

Table of Contents

Table of Contents	1
Первоначальная настройка	2
Описание	3
Требования к сетевому окружению	4
Развертывание виртуального образа	5
Подключение к UserGate и первоначальная настройка	6

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: 

Version: 6.1.9, 5.x

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

- Сервер регистрации - reg2.entensys.com, порты TCP 80, 443.
- Сервер обновления списков и ПО UserGate - static.entensys.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.

Развертывание виртуального образа

Documentation: ☒

Version: 6.x

UserGate 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.

ПримечаниеДля 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 12Gb и добавьте по 1Gb на каждые 100 пользователей.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины	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.
Шаг 5. Настройте виртуальные сети	UserGate поставляется с четырьмя интерфейсами, назначенными в зоны: • Management - первый интерфейс виртуальной машины. • Trusted - второй интерфейс виртуальной машины. • Untrusted - третий интерфейс виртуальной машины. • DMZ - четвертый интерфейс виртуальной машины.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину UserGate. 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.

Documentation: ☒
Version: 5.x, 6.1.9

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 \(CLI\)](#).

ПримечаниеДля первоначального доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

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 Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate. После загрузки UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. Статический IP-адрес Включить UserGate. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGate_IP_address:8001.
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: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). • Зона Untrusted (Internet). • Зона DMZ. • Зона Cluster. • Зона VPN for remote access. • Зона VPN for Site-to-Site.
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. 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 продукт UserGate.	Для регистрации продукта ввести ПИН-код и заполнить форму. Для активации системы необходим доступ UserGate в Интернет. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate.

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 ». Подробнее 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. Подробнее 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 UserGate с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя Any во всех правилах). 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). 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. 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. Более подробно о дешифровании HTTPS читайте в главе Инспектирование SSL .

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

