

Table of Contents

Table of Contents	1
Первоначальная настройка	2
Общие сведения	3
Развертывание виртуального образа	4
Автоматизация развертывания UserGate DCFW с помощью Cloud-init	6
Требования к сетевому окружению	8
Подключение к UserGate DCFW	9

Первоначальная настройка

Общие сведения

Product: DCFW

Version: 8.x

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

Развертывание виртуального образа

Product: DCFW

Version: 8.x

UserGate DCFW Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают платформы 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 32 ГБ оперативной памяти и 4-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Примечание Для корректной работы внутренней базы данных требуется поддержка набора микрокоманд SSE4.2 архитектуры x86 процессорами виртуальной среды. Любой процессор на базе архитектуры x86, выпущенный после 2008 года, должен поддерживать SSE4.2.

Работа с виртуальным образом

Для начала работы с виртуальным образом выполните следующие шаги:

1. Скачайте последнюю версию виртуального образа [с официального сайта UserGate](#).
2. Импортируйте образ в свою систему виртуализации. Инструкцию по импорту образа вы можете найти на сайтах систем виртуализации, например VirtualBox или 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.
3. Настройте параметры виртуальной машины. Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8 ГБ и добавьте по 1 ГБ на каждые 100 пользователей.
4. Добавьте дополнительный диск нужного размера.

Размер диска по умолчанию составляет 100 ГБ, чего обычно недостаточно для хранения всех журналов и параметров. Используя свойства виртуальной машины, увеличьте размер диска. Рекомендованный размер — 1 ТБ.

Для систем виртуализации QEMU-KVM размер системной области по умолчанию составляет 8 ГБ. При первом запуске система сама определит наличие дополнительного диска и расширит свои системные разделы.

Пример команды для добавления диска размером 100 ГБ для систем QEMU-KVM:

```
qemu-img create -f qcow2 -o preallocation=metadata,refcount_bits=16,lazy_refcounts=on,cluster_size=4K <имя-вашего-диска>.qcow2 100G
```

5. Запустите виртуальную машину UserGate. Во время загрузки выполняется **Factory reset**. Система UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в четвертом пункте.

UserGate DCFW поставляется с четырьмя интерфейсами, на каждом из которых назначена своя зона:

- **Management** — на первом интерфейсе виртуальной машины;
- **Trusted** — на втором интерфейсе виртуальной машины;
- **Untrusted** — на третьем интерфейсе виртуальной машины;
- **DMZ** — на четвертом интерфейсе виртуальной машины.

Примечание Если сетевые интерфейсы на виртуальной машине с DCFW были удалены средствами гипервизора, они будут помечены как удаленные в веб-интерфейсе с помощью перечеркнутого значка.

Примечание Если виртуальная машина UserGate клонируется через vSphere, то в VMX-файле параметров скопированной виртуальной машины необходимо удалить MAC-адреса, принадлежащие виртуальной машине источника.

Оптимизация производительности сетевых интерфейсов на основе virtio

Для оптимизации производительности сетевых интерфейсов на основе virtio в средах виртуализации KVM, oVirt, zVirt рекомендуется на гипервизоре включать режим Multi Queues и устанавливать 8 очередей на сетевой интерфейс.

Например, в случае платформы oVirt (см. [документацию oVirt](#)), для того чтобы выставить 8 очередей для vNIC, необходимо подключиться к CLI гипервизора и ввести команду:

```
engine-config -s "CustomDeviceProperties={type=interface;prop={other-nic-properties;queues=[1-9][0-9]*}}"
```

Вместо параметра other-nic-properties нужно вставить список существующих кастомизированных правил (если есть). Посмотреть, существуют ли такие правила, можно командой:

```
engine-config -g "CustomDeviceProperties"
```

После ввода команды необходимо на портале администратора зайти в профили vNIC:

Выбрать редактирование профиля сетевых карт, назначенного для DCFW, в выпадающем списке **Custom Properties** выбрать **queues**, после чего ввести нужное количество очередей:

Автоматизация развертывания UserGate DCFW с помощью Cloud-init

Product: NGFW

Version: 8.x

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

- С помощью команд CLI (файл с заголовком #utm-config). Возможно использовать все CLI-команды для полной настройки виртуальной машины.
- Посредством активации 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")
```

— обозначает начало комментария, обратный слеш — переход на следующую строку.

В данный файл можно добавлять все доступные для администратора команды CLI. Подробнее о CLI-командах — в разделе [«Интерфейс командной строки»](#).

Активировать создаваемый инстанс можно 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 формат multipart:

```
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 DCFW:

- Через облачный провайдер. Например, в провайдере 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 через другие поставщики облачных услуг.
- Через подключаемый ISO-диск. На диске должны быть файлы meta-data, user-data, vendor-data со следующим содержанием:

- 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 на 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.

Требования к сетевому окружению

Product: DCFW

Version: 8.x

Для корректной работы UserGate DCFW должен иметь доступ к следующим серверам, расположенным в интернете:

- сервер регистрации — reg2.usergate.com, порты TCP 80, 443;
- сервер обновления ПО UserGate — updates.usergate.com, порты TCP 80, 443.

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

- репликация настроек — порты TCP 4369, TCP 9000-9100;
- сервис веб-консоли — TCP 8001.

Подробнее о требованиях сетевой доступности — в приложении « [Требования к сетевому окружению](#) ».

Подключение к UserGate DCFW

Product: DCFW
Version: 8.x

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, его можно явно задать, используя CLI (Command Line Interface). Подробнее об использовании CLI — в разделе [«Интерфейс командной строки»](#).

Примечание Если устройство не прошло первоначальную инициализацию, для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — usergate.

Остальные интерфейсы отключены и требуют последующей настройки.

Для первоначальной настройки выполните следующие шаги:

Шаг	Описание
1. Подключитесь к интерфейсу управления	<p>Подключитесь к интерфейсу устройства:</p> <ul style="list-style-type: none">• При наличии DHCP-сервера. Подключите интерфейс port0 к сети предприятия с работающим DHCP-сервером. Включите UserGate DCFW. После загрузки в консоли DCFW будет указан полученный интерфейсом IP-адрес. Подключитесь к веб-консоли устройства по адресу: <code>https://<DCFW_IP_address>:8001</code> для дальнейшей активации продукта.• Статический IP-адрес. Включите UserGate DCFW. Используя CLI, назначьте необходимый IP-адрес на интерфейс port0. Произведите первоначальную инициализацию в интерфейсе командной строки или подключитесь к веб-консоли DCFW по указанному адресу (он должен иметь вид: <code>https://<DCFW_IP_address>:8001</code>). <p>Подробнее об использовании CLI — в разделе «Интерфейс командной строки».</p>
2. Выберите язык	
3. Задайте пароль	
4. Настройте зоны, IP-адреса интерфейсов, подключите UserGate NGFW в сеть предприятия	<p>В разделе Настройки → Сеть → Интерфейсы включите необходимые интерфейсы, установите корректные IP-адреса, соответствующие вашим сетям, и назначьте интерфейсы соответствующим зонам. Подробнее об управлении интерфейсами — в разделе «Настройка интерфейсов».</p> <p>Система поставляется с предопределенными зонами:</p> <ul style="list-style-type: none">• Management (сеть управления), интерфейс port0;• Trusted (LAN);• Untrusted (Internet);• DMZ;• Cluster;• VPN for remote access;• VPN for Site-to-Site;• Tunnel inspection zone.
5. Настройте шлюз в интернет	<p>В разделе Настройки → Сеть → Шлюзы укажите IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет (зона Untrusted). Подробнее о настройке шлюзов — в разделе «Настройка шлюзов».</p>
6. Укажите системные DNS-серверы	<p>В разделе Настройки → Сеть → DNS укажите IP-адреса серверов DNS вашего провайдера или серверов, используемых в вашей организации.</p> <p>Подробнее об управлении DNS — в разделе «Настройка DNS».</p>
7. Настройте время сервера	<p>В разделе Настройки → UserGate → Настройки → Настройка времени сервера настройте синхронизацию времени с серверами NTP.</p>

Шаг	Описание
8. Зарегистрируйте NGFW	<p>В разделе Дашборд в виджете Лицензия нажмите Нет лицензии и введите ПИН-код для регистрации продукта. Для активации системы необходим доступ в интернет.</p> <p>Подробнее о лицензировании продукта — в разделе «Лицензирование».</p>
9. Создайте правила NAT	<p>В разделе Настройки → Политики сети → NAT и Маршрутизация создайте необходимые правила NAT. Для доступа в интернет пользователей сети Trusted правило NAT уже создано: NAT from Trusted to Untrusted.</p> <p>Подробнее о правилах NAT — в разделе «NAT и маршрутизация».</p>
10. Создайте правила межсетевого экрана	<p>В разделе Настройки → Политики сети → Межсетевой экран создайте необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети Trusted уже создано правило Allow trusted to untrusted, необходимо только включить его.</p> <p>Подробнее о правилах межсетевого экрана — в разделе «Межсетевой экран».</p>

После выполнения этих шагов UserGate DCFW готов к работе. Вы также можете дополнительно настроить другие параметры.

Шаг	Описание
Создать дополнительных администраторов	<p>В разделе Настройки → UserGate → Администраторы UserGate создайте дополнительных администраторов системы, наделите их необходимыми полномочиями (ролями).</p>
Настроить авторизацию пользователей	<p>В разделе Настройки → Пользователи и устройства создайте необходимые методы авторизации пользователей. Самый простой вариант — создать локальных пользователей DCFW в разделе Настройки → Пользователи и устройства → Пользователи с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя Any во всех правилах).</p> <p>О других вариантах авторизации пользователей — в разделе «Пользователи и устройства».</p>

