

Система управления и мониторинга «FortMan»

Программное обеспечение для централизованного управления сетевыми устройствами различных производителей через протокол NETCONF(далее – «FortMan»).

Руководство по настройке «FortMan»»

On-premise

Если возникли проблемы с настройкой FortMan, отправьте электронное письмо по адресу support@fortman.tech, и наши инженеры вам помогут.

Оглавление

Часть #1: Установка и настройка FortMan	3
Шаг 1: Загрузка и распаковка установщика	3
Шаг 2: Установка Системы управления	3
Шаг 3: Проверка работоспособности Системы управления	3
Шаг 4: Открыть Систему управления FortMan	3
Шаг 5: Авторизация	3
Часть #2: Создание клиента и пользователя	5
Часть #3: Настройка Firewall	6
ШАГ 1: Добавление устройства (CPE) в систему управления FortMan	6
ШАГ 2: Добавление конфигурации и правил Firewall	7
Способ 1:	9
Способ 2:	9
Способ 3:	9
ШАГ 3: Добавление в конфигурацию DHCP-сервера (опционально)	10
Шаг 4: Включение функции NAT-PMP (опционально)	10
Шаг 5: Настройка сетвых функций конфигурации (опционально)	11
Шаг 6: Настройка WireGuard (опционально)	11
Часть #4: Присвоение конфигурации устройству	12
ШАГ 1: Присвоение Устройство созданной конфигурации	12
Часть #5: Создание группы и присоединение устройства к группе	13
ШАГ 1: Создание группы и присоединение устройства к группе	13
Часть #6: Статистика и контроль устройств	14
ШАГ 1: Просмотр системных данных	14
ШАГ 2: Получение статистики интерфейсов	14

Часть #1: Установка и настройка FortMan

Шаг 1: Загрузка и распаковка установщика¹

Перейдите на fortman.tech/downloads, выбрав совместимую с ОС версию нажмите «Загрузить».

Начнется загрузка файла `fortmanager.tar.gz`.

После успешной загрузки требуется разместить файл на съемном носителе. Извлеките съемный носитель и вставьте его в сервер, на котором должна располагаться Система управления FortMan.

Разархивируйте файл командой:

```
tar -xzf fortmanager.tar.gz
```

Войдите в папку установщика командой `cd ./installer`.

Шаг 2: Установка Системы управления²

Пропишите в командной строке: `sudo ./install.sh -i`

Шаг 3: Проверка работоспособности Системы управления³

Пропишите команду: `systemctl status isabelle-core.service`.

Вывод команды отразит работоспособность сервиса строкой:

```
Active: active (running)
```

Шаг 4: Открыть Систему управления FortMan

Для входа в панель Системы управления FortMan достаточно с любого устройства в той же сети перейти по: <https://<IP адрес сервера>>

Шаг 5: Авторизация

Авторизация происходит после ввода следующих данных:

```
User: admin Password: admin
```

¹Все описанные действия производятся в предварительно установленной системе Linux Debian

²Если установка не началась, то можно прописать команду `sudo ./install.sh -i`, а затем вновь прописать команду `sudo ./install.sh -i`.

³ Предварительно требуется проверить не установлены ли в системе следующие пакеты: `libnetconf2-2`, `libnetconf2-dev`, `libyang2`, `libyang2-dev`. Если они присутствуют в системе, удалите их командой `apt-remove`, так как они будут конфликтовать с пакетами, которые будут установлены

Правила при создании клиента и пользователя⁴

1. Login, полное имя, адрес e-mail и дата регистрации должны быть заполнены у любого пользователя. Совпадение login или e-mail в системе недопустимы.
2. Пользователь и клиент хранятся в системе под своими внутренними номерами, поэтому при изменении названия, полного имени или любого другого реквизита - его отношения с другими объектами сохраняются.
3. Удаление клиента приводит к автоматическому удалению всех связанных с ним пользователей и других объектов. Удаление пользователя ни на что не влияет.
4. В системе с самого начала зарегистрирован единственный пользователь – Administrator. Он не принадлежит ни к какому клиенту. Только он может создать другого пользователя с аналогичными атрибутами, и только они могут видеть всех пользователей, всех клиентов, зарегистрированных в системе.
5. Пользователь, привязанный к клиенту и имеющий флажок admin, может видеть, создавать и редактировать пользователей для того же клиента. Других пользователей, привязанных к иному клиенту, увидеть невозможно.

Правила при добавлении конфигурации⁵

1. Пользователь с правом admin, не привязанный ни к какому клиенту, может видеть и изменять Default Configuration - базовую конфигурацию, на основе которой строятся конфигурации всех устройств.
2. Любой пользователь может видеть только свои конфигурации, но, создавая конфигурации, получает в них данные из общей Default Configuration, которую предварительно мог настроить Administrator.

Дальнейшая настройка производится от лица созданного пользователя, привязанного к клиенту.

⁴ Относится к «Часть #3».

⁵ Относится к «Часть #4, Шаг 2»

Часть #2: Создание клиента и пользователя

Шаг 1: Авторизация и создание нового клиента

После входа в учетную запись Администратора требуется создать клиента:

После успешного создания клиента требуется создать пользователя, заполнив все необходимые данные:

После создания пользователя требуется зайти в меню редактирования и изменить его пароль.

Часть #3: Настройка Firewall

ШАГ 1: Добавление устройства (CPE) в систему управления FortMan

Перейдите в раздел CPE и нажмите **Добавить**:

The screenshot shows the 'Система управления' (Management System) interface. At the top, there are navigation tabs: 'Конфигурации' (Configurations), 'CPE', 'Группы CPE' (CPE Groups), 'Пользователи' (Users), and '1@'. The 'CPE' tab is selected. Below the tabs, the title 'CPE' is displayed. Underneath, there is a search bar with the text '0 CPE' on the left, a search icon, the text 'Найти CPE', and a 'Поиск' (Search) button. On the right side, there is a 'Все' (All) button and a '+ Добавить' (Add) button.

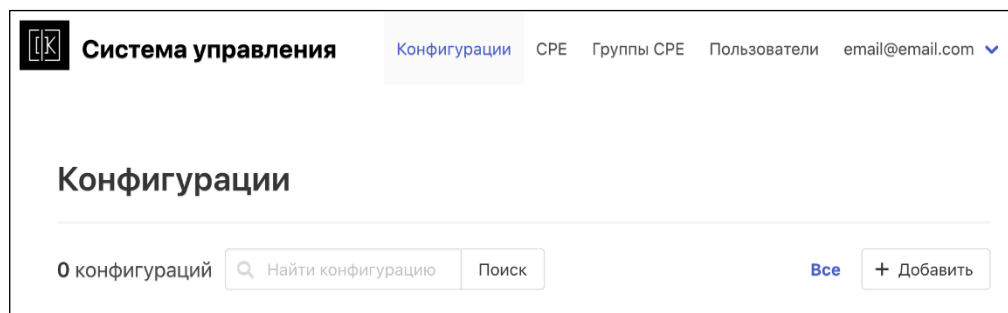
В открывшемся окне впишите Серийный номер и статический IP адрес устройства:

The screenshot shows the 'Редактировать данные CPE' (Edit CPE Data) form. At the top, there are navigation tabs: 'Конфигурации' (Configurations), 'CPE', 'Группы CPE' (CPE Groups), 'Пользователи' (Users), and 'email@email.com'. The 'CPE' tab is selected. Below the tabs, the title 'Редактировать данные CPE' is displayed. Underneath, there is a 'Состояние конфигурации' (Configuration Status) section with the text 'Применено 19.05.2025 21:20:47 +03:00'. Below this, there are several input fields: 'Серийный номер' (Serial Number) with the value 'V100-0000011', 'IP/FQDN' with the value '192.168.1.1', 'Группа' (Group) with the value 'Не задано' (Not specified), 'Конфигурация' (Configuration) with the value 'config1', and 'Организация' (Organization) with a dropdown menu. At the bottom, there is a blue 'Сохранить' (Save) button and a note: 'Редактировать параметры клиента WireGuard'.

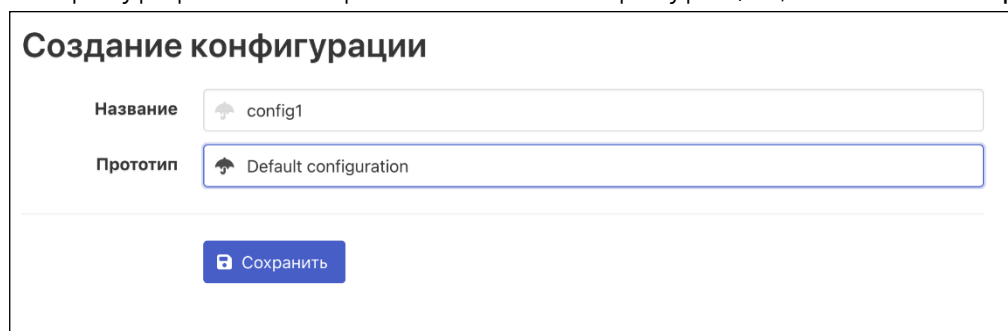
Нажмите на **Сохранить**.

ШАГ 2: Добавление конфигурации и правил Firewall

Перейдите во вкладку Конфигурации.

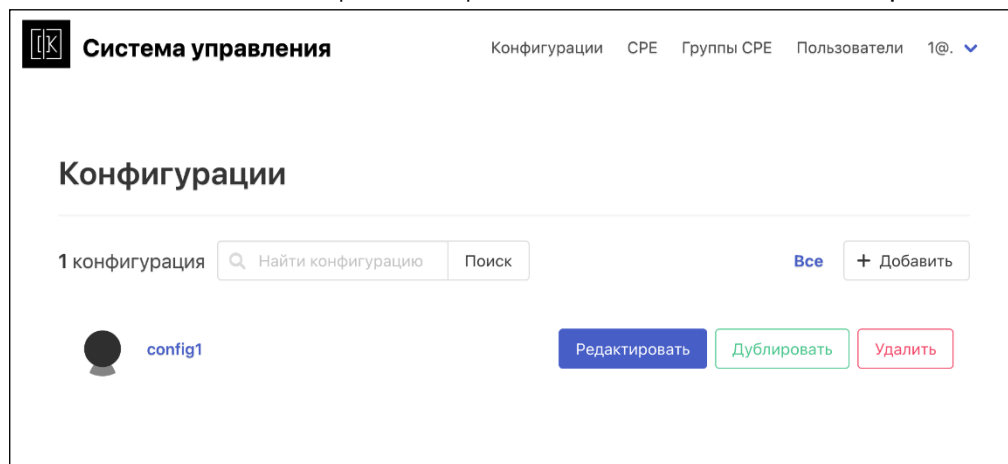


В открывшейся вкладке нажмите **Добавить**, после чего перед вами откроется меню конфигурирования. Присвоив имя конфигурации, нажмите **Сохранить**:



После сохранения, в разделе **Конфигурации** появится ваша конфигурация.

Для того чтобы её отредактировать – нажмите **Редактировать**:



Выберите те модули, которые после редактирования должны отличаться от базовых настроек:

The screenshot shows the 'Redaction of configuration' (Редактирование конфигурации) page. At the top, there is a navigation bar with 'Система управления' and several menu items: 'Конфигурации', 'CPE', 'Группы CPE', 'Пользователи', and 'email@email.com'. The main heading is 'Редактирование конфигурации'. Below it, there are two input fields: 'Название' (Name) with the value 'config1' and 'Прототип' (Prototype) with the value 'Default configuration'. A section titled 'Выбрать и редактировать модули, отличные от конфигурации прототипа:' (Select and edit modules, different from the prototype configuration:) contains a list of checkboxes for various modules: Interfaces, Management, DHCP Server, Port Mapping, CPE networking, WireGuard client, IDS/IPS, and Syslog. At the bottom, there are two buttons: 'Сохранить' (Save) and 'Сохранить в файле' (Save to file).

Нажмите Сохранить. Перейдите в раздел IDS/IPS:

В открывшейся вкладке настраиваются правила Firewall:

The screenshot shows the 'Redaction of the IDS/IPS module for configuration config1' (Редактирование модуля IDS/IPS для конфигурации config1) page. The navigation bar is the same as in the previous screenshot. The main heading is 'Редактирование модуля IDS/IPS для конфигурации config1'. Below the heading, there is a blue button 'Назад к списку модулей' (Back to module list). There is a checkbox labeled 'enabled:' which is currently unchecked. Below that, there is a section titled 'Rule' with a green 'Add rule' button. At the bottom, there is a 'Сохранить' (Save) button, a 'Выбрать файлы' (Select files) button with the text 'Файл не выбран' (File not selected), and an 'Upload rules file' button.

В данный момент доступно 3 способа добавления правил: вручную, структурно и с помощью конфигурационного файла.

Способ 1:

Нажмите **Add rule**:

Появится редактируемое правило.

Перед вами появится редактор правил.

В редакторе вы можете присвоить имя, добавить правило, а также скрыть и удалить его.

Нажмите **Сохранить**.

Способ 2:

Нажмите **Add rule**.

Присвойте правилу имя, выберите формат **Structured**, после чего начните его редактировать.

Отредактировав первую часть правила, отвечающего за его функции, переходите ко второй части, расположенной ниже на странице.

После заполнения всей структуры правила нажмите **Сохранить**.

Способ 3:

Нажмите **Выбрать файлы** и выберите подготовленный файл с правилами.

Загрузите файл нажатием **Upload rules file**.

Нажмите на кнопку **Show**.

Отредактируйте название и структуру правил, если это необходимо.

Нажмите **Сохранить**.

ШАГ 3: Добавление в конфигурацию DHCP-сервера (опционально)

Перейдите в раздел Конфигурации.

Выберите одну из ваших конфигураций и нажмите Редактировать.

Перейдите в раздел DHCP Server.

В этом разделе необходимо указать данные по вашему усмотрению.

Нажмите Сохранить.

Шаг 4: Включение функции NAT-PMP (опционально)

Перейдите в раздел Конфигурации.

Выберите одну из ваших конфигураций и нажмите Редактировать.

Перейдите в раздел Port Mapping.

В этом разделе необходимо включить функцию, а также, при надобности, сконфигурировать её.

Нажмите Сохранить.

Шаг 5: Настройка сетвых функций конфигурации (опционально)

Перейдите в раздел Конфигурации.

Выберите одну из ваших конфигураций и нажмите Редактировать.

Перейдите в раздел CPE networking.

В этом разделе необходимо настроить сетевые функции устройства⁶.

Нажмите Сохранить.

Шаг 6: Настройка WireGuard (опционально)

Перейдите в раздел Конфигурации.

Выберите одну из ваших конфигураций и нажмите Редактировать.

Перейдите в раздел WireGuard client.

В этом разделе необходимо настроить сетевые функции устройства.

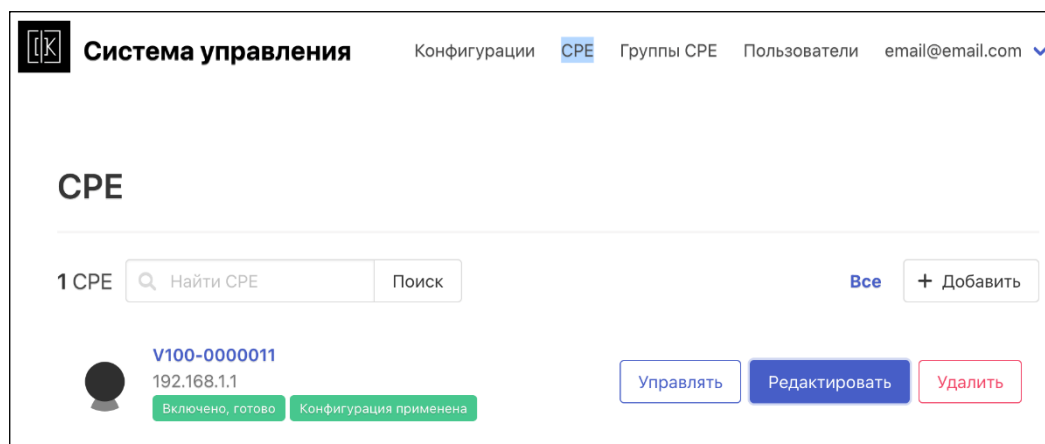
Нажмите Сохранить.

⁶ Предупреждение: Совместная работа функции fastpath и правил, настроенных в разделе IDS/IPS, может привести к ложно-низкому результату измерения производительности TCP-соединения.

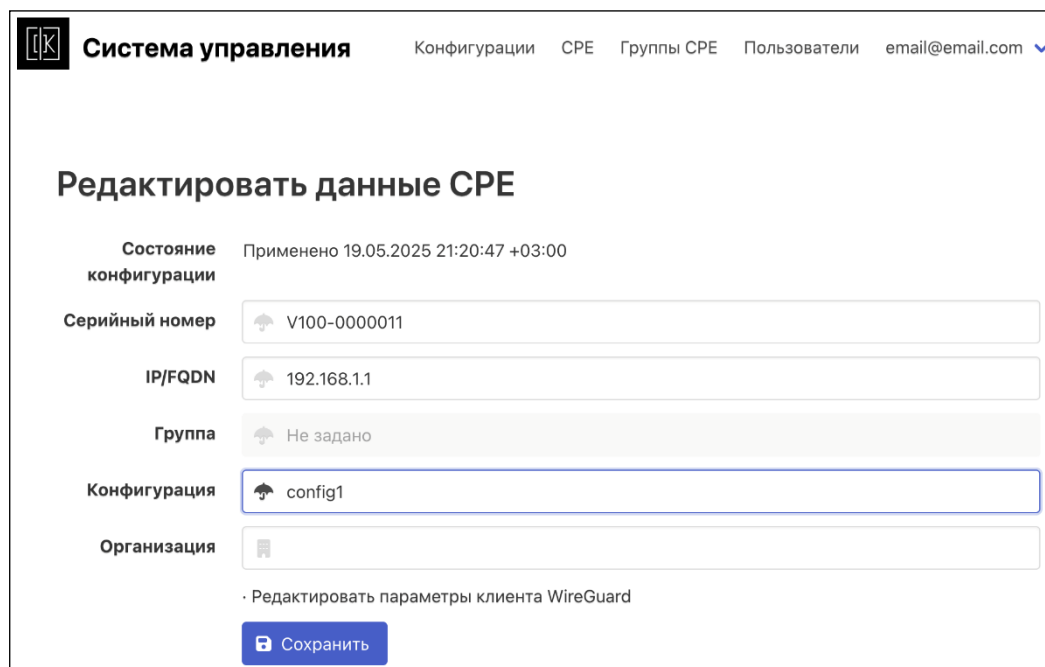
Часть #4: Присвоение конфигурации устройству

ШАГ 1: Присвоение Устройство созданной конфигурации⁷

Выберите ваше устройство во вкладке CPE, нажмите Редактировать:



В строке Конфигурация выберите вашу конфигурацию:



После выбора конфигурации нажмите Сохранить.

Примечание. Если у вас несколько устройств, данный шаг нужно проделать с каждым устройством. Также, если у вас несколько FORT-V, предназначенных для работы с разными правилами, выборочно добавьте устройства в разные конфигурации.

⁷ Если вы управляете сразу несколькими устройствами и хотите добавить их в группу, перейдите к «Часть #6» данной инструкции

Часть #5: Создание группы и присоединение устройства к группе

ШАГ 1: Создание группы и присоединение устройства к группе⁸

Перейдите во вкладку Группы CPE.

Нажмите **Добавить** для создания группы:

Дайте группе название и присвойте одну из настраиваемых ранее конфигураций:

Нажмите **Сохранить**.

Далее перейдите в раздел CPE и выбрав устройство нажмите кнопку **Редактировать**:

Присоедините устройство к группе и нажмите **Сохранить**.

⁸ Таким образом вы сможете контролировать группу устройств, а также одновременно присвоить всем одинаковую конфигурацию.

Часть #6: Статистика и контроль устройств

ШАГ 1: Просмотр системных данных

Для того чтобы просмотреть системные сообщения, появившиеся во время работы, требуется:

В разделе СРЕ нажать **Управлять** напротив одного из устройств, в открывшемся окне нажать **Получить журнал**.

В открывшемся разделе **Системный журнал СРЕ** вы можете наблюдать системные события.

ШАГ 2: Получение статистики интерфейсов

Для получения статистики интерфейсов устройств достаточно выполнить несколько действий:

В разделе СРЕ нажать на кнопку **Управлять**; напротив одного из устройств в открывшемся окне нажать кнопку **Получить статистику**.

В открывшемся разделе **Статистика по интерфейсам СРЕ** вы можете наблюдать всю статистику интерфейсов устройства.