



Программный комплекс INFOWATCH ARMA СТЕНА

Межсетевой экран нового поколения
для промышленных и корпоративных сетей



Руководство администратора

версия 1 ред. от 30.05.2024

Листов 22

СОДЕРЖАНИЕ

1	Требования к среде функционирования	6
1.1	Требования к аппаратной платформе.....	6
1.2	Требования к виртуальной платформе	6
1.2.1	Требования к настройке среды виртуализации	7
2	Установка и первоначальная настройка системы	9
2.1	Установка	9
2.1.1	Загрузка в режиме «live»	9
2.1.2	Установка образа	10
2.2	Первоначальная настройка.....	11
3	Описание локального консольного интерфейса	13
3.1	Управление питанием.....	13
3.1.1	Перезагрузка	13
3.1.2	Выключение.....	13
3.2	Конфигурации.....	13
3.2.1	Режим конфигурирования.....	13
3.2.1.1	Основные команды.....	14
3.2.1.2	Дополнительные команды.....	16
3.3	Расширенные настройки	17
3.3.1	SSH	17
3.3.2	Интерфейсы.....	18
4	Варианты развёртывания	20
4.1	Маршрутизация	20
4.2	Отказоустойчивый кластер.....	20
5	Контроль управления доступом.....	22
5.1	Аутентификация.....	22
5.1.1	Локальная база данных пользователей.....	22
5.2	Пользовательские учетные записи	22
5.2.1	Добавление пользовательских учетных записей.....	22

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. [Таблица «Термины и сокращения»](#)).

Таблица «Термины и сокращения»

Термины и сокращения	Значение
ИБ	Информационная безопасность
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
ЦП	Центральный процессор
ARMA Стена	InfoWatch ARMA Стена
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
DVI	Digital Visual Interface – цифровой видеоинтерфейс
FTP	File Transfer Protocol – протокол передачи файлов по сети
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
LAN	Local Area Network – локальная вычислительная сеть
SSD	Solid-State Drive – твердотельный накопитель
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить

Термины и сокращения	Значение
	удалённое управление операционной системой и туннелирование TCP-соединений
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
USB	Universal Serial Bus – универсальная последовательная шина
VGA	Video Graphics Array – компонентный видеоинтерфейс
VRRP	Virtual Router Redundancy Protocol, протокол резервирования виртуального маршрутизатора – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
WAN	Wide Area Network – глобальная вычислительная сеть

В настоящем руководстве использованы ссылки на документы, представленные в таблице (см. [Таблица «Смежные документы»](#)).

Таблица «Смежные документы»

Сокращённое наименование	Полное наименование
Руководство пользователя ARMA Стена	Руководство пользователя по эксплуатации InfoWatch ARMA Стена

АННОТАЦИЯ

Настоящее руководство администратора предназначено для пользователей, производящих установку, запуск и первоначальную настройку конфигурации работы **InfoWatch ARMA Стена v.4.2**.

К первоначальным настройкам относятся:

- настройка IP-адресов;
- активация лицензии;
- создание пользовательских учётных записей.

Роль пользователя и администратора может выполнять один сотрудник предприятия.

1 ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

Инсталляция **ARMA Стена** производится на аппаратную или виртуальную платформы.

Установка на аппаратную платформу производится с использованием USB-накопителя с записанным образом **ARMA Стена** в формате «img».

Установка на виртуальную платформу производится с помощью образа оптического диска в формате «iso».

Примечание:

Во избежание некорректной работы **ARMA Стена** не рекомендуется допускать незапланированные отключения питания оборудования. В случае отключения питания во время активации лицензии, изменения конфигурации, создания/удаления правил МЭ и т.п. внесённые изменения сохранены не будут.

1.1 Требования к аппаратной платформе

Технические требования, предъявляемые к аппаратной платформе:

1. Микропроцессорная архитектура x64.
2. Для корректного функционирования **ARMA Стена** с общей пропускной способностью 1 Гбит/с при работе функций МЭ и COB минимальные требования к оборудованию:
 - **Процессор** – 2,0 ГГц, двухъядерный, x64;
 - **ОЗУ** – 4 ГБ;
 - **Интерфейсы** – Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры;
 - **Жёсткий диск** – 120 ГБ, SSD;
 - **Сетевой интерфейс** – Не менее 2 x Ethernet 1 Гбит/сек.

1.2 Требования к виртуальной платформе

Технические требования, предъявляемые к виртуальной платформе:

1. Виртуализация **ARMA Стена** поддерживается для следующих гипервизоров:
 - HyperV Generation 1;
 - VirtualBox версии 6.0.4 и выше;
 - VMware ESXi версии 7.0 и выше;
 - QEMU/KVM.

2. Для корректного функционирования **ARMA Стена** с общей пропускной способностью 1 Гбит/с при работе функций МЭ и СОВ минимальные требования к виртуальной среде:

- Количество ядер процессора – 8;
- Объём оперативной памяти – 4 ГБ;
- Размер виртуального диска – 25 ГБ;
- Количество сетевых интерфейсов – 2.

В случае необходимости обеспечения более высокой производительности и хранения большего количества записей журналов рекомендуется соблюдать следующие требования:

- Количество ядер процессора – 8;
- Объём оперативной памяти – 16 ГБ;
- Размер виртуального диска – 120 ГБ;
- Количество сетевых интерфейсов – 2.

Примечание:

Все необходимые сетевые интерфейсы для виртуальной машины должны быть добавлены до начала процесса установки **ARMA Стена**.

К сетевым адаптерам **ARMA Стена** предъявляются следующие требования:

- модели используемых сетевых адаптеров должны быть идентичными;
- не используемые сетевые адаптеры должны быть отключены на аппаратном уровне.

1.2.1 Требования к настройке среды виртуализации

Для уточнения возможности включения технологии виртуализации для физической платформы необходимо обратиться к описанию по использованию данной платформы.

Проверка работоспособности технологии виртуализации осуществляется следующим образом:

1. Для ОС семейства Linux необходимо выполнить команду «`cat /proc/cpuinfo | grep vmx svm`» и убедиться, что вывод команды пуст, в противном случае имеются ошибки в настройках или в системе отсутствуют необходимые расширения.

2. Для ОС семейства Windows – убедиться в поддержке виртуализации, руководствуясь документацией к данной ОС, либо успешной попыткой запуска произвольной VM.

2 УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ

2.1 Установка

Для записи установочного образа **ARMA Стена** на USB-накопитель необходимо использовать ПО для записи образа на внешние накопители, например, ПО «Rufus» (<https://rufus-usb.ru.uptodown.com/windows>). Запись образа производится в соответствии с описанием по использованию данного ПО.

Для установки **ARMA Стена** необходимо выполнить следующие шаги:

1. Загрузить **ARMA Стена** в режиме «live».
2. Выполнить установку образа.

2.1.1 Загрузка в режиме «live»

Для загрузки **ARMA Стена** в режиме «live» необходимо выполнить следующие действия:

1. Выбрать в течение 10 секунд с помощью **клавиш клавиатуры со стрелками вверх и вниз**, в открывшемся меню способ загрузки:
 - «**Live (amd64-ngfwos)**» – стандартная загрузка, выполняется по умолчанию;
 - «**Live (amd64-ngfwos failsafe)**» – отказоустойчивая загрузка.
2. Нажать **клавишу «ENTER»** для подтверждения выбранного способа и начала загрузки.

Примечание:

Загрузка **ARMA Стена** в режиме «live» по умолчанию автоматически выполняется в следующих ситуациях:

- в случае бездействия пользователя в меню загрузки в течение 10 секунд;
- в случае неподтверждённого выбора способа загрузки и последующего бездействия пользователя в течение 5 минут.

3. После появления приглашения на вход в консольном интерфейсе, указать следующие учётные данные и нажать **клавишу «ENTER»** после каждого ввода:
 - «**ngfwos login:**» – «admin»;
 - «**Password:**» – «admin».

Примечание:

Пароль пользователя не отображается при наборе.

После успешной аутентификации будет отображён интерфейс командной строки (см. [Рисунок – Интерфейс командной строки](#)).

```
ngfwos login: admin
Password:
Welcome to NGFWOS!
admin@ngfwos:~$
```

Рисунок – Интерфейс командной строки

2.1.2 Установка образа

В качестве примера приведено описание установки образа **ARMA Стена** на один жёсткий диск, без деления на несколько разделов. Вводимые команды могут отличаться для каждой конкретной ситуации.

Для запуска процесса установки образа **ARMA Стена** необходимо выполнить следующие действия:

1. Ввести команду «**install image**»:

```
admin@ngfwos:~$ install image
```

и нажать **клавишу «ENTER»**.

В процессе установки системой будут выводиться запросы, в некоторых случаях содержащие предлагаемый ответ по умолчанию, заключённый в квадратные скобки.

При необходимости отмены выполнения команды, следует нажать комбинацию **клавиш «CTRL» + «C»**.

2. Нажать **клавишу «ENTER»** на запрос:

```
Would you like to continue? (Yes/No) [Yes]:
```

3. Ввести «**а**» и нажать **клавишу «ENTER»** на запрос:

```
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted? If
you have already setup your partitions, you may skip this step
```

```
Partition (Auto/Parted/Skip) [Auto]:
```

4. Нажать **клавишу «ENTER»** на запрос:

```
Install the image on? [sda]:
```

5. Ввести «**у**» и нажать **клавишу «ENTER»** на запрос:

```
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]:
```

Примечание:

Все данные на диске будут безвозвратно удалены.

6. Ввести размер выделяемого раздела в мегабайтах, в пределах предлагаемого диапазона и нажать **клавишу «ENTER»** на запрос:

```
How big of a root partition should I create? (2000MB – 17179MB) [17179]MB:
```

7. Ввести имя образа и нажать **клавишу «ENTER»** на запрос:

```
What would you like to name this image? [4.2–202404051429]:
```

8. Нажать **клавишу «ENTER»** на запрос:

```
Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:
```

9. Ввести новый пароль для УЗ «admin» и нажать **клавишу «ENTER»** на запрос:

```
Enter password for user 'admin':
```

10. Повторить ввод пароля для УЗ «admin» и нажать **клавишу «ENTER»** на запрос:

```
Retype password for user 'admin':
```

11. Нажать **клавишу «ENTER»** на запрос:

```
Which drive should GRUB modify the boot partition on? [sda]:
```

По окончании процесса установки следует выполнить перезагрузку **ARMA Стена** (см. [Перезагрузка](#)).

2.2 Первоначальная настройка

Загрузка **ARMA Стена** завершается приглашением к авторизации:

```
Welcome to NGFWOS – ngfwos tty1

ngfwos login:
```

Для входа в локальный консольный интерфейс необходимо указать учётные данные и нажать **клавишу «ENTER»** после каждого ввода:

- **«ngfwos login:»** – «admin»;
- **«Password:»** – пароль, заданный на этапе установки образа **ARMA Стена**.

Настройка системы производится в режиме конфигурирования. Подробное описание работы в режиме конфигурирования представлено в разделе [Режим конфигурирования](#) настоящего руководства.

Для безопасного конфигурирования **ARMA Стена** может потребоваться настройка передачи данных по протоколу SSH. Подробное описание включения SSH представлено в разделе [SSH](#) настоящего руководства.

На первоначальном этапе конфигурирования **ARMA Стена** необходимо настроить сетевые интерфейсы. Подробное описание конфигурирования сетевых интерфейсов представлено в разделе [Интерфейсы](#) настоящего руководства.

3 ОПИСАНИЕ ЛОКАЛЬНОГО КОНСОЛЬНОГО ИНТЕРФЕЙСА

В консольном интерфейсе управление происходит только с использованием клавиатуры. Выбор осуществляется с помощью **клавиш со стрелками вверх и вниз**, а подтверждение выбора – с помощью **клавиши «ENTER»**.

3.1 Управление питанием

3.1.1 Перезагрузка

Для перезагрузки **ARMA Стена** необходимо ввести команду **«reboot»**, а затем ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Are you sure you want to reboot this system? [y/N]»**.

```
admin@ngfwos:~$ reboot
Are you sure you want to reboot this system? [y/N] y
```

3.1.2 Выключение

Для выключения **ARMA Стена** необходимо ввести команду **«poweroff»**, а затем ввести **«y»** и нажать **клавишу «ENTER»** на запрос **«Are you sure you want to poweroff this system? [y/N]»**.

```
admin@ngfwos:~$ poweroff
Are you sure you want to poweroff this system? [y/N] y
```

3.2 Конфигурации

Различаются три типа конфигурации **ARMA Стена**:

1. **Активная** – конфигурация, содержащая зафиксированные изменения, используемые ОС до перезагрузки.
2. **Рабочая** – конфигурация, содержащая незафиксированные изменения, внесённые в текущий момент в режиме конфигурирования.
3. **Сохранённая** – конфигурация, сохранённая в файл, по умолчанию **«config.boot»**. Используется ОС при загрузке.

Для просмотра параметров активной конфигурации необходимо ввести команду **«show configuration»**.

Навигация, для просмотра всей выведенной информации, осуществляется с помощью **клавиш клавиатуры со стрелками вверх и вниз**. Для завершения просмотра параметров конфигурации следует нажать **клавишу «q»**.

3.2.1 Режим конфигурирования

Режим конфигурирования предназначен для внесения и фиксации изменений конфигурации, а также сохранения конфигурационных файлов.

Для входа в режим конфигурирования необходимо ввести команду «**configure**».

```
admin@ngfwos:~$ configure
[edit]
admin@ngfwos#
```

Подтверждением входа в режим конфигурирования является отображение символа «**#**» в командной строке.

Примечание:

Наличие символов «**admin@ngfwos:~\$**» в примерах кода указывает на то, что команда вводится не в режиме конфигурирования.

3.2.1.1 Основные команды

1. «**set**» – добавить значение параметра конфигурации, например, назначить IP-адрес для интерфейса «eth1».

```
[edit]
admin@ngfwos# set interfaces ethernet eth1 address 192.168.22.1/24
```

2. «**delete**» – удалить значение параметра конфигурации, например, удалить IP-адрес для интерфейса «eth1».

```
[edit]
admin@ngfwos# delete interfaces ethernet eth1 address 192.168.22.1/24
```

3. «**edit**» – перейти к другому уровню редактирования конфигурации, например, к редактированию интерфейса «eth1».

```
[edit]
admin@ngfwos# edit interfaces ethernet eth1
[edit interfaces ethernet eth1]
admin@ngfwos# set address 192.168.22.1/24
admin@ngfwos# set description "LAN"
```

4. «**exit**» – выйти из режима конфигурирования. Также команда может использоваться для перехода из какого-либо уровня редактирования конфигурации.

```
[edit interfaces ethernet eth1]
admin@ngfwos# exit
[edit]
admin@ngfwos# exit
exit
admin@ngfwos:~$
```

Примечание:

Команда **«exit»** не применится для выхода из режима конфигурирования в случае наличия в конфигурации незафиксированных изменений.

```
[edit]
admin@ngfwos# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
```

5. **«exit discard»** – выйти из режима конфигурирования без сохранения изменений.

6. **«commit»** – зафиксировать изменения, внесённые в конфигурацию.

После фиксации изменений «рабочая» конфигурация становится «активной».

Примечание:

При выходе из режима конфигурирования без предварительного выполнения команды **«commit»** настройки не будут применены.

7. **«commit-confirm»** – зафиксировать изменения конфигурации и по истечении 10 минут автоматически перезагрузить систему с использованием предыдущей сохранённой конфигурации.

Для подтверждения выполнения команды следует ввести **«y»** на запрос:

```
commit confirm will be automatically reboot in 10 minutes unless confirmed
Proceed? [confirm]
```

Примечание:

Возможно дополнить команду указанием исчисляемого в минутах промежутка времени до перезагрузки системы, например **«commit-confirm 25»**.

8. **«save»** – сохранить конфигурационный файл «config.boot». Сохранённая конфигурация будет использоваться ОС при загрузке.

```
[edit]
admin@ngfwos# save
Saving configuration to '/config/config.boot'...
Done
```

3.2.1.2 Дополнительные команды

1. **«show system commit»** – вывести нумерованный список активных конфигураций. Перед вводом команды необходимо предварительно выйти из режима конфигурирования.

```
admin@ngfwos:~$ show system commit
```

Последняя добавленная активная конфигурация будет иметь порядковый номер «0».

2. **«run»** – выполнить команду в режиме конфигурирования без предварительного выхода из него.

```
[edit]
admin@ngfwos# run show system commit
```

3. **«compare»** – показать изменения между рабочей и активной конфигурациями.

```
[edit]
admin@ngfwos# compare
```

«compare 4» – показать изменения между рабочей и выбранной активной конфигурациями, где «4» – порядковый номер активной конфигурации.

«compare 1 4» – показать изменения между выбранными активными конфигурациями, где «1» и «4» – порядковые номера сравниваемых активных конфигураций.

4. **«rollback 5»** – применить и зафиксировать изменения, приводящие рабочую конфигурацию к состоянию аналогичному выбранной активной, а затем сохранить конфигурацию.

Требуется перезагрузка ОС, для выполнения которой следует ввести **«y»** на запрос **«Proceed with reboot? [confirm]»**.

```
[edit]
admin@ngfwos# rollback 5
Proceed with reboot? [confirm]y
```

где «5» – порядковый номер выбранной активной конфигурации.

5. **«set system config-management commit-revision 200»** – установить максимально возможное количество хранящихся активных конфигураций, где «200» – устанавливаемое значение, которое возможно указать в диапазоне от «0» до «65535». По умолчанию используется значение «100».

3.3 Расширенные настройки

3.3.1 SSH

Сервер SSH обеспечивает безопасный удалённый доступ к управлению функциями локального консольного интерфейса **ARMA Стена**.

Для включения SSH необходимо ввести команду **«set service ssh port 22»**:

```
[edit]
admin@ngfwos# set service ssh port 22
```

где «22» – назначаемый порт.

Для указания IP-адреса, прослушиваемого сервисом «SSH», необходимо ввести команду **«set service ssh listen-address 192.168.2.11/24»**:

```
[edit]
admin@ngfwos# set service ssh listen-address 192.168.2.11/24
```

где «192.168.2.11/24» – IP-адрес в формате CIDR, приведён в качестве примера.

Для указания алгоритма шифрования необходимо ввести команду **«set service ssh ciphers aes128-ctr»**:

```
[edit]
admin@ngfwos# set service ssh ciphers aes128-ctr
```

где «aes128-ctr» – алгоритм шифрования, приведён в качестве примера.

Поддерживаются следующие алгоритмы шифрования:

- **3des-cbc;**
- **aes128-cbc;**
- **aes192-cbc;**
- **aes256-cbc;**
- **aes128-ctr;**
- **aes192-ctr;**
- **aes256-ctr;**
- **arcfour128;**

- **arcfour256;**
- **arcfour;**
- **blowfish-cbc;**
- **cast128-cbc.**

3.3.2 Интерфейсы

Просмотр конфигурации интерфейсов возможен с помощью команды «**show interfaces**». В случае выполнения вышеуказанной команды в режиме конфигурирования дополнительно будет отображена информация о MAC-адресах.

Интерфейсам по умолчанию назначается имя «ethN», где «N» – идентификатор, присвоенный интерфейсу системой.

Используемые далее имена интерфейсов и IP-адреса приведены в качестве примера и могут отличаться для каждой конкретной ситуации.

Для назначения IP-адреса на интерфейсе необходимо ввести команду «**set interfaces ethernet eth1 address 192.168.22.1/24**»:

```
[edit]
admin@ngfwos# set interfaces ethernet eth1 address 192.168.22.1/24
```

где «eth1» – имя интерфейса; «192.168.22.1/24» – IP-адрес в формате CIDR.

При необходимости получения IP-адреса на интерфейсе «eth0» по протоколу «DHCP» необходимо ввести команду «**set interfaces ethernet eth0 address dhcp**»:

```
[edit]
admin@ngfwos# set interfaces ethernet eth0 address dhcp
```

Возможно добавление описания интерфейса с помощью команды «**set interfaces ethernet eth1 description LAN**»:

```
[edit]
admin@ngfwos# set interfaces ethernet eth1 description LAN
```

где «LAN» – описание для интерфейса.

Пример вывода информации о настроенных интерфейсах:

```
[edit]
admin@ngfwos# show interfaces
  ethernet eth0 {
    address dhcp
    description WAN
    hw-id 00:50:56:bd:ca:9e
  }
  ethernet eth1 {
    address 192.168.22.1/24
    description LAN
    hw-id 00:50:56:bd:f5:cd
  }
  loopback lo {
  }
```

4 ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

Предусмотрены следующие варианты развертывания **ARMA Стена** в ЛВС:

- режим маршрутизации;
- режим отказоустойчивого кластера.

Каждый вариант отличается настройкой сетевых интерфейсов.

4.1 Маршрутизация

В режиме маршрутизации **ARMA Стена** работает как МЭ с функцией обнаружения и предотвращения вторжений, обеспечивая защиту передачи информации на уровне L3 с возможностью маршрутизации. Режим маршрутизации может использоваться при объединении сетей, имеющих разное адресное пространство.

Общая схема подключения **ARMA Стена** в режиме маршрутизации представлена на рисунке (см. [Рисунок – Режим маршрутизации](#)).

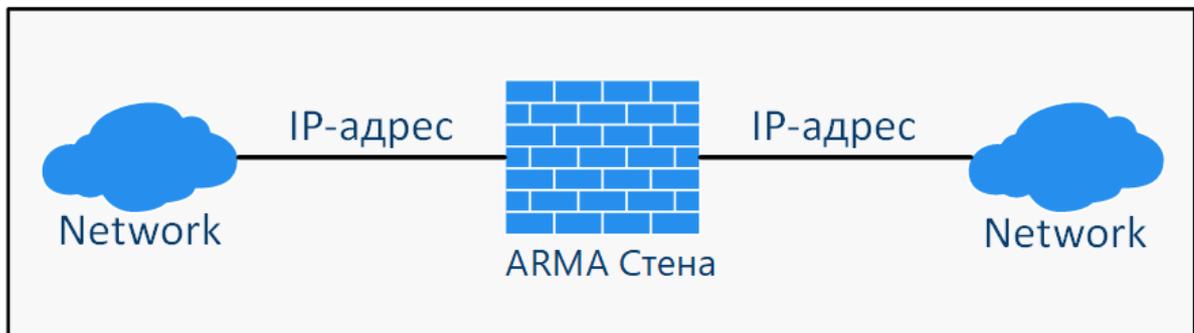


Рисунок – Режим маршрутизации

4.2 Отказоустойчивый кластер

В режиме отказоустойчивого кластера несколько **ARMA Стена** объединяются в единый кластер в режиме «active-backup».

В случае объединения нескольких **ARMA Стена** в каждый момент времени только одно устройство **ARMA Стена** в кластере обрабатывает весь трафик, такое устройство считается ведущим. При выходе из строя ведущего устройства его подменяет одно из резервных устройств, которое само становится ведущим и начинает обрабатывать трафик. В случае если изначально ведущее устройство вновь переходит в рабочее состояние, то текущее ведущее устройство возвращается в статус подчинённого резервного устройства.

Общая схема подключения **ARMA Стена** в режиме отказоустойчивого кластера представлена на рисунке (см. [Рисунок – Режим отказоустойчивого кластера](#)).

Подробная информация о настройке отказоустойчивого кластера описана в разделе «**Настройка отказоустойчивого кластера**» Руководства пользователя **ARMA Стена**.

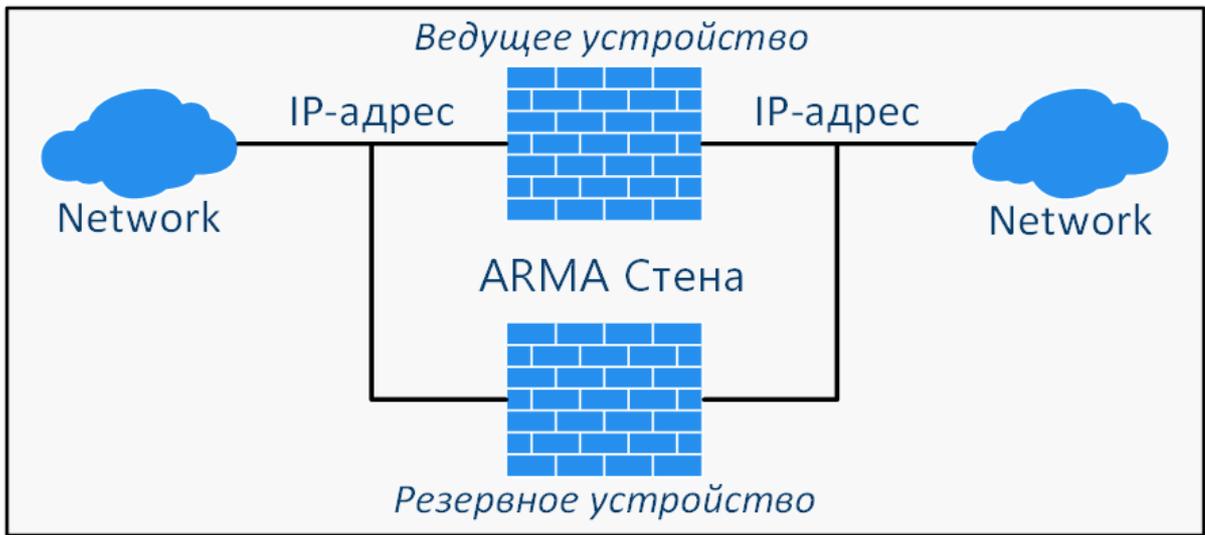


Рисунок – Режим отказоустойчивого кластера

5 КОНТРОЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

5.1 Аутентификация

Аутентификация – это процесс проверки подлинности введённых пользователем имени и пароля. В **ARMA Стена** возможна аутентификация с использованием локальной или внешней БД пользователей. В качестве внешней БД служат различные внешние серверы авторизации.

5.1.1 Локальная база данных пользователей

Для хранения УЗ пользователей по умолчанию используется локальная БД, например, запись суперпользователя по умолчанию – «admin».

5.2 Пользовательские учетные записи

5.2.1 Добавление пользовательских учетных записей

Для создания пользовательской УЗ необходимо в режиме конфигурирования ввести следующие команды с указанием учётных данных:

```
set system login user User1 full-name "Fedor Volov"
```

где «User1» – логин, «Fedor Volov» – имя пользователя.

```
set system login user User1 authentication plaintext-password PasswordUser1
```

где «PasswordUser1» – пароль.

Учётные данные приведены в качестве примера.