**Table of Contents**


Table of Contents 1
Первоначальная настройка 2
- Описание 3
- Требования к сетевому окружению 4
- Развертывание виртуального образа 5
- Подключение к UserGate NGFW 6
- Автоматизация развертывания UserGate NGFW с помощью Cloud-init 8

Первоначальная настройка

## Описание

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Межсетевой экран UserGate поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины межсетевой экран UserGate поставляется с десятью Ethernet-интерфейсами. В случае поставки в виде ПАК — может содержать от 2 до 64 Ethernet-портов.

# Требования к сетевому окружению

Documentation:
Product: NGFW
Version: 7.0.1

Для корректной работы межсетевого экрана UserGate должен иметь доступ до следующих серверов, расположенных в сети интернет:

- Сервер регистрации — reg2.usergate.com, порты TCP 80, 443.
- Сервер обновления списков и ПО UserGate — updates.usergate.com, порты TCP 80, 443.

При создании кластера конфигурации необходимо обеспечить прохождение следующих протоколов между узлами:

- Обеспечение репликации настроек — порты TCP 4369, TCP 9000-9100.
- Сервис веб-консоли — TCP 8001.

Подробнее о требованиях сетевой доступности читайте в Приложение 4. Требования к сетевому окружению.

# Развертывание виртуального образа

Documentation:
Product: NGFW
Version: 7.0.1, 7.1.0

UserGate NGFW Virtual Appliance позволяет быстро развернуть виртуальную машину, с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox, и Qcow2 для систем виртуализации QEMU-KVM. Для Microsoft Hyper-v поставляется образ диска виртуальной машины.

**Примечание**Для корректной работы виртуальной машины рекомендуется использовать минимум 12 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом, выполните следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Скачайте образ и распакуйте | Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru. |
| **Шаг 2.** Импортируйте образ в свою систему виртуализации | Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины. |
| **Шаг 3.** Настройте параметры виртуальной машины | Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb и добавьте по 1Gb на каждые 100 пользователей. |
| **Шаг 4.**<br>**Важно!** Самостоятельно добавьте дополнительный диск, нужного размера | Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 200Gb или более. Рекомендованный размер — 300Gb или более.<br><br>Для систем виртуализации QEMU-KVM: размер системной области, по умолчанию, составляет 8Гб. Система, при первом запуске, сама определит наличие дополнительного диска и расширит свои системные разделы.<br><br>Команда для добавления диска размером 100 ГБ для систем QEMU-KVM:<br><br>qemu-img create -f qcow2 -o preallocation=metadata,refcount_bits=16,lazy_refcounts=on,cluster_size=4K имя-вашего-диска.qcow2 100G |
| **Шаг 5.** Настройте виртуальные сети | UserGate поставляется с четырьмя интерфейсами, назначенными в зоны:<br>• **Management** — первый интерфейс виртуальной машины.<br>• **Trusted** — второй интерфейс виртуальной машины.<br>• **Untrusted** — третий интерфейс виртуальной машины.<br>• **DMZ** — четвертый интерфейс виртуальной машины. |
| **Шаг 6.** Выполните сброс к заводским настройкам | Запустите виртуальную машину UserGate.<br><br>Во время загрузки выберите **Support Menu** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте. |

# Подключение к UserGate NGFW

Documentation:
Product: NGFW
Version: 7.0.1

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Подключиться к интерфейсу управления. | **При наличии DHCP-сервера**<br><br>Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate. После загрузки NGFW укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта.<br><br>**Статический IP-адрес**<br><br>Включить NGFW. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Произвести первоначальную инициализацию в интерфейсе командной строки или подключиться к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом: https://NGFW_IP_address:8001.<br><br>Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). |
| **Шаг 2.** Выбрать язык. | Выбрать язык, на котором будет продолжена первоначальная настройка. |
| **Шаг 3.** Задать пароль. | Задать логин и пароль для входа в веб-интерфейс управления. |
| **Шаг 4.** Настроить зоны, IP-адреса интерфейсов, подключить UserGate в сеть предприятия. | В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами:<br>• Зона Management (сеть управления), интерфейс port0.<br>• Зона Trusted (LAN).<br>• Зона Untrusted (Internet).<br>• Зона DMZ.<br>• Зона Cluster.<br>• Зона VPN for remote access.<br>• Зона VPN for Site-to-Site.<br>• Зона Tunnel inspection zone. |
| **Шаг 5.** Настроить шлюз в Интернет. | В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет, зона **Untrusted**. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов. |
| **Шаг 6.** Указать системные DNS-серверы. | В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации.<br><br>Подробно об управлении DNS читайте в главе Настройка DNS. |
| **Шаг 7.** Настроить время сервера. | В разделе **UserGate → Настройки → Настройка времени сервера** настроить синхронизацию времени с серверами NTP. |
| **Шаг 8.** Зарегистрировать NGFW. | Для регистрации продукта ввести ПИН-код и заполнить форму. Для активации системы необходим доступ NGFW в Интернет.<br><br>Более подробно о лицензировании продукта читайте в главе Лицензирование. |

| Наименование | Описание |
|---|---|
| **Шаг 9.** Создать правила NAT. | В разделе **NAT и Маршрутизация** создать необходимые правила NAT. Для доступа в интернет пользователей сети **Trusted** правило NAT уже создано: «**NAT from Trusted to Untrusted**».<br><br>Подробно о правилах NAT читайте в главе NAT и маршрутизация. |
| **Шаг 10.** Создать правила межсетевого экрана. | В разделе **Межсетевой экран** создать необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети **Trusted** правило межсетевого экрана уже создано — « **Allow trusted to untrusted**», необходимо только включить его.<br><br>Подробно о правилах межсетевого экрана читайте в главе Межсетевой экран. |
| **Шаг 11.** Создать дополнительных администраторов (опционально). | В разделе **Администраторы UserGate** создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями). |
| **Шаг 12.** Настроить авторизацию пользователей (опционально). | В разделе **Пользователи и устройства** создать необходимые методы авторизации пользователей. Самый простой вариант - это создать локальных пользователей NGFW с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя **Any** во всех правилах).<br><br>Для других вариантов авторизации пользователей смотрите главу Пользователи и устройства. |
| **Шаг 13.** Создать правила контентной фильтрации (опционально). | В разделе **Фильтрация контента** создать правила фильтрации HTTP(S).<br><br>Более подробно о фильтрации контента читайте в главе Фильтрация контента. |
| **Шаг 14.** Создать правила веб-безопасности (опционально). | В разделе **Веб-безопасность** создать дополнительные правила защиты веб.<br><br>Более подробно о веб-безопасности читайте в главе Веб-безопасность. |
| **Шаг 15.** Создать правила инспектирования SSL (опционально). | В разделе **Инспектирование SSL** создать правила для перехвата и расшифровывания HTTPS-трафика.<br><br>Более подробно о дешифровании HTTPS читайте в главе Инспектирование SSL. |

После выполнения вышеперечисленных действий NGFW готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

# Автоматизация развертывания UserGate NGFW с помощью Cloud-init

Documentation:
Product: NGFW
Version: 7.0.1, 7.1.0

Cloud-init — индустриальный стандарт для кросс-платформенной инициализации виртуальных машин (инстансов) в облаках провайдеров. Межсетевой экран UserGate поддерживает возможность первоначальной настройки с помощью механизма Cloud-init. Настройка межсетевого экрана осуществляется с помощью двух модулей:

- Настройка с помощью команд CLI (файл с заголовком #utm-config). Возможно использовать все CLI-команды для полной настройки инстанса.
- Активация лицензии (файл с заголовком #utm-license).

Другие модули Cloud-init не поддерживаются.

Пример файла конфигурации с CLI командами (user-data):

```
#utm-config
#set password for initial Administrator (Admin). Obligatory comand.
password 123
#Set addresses and settings for network interfaces:
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
set network interface adapter port2 \
ip-addresses [ 172.16.8.9/24 ] \
enabled on \
zone "Untrusted"
set network interface adapter port3 \
ip-addresses [ 172.16.7.9/24 ] \
enabled on \
zone "DMZ"
#Create network gateway to Internet:
create network gateway \
ip 172.16.8.2 \
default on \
interface port2 \
virtual-router default \
enabled on
#Create firewall rule to allow traffic from Trusted to untrusted security zones:
create network-policy firewall \
position 1 upl-rule ALLOW \
src.zone = Trusted \
dst.zone = Untrusted \
enabled(true) \
name("Cloud-Init: Allow from Trusted to Untrusted")
```

В данный файл можно добавлять все доступные для администратора команды CLI. Подробно о CLI-командах смотрите в разделе Интерфейс командной строки (CLI).

# — обозначает начало комментария, обратный слэш — переход на следующую строку.

Если необходимо активировать создаваемый инстанс, то это можно сделать через указание параметров для лицензирования в отдельном файле. Следует учитывать, что активация возможна только при наличии у инстанса доступа в сеть интернет. Пример содержимого файла для активации лицензии (vendor-data):

```
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email:  email@company.com
user_name: Alexander
last_name: Petrov
company: UserGate
country: Russia
region: Novosibirsk
```

Оба файла можно объединить в один файл, используя multipart формат:

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0
--//
Content-Type: text/utm-config; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config.txt"
#utm-config
password 123
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
```

```
enabled on \
zone "Trusted"
set network interface adapter port2 \
ip-addresses [ 172.16.8.9/24 ] \
enabled on \
zone "Untrusted"
set network interface adapter port3 \
ip-addresses [ 172.16.7.9/24 ] \
enabled on \
zone "DMZ"
create network gateway \
ip 172.16.8.2 \
default on \
interface port2 \
virtual-router default \
enabled on
create network-policy firewall \
position 1 upl-rule ALLOW \
src.zone = Trusted \
dst.zone = Untrusted \
enabled(true) \
name("Cloud-Init: Allow from Trusted to Untrusted")
--//
Content-Type: text/utm-license; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license.txt"
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email:  email@company.com
user_name: Alexander
last_name: Petrov
company: UserGate
country: Russia
region: Novosibirsk
--//
```

Настройки могут быть переданы в NGFW:

1. Методами, реализуемыми облачными провайдер, например, у провайдера Digital Ocean при создании виртуальной машины (droplet) настройки необходимо вставить в опциональное поле **User data** (**Select additional options → User data**). Аналогичным образом настройки можно передать и у других поставщиков облачных услуг.

2. Через подключаемый iso-диск. Диск должен содержать файлы meta-data, user-data, vendor-data следующего содержимого:

meta-data: instance-id: vm1  user-data — с CLI-командами настройки инстанса:

```
#utm-config
#set password for initial Administrator (Admin). Obligatory comand.
password 123
#Set addresses and settings for network interfaces:
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
...
```

vendor-data — с информацией о лицензировании (опционально):

```
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email: email@company.com
...
```

Для создания iso-диска в Linux можно использовать следующую утилиту:

```
mkisofs -joliet -rock -volid "cidata" -output nocloud.iso meta-data user-data vendor-data
```

Полученный iso-диск необходимо подключить к виртуальной машине UserGate. После успешной первой загрузки виртуальная машина получит все настройки, указанные для нее в созданных файлах.