

Table of Contents

Table of Contents	1
Первоначальная настройка	2
Общие сведения	3
Развертывание виртуального образа	4
Требования к сетевому окружению	7
Подключение к UserGate WAF	9
Автоматизация развертывания UserGate WAF с помощью Cloud-init	11

Первоначальная настройка

Общие сведения

Product: WAF

Version: 7.7.x

UserGate WAF 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 межсетевой экран UserGate WAF поставляется с десятью Ethernet-интерфейсами. В случае поставки в виде ПАК — может содержать от 2 до 64 Ethernet-портов.

Развертывание виртуального образа

Documentation: 

Product: WAF

Version: 7.7.x

UserGate WAF Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают системы виртуализации VMware, Oracle VirtualBox, и в формате 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 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 посмотреть 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. В зависимости от ожидаемой нагрузки увеличьте размер оперативной памяти виртуальной машины. Рекомендованное минимальное значение — 12 ГБ.
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, установите размер диска не меньше 200 ГБ. Рекомендованный размер — 300 ГБ или более.

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

Команда 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 поставляется с четырьмя интерфейсами, на каждом из которых назначена своя зона: **Management, Trusted, Untrusted, DMZ**.

Порядок нумерации интерфейсов в виртуальной среде

В веб-консоли администратора сетевые интерфейсы отображаются по своим названиям. Сопоставление названия интерфейса и его адреса (H/W path или MAC) называется маппингом. Данные о маппинге интерфейсов хранятся в специальном системном файле. Посмотреть содержимое файла маппинга интерфейсов можно с помощью CLI-команды:

```
Admin@nodename> show network interface-mapping
```

При первоначальном старте, после сброса в первоначальное состояние (factory reset) при изменении количества сетевых адаптеров в системе (при добавлении или удалении адаптеров средствами гипервизора) происходит сортировка интерфейсов и их маппинг.

Выбор метода сортировки (по H/W path или по MAC-адресам) зависит от типа гипервизора и используемого эмулятора аппаратного обеспечения. В некоторых случаях (VirtualBox, QEMU, Bochs) сортировка интерфейсов производится по параметру H/W path, в остальных — по MAC-адресам интерфейсов.

При сортировке интерфейсов по параметру H/W path :

- Все имеющиеся на устройстве интерфейсы при любом изменении их количества (удаление, добавление) будут пересортированы в порядке возрастания аппаратных адресов (H/W path). Системный файл с данными маппинга будет полностью перезаписан.

- Удалённые интерфейсы отображаются как неиспользуемые, помечаются соответствующим значком и помещаются в конец списка интерфейсов в веб-консоли.

При сортировке интерфейсов по MAC-адресам :

- Интерфейсы, уже добавленные в систему, остаются на своих местах.
- Удаляемые интерфейсы отмечаются в веб-консоли как неиспользуемые и помечаются специальными значками.
- Новые добавленные интерфейсы добавляются в конец списка в порядке возрастания MAC-адресов.

Если использовать консольную команду `clear network interface-mapping`, файл существующего маппинга интерфейсов будет удален и все имеющиеся интерфейсы после рестарта машины будут пересортированы заново по принципу возрастания адресов.

Важно! Виртуальный образ устройства UserGate, доступный для скачивания в Личном кабинете, не имеет файла маппинга интерфейсов. Сортировка интерфейсов и их маппинг происходят при первом запуске в виртуальной среде пользователя. При подготовке пользователями собственного виртуального образа устройства UserGate для разворачивания его впоследствии на облачной платформе необходимо также удалить данные маппинга сетевых адаптеров перед сохранением образа. Файл маппинга можно удалить консольной командой `clear network interface-mapping`.

Примечание Если виртуальная машина UserGate клонируется через vSphere, то в VMX-файле настроек скопированной виртуальной машины необходимо удалить MAC-адреса, принадлежащие vm 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 WAF, в выпадающем списке **Custom Properties** выбрать **queues**, после чего ввести нужное количество очередей.

Требования к сетевому окружению

Product: WAF
Version: 7.7.x

Для корректной работы UserGate WAF должен иметь доступ к следующим серверам в интернете:

- 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 — в таблице ниже.

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб-консоли UserGate WAF)	Доступ к веб-интерфейсу управления устройством.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4040	Входящий (к UserGate по API)	Управление устройством UserGate по API.
XML-RPC поверх HTTPS	TCP	4443	Входящий (к UserGate по API)	Доступ к API поверх HTTPS.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверам технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)/Входящий (от клиентов до сервера UserGate, если он используется в качестве сервера точного времени)	Синхронизация времени.
DNS	TCP/UDP	53	Входящий (от клиентов к серверу UserGate, если он выступает в качестве DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
	UDP	53	Исходящий (до серверов DNS)	
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Регистрация продуктов UserGate: доступ до сервера reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Резерв для кластера	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Резерв для UserGate Management Center	TCP	9712	Исходящий (от UG WAF до UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от UG WAF до UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Резерв для UserGate Log Analyzer	TCP	9713	Входящий (от LogAn к UG WAF)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Log Analyzer.
		2023	Входящий (от LogAn к UG WAF)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	TCP	Для версий 6.1.x: 1269 (передача данных на LogAn 6.1.x), 22699 (передача данных на LogAn 7.x.x) Для версий 7.0.x: 22699 (передача данных на LogAn 6.1.x), 22711 (передача данных на LogAn 7.x.x, с использованием SSL)	Исходящий (от UG WAF к LogAn)	Передача журналов и телеметрии на сервер LogAn.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
Kerberos	TCP/UDP	88	Исходящий (на сервер аутентификации Kerberos)	Аутентификация пользователей по протоколу Kerberos.
NTLM	TCP	445	Исходящий (на сервер аутентификации NTLM)	Аутентификация пользователей по протоколу NTLM.
RADIUS	UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
Агент терминального сервиса	UDP	1812, 1813	Входящий (от агента на UG WAF)	Доступ к серверу UserGate, необходимый для работы терминального агента.
Агент аутентификации для Windows	UDP	1812, 1813	Входящий (от агента на UG WAF)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows.
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.

Подключение к UserGate WAF

Product: WAF
Version: 7.7.x

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка выполняется 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, то для доступа к CLI необходимо использовать в качестве логина `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	Подключитесь к интерфейсу устройства: • При наличии DHCP-сервера. Подключите интерфейс port0 к сети предприятия с работающим DHCP-сервером. Включите WAF. После загрузки в консоли WAF будет указан полученный интерфейсом IP-адрес. Подключитесь к веб-консоли устройства по адресу: <code>https://<WAF_IP_address>:8001</code> для дальнейшей активации продукта. • Статический IP-адрес. Включите UserGate WAF. Используя CLI, назначьте необходимый IP-адрес на интерфейс port0. Произведите первоначальную инициализацию в интерфейсе командной строки или подключитесь к веб-консоли UserGate WAF по указанному адресу (он должен иметь вид: <code>https://<WAF_IP_address>:8001</code>). Подробнее об использовании CLI — в разделе «Интерфейс командной строки»
2. Выберите язык	
3. Задайте пароль	
4. Настройте зоны, IP-адреса интерфейсов, подключите UserGate WAF в сеть предприятия	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». Система поставляется с предопределенными зонами: • Management (сеть управления), интерфейс port0; • Trusted (LAN); • Untrusted (Internet); • DMZ
5. Настройте шлюз в интернет	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»
6. Укажите системные DNS-серверы	В разделе Настройки → Консоль администратора → Настройки в секции Серверы DNS укажите IP-адреса DNS-серверов вашего провайдера или серверов, используемых в вашей организации. Подробнее об управлении DNS — в разделе «Настройка общих параметров»
7. Настройте время сервера	В разделе Настройки → Консоль администратора → Настройки → Настройка времени сервера настройте синхронизацию времени с серверами NTP
8. Зарегистрируйте WAF	В разделе Дашборды на вкладке НОС в виджете Лицензия нажмите Нет лицензии и введите ПИН-код для регистрации продукта. Для активации системы необходим доступ в интернет. Подробнее о лицензировании продукта — в разделе «Лицензирование»
9. Создайте правила межсетевого экрана	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. Подробнее о правилах межсетевого экрана — в разделе «Межсетевой экран»

Шаг	Описание
10. Если необходимо, создайте дополнительных администраторов	В разделе Настройки → Консоль администратора → Администраторы создайте дополнительных администраторов системы, наделите их необходимыми полномочиями (ролями).

После выполнения этих шагов UserGate WAF готов к работе. Для более детальной настройки обратитесь к необходимым главам руководства администратора.

Автоматизация развертывания UserGate WAF с помощью Cloud-init

Product: WAF

Version: 7.7.x

Cloud-init — индустриальный стандарт для кросс-платформенной инициализации виртуальных машин (инстансов) в облачных сервисах провайдеров. UserGate WAF 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 об использовании CLI — 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 WAF:

- Через облачный 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 через другие поставщики облачных услуг.
- Через подключаемый ISO-диск. Диск должен содержать 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.

