меню **Настройки** → **Система** → **Обновления** имеются кнопки **Перезагрузить** (“мягкая” перезагрузка с сохранением настроек пользователя) и **Hard Reset** (сброс всех настроек пользователя и возврат к системным настройкам).



Процесс обновления обычно занимает до 20 минут. При этом все настройки сохранятся, а после завершения обновления вновь потребуется авторизоваться в системе с существующим логином и паролем.

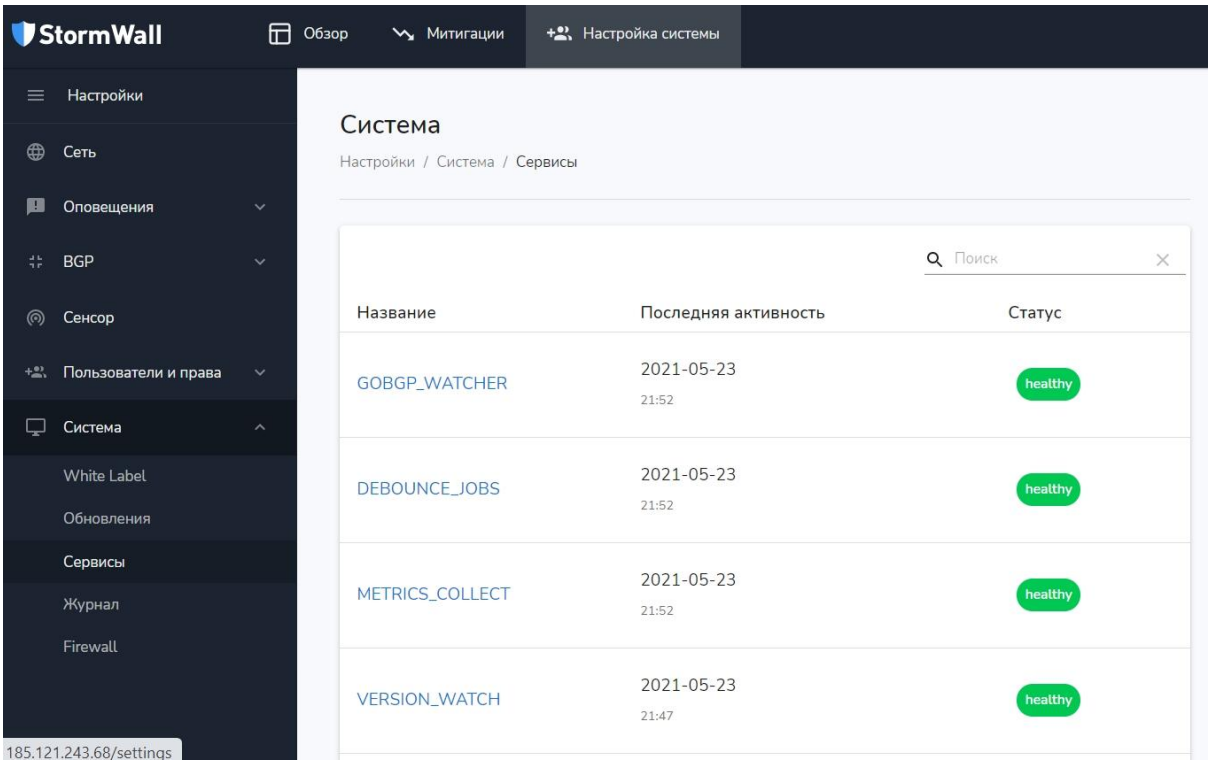
Проверка на доступные обновления осуществляется автоматически в фоновом режиме, именно поэтому необходимо чтобы была связь с сервером обновлений по адресу sb.stormwall.pro

Сервисы

Меню **Настройки** → **Система** → **Сервисы** позволяет следить за работоспособностью системных процессов, каждый из которых отвечает за выполнение какой-либо задачи. Оно включает в себя следующие службы:

- **GOBGP_WATCHER**. Процесс, наблюдающий за работой BGP-маршрутизации и отвечающий за соблюдение консистентности настроек BGP и базы данных. В случае падения и сбоя BGP, настройки восстанавливаются автоматически с помощью GOBGP_WATCHER;
- **DEBOUNCE_JOBS**. Процесс, отвечающий за очередность перезагрузки сервисов. Он позволяет сделать паузу перед перезагрузкой сервиса, чтобы избежать его многократной перезагрузки, когда с системой работает несколько пользователей одновременно;
- **METRICS_COLLECT**.Сборщик данных о загрузке процессора и о потреблении оперативной памяти;
- **VERSION_WATCH**. Процесс, мониторящий появление новых версий и их доступность для загрузки и установки;
- **NOTIFIER**. Процесс, отвечающий за группировку атак и постановку их в очередь на отправку;
- **EVENTS**. Сервис оповещений пользователя. Подробнее см. Оповещения;
- **SMTP_SENDER**. При детектировании атаки, этот процесс генерирует оповещения по электронной почте для всех пользователей, которых затрагивает эта атака. Подробнее см. SMTP;
- **WEBHOOK_SENDER**. Настройка оповещений об атаках, для их получения в различных приложениях, например. Подробнее см. Webhooks;
- **GARBAGE COLLECTOR**. Процесс, отвечающий за сбор и очистку от системного мусора (устаревших данных);
- **ATTACK_SNAPSHOT**. Процесс, фиксирующий “снимок” атаки;

- **MITIGATION_STATS**. Процесс, обрабатывающий данные для каждой митигации;
- **LICENSE_WATCHER**. Процесс, проверяющий действительность пользовательской лицензии для работы системы.

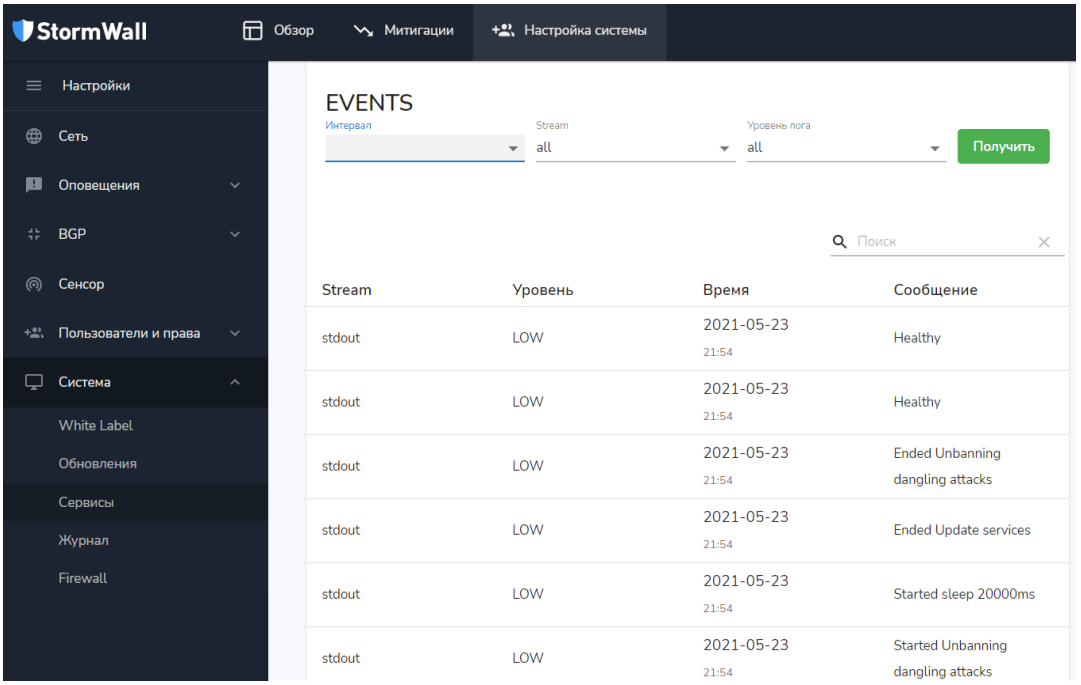


Возле каждого процесса расположена зеленая иконка с надписью **healthy** или красная иконка с надписью **unhealthy**. Зеленая иконка обозначает, что сервис работает нормально, а красная сигнализирует о каких-либо проблемах.

Внимание! Если какой-либо сервис находится в статусе unhealthy, следует обратиться в службу технической поддержки.

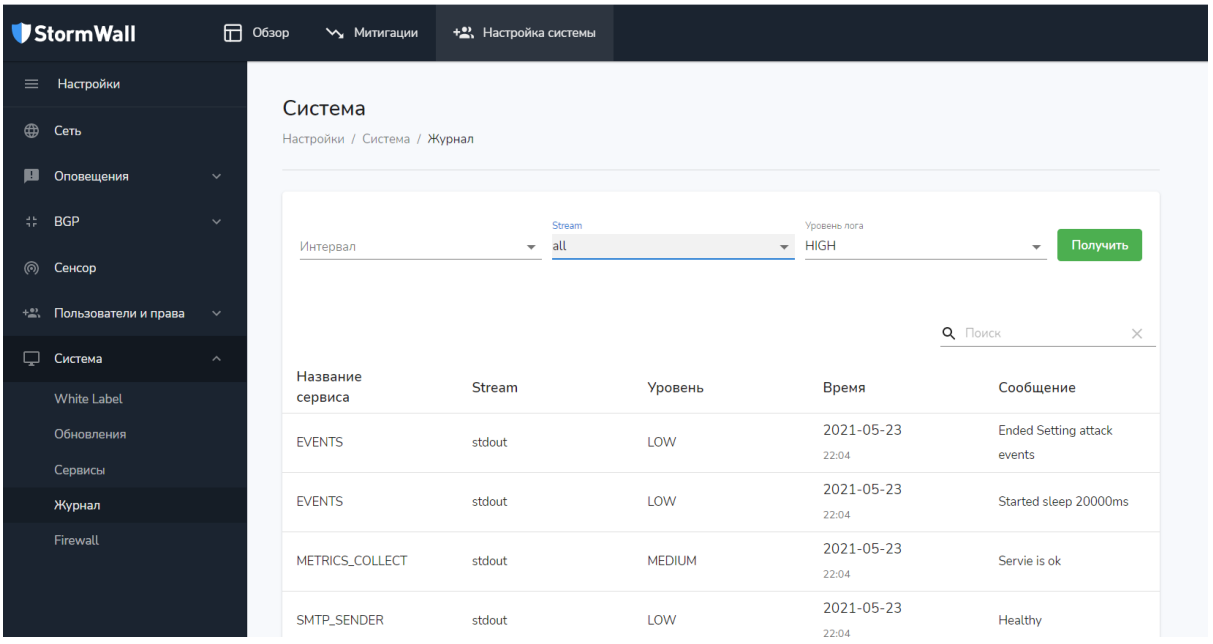
Каждый сервис в меню **Сервисы** представляет собой ссылку, нажав на которую вы попадаете на страницу событий, связанных с этим сервисом. События можно искать и сортировать по трем параметрам:

- Временной интервал;
- Поток;
- Уровень лога (уровень события).



Журнал

Меню **Настройки** → **Система** → **Журнал** представляет собой сводный журнал работы всех сервисов. В отличие от меню **Настройки** → **Система** → **Сервисы**, где можно по нажатию на каждый отдельный сервис просматривать связанные с ним события, то здесь доступен общий сводный лог.

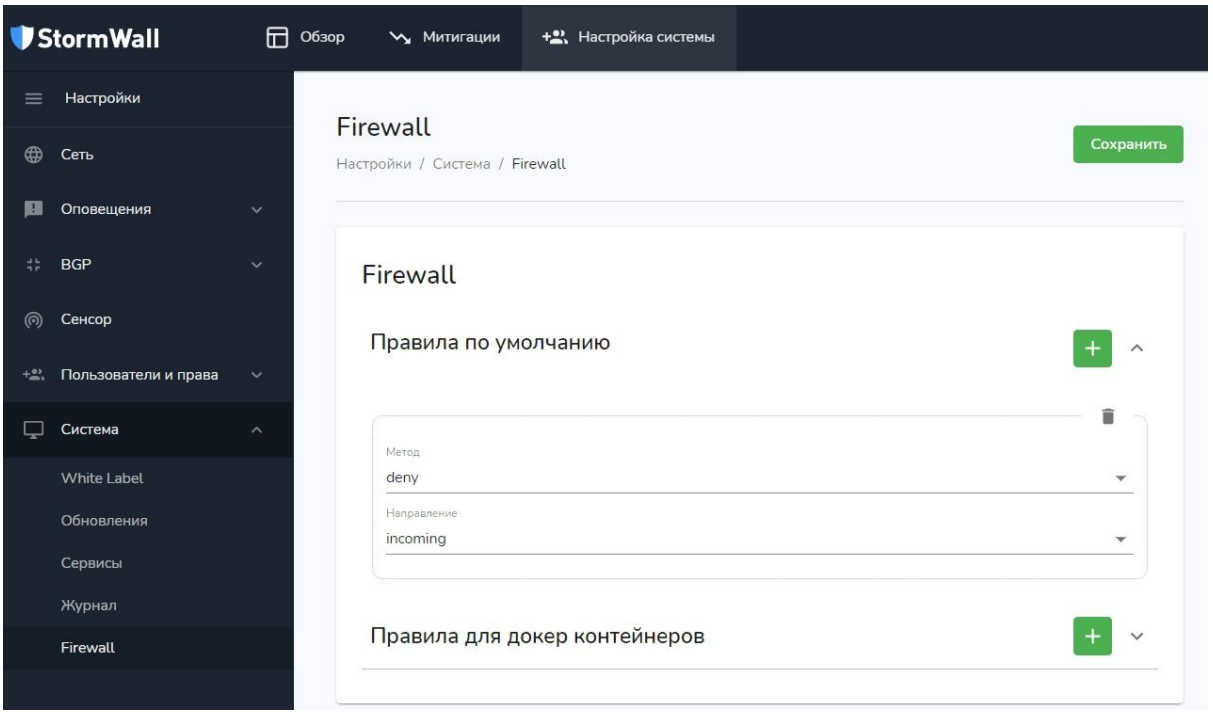


Firewall

Меню **Настройки** → **Система** → **Firewall** позволяет установить глобальные параметры управления трафиком. В меню имеется два раздела:

- **Правила по умолчанию** (общие правила обработки трафика для Sensor Appliance (**deny**, **allow** для **incoming** и **outgoing**);
- **Правила для докер контейнеров**. Система состоит из множества контейнеров, и данное меню позволяет настроить правила обработки трафика для каждого контейнера (**Метод** (deny, allow), **Откуда** (источник трафика), **Порты**, **Название**, **Протокол**).

Можно создавать любое количество правил. Для создания правила нажмите на кнопку с изображением плюса. Для удаления ошибочного или более ненужного правила нажмите на изображение корзины. После настройки каждого правила следует нажать на кнопку **Сохранить**.

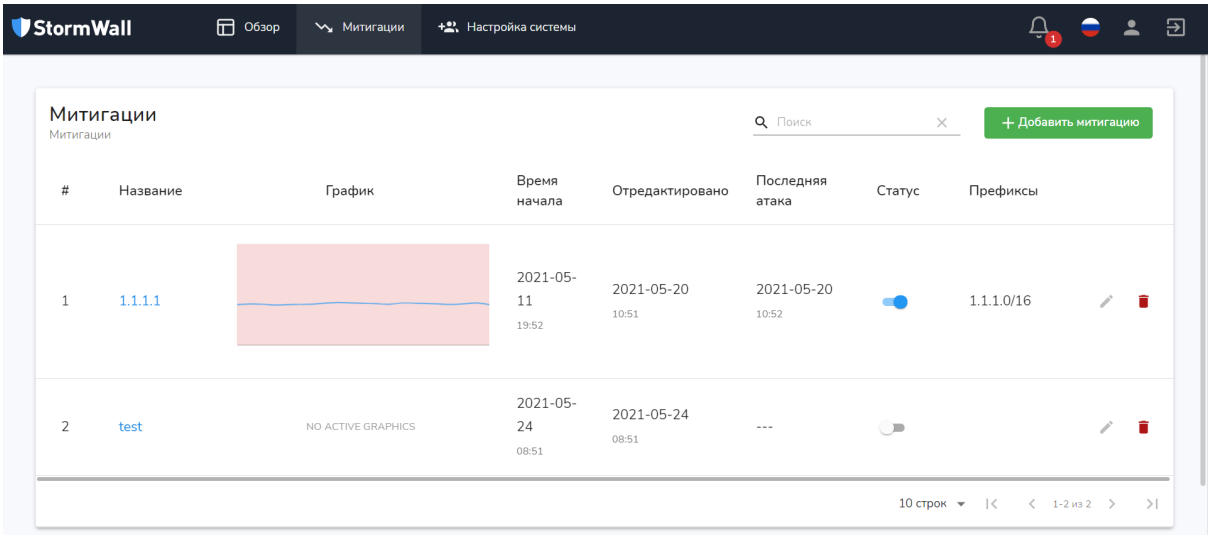


Митигации

Митигацией можно назвать определенные рамки и сетевые границы, в которых отслеживаются и детектируются атаки, а также преднастроенный свод правил, как система должна реагировать на эти атаки.

В меню **Митигации** находится список всех митигаций. Информация сгруппирована по параметрам:

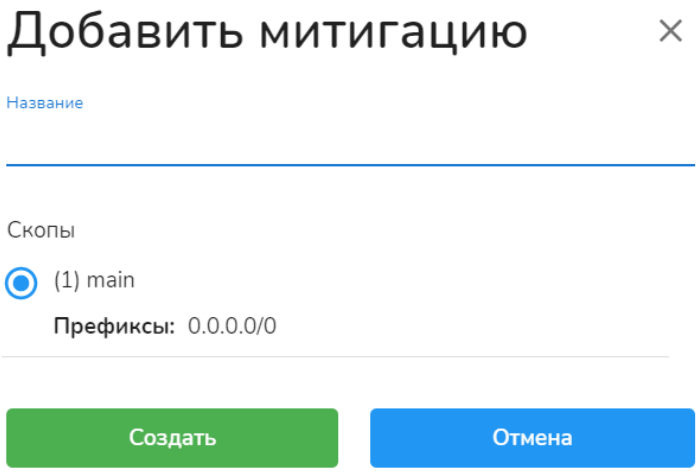
- **Название митигации**;
- **График в миниатюре**;
- **Время начала митигации**;
- **Отредактировано** (время последнего редактирования митигации);
- **Последняя атака**;
- **Статус**;
- **Префиксы**.



Можно создать любое число митигаций, а уже существующие редактировать (нажав на изображение карандаша) и удалять (нажав на изображение корзины).

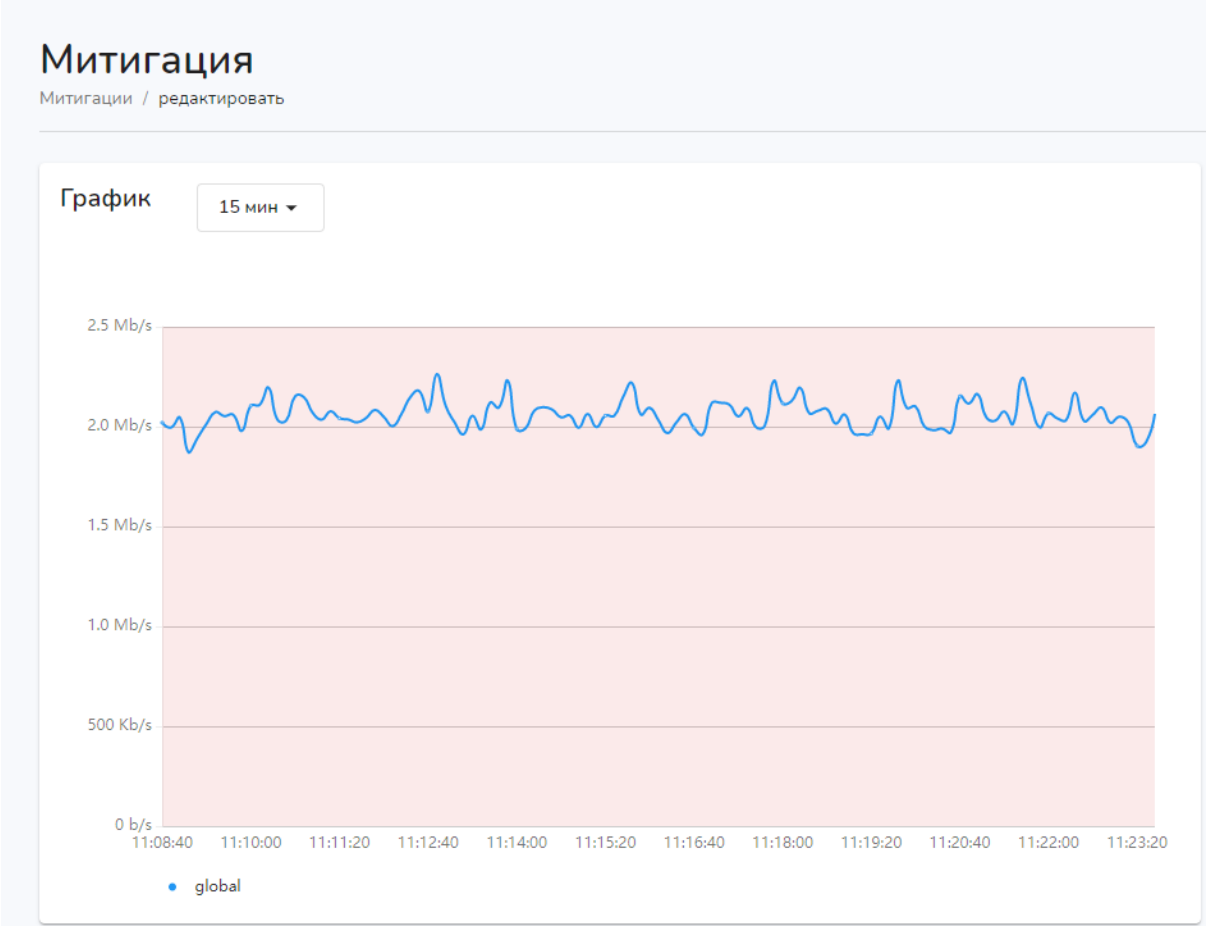
Добавление митигации

Для добавления новой митигации выберите в главном меню пункт **Митигации** и на открывшейся странице **Митигации** нажмите на кнопку **Добавить митигацию**.

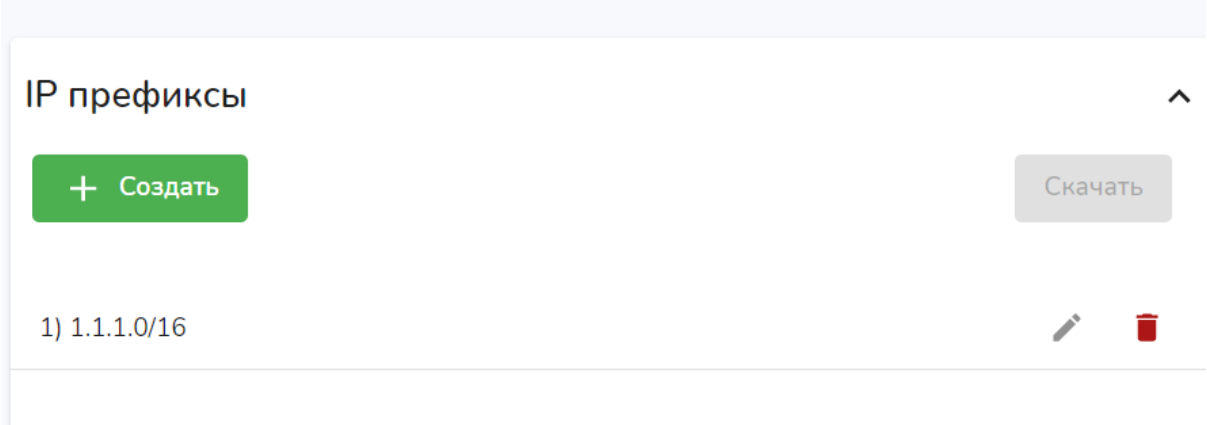


В окне **Добавить митигацию** укажите название новой митигации и скопы (подробнее см. Скопы). Затем нажмите на кнопку **Создать**.
При создании новой митигации необходимо настроить следующие параметры:

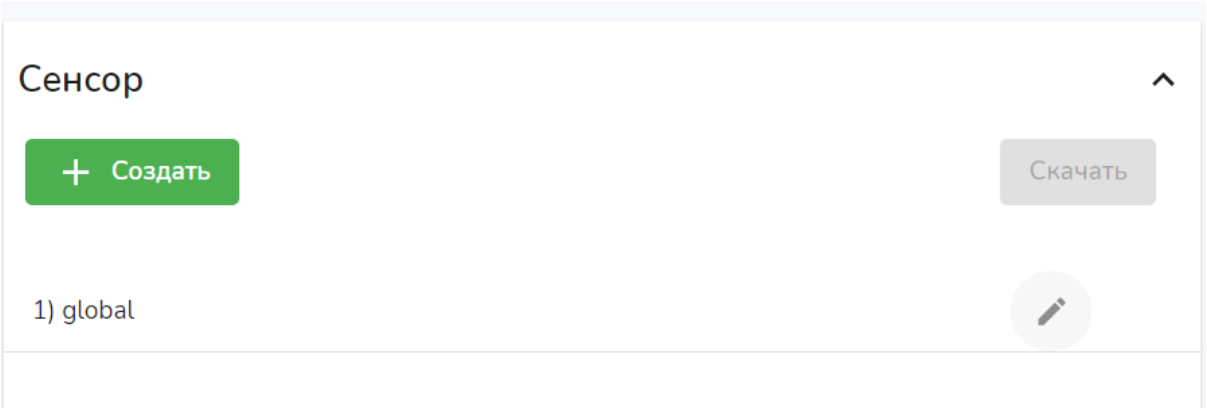
- **График** (частота обновления);



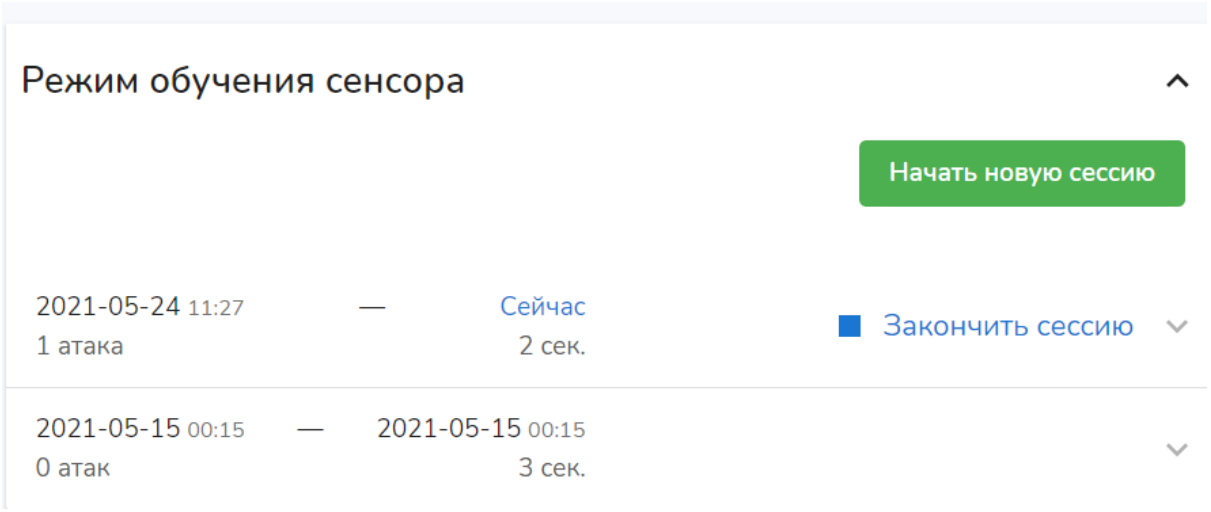
- **IP префиксы** (в рамках которых будет работать митигация);



- **Сенсор** (подробнее см. Настройка сенсора). Для каждого IP-префикса можно вводить собственные настройки сенсора;



- **Режим обучения сенсора** (можно открывать и закрывать новые сессии для обучения). В этом режиме пользователь может собрать статистику по проходящему трафику в рамках текущей митигации для более корректного и удобного выставления порогов сенсора.



Обучение сенсора

1. Чтобы начать процесс обучения сенсора, войдите в меню **Митигация** → **Режим обучения сенсора** и нажмите на кнопку **Начать новую сессию**. В зависимости от проходящего трафика, система накапливает данные, которые затем можно использовать для обучения сенсора.
2. По прошествии определенного периода времени (от нескольких часов до нескольких дней), войдите в меню **Митигация** → **Режим обучения сенсора** и нажмите на изображение галочки, расположенное возле ссылки **Закончить сессию**.
3. Развернется меню с рекомендуемыми системой настройками сенсора, это меню составлено в зависимости от особенностей трафика и атак, зафиксированных во время сессии.
4. В меню **Митигация** → **Режим обучения сенсора** → **История атак** зафиксированы все атаки, зафиксированные системой во время сессии.
5. Чтобы увидеть полную информацию о каждой из атак, нажмите на IP-адрес источника атаки, который является ссылкой. На открывшейся странице будет

доступна вся информация об атаке, на основании которой можно принять решение о том, стоит ли ее использовать для обучения системы:

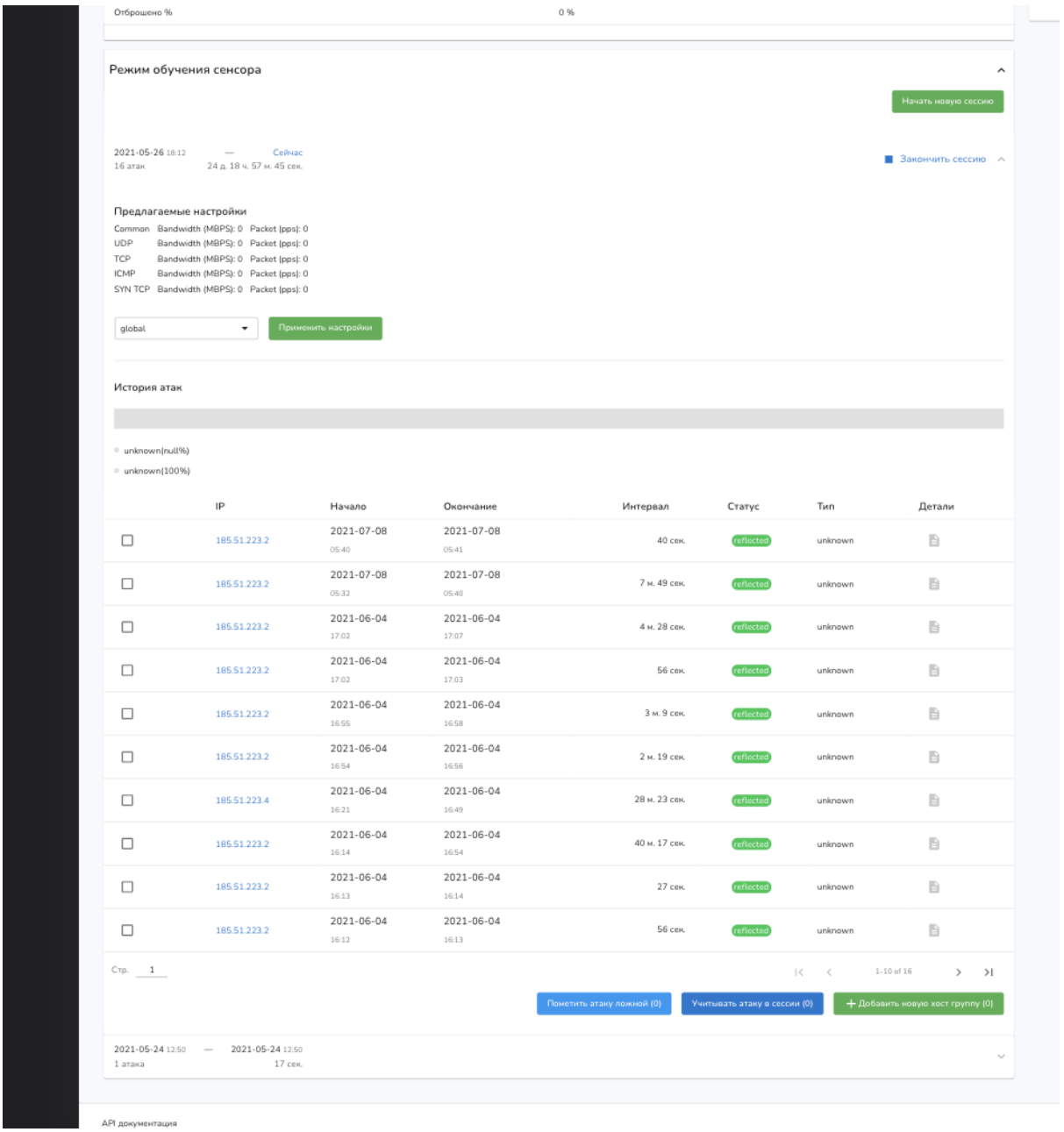
   a. Если вы не хотите использовать одну или несколько атак для обучения сенсора, отметьте их галочкой в меню **Митигация → Режим обучения сенсора → История атак** и нажмите на кнопку **Отметить атаку ложной**. В результате автоматические настройки сенсора, скомпонованные на основании этих атак, будут сброшены.
   b. Если вы хотите использовать одну и несколько атак атак для обучения сенсора, отметьте их галочкой в меню **Митигация → Режим обучения сенсора → История атак** и нажмите на кнопку **Учитывать атаку в сессии**. В результате автоматические настройки сенсора, скомпонованные на основании этих атак, будут сохранены.

6. Чтобы применить автоматические скомпонованные настройки сенсора, в меню **Митигация → Режим обучения сенсора** выберите из выпадающего списка сенсор (по умолчанию доступен один сенсор - **global**) и нажмите на кнопку **Применить настройки**.
7. Для закрытия сессии обучения сенсора нажмите на ссылку **Закончить сессию**. Сессия будет завершена, настройки сенсора при этом сохранятся.

Создание нового сенсора

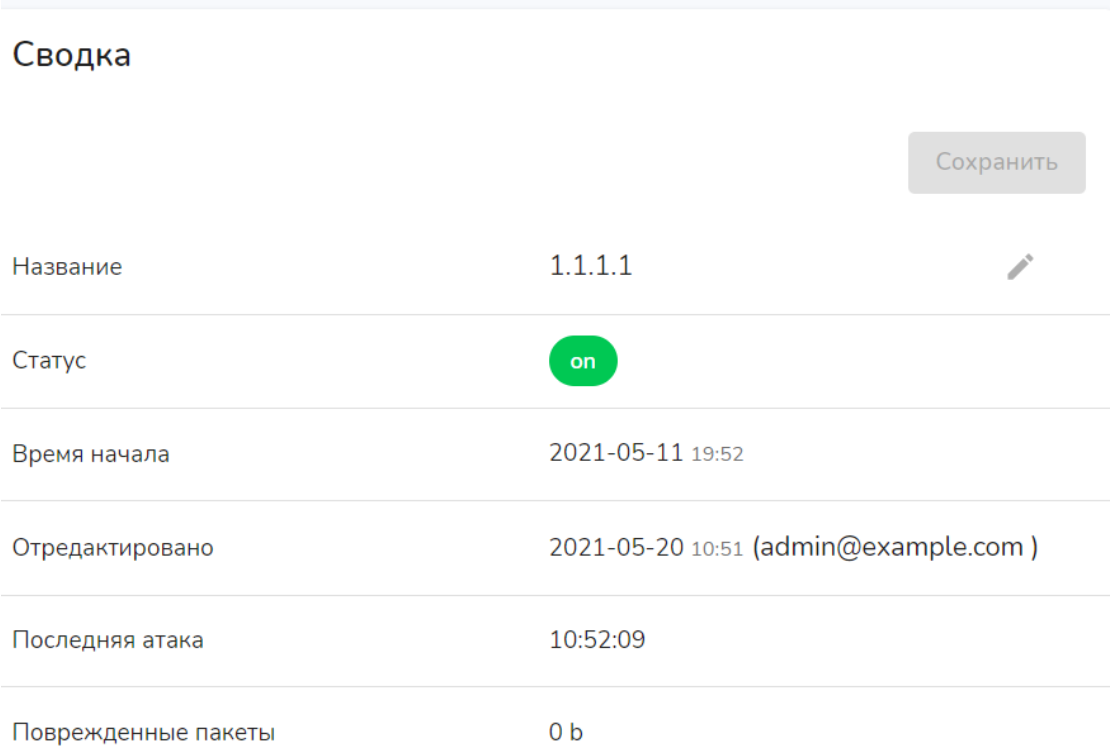
Новый сенсор, настройки которого отличаются от **global**, необходимо создавать в тех случаях, когда требуется выделить определенный пул IP-адресов или префиксы, трафик с которых напоминает атаки, однако таковыми не является. Создать новый сенсор можно двумя способами:

1. В меню **Митигация → Режим обучения сенсора → История атак** отметьте галочкой несколько атак и нажмите на кнопку **Добавить новую хост-группу**. В открывшемся окне введите настройки для нового сенсора и сохраните изменения.
2. В меню **Митигация → Сенсор** нажмите на кнопку **Создать**. В открывшемся окне вручную введите IP-адреса и нужные настройки, а затем нажмите на кнопку **Создать**.

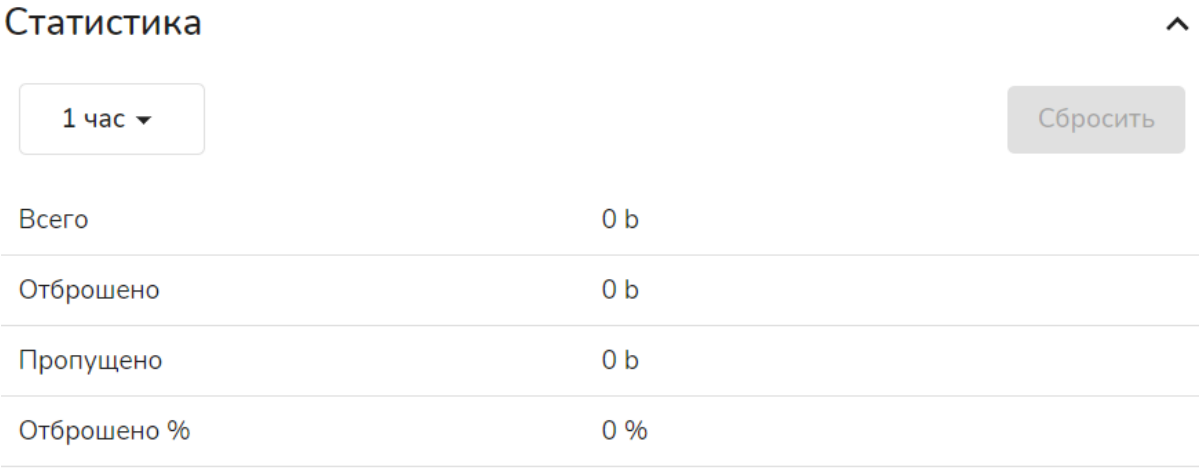


Для просмотра информации о работе каждой митигации предназначены пункты:

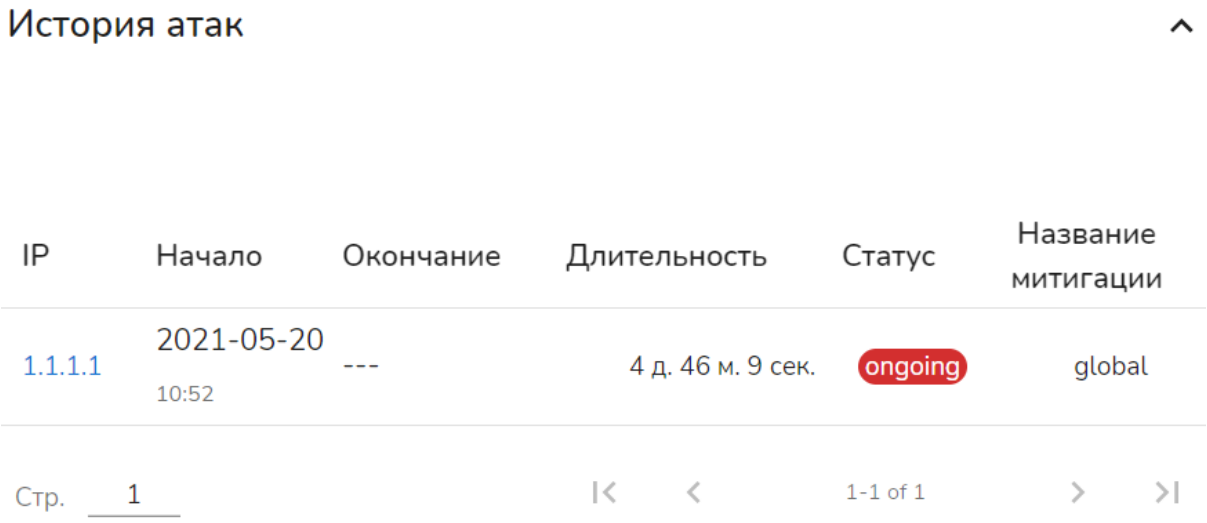
- **Сводка**;



- **Статистика**;



- **История атак**.



Созданную митигацию нужно сохранить, нажав на кнопку **Сохранить,** а затем, при необходимости сразу включить, передвинув ползунок в статус **Включено** (это можно сделать и позднее).

Редактирование митигации

Вы можете отредактировать ранее созданные митигации. Это можно сделать двумя способами:

- Нажав на изображение карандаша в списке митигаций;
- Нажав на название митигации в списке митигаций.

Процесс редактирования митигации аналогичен процессу добавления митигации. Подробнее см. Добавление митигации.

Удаление митигации

Вы можете удалить ненужную или ошибочно созданную митигацию. Это можно сделать двумя способами:

- Нажав на изображение корзины в списке митигаций;
- Открыть митигацию из списка, нажав на ее название, а затем нажав на кнопку **Удалить**.

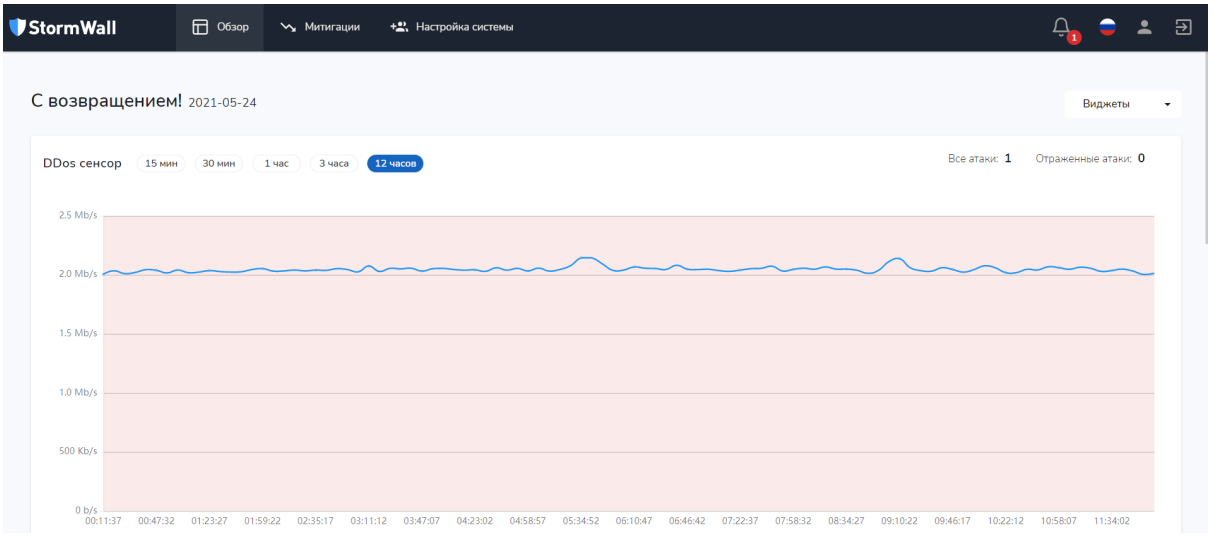
Обзор

Меню **Обзор** открывается по умолчанию при входе в систему. Оно состоит из нескольких виджетов, которые можно включить или отключить:

- **DDoS-сенсор**;
- **RAM**;
- **История атак**;
- **Загрузка CPU**.

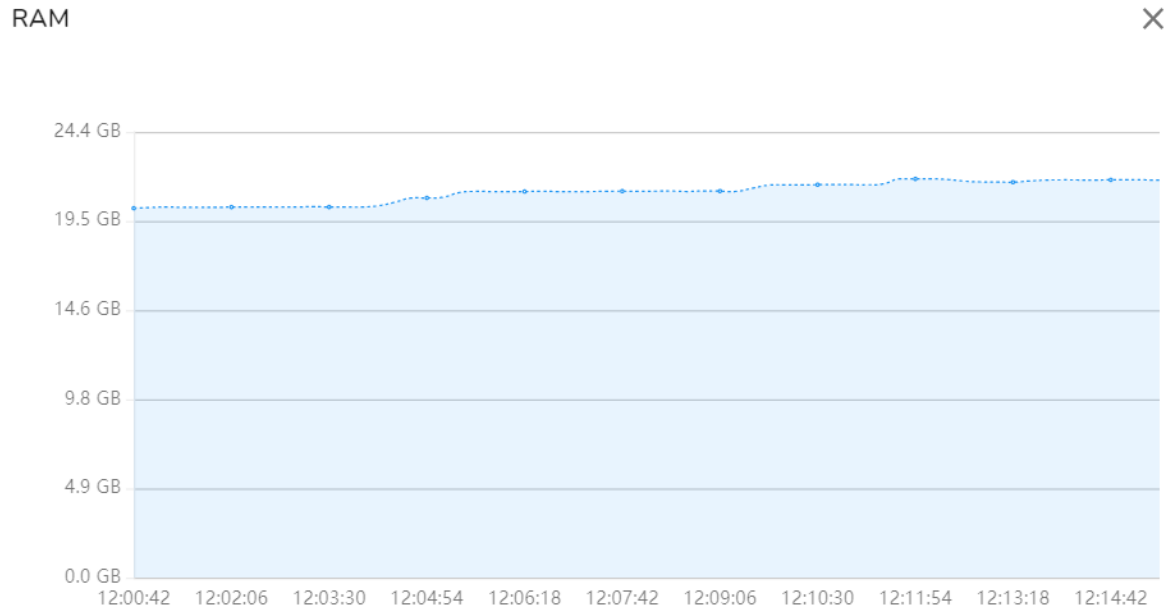
DDoS-сенсор

Виджет **DDoS-сенсор** представляет собой графическое отображение трафика в режиме реального времени. Атаки помечаются розовым цветом. График расположен на временной шкале, длительность которой можно настроить в интервале от 15 мин. до 12 часов.



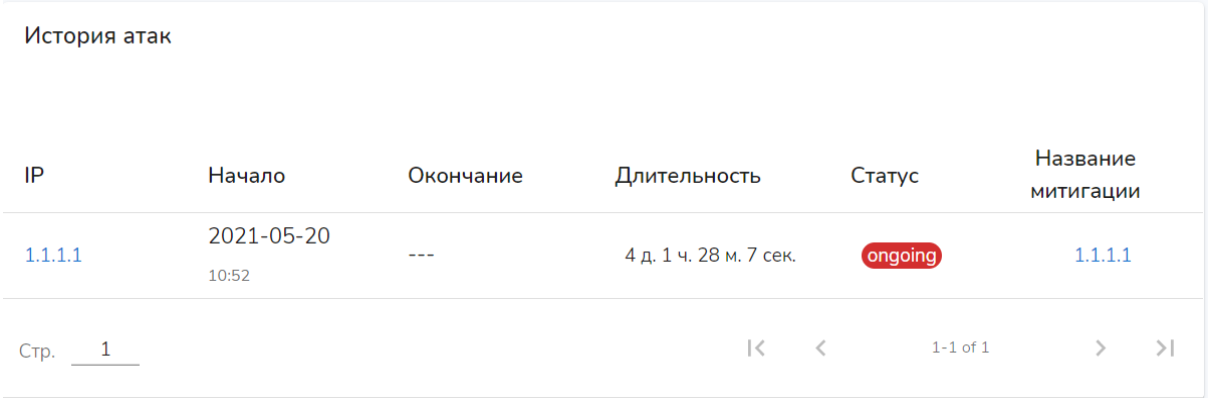
RAM

Виджет **RAM** в виде графика на временной шкале отображает нагрузку на оперативную память.



История атак

Виджет **История атак** показывает сводную информацию по текущим атакам. Он включает в себя оповещения о последних атаках, а также статистику по зафиксированным и отраженным атакам за час/день/неделю/месяц.

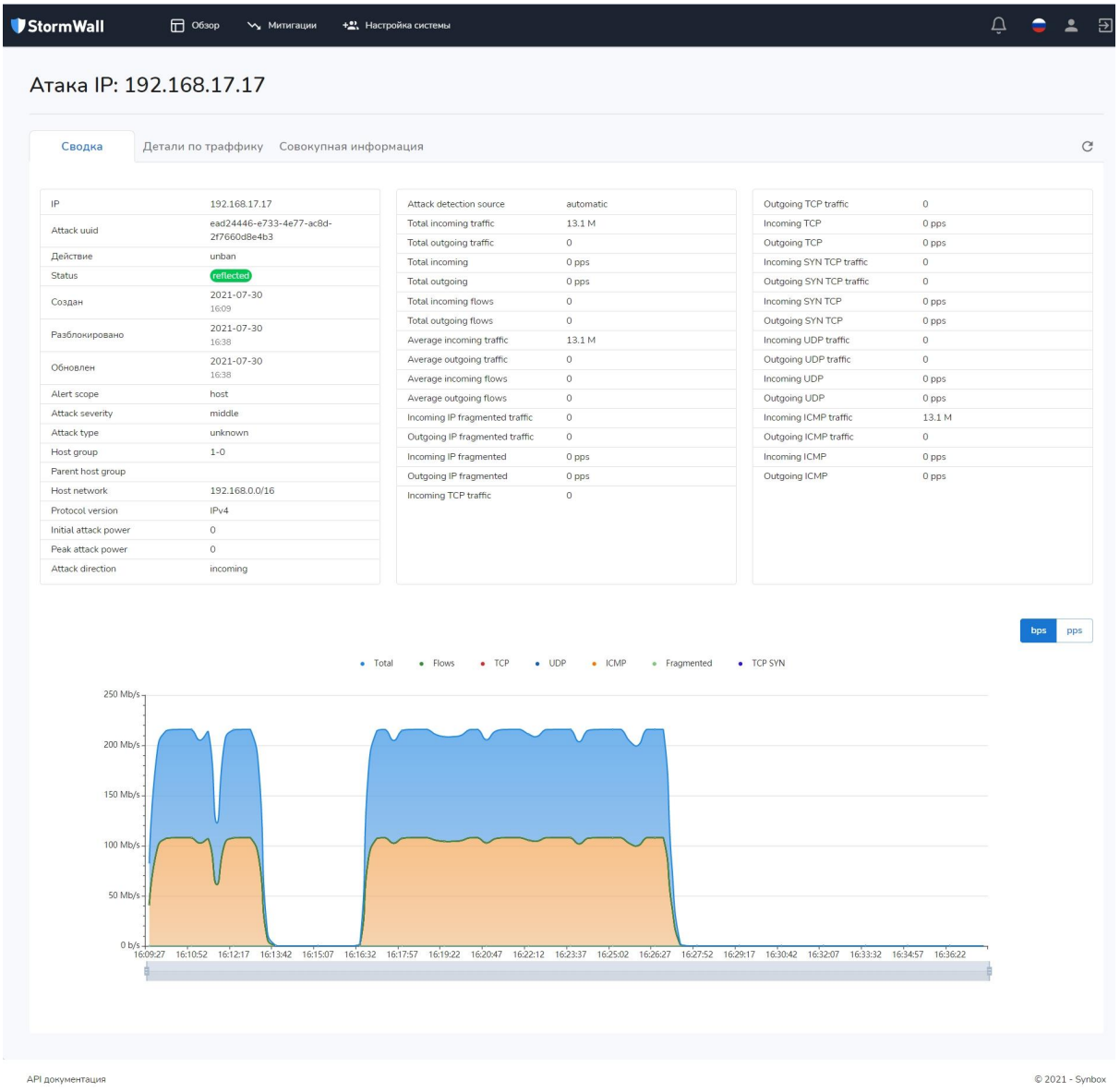


Просмотр деталей атаки

Для просмотра деталей конкретной атаки, выберите ее в списке виджета **История атак** и нажмите на IP-адрес назначения данной атаки. Откроется страница, содержащая детальную информацию по атаке. Она включает в себя три вкладки:

- Сводка (открывается по умолчанию);
- Детали по трафику;
- Совокупная информация.

Сводка



Детали по трафику

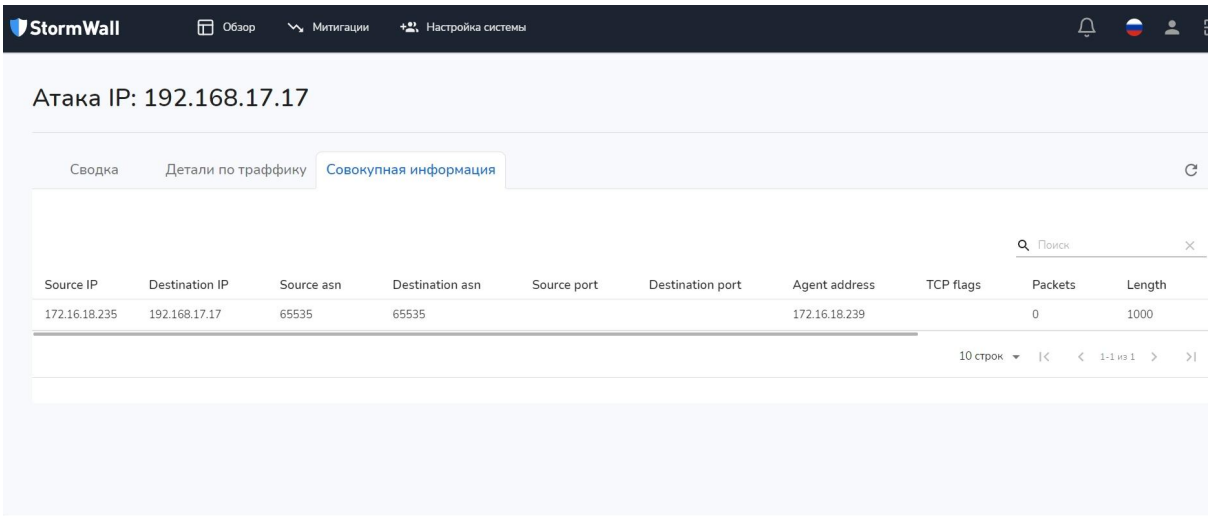
Во вкладке **Детали по трафику** демонстрируется график атаки (в разрезах **bps** и **pps**), а также следующие параметры, относящиеся к атаке:

- Список автономных сетевых систем (ASN);
- Список IP-адресов, с которых осуществлялась атака;
- Список протоколов;
- Список TCP-портов атакующей стороны;
- Список TCP-портов цели атаки;
- Список UDP-портов атакующей стороны;
- Список UDP-портов цели атаки.

По каждому параметру указан атакующий или атакуемый порт, общий объем трафика в битах и общая скорость трафика.

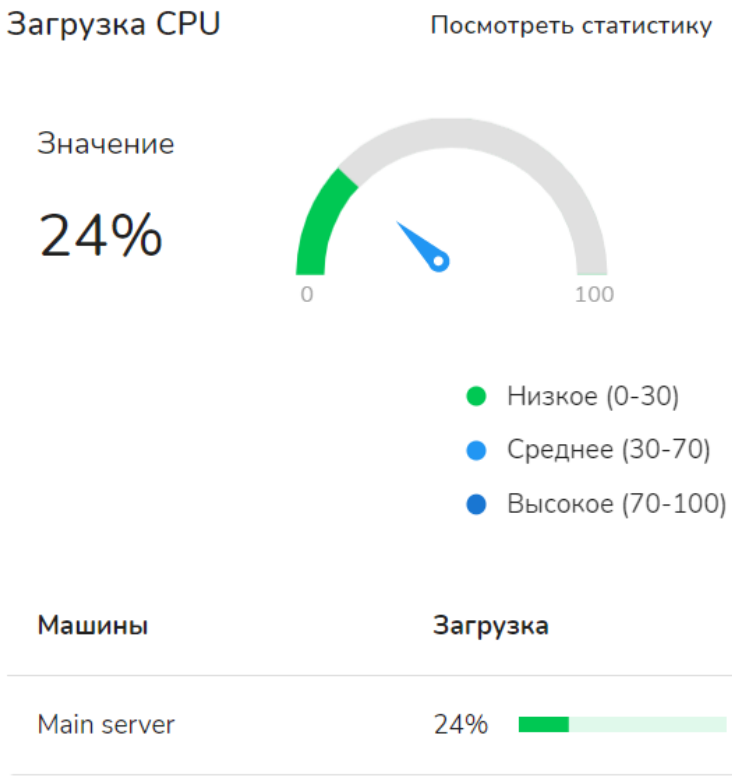
Совокупная информация

Во вкладке Совокупная информация отображены краткие сведения об атаке, которые можно почерпнуть и из других вкладок.

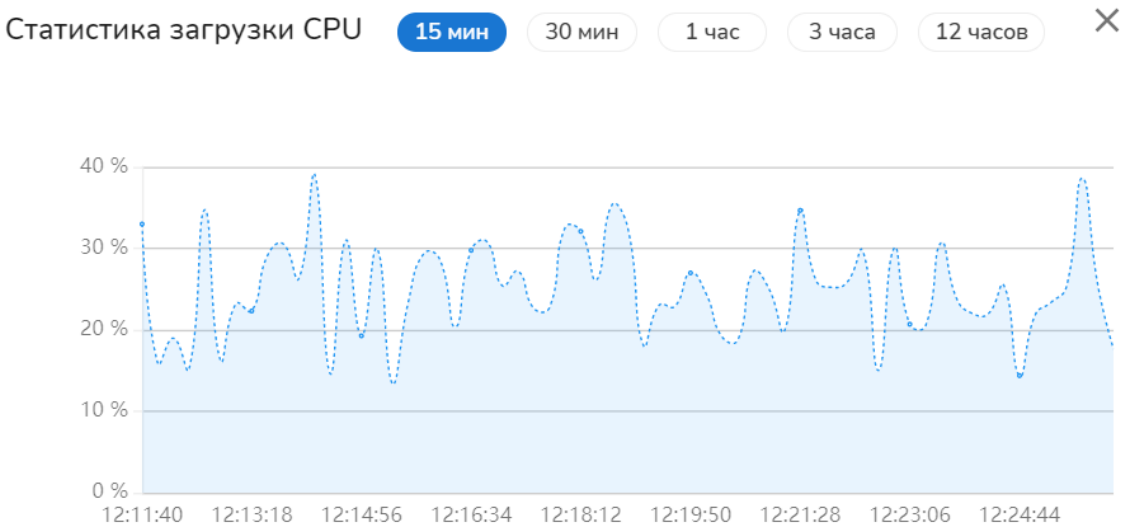


Загрузка CPU

Виджет загрузка CPU отображает текущий уровень загрузки процессора.



Для просмотра статистики нажмите на пункт **Посмотреть статистику**. Она демонстрируется в виде графика на временной шкале.



API

StormWall Sensor Appliance поддерживает работу по REST API (Application Programming Interface). API позволяет автоматизировать работу с объектами системы и напрямую осуществлять запросы на выполнение различных операций. API можно встроить в любые приложения и интернет-ресурсы. С помощью API можно совершать любые операции с Sensor Appliance.

Для авторизации API-запросов необходим ключ. Его необходимо сгенерировать в Личном кабинете пользователя. Подробнее см. Создание API-ключа. Ключ можно привязать к API-клиенту и/или использовать для авторизации при тестировании и работе с API-запросами.

Для клиентов, уже установивших Sensor Appliance, перечень поддерживаемых методов API и их описание доступны по адресу: https://<IP-адрес установленной системы>/docs/index.html.

Ниже приводится таблица с кратким описанием методов API:

Авторизация	Метод	URL	Операция
	POST	/api/auth/restore-password	Восстановление пароля
Работа с регистрационными данными	POST	/api/user/change-email	Изменение email текущего пользователя

пользователя	POST	/api/user/change-password	Изменение пароля текущего пользователя
	GET	/api/user/profile	Получение профиля пользователя
	POST	/api/user/profile	Обновление профиля пользователя
	DELETE	/api/user/token/{id}	Удаление токена
	GET	/api/user/token	Получение токена
	POST	/api/user/token	Создание токена
	GET	/api/user	Получение информации о текущем пользователе
	PUT	/api/user	Обновление свойств текущего пользователя
	GET	/api/timezones	Получение информации о временных зонах
Виджеты	POST	/api/dashboard/charts	Получение всех графиков
	GET	/api/dashboard/widget/attack-history	Получение истории атак
	POST	/api/dashboard/widget/attack-history-watcher	Получение данных о новых атаках и проверка старых
	GET	/api/dashboard/widget/cluster-cpu-usage	Получение данных о загрузке CPU

	GET	/api/dashboard/widget/attack-history-time-frame	Получение сведений об атаках за период времени
Статус	GET	/api/public/status	Получение статуса системы
Митигации	POST	/api/mitigation	Создание новой митигации
	GET	/api/mitigation	Получение митигации
	PUT	/api/mitigation/{id}	Редактирование митигации
	GET	/api/mitigation/{id}	Получение митигации
	DELETE	/api/mitigation/{id}	Удаление митигации
	GET	/api/mitigation/{id}/stats	Получение статистики митигации
	POST	/api/mitigation/{id}/attack-history-watcher	Получение новых атак и проверка старых в рамках митигации
	GET	/api/mitigation/{id}/attack-history	Получение истории атак в рамках митигации
	GET	/api/mitigation/charts	Получение графиков в рамках митигации
	PUT	/api/mitigation/order	Обновление порядка митигаций
Скопы	GET	/api/scope	Получить все скопы

	POST	/api/scope	Создание новой скопы
	GET	/api/scope/{id}	Получение одной скопы
	PUT	/api/scope/{id}	Редактирование префиксов одной скопы
	DELETE	/api/scope/{id}	Удаление одной скопы
Пользователи	GET	/api/users	Получение списка всех пользователей
	POST	/api/users	Создание нового пользователя
	DELETE	/api/users/{id}	Удаление пользователя
	GET	/api/users/{id}	Получение информации о пользователе
	PUT	/api/users/{id}	Обновление данных пользователя
Роли	POST	/api/role	Создание новой роли
	GET	/api/role	Получить список всех ролей
	PUT	/api/role/{id}	Редактирование роли
	GET	/api/role/{id}	Получение информации об одной роли
	DELETE	/api/role/{id}	Удаление роли

Атаки	GET	/api/attacks/{id}	Получение информации об атаке
Настройка BGP	POST	/api/settings/bgp	Настройка конфигурации роутера BGP
	GET	/api/settings/bgp	Получение конфигурации роутера BGP
Настройка маршрутов BGP	GET	/api/settings/bgp-paths	Получение данных о маршрутах BGP
	DELETE	/api/settings/bgp-paths/{id}	Удаление маршрута BGP
Настройка сенсора	GET	/api/settings/sensor/counters	Получение данных счетчиков сенсора
	POST	/api/settings/sensor	Обновление настроек сенсора
	GET	/api/settings/sensor	Получение конфигурации сенсора
Настройка сети	POST	/api/settings/network/update-interfaces	Обновление настроек сетевых интерфейсов
	PUT	/api/settings/network/{id}	Обновление настроек сети
	GET	/api/settings/network	Получение сетевых настроек
Глобальная настройка сети	POST	/api/settings/global-network	Обновление глобальных настроек сети
	GET	/api/settings/global-network	Получение глобальных настроек сети
Настройка SMTP	POST	/api/settings/check-smtp-server	Проверка соединения с SMTP-сервером

	POST	/api/settings/smtp	Обновление настроек SMTP-сервера
	GET	/api/settings/smtp	Получение настроек SMTP-сервера
Настройка webhook-оповещений	GET	/api/settings/messages-webhook	Получение всех webhook-оповещений
	POST	/api/settings/messages-webhook	Настройка webhook-оповещений
	POST	/api/settings/check-webhook	Проверка доступности webhook-оповещений
Настройка White Label	GET	/api/settings/white-label	Получение данных White Label
	POST	/api/settings/white-label	Настройка профиля организации для White Label
	POST	/api/settings/white-label/save-logo	Сохранение логотипа организации
	POST	/api/settings/white-label/save-crt	Сохранение сертификата SSL
	POST	/api/settings/white-label/save-key	Сохранение ключа SSL
Настройка Firewall	POST	/api/settings/firewall	Добавление правил для Firewall
	GET	/api/settings/firewall	Получение списка правил для Firewall
Работа с событиями	GET	/api/events	Получение всех событий

	POST	/api/events/mark-read-by-ids	Маркировка события, как прочитанного пользователем
	POST	/api/events/mark-all-read	Маркировка всех событий, как прочитанных
	GET	/api/events/records-count	Получение количества записей о событиях
Работа с обновлениями	GET	/api/versions	Получение информации обо всех версиях
	POST	/api/update-Sensor Appliance	Запуск обновления Sensor Appliance до последней версии
Работа с журналом	GET	/api/logs/services	Получение данных об имеющихся сервисах и их доступности
	GET	/api/logs/services-logs	Получение лог-файлов сервисов
Базовые операции	GET	/api/validation-schema	Получение схемы соответствия
	POST	/api/reboot	Перезагрузка Sensor Appliance
	GET	/api/get-image/{fileName}	Получение образа
	POST	/api/hard-reset	Возврат Sensor Appliance к первоначальным настройкам
Митигации/обучение сенсора	POST	/api/mitigation/{mitigationId}/sensor-learning-session	Создание новой обучающей сессии

	GET	/api/mitigation/{mitigationId}/sensor-learning-session	Получение списка обучающих сессий
	PUT	/api/mitigation/{mitigationId}/sensor-learning-session/{id}	Исключение атаки из обучающей сессии
	GET	/api/mitigation/{mitigationId}/sensor-learning-session/{id}	Получение информации об обучающей сессии
	DELETE	/api/mitigation/{mitigationId}/sensor-learning-session/{id}	Маркировка обучающей сессии, как завершенной.

Инструкция по установке

Для получения дистрибутива Sensor Appliance обратитесь в отдел продаж компании StormWall. Это можно сделать двумя способами:

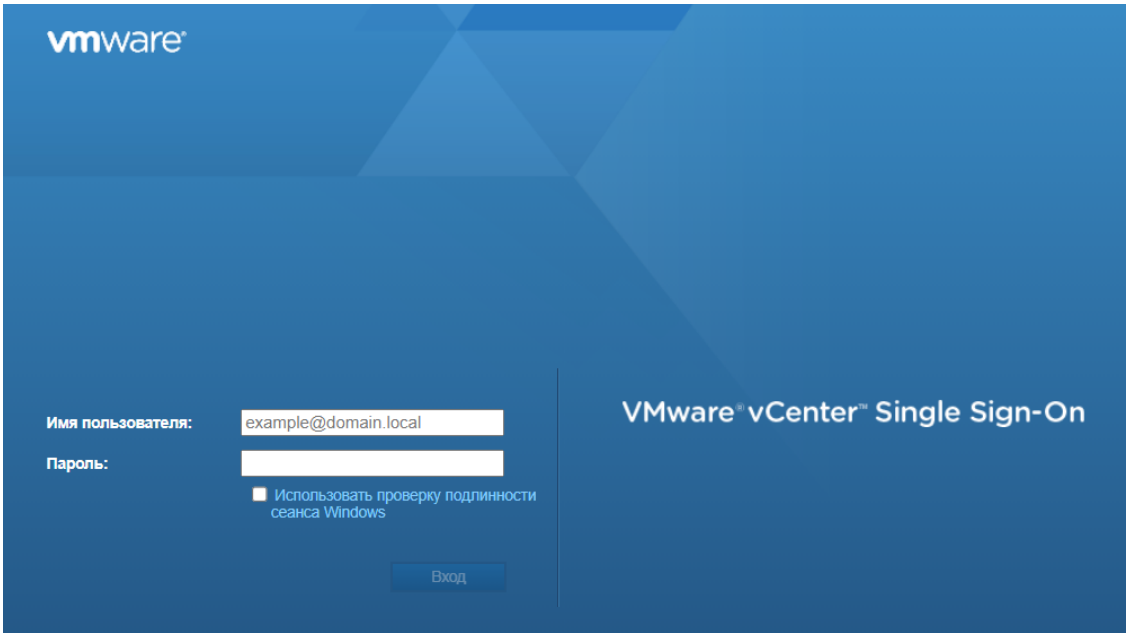
- На сайте stormwall.pro откройте форму онлайн-сообщения **Напишите нам, мы онлайн!** и отправьте сообщение в произвольной форме;
- Напишите письмо по адресу sales@stormwall.pro.

В ответ на обращение вы получите письмо со ссылкой на ISO-образ приложения и ключом активации для него. Скачайте ISO-образ.

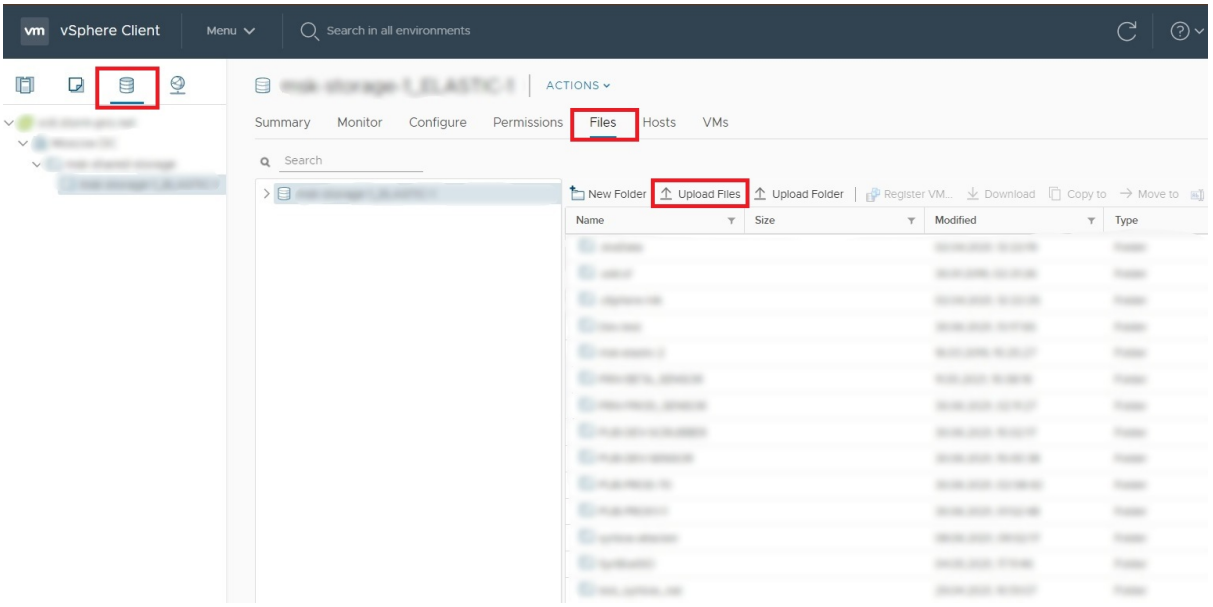
Образ можно установить на виртуальную машину, работающую на любой платформе виртуализации, либо на “чистое железо” (Bare Metal). Ниже приводятся примеры установки Sensor Appliance на виртуальные машины VMware® и Oracle® VirtualBox™. Вы должны обладать лицензией на соответствующие продукты.

Установка на VMware® vSphere™

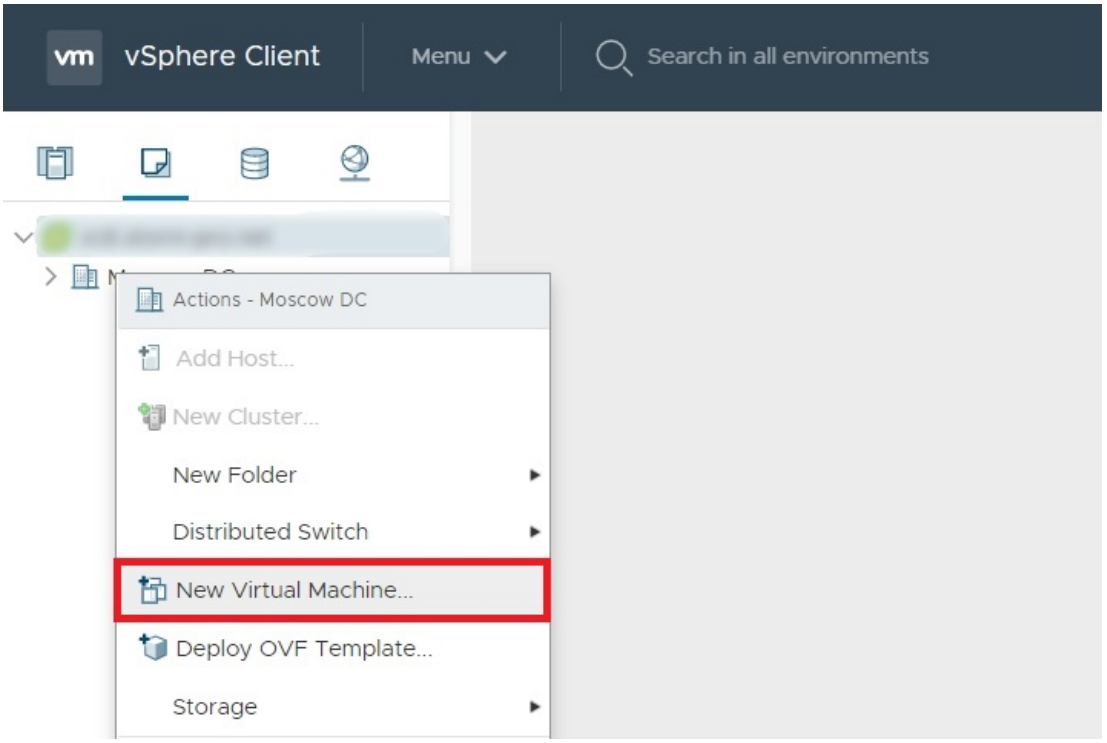
Авторизуйтесь в приложении VMware® vCenter™.



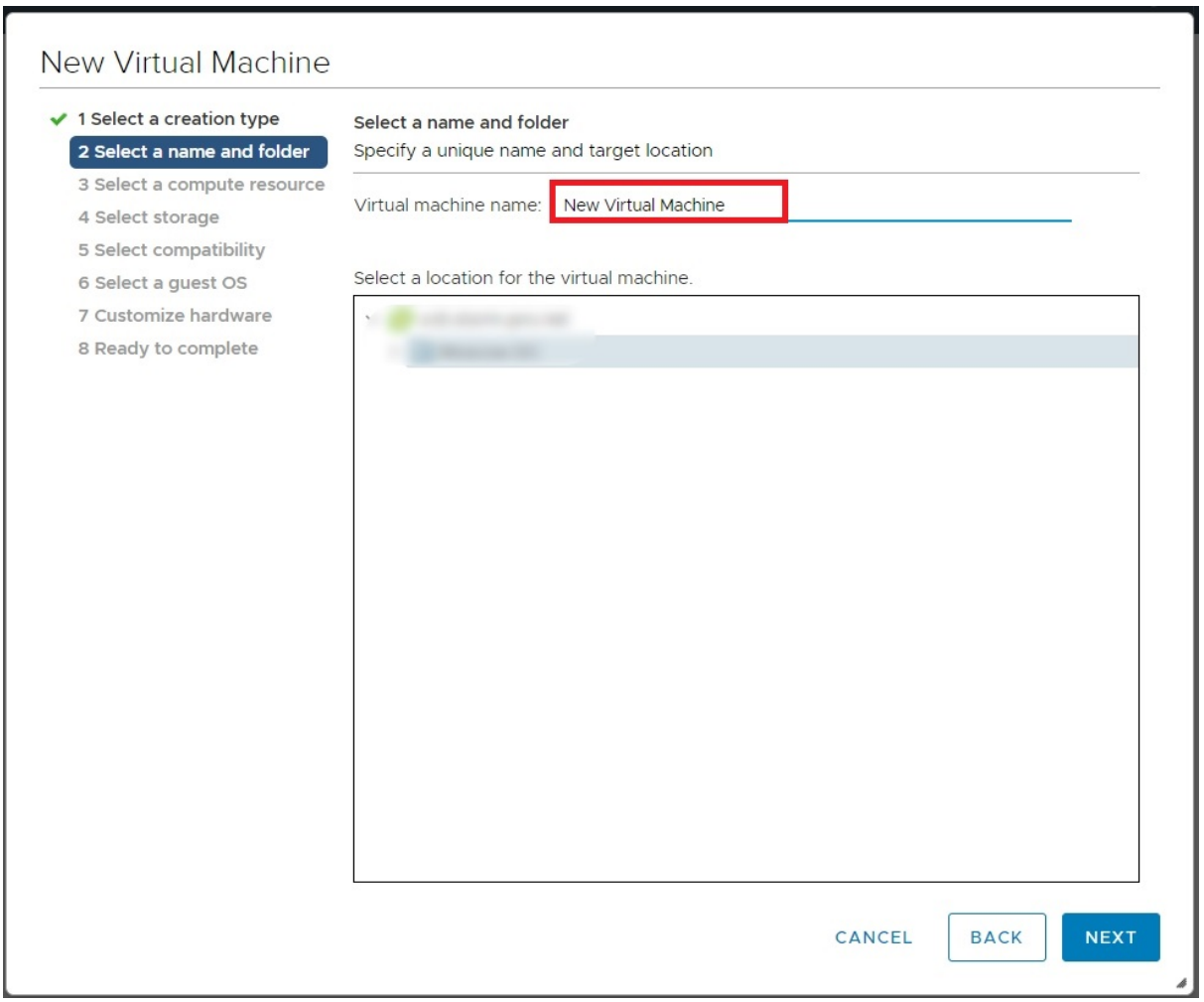
Загрузите ранее полученный ISO-файл с дистрибутивом Sensor Appliance в VMware® vSphere™.



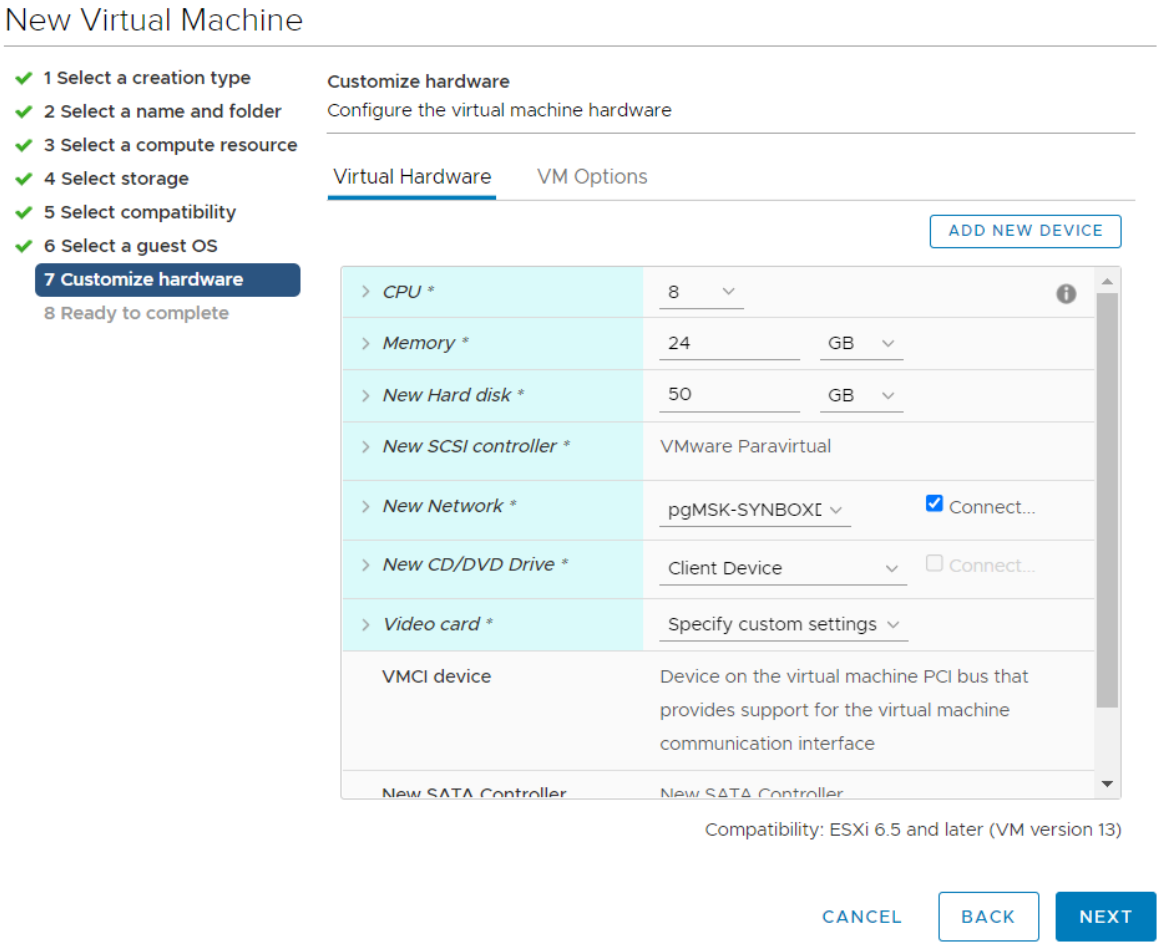
1. Создайте виртуальную машину:
    a. В левом меню выберите каталог, правой кнопкой мыши вызовите контекстное меню, в котором выберите пункт **New Virtual Machine**.



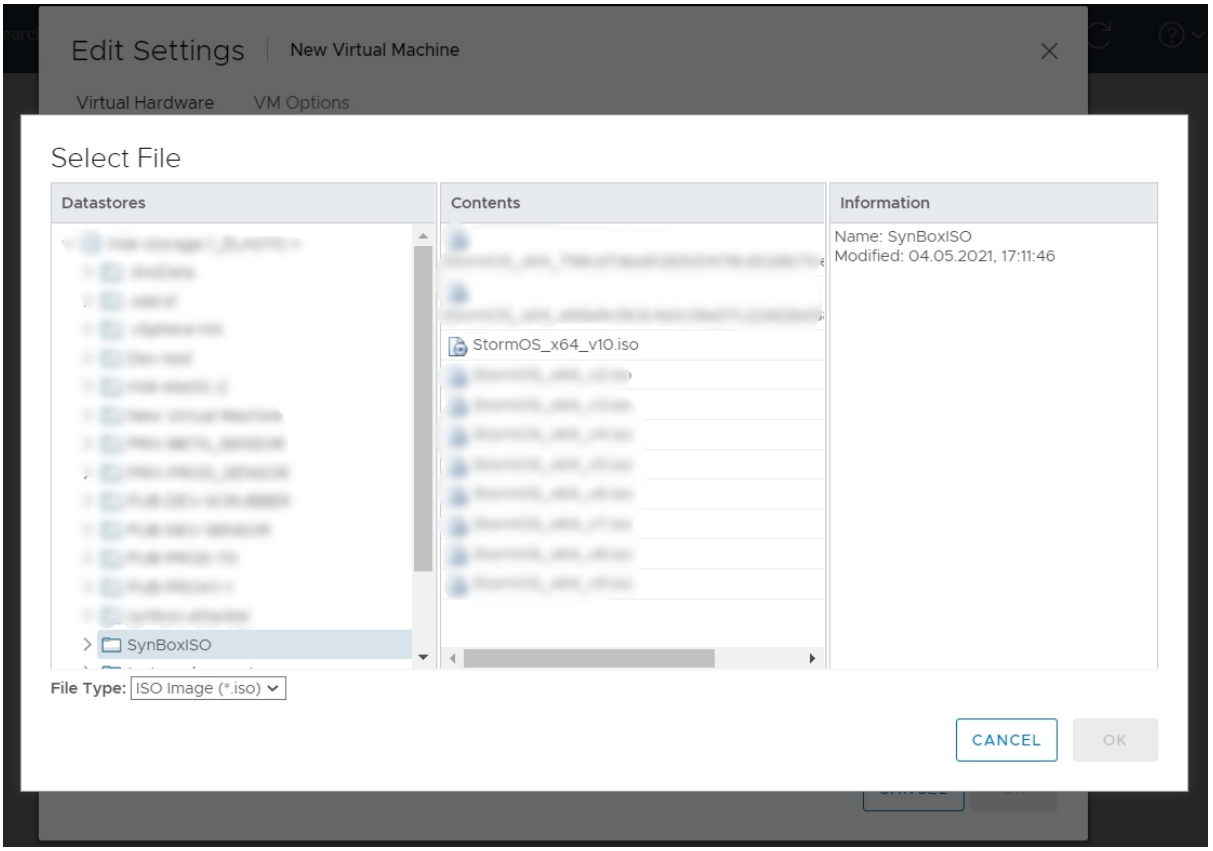
b. В 1-м пункте меню **New Virtual Machine** выберите **Create a new virtual machine**.
c. Во 2-м пункте выберите каталог для виртуальной машины и введите ее название.



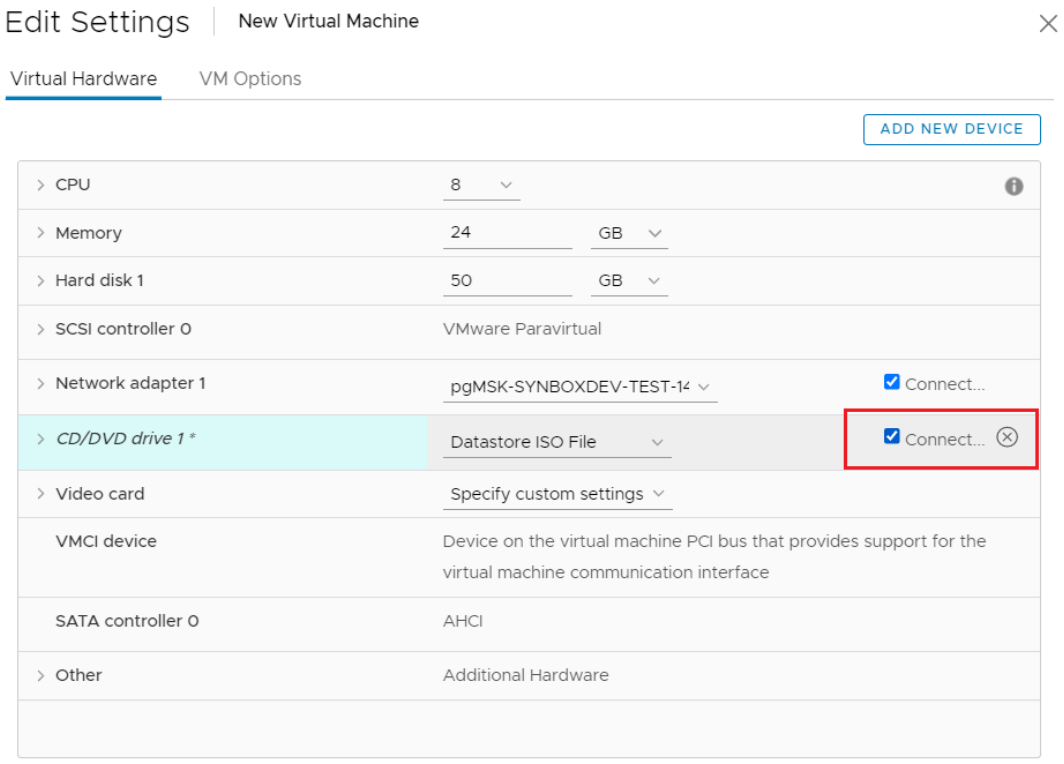
d. В 3-м, 4-м и 5-м пунктах выберите расположение создаваемой виртуальной машины.
e. В 6-м пункте в качестве гостевой операционной системы укажите CentOS 7 64-bit, либо другую систему Linux на базе Kernel не ниже 5.0.
f. В 7-м пункте настройте аппаратную конфигурацию виртуальной машины. Минимальные системные требования:
    - Процессор не менее 8 ядер;
    - Оперативная память не ниже 16 ГБ;
    - SSD-накопитель не менее 50 ГБ.



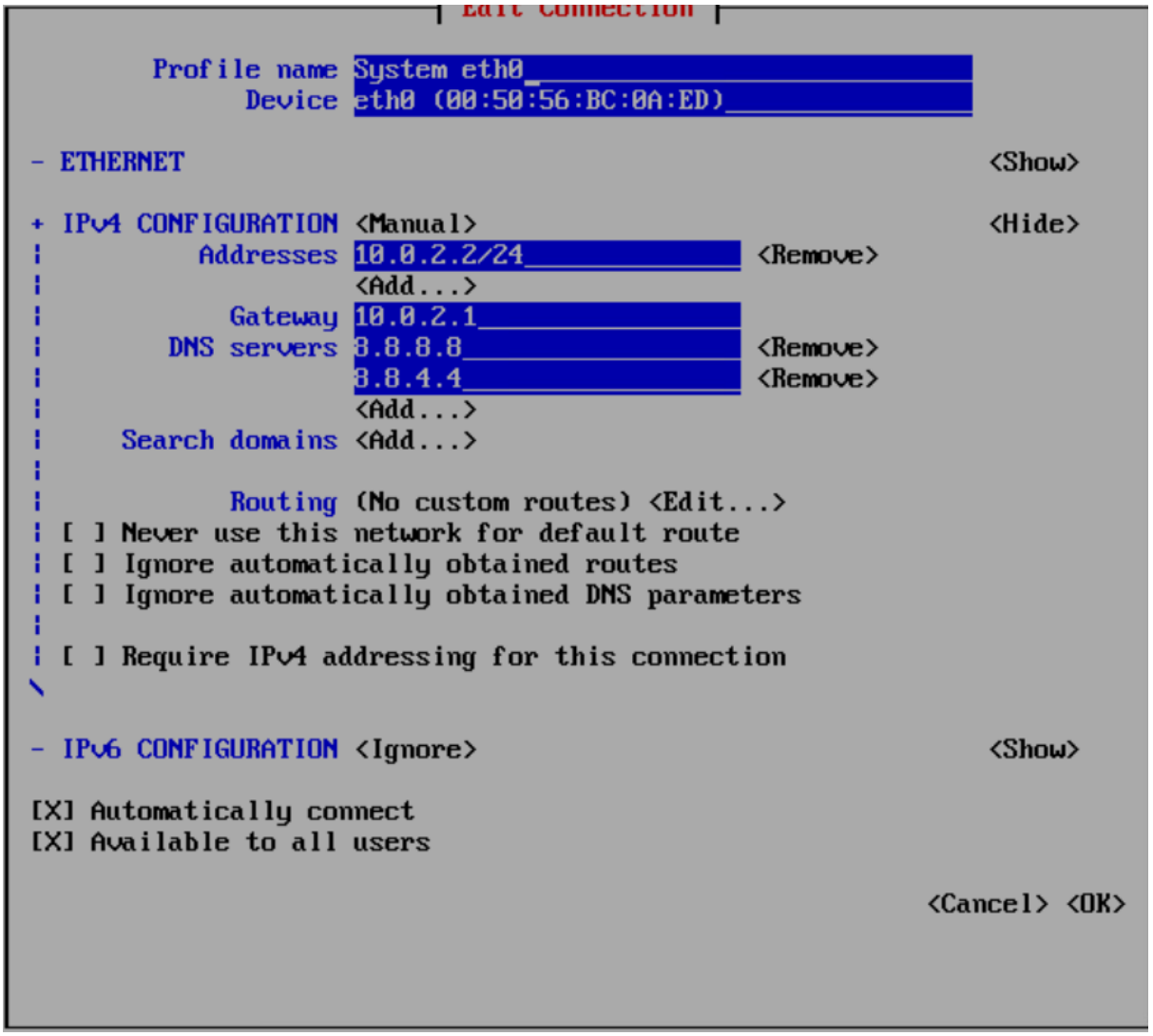
g. В 8-м пункте проверьте заполненные данные и сохраните их.
h. Нажмите правой кнопкой мыши на созданной виртуальной машине и выберите пункт **Edit Settings**. В поле **CD/DVD drive 1** выберите **Datastore ISO File** и укажите ранее загруженный ISO-образ Sensor Appliance.



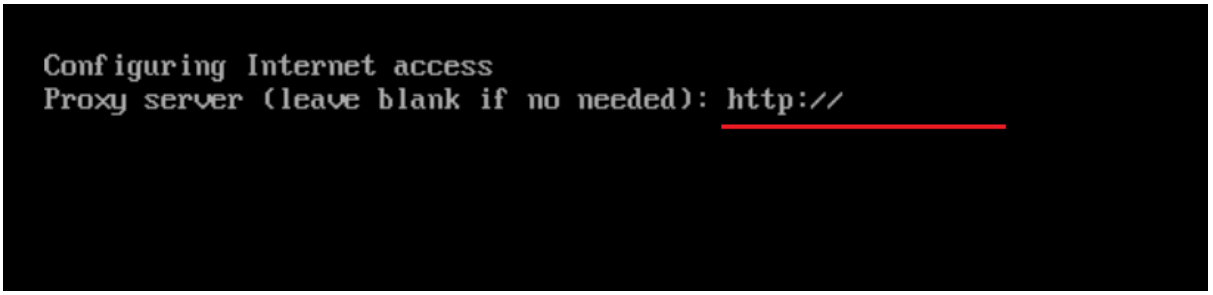
i. После выбора образа отметьте галочкой пункт **Connections** и сохраните изменения.



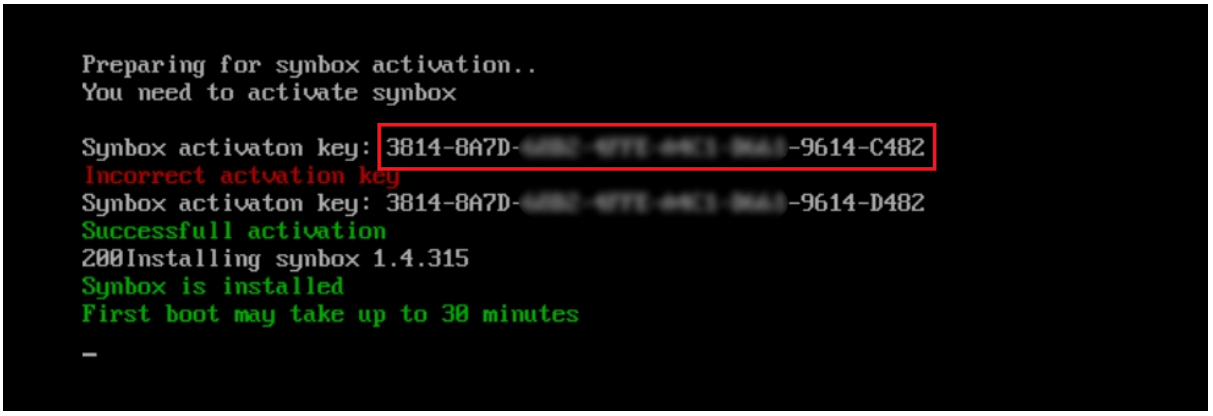
2. Запустите виртуальную машину, для этого нажмите правой кнопкой мыши на созданной виртуальной машине, и в контекстном меню выберите пункт **Power/Power On**.
3. Настройте виртуальную машину. Выполните следующие действия:
    a. Откройте консоль. Дождитесь появления в консоли меню инсталляции.
    b. Введите следующие параметры настройки сети:
        - В пункте **IPv4 CONFIGURATION** выберите **Automatic** (автоматический) или **Manual** (ручной).
        - Если вы выбрали **Manual**, установите **Addresses**, **Gateway**, **DNS servers**.
        - Обязательно заполните маску подсети и DNS!
        - При выборе режиме **Automatic** оставьте все поля пустыми.
        - Остальные параметры оставьте установленными по умолчанию.



    - При необходимости укажите адрес proxy-сервера.



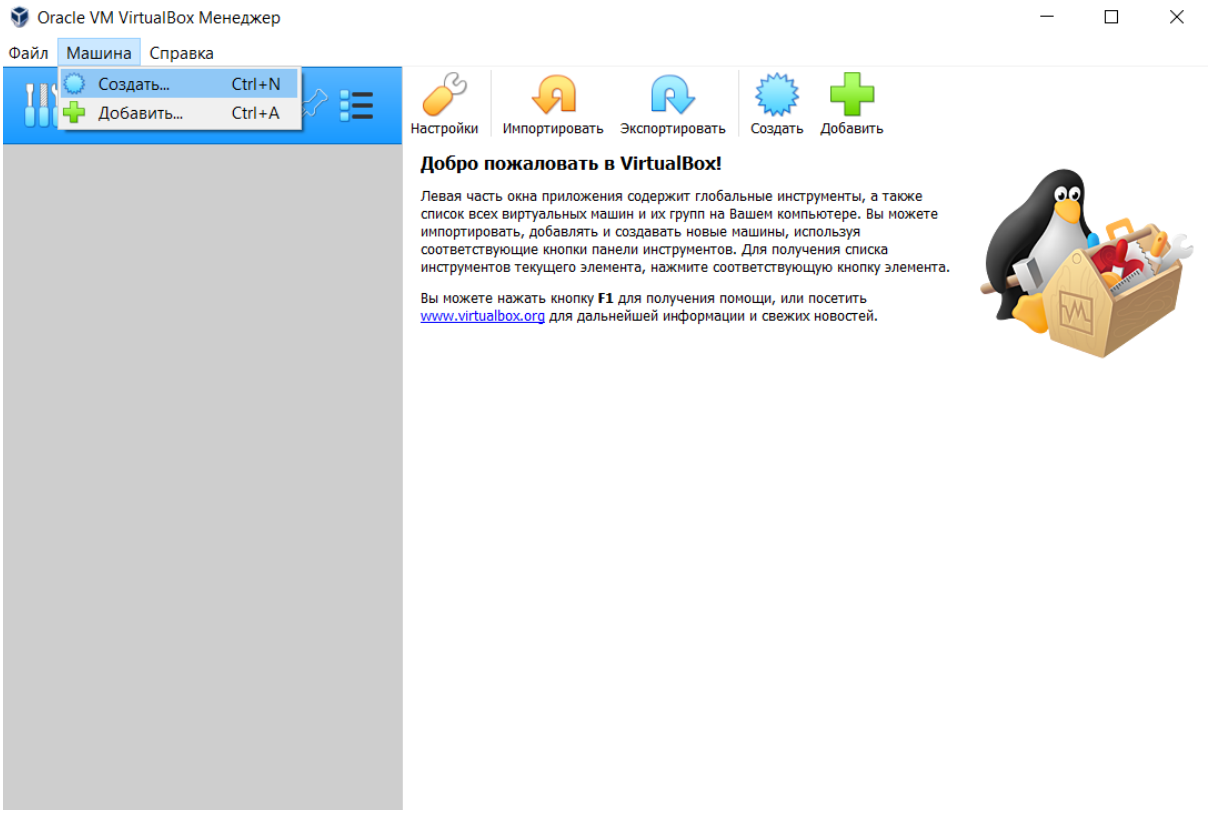
c. Если в процессе инсталляции возникла ошибка, необходимо проверить и исправить параметры в меню инсталляции.
d. При отсутствии ошибок система попросит ввести ключ активации, который был ранее выдан в отделе продаж компании StormWall. При правильном вводе ключа начнется процесс установки Sensor Appliance. В случае появления сообщения об ошибке необходимо проверить корректность вводимого ключа.



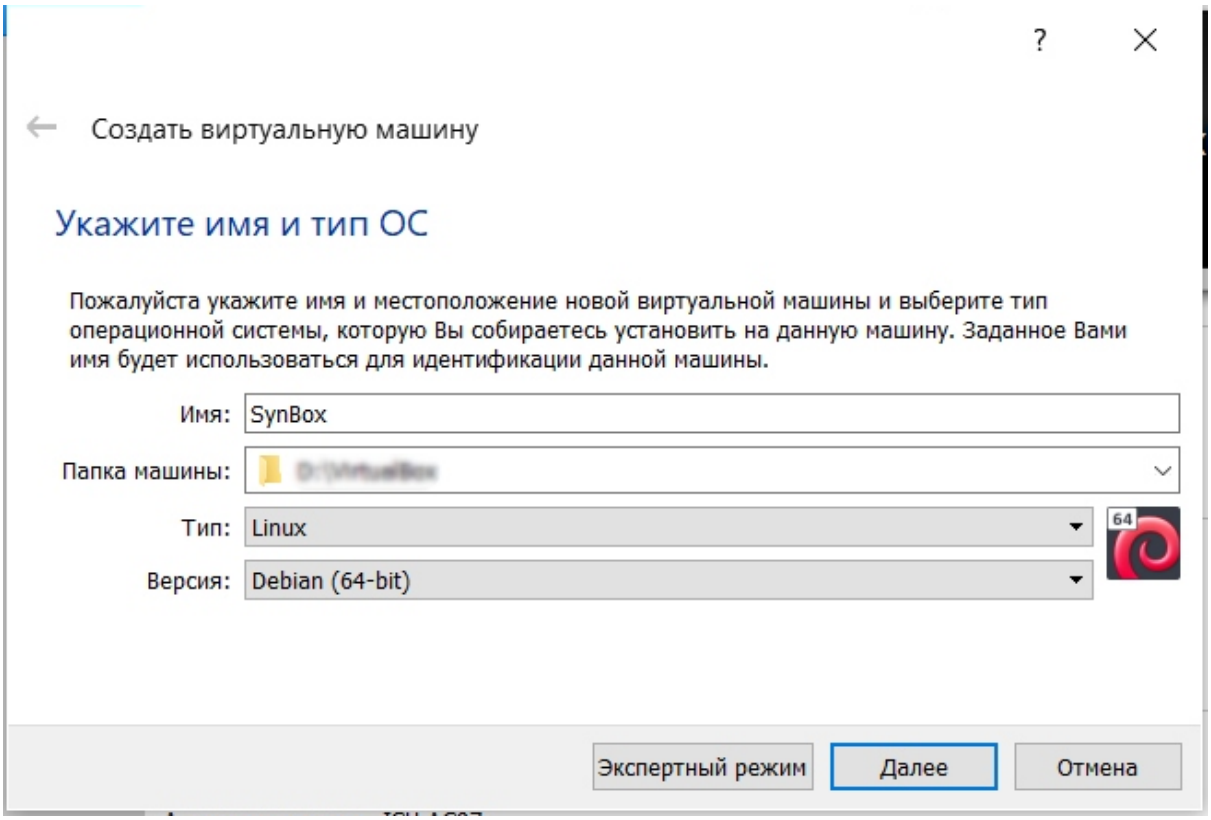
4. Установка Sensor Appliance может занять до 30 минут. После завершения процесса установки можно приступить регистрации Администратора системы (см. подробнее Регистрация Администратора).

Установка на Oracle® VirtualBox™

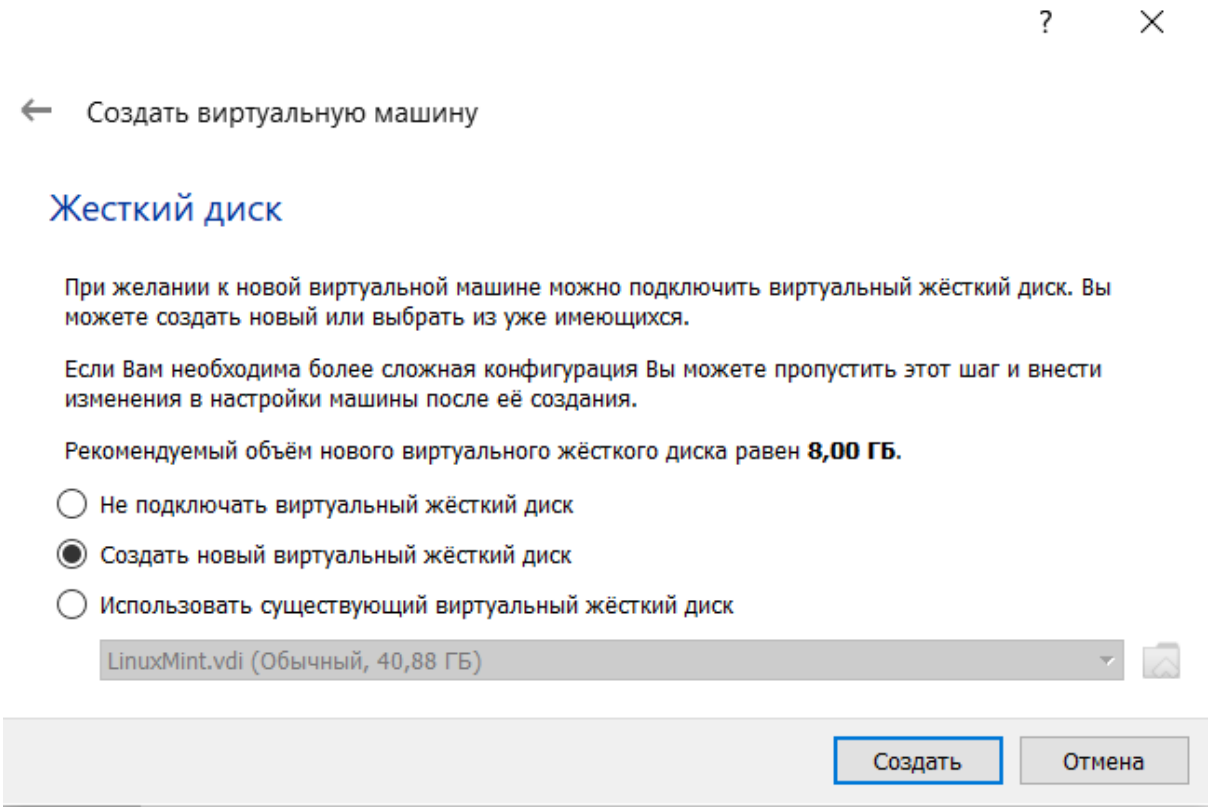
1. Создайте виртуальную машину.
    a. В главном меню выберите **Машина** → **Создать**.



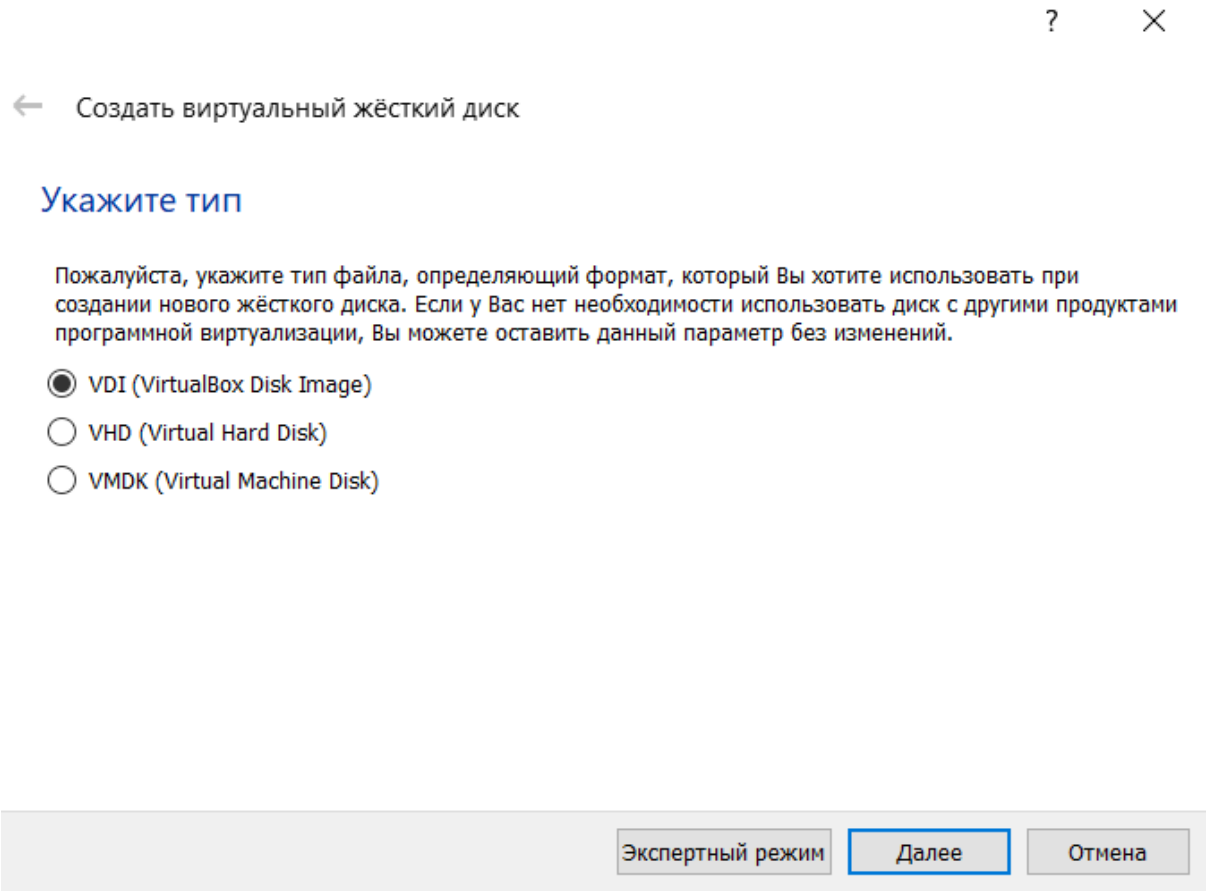
b. В окне **Укажите имя и тип ОС** в поле **Имя** введите название виртуальной машины, например, Sensor Appliance. В поле **Тип** выберите Linux, в поле **Версия** выберите из списка любой 64-х битный вариант.



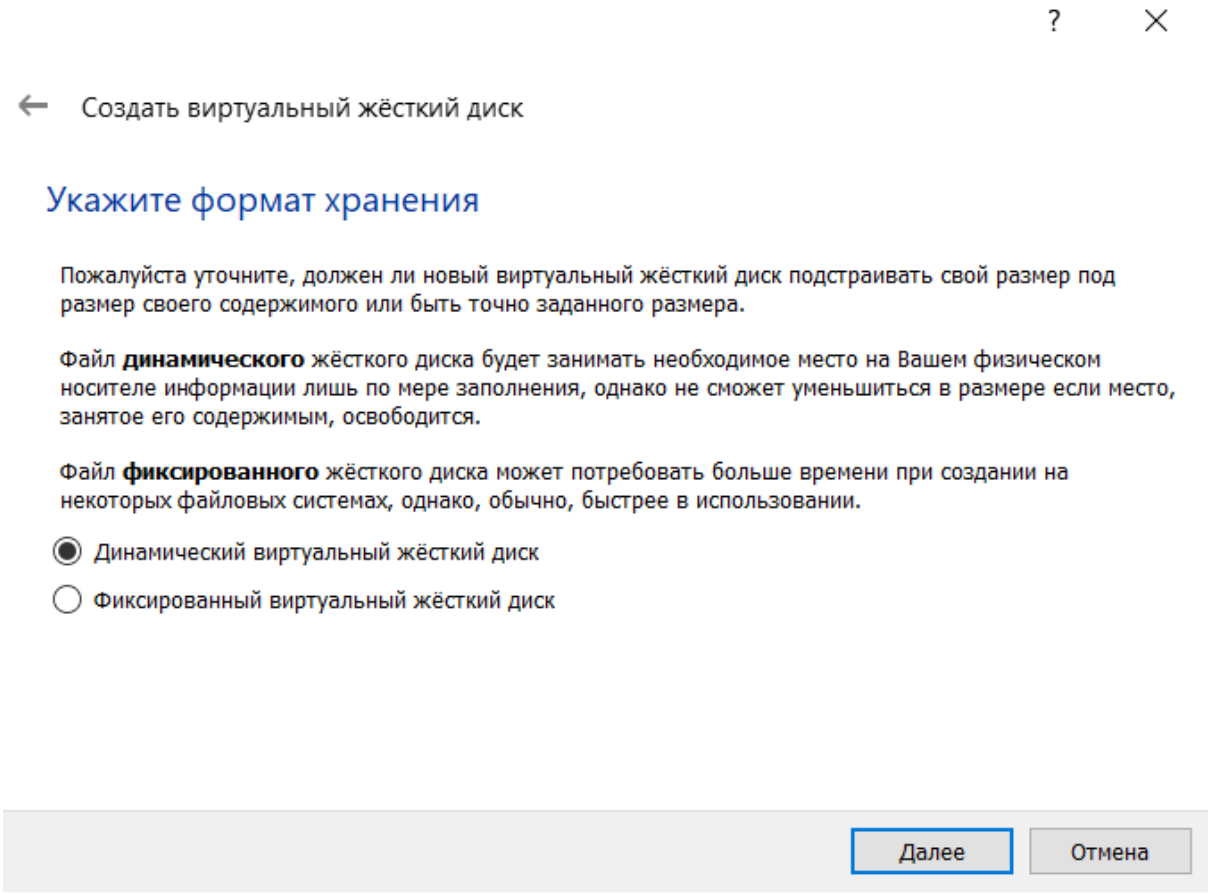
c. В окне **Укажите объем памяти** укажите минимально допустимое для установки Sensor Appliance значение - 16384 МБ (16 ГБ).
d. В окне **Жесткий диск** отметьте галочкой пункт **Создать новый виртуальный жесткий диск**.



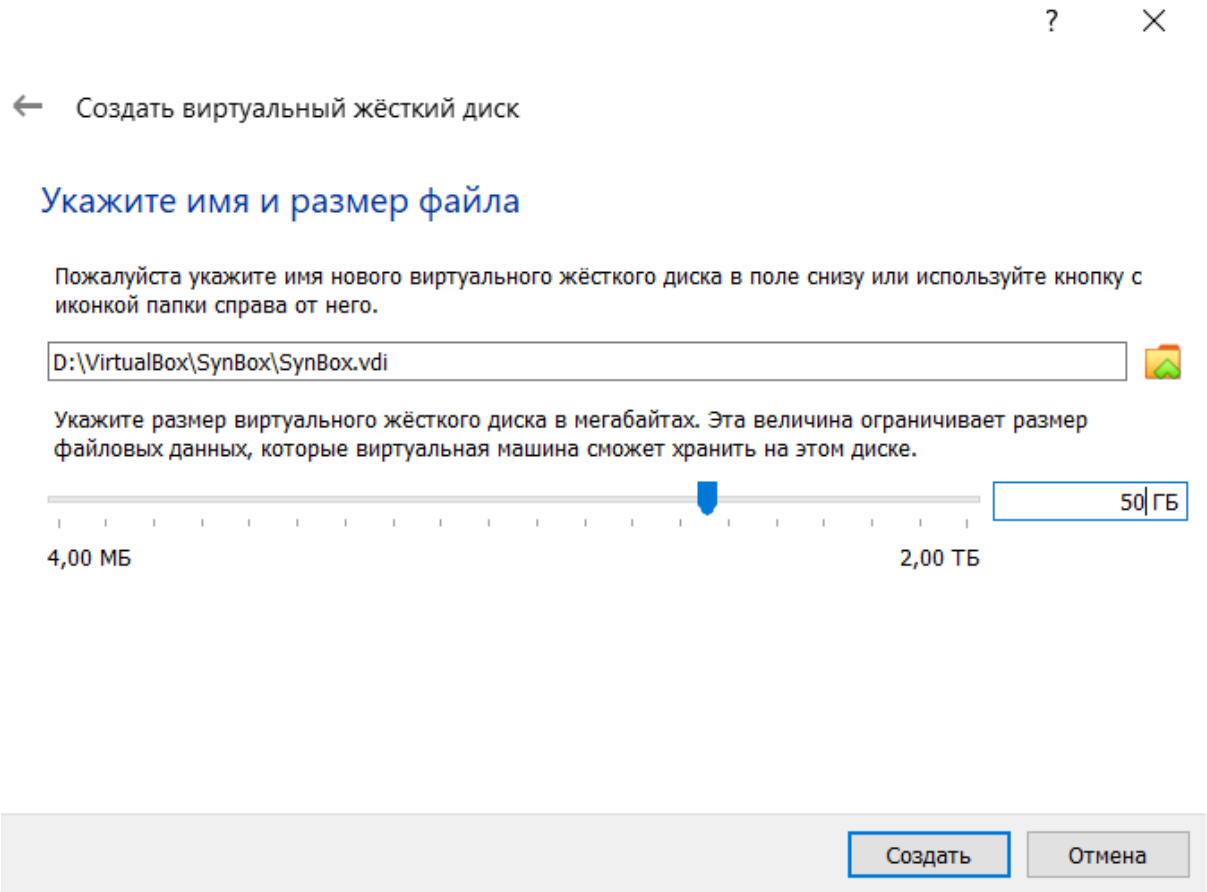
e. В окне **Укажите тип** отметьте галочкой пункт **VDI**.



f. В окне **Укажите формат хранения** отметьте галочкой пункт **Динамический виртуальный жесткий диск**.

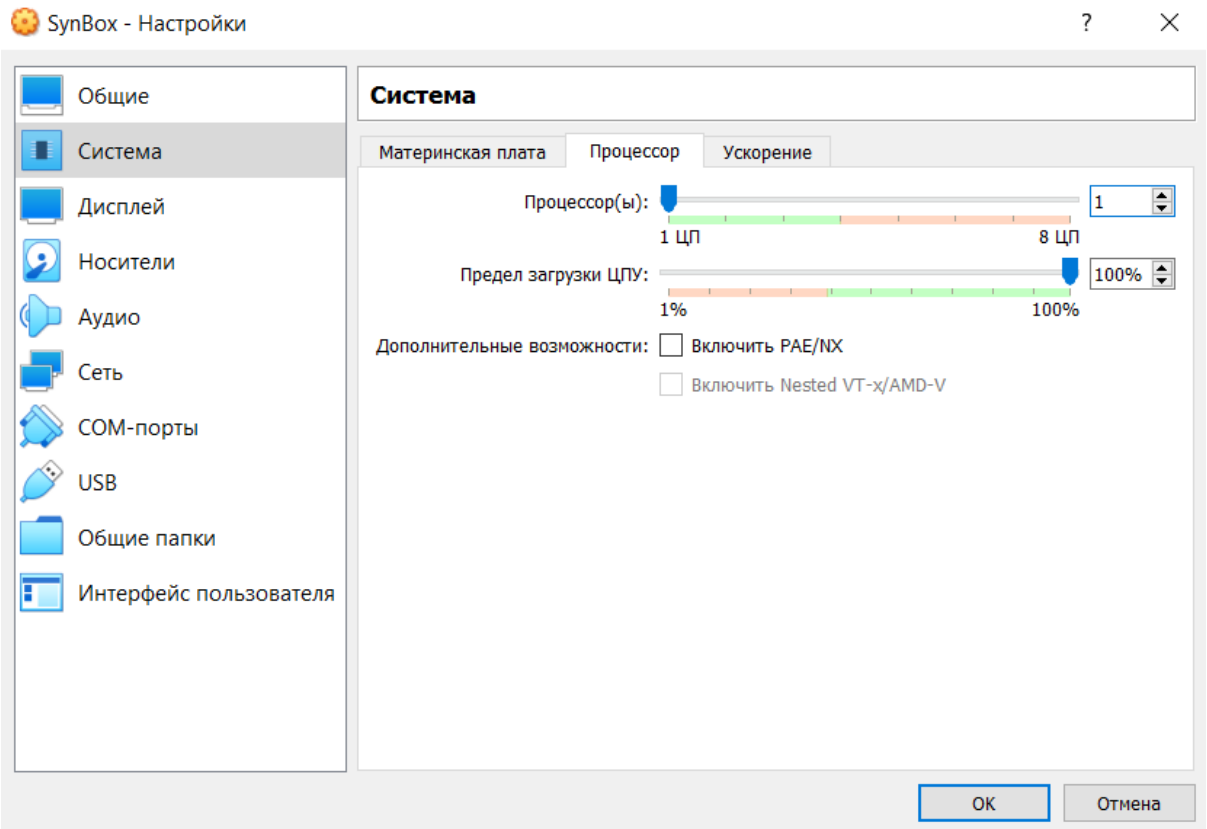


g. В окне **Укажите имя и размер файла** укажите минимально допустимое для установки Sensor Appliance значение - 50 ГБ.

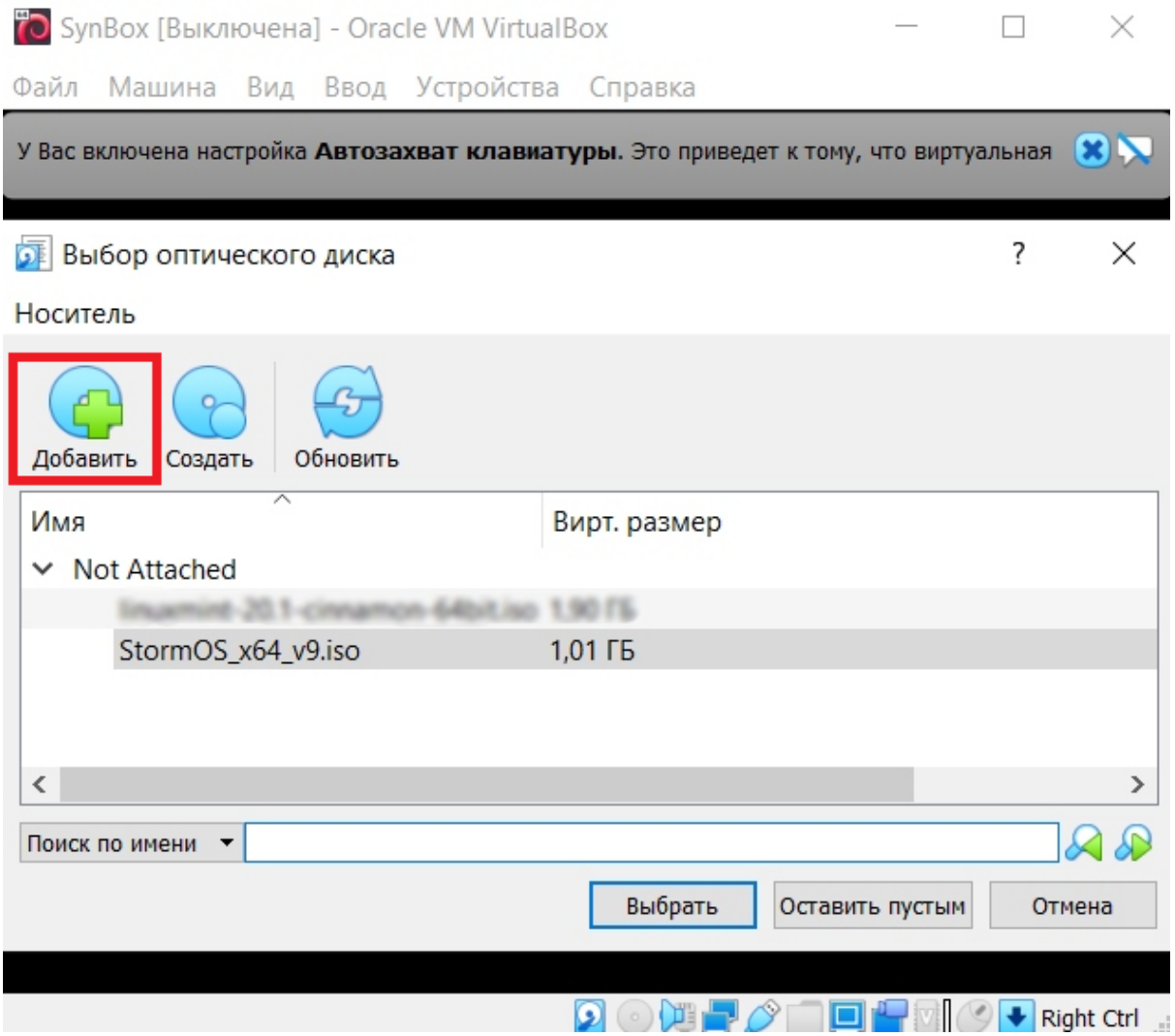


h. Нажмите на кнопку **Создать**. Виртуальная машина создана.

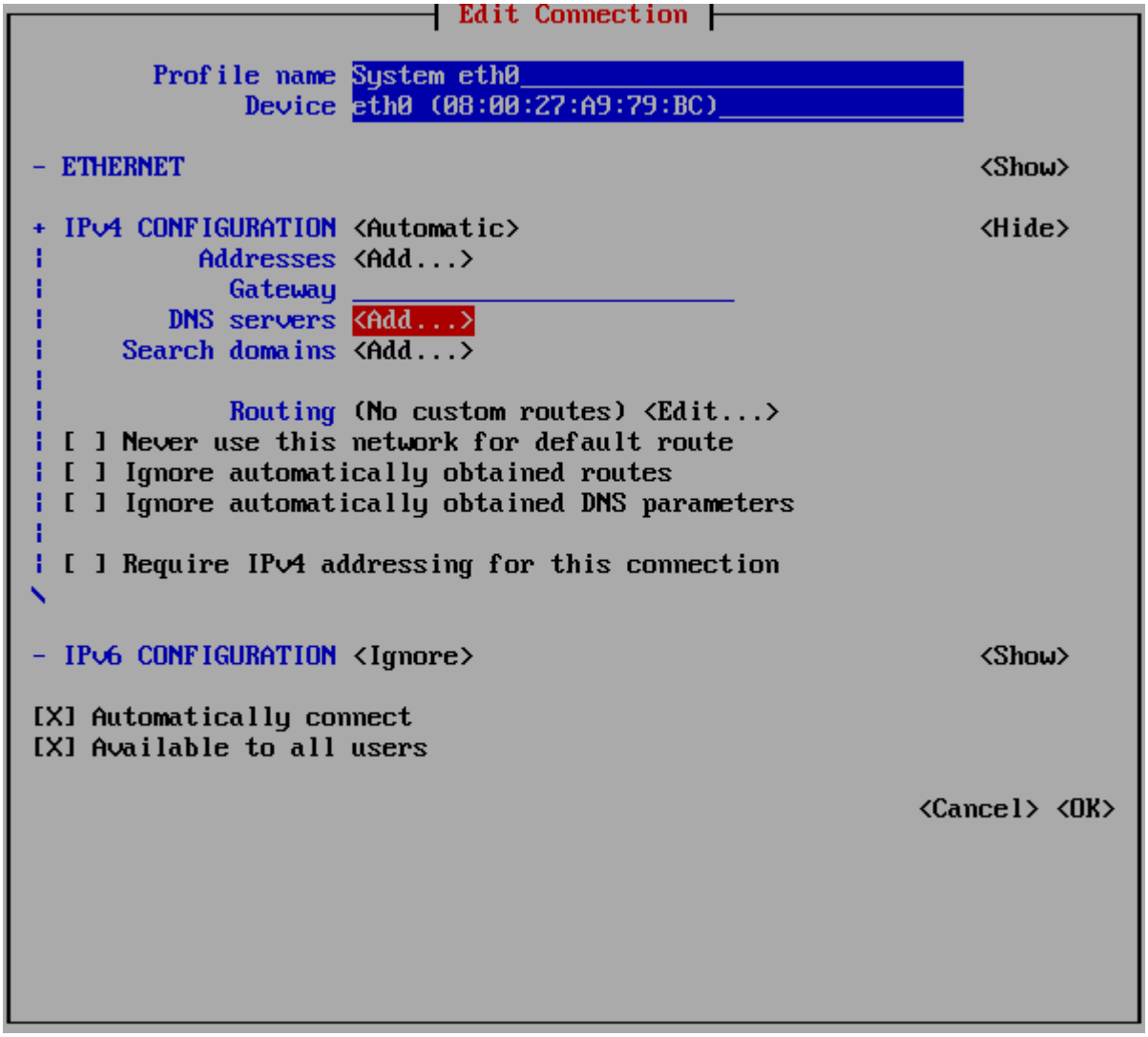
2. Настройте виртуальную машину.
   a. Выберите в левой части главного окна созданную виртуальную машину.
   b. Войдите в меню **Настроить** → **Система** → **Процессор**.
   c. В поле **Процессоры(ы)** укажите минимально допустимое для установки Sensor Appliance значение - 8 ЦП.



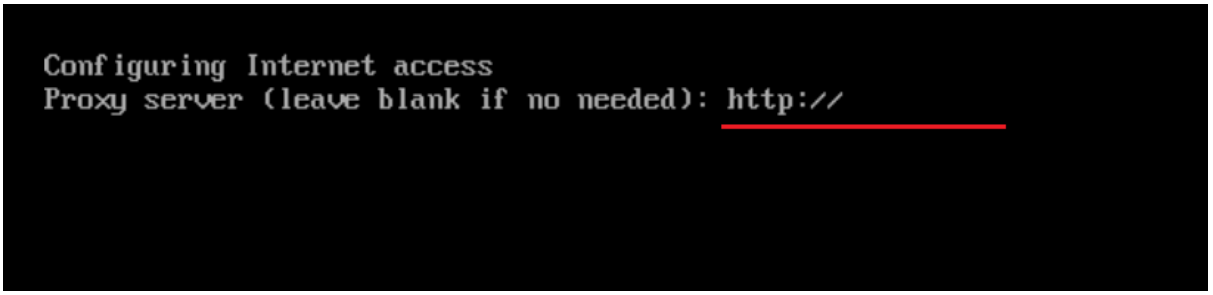
d. Войдите в меню **Настроить** → **Носители** и нажмите на кнопку с изображением оптического диска.
e. В окне **Выбор оптического диска** нажмите на кнопку **Добавить** и выберите ISO-файл, ранее загруженный по ссылке, полученной в отделе продаж компании StormWall. Нажмите на кнопку **Выбрать**.



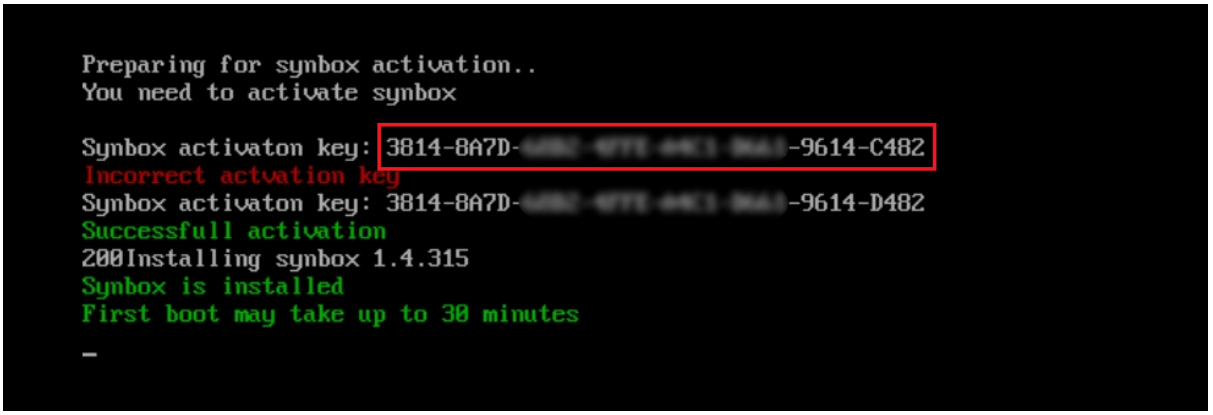
3. Установите Sensor Appliance.
    a. Выберите в левой части главного окна созданную виртуальную машину и нажмите на кнопку **Запустить**.
    b. Дождитесь появления в консоли меню инсталляции.
    c. Введите следующие параметры настройки сети:
        - В пункте **IPv4 CONFIGURATION** выберите **Automatic** (автоматический) или **Manual** (ручной);
        - Если вы выбрали **Manual**, установите **Addresses**, **Gateway**, **DNS servers**;
        - Обязательно заполните маску подсети и DNS!;
        - При выборе режиме **Automatic** оставьте все поля пустыми;
        - Остальные параметры оставьте установленными по умолчанию;



- При необходимости укажите адрес proxy-сервера.



d. Если в процессе инсталляции возникла ошибка, необходимо проверить и исправить параметры в меню инсталляции.
e. При отсутствии ошибок система попросит ввести ключ активации, который был ранее выдан в отделе продаж компании StormWall. При правильном вводе ключа начнется процесс установки Sensor Appliance. В случае появления сообщения об ошибке необходимо проверить корректность вводимого ключа.



4. Установка Sensor Appliance может занять до 30 минут. После завершения процесса установки можно приступить регистрации Администратора системы (см. подробнее Регистрация Администратора).