

FORT-V

Межсетевой экран нового поколения

Руководство по настройке меж сетевого экрана FORT-V

On-premise

Если возникли проблемы с настройкой FORT-V, отправьте электронное письмо по адресу support@fortv.ru, и наши инженеры вам помогут.

Навигатор

Часть #1: Распаковка и подключение устройства.....	3
ШАГ 1: Распаковка.....	3
ШАГ 2: Подготовка к монтажу.....	3
ШАГ 3: Подключение устройства.....	3
Часть #2: Установка и настройка Системы управления.....	4
Шаг 1: Загрузка и распаковка установщика.....	4
Шаг 2: Установка Системы управления.....	4
Шаг 3: Проверка работоспособности Системы управления.....	4
Шаг 4: Открыть Систему управления.....	4
Шаг 5: Авторизация.....	4
Часть #3: Настройка Firewall.....	5
ШАГ 1: Добавление FORT-V в систему менеджмента.....	5
ШАГ 2: Добавление конфигурации и правил Firewall.....	6
Способ 1:.....	9
Способ 2:.....	10
Способ 3:.....	10
ШАГ 3: Добавление в конфигурацию DHCP-сервера (опционально).....	11
Шаг 4: Включение функции NAT-PMR (опционально).....	11
Шаг 5: Настройка сетевых функций конфигурации (опционально).....	11
Шаг 6: Настройка WireGuard (опционально).....	12
Часть #4: Присвоение конфигурации устройству.....	13
ШАГ 1: Присвоение FORT-V созданной конфигурации.....	13
Часть #5: Создание группы и присоединение устройства к группе.....	14
ШАГ 1: Создание группы и присоединение устройства к группе.....	14
Часть #6: Статистика и контроль устройства.....	15
ШАГ 1: Просмотр системных данных.....	15
ШАГ 2: Получение статистики интерфейсов.....	15

Часть #1: Распаковка и подключение устройства

ШАГ 1: Распаковка

В комплект поставки входит: руководство по настройке и использованию, устройство FORT-V (далее – устройство), крепление для стойки 19", кабель питания и сетевое устройство.

ШАГ 2: Подготовка к монтажу

Крепление для стойки 19" расположите в удобном для вас месте, после чего установите FORT-V в монтажную область.

ШАГ 3: Подключение устройства

В левый порт устройства подключите кабель ведущий в локальную сеть. В правый порт устройства подключите провод интернета со статическим IP адресом. Подключите устройство к питанию.

Часть #2: Установка и настройка Системы управления

Шаг 1: Загрузка и распаковка установщика¹

Перейдите на fortv.ru/downloads, нажмите на «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.

Разархивируйте файл командой:

```
tar -xz -f 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

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

Шаг 5: Авторизация

Авторизация происходит после ввода следующих данных:

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

¹Все описанные действия производятся в предварительно установленной системе Linux Debian

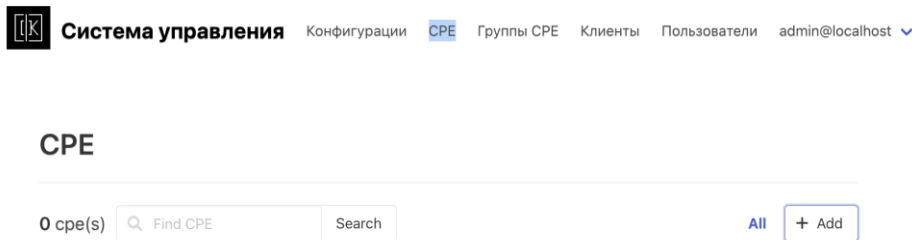
²Если установка не началась, то можно прописать команду `sudo ./install.sh -u`, а затем вновь прописать команду `sudo ./install.sh -i`.

³ Предварительно требуется проверить не установлены ли в системе следующие пакеты: `libnetconf2-2`, `libnetconf2-dev`, `libayang2`, `libayang2-dev`. Если они присутствуют в системе, удалите их командой `apt-remove`, так как они будут конфликтовать с пакетами, которые будут установлены

Часть #3: Настройка Firewall

ШАГ 1: Добавление FORT-V в систему менеджмента

Перейдите в раздел CPE и нажмите на кнопку + Add:



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

Edit CPE

Configuration status Not set

Serial Number

IP/FQDN

Group

Configuration

Organization

Edit the WireGuard client parameters

Нажмите на Save.

ШАГ 2: Добавление конфигурации и правил Firewall

Перейдите во вкладку **Configurations**.

В открывшейся вкладке нажмите на **Clone**, после чего перед вами откроется меню конфигурации:

Система управления | Конфигурации | CPE | Группы CPE | Клиенты | Пользователи | admin@localhost

Конфигурации

2 configuration(s) | Find configuration | Search | All | + Add

- Default configuration | Edit | Clone
- Identity configuration

Присвоив имя конфигурации, нажмите на **Save**:

Create configuration

Name

Parent

Save

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

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

Конфигурации

3 configuration(s)

All

+ Add



<name configuration>

Edit

Clone

Remove

Перейдите в раздел **Management**:

Edit configuration

Name

Parent

Edit configuration modules:

- Interfaces
- Management
- DHCP Server
- Port Mapping
- CPE networking
- WireGuard client
- IDS/IPS
- Syslog

Save

Download as a file

Здесь вам необходимо вписать имя вашего хоста - **coldStart**, а в строке **agent** прописать IP адрес сервера с Системы управления, находящейся в одной локальной сети с FORT-V.

Edit Management module for <name configuration>

Management
Snmp

engine-id: <user-engine-id>

security-name: <user-security-name>

password: <user-password>

Trap

name: coldStart

enabled:

agent: 10.150.0.253

Remove trap

Add trap

Authorization
PublicKey

Add public-key

Save

Нажмите на **Save**.

Для возвращения к разделу конфигурирования нажмите на **Back to modules list**.

Перейдите в раздел **IDS/IPS**:

Edit configuration modules:

- Interfaces
- Management
- DHCP Server
- Port Mapping
- CPE networking
- WireGuard client
- **IDS/IPS**
- Syslog

В открывшейся вкладке настраиваются правила Firewall:

Edit IDS/IPS module for <name configuration>

IDS/IPS

enabled:

Rule

Add rule

Выбрать файлы Файл не выбран

Upload rules file

Save

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

Способ 1:

Нажмите **Add rule**:

Появится редактируемое правило.

Нажмите на **Show**:

Перед вами появится редактор правил.

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

Нажмите на **Save**

Способ 2:

Нажмите **Add rule**.

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

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

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

Способ 3:

Нажмите на **Browse** 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 на **Save**.

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

Перейдите в раздел **Configurations**.

Выберите одну из ваших конфигураций и нажмите **Edit**.

Перейдите в раздел **DHCP Server**.

В этом разделе необходимо указать данные по вашему усмотрению.

Нажмите **Save**.

Шаг 4: Включение функции NAT-PMP (опционально)

Перейдите в раздел **Configurations**.

Выберите одну из ваших конфигураций и нажмите **Edit**.

Перейдите в раздел **Port Mapping**.

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

Нажмите **Save**.

Шаг 5: Настройка сетвых функций конфигурации (опционально)

Перейдите в раздел **Configurations**.

Выберите одну из ваших конфигураций и нажмите **Edit**.

Перейдите в раздел **CPE networking**.

В этом разделе необходимо настроить сетевые функции устройства⁴.

Нажмите **Save**.

⁴ **Предупреждение:** Совместная работа функции fastpath и правил, настроенных в разделе IDS/IPS, может привести к ложно-низкому результату измерения производительности TCP-соединения.

Шаг 6: Настройка WireGuard (опционально)

Перейдите в раздел **Configurations**.

Выберите одну из ваших конфигураций и нажмите **Edit**.

Перейдите в раздел **WireGuard client**.

В этом разделе необходимо настроить сетевые функции устройства.

Нажмите **Save**.

Часть #4: Присвоение конфигурации устройству

ШАГ 1: Присвоение FORT-V созданной конфигурации⁵

Выберите ваше устройство во вкладке CPE, нажмите **Edit**:

В строке **Configuration** выберите вашу конфигурацию:

Edit CPE

Configuration status Not set

Serial Number

IP/FQDN

Group

Configuration

Organization

· Edit the WireGuard client parameters

После выбора конфигурации нажмите **Save**.

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

⁵ Если вы управляете сразу несколькими устройствами и хотите добавить их в группу, перейдите к «Часть #5» данной инструкции

Часть #5: Создание группы и присоединение устройства к группе

ШАГ 1: Создание группы и присоединение устройства к группе⁶

Перейдите во вкладку CPE groups.

Нажмите + **Add** для добавления группы:

Система управления | Конфигурации | CPE | **Группы CPE** | Клиенты | Пользователи | admin@localhost

Группы CPE

0 CPE groups(s) Search All + Add

Дайте группе имя и присвойте одну из настраиваемых ранее конфигураций:

Edit CPE group

Name

Configuration

Нажмите **Save**.

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

Edit CPE

Configuration status Not set

Serial Number

IP/FQDN

Group

Configuration

Organization

- Edit the WireGuard client parameters

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

⁶ Таким образом вы сможете контролировать группу устройств, а также одновременно присвоить всем одинаковую конфигурацию.

Часть #6: Статистика и контроль устройства

ШАГ 1: Просмотр системных данных

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

В разделе CPE нажать на кнопку **Manage** одного из устройств, в открывшемся окне нажать **Get logs**.

В открывшемся разделе CPE Syslog вы можете наблюдать системные события.

ШАГ 2: Получение статистики интерфейсов

Для получения статистики интерфейсов FORT-V достаточно выполнить несколько действий:

В разделе CPE нажать на кнопку **Manage** одного из устройств, в открывшемся окне нажать кнопку **Get statistics**.

В открывшемся разделе CPE interface statistic вы можете наблюдать всю статистику интерфейсов устройства.