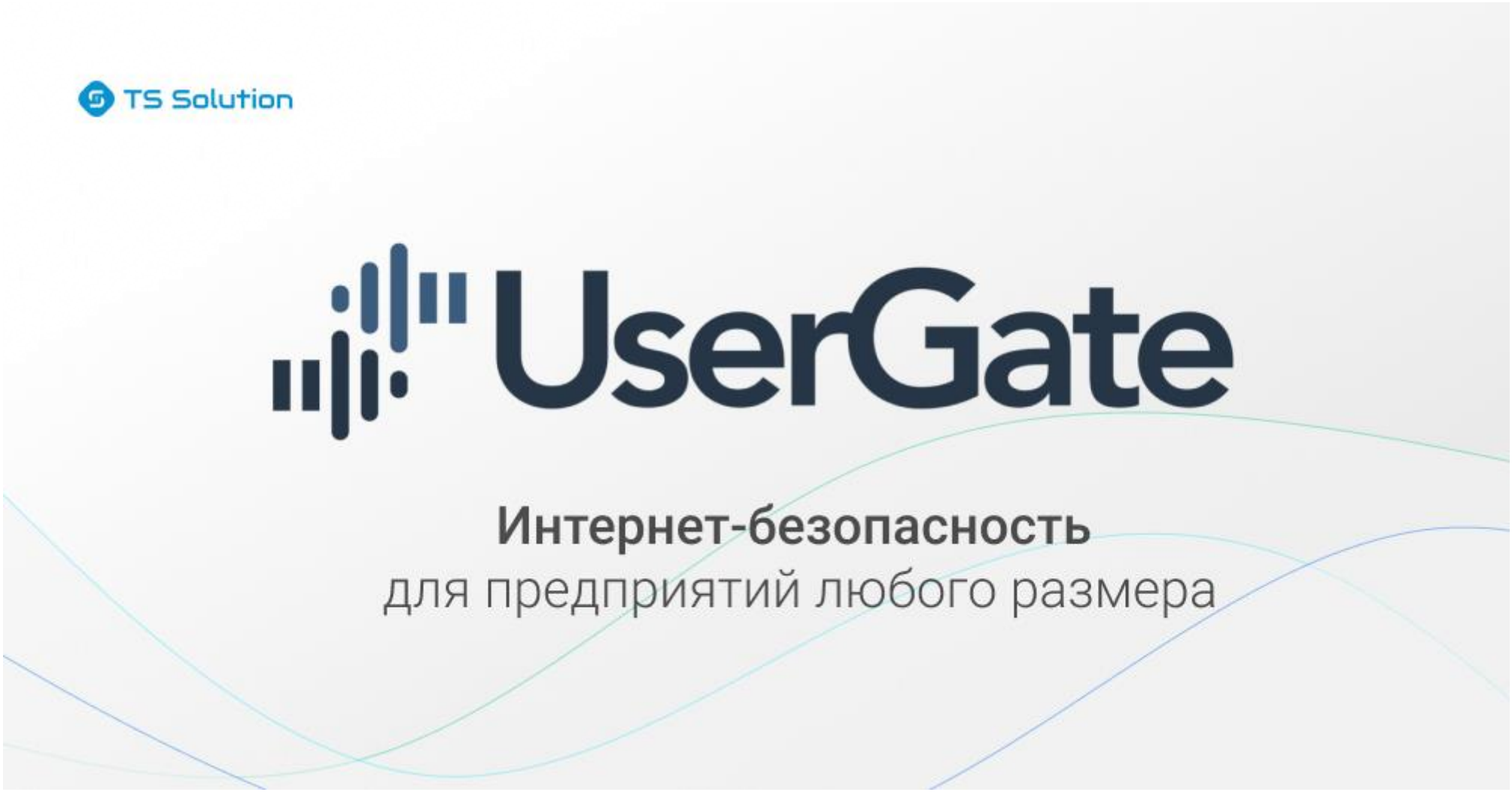
UserGate Getting Started. Требования, установка



1. Введение

Имеются различные способы внедрения данного шлюза в сеть. Хочу заметить, что в зависимости от выбранного варианта подключения определенный функционал шлюза может быть недоступен. Решение UserGate поддерживает следующие режимы подключения:

- L3-L7 брандмауэр
- L2 прозрачный мост
- L3 прозрачный мост
- Виртуально в разрыв, с применением протокола WCCP
- Виртуально в разрыв, с применением Policy Based Routing
- Router on a Stick
- Явно заданный WEB-прокси
- UserGate, как шлюз по умолчанию
- Мониторинг Mirror-порта

UserGate поддерживает 2 типа кластеров:

1. Кластер конфигурации. Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
2. Кластер отказоустойчивости. До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив. Возможно собрать несколько кластеров отказоустойчивости.

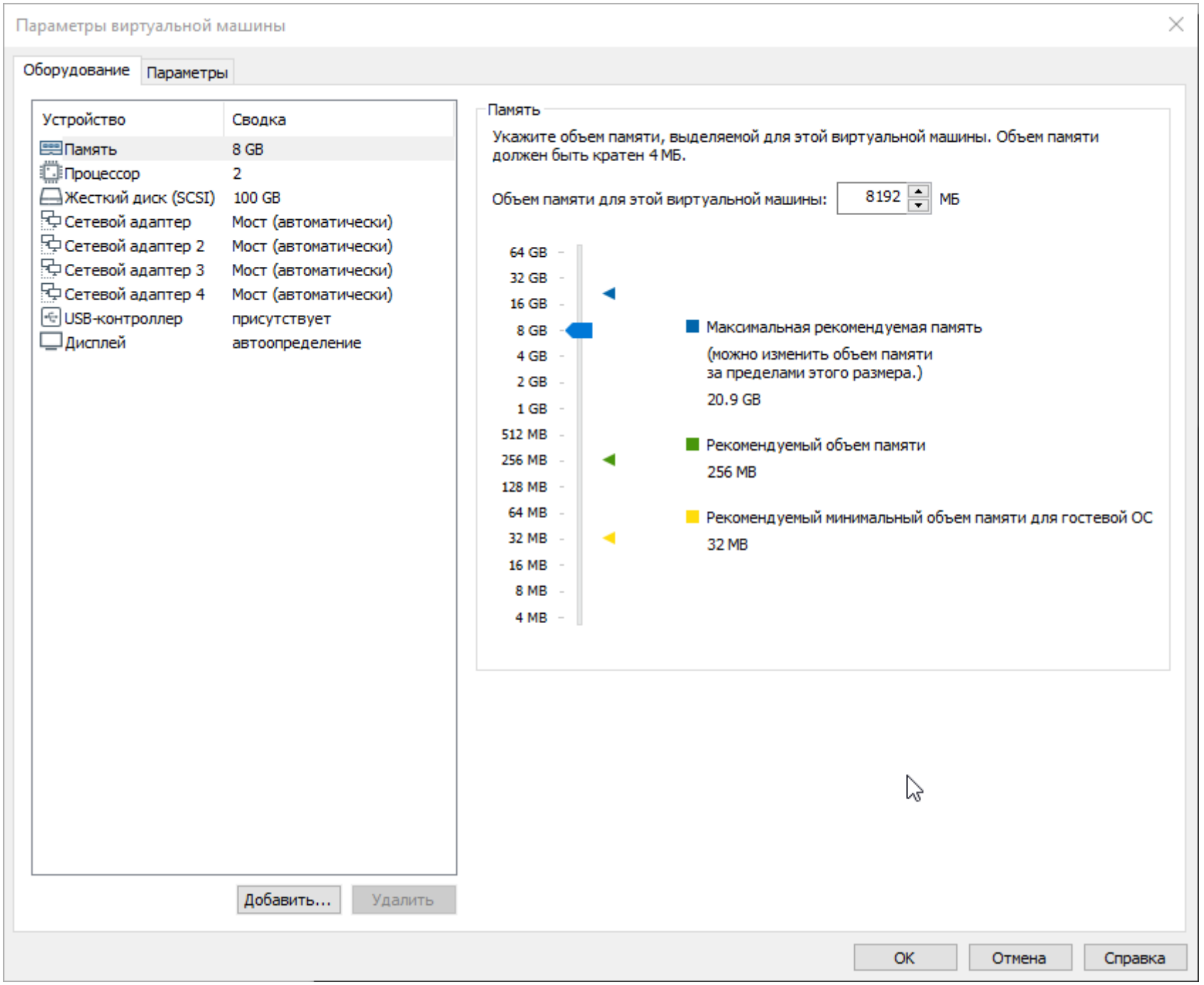
2. Установка

UserGate поставляется в виде программно-аппаратного комплекса или разворачивается в виртуальной среде. Из личного кабинета на сайте UserGate скачиваем образ в формате OVF (Open Virtualization Format), данный формат подходит для вендоров VMWare и Oracle Virtualbox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

По данным сайта UserGate для корректной работы виртуальной машины рекомендуется использовать минимум 8Gb оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Установка начинается с импорта образа в выбранный гипервизор (VirtualBox и VMWare). В случае с Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, после чего отключить службы интеграции в настройках созданной виртуальной машины.

По умолчанию после импорта в VMWare создается виртуальная машина со следующими настройками:


Параметры виртуальной машины
Оборудование
Параметры
Устройство
Сводка
Память
8 GB
Процессор
2
Жесткий диск (SCSI)
100 GB
Сетевой адаптер
Мост (автоматически)
Сетевой адаптер 2
Мост (автоматически)
Сетевой адаптер 3
Мост (автоматически)
Сетевой адаптер 4
Мост (автоматически)
USB-контроллер
присутствует
Дисплей
автоопределение
Добавить...
Удалить
Память
Укажите объем памяти, выделяемой для этой виртуальной машины. Объем памяти должен быть кратен 4 МБ.
Объем памяти для этой виртуальной машины:
8192
МБ
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Максимальная рекомендуемая память
(можно изменить объем памяти
за пределами этого размера.)
20.9 GB
Рекомендуемый объем памяти
256 MB
Рекомендуемый минимальный объем памяти для гостевой ОС
32 MB
OK
Отмена
Справка

Оперативной памяти должно быть, как минимум 8Gb и в дополнении нужно добавить по 1Gb на каждые 100 пользователей. Размер жесткого диска по умолчанию составляет 100Gb, однако этого обычно недостаточно для хранения всех журналов и настроек. Рекомендованный размер – 300Gb или более. Поэтому в свойствах виртуальной машины изменяем размер диска на нужный. Изначально виртуальный UserGate UTM поставляется с четырьмя интерфейсами, назначенными в зоны:

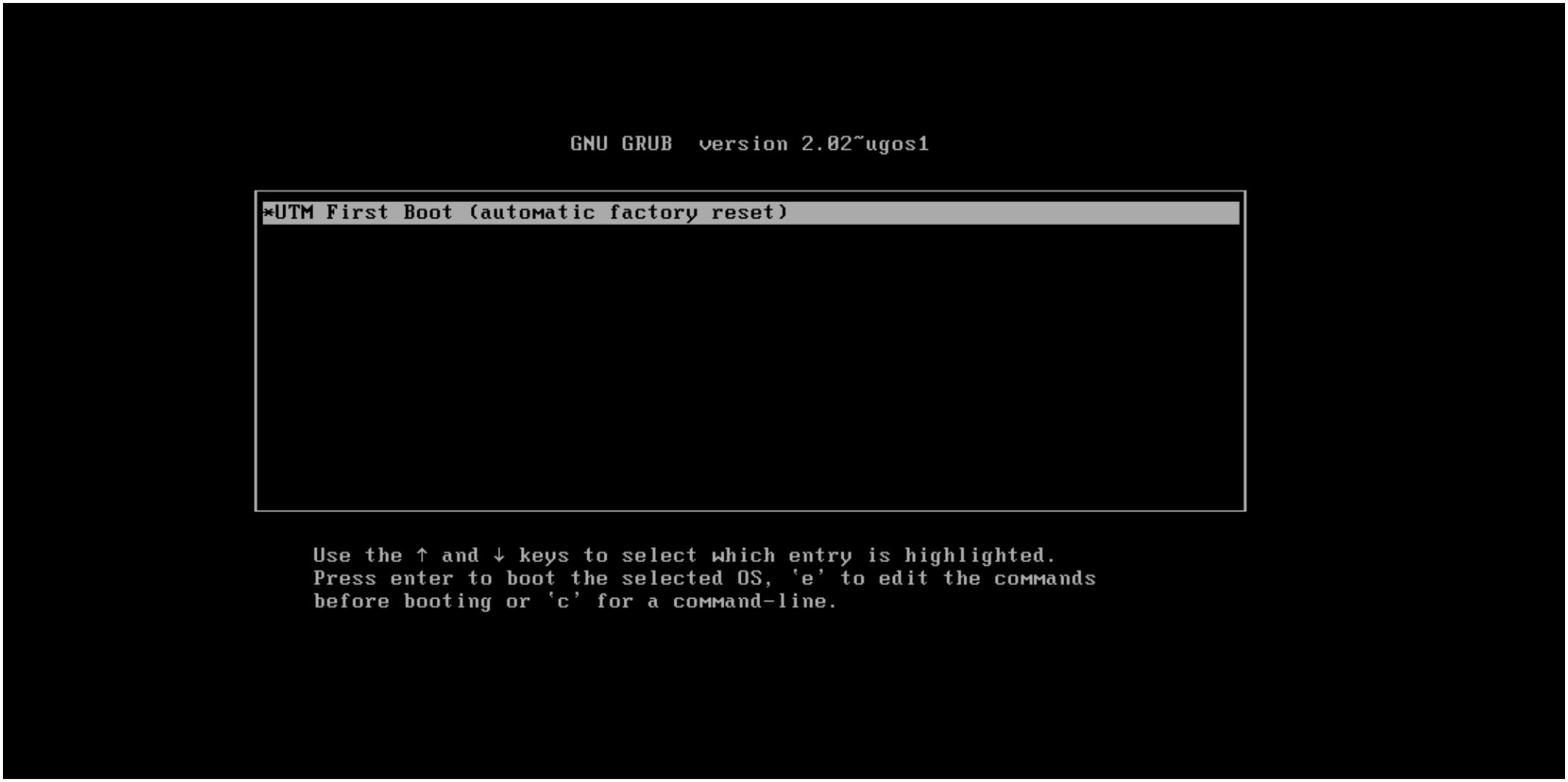
Management - первый интерфейс виртуальной машины, зона для подключения доверенных сетей, из которых разрешено управление UserGate.

Trusted - второй интерфейс виртуальной машины, зона для подключения доверенных сетей, например, LAN-сетей.

Untrusted - третий интерфейс виртуальной машины, зона для интерфейсов, подключенных к не доверенным сетям, например, к интернету.

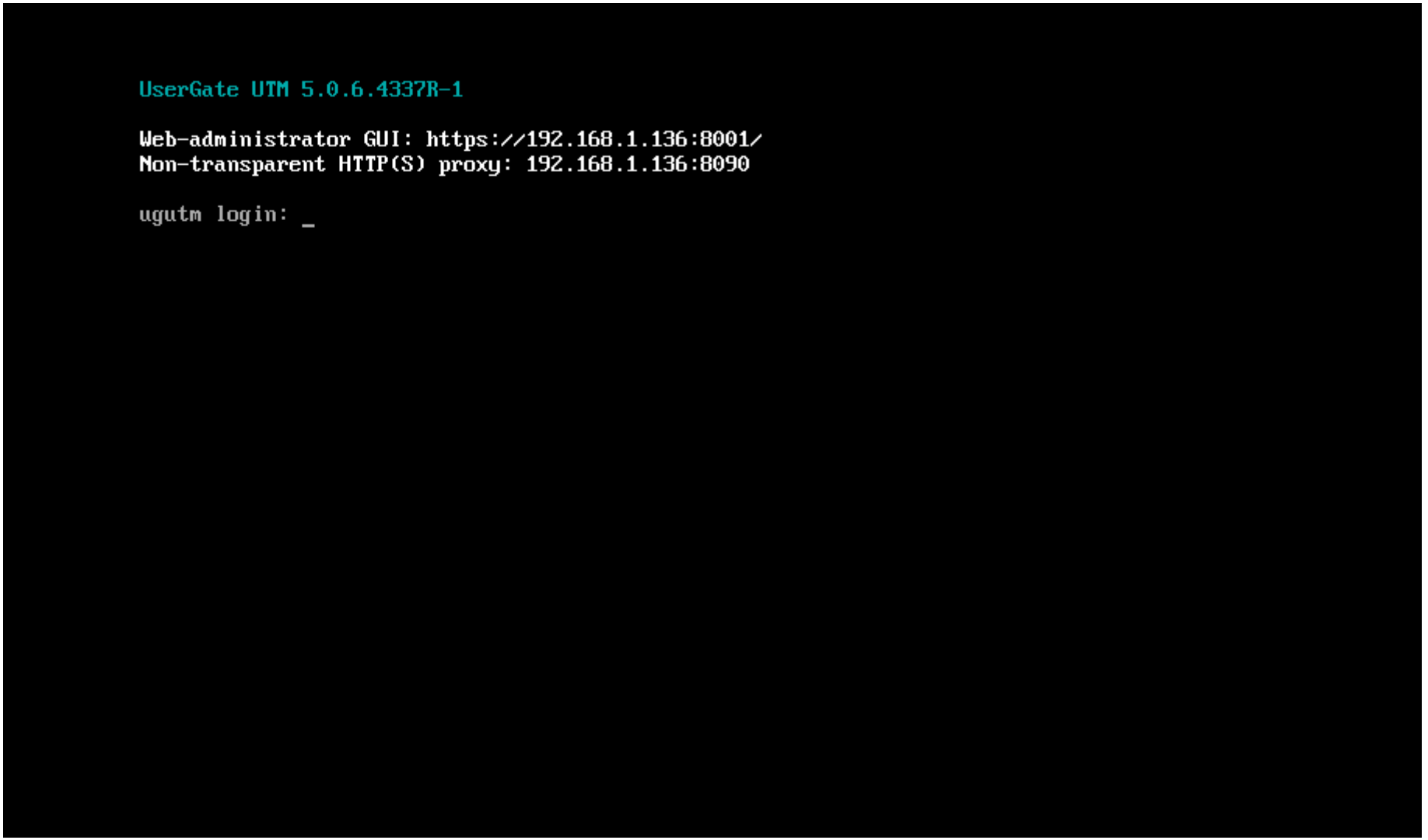
DMZ - четвертый интерфейс виртуальной машины, зона для интерфейсов, подключенных к сети DMZ.

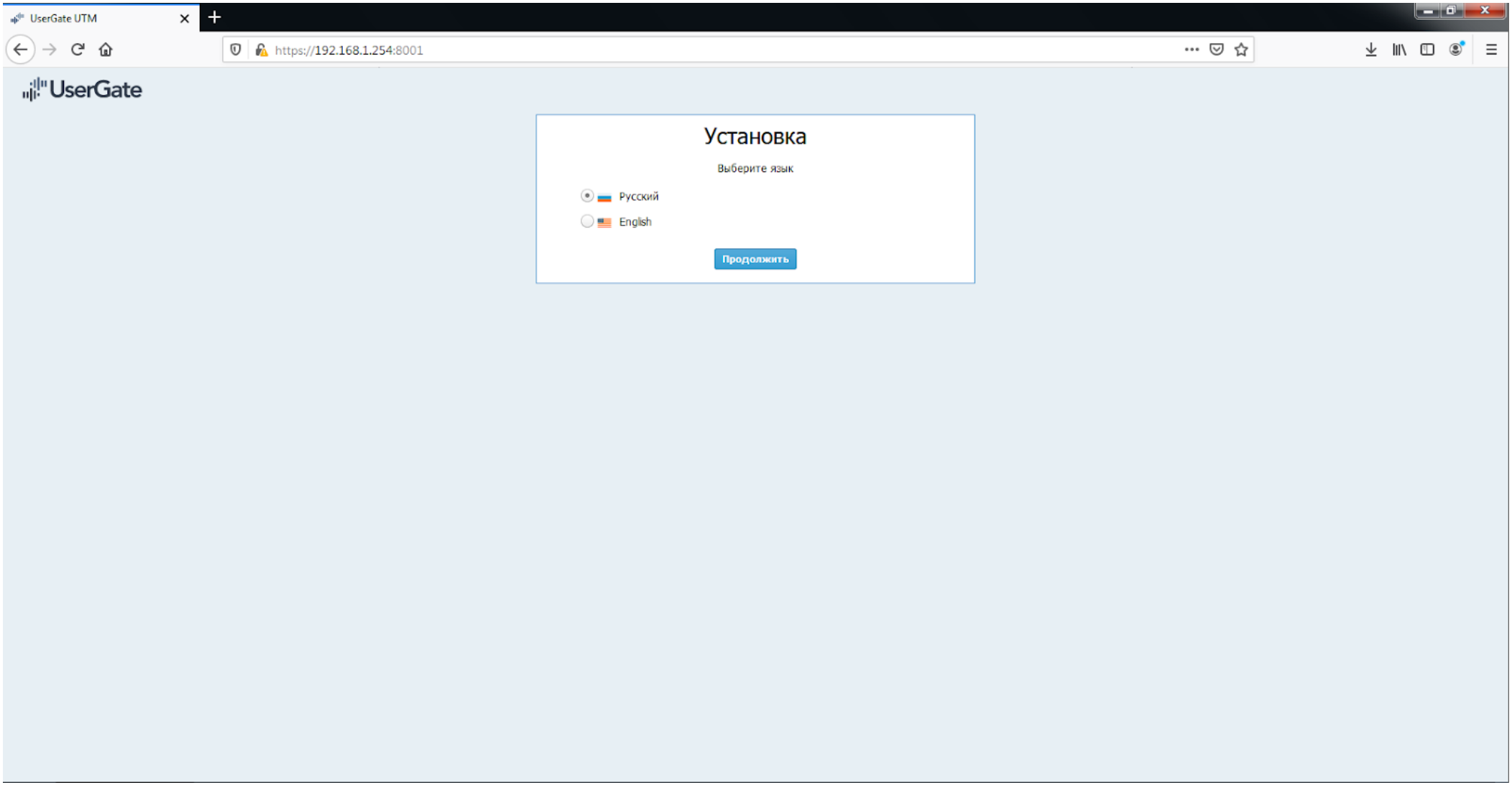
Далее запускаем виртуальную машины, хоть в руководстве и написано, что нужно выбрать Support Tools и выполнить Factory reset UTM, но как видим есть только один выбор (UTM First Boot). Во время этого шага UTM настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска:



Для подключения к веб интерфейсу UserGate необходимо заходить через Management зону, за это отвечает интерфейс eth0, который настроен на получение IP-адреса в автоматическом режиме (DHCP). Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Для этого нужно войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin с Заглавной буквы).

Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля – utm. И набрать команду на подобии iface config –name eth0 –ipv4 192.168.1.254/24 –enable true –mode static. Позже переходим к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGateIPaddress:8001:

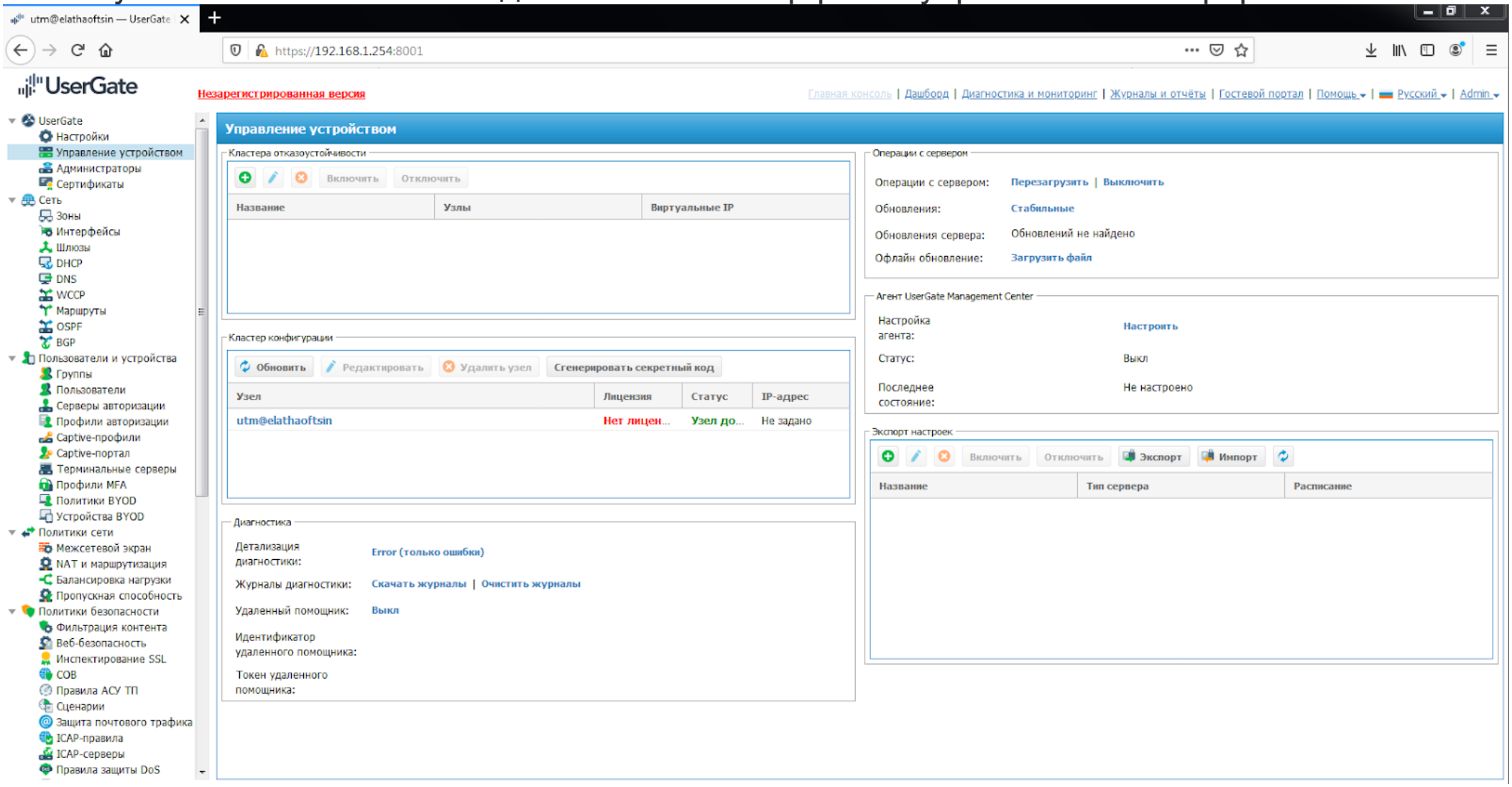

UserGate UTM 5.0.6.4337R-1
Web-administrator GUI: https://192.168.1.136:8001/
Non-transparent HTTP(S) proxy: 192.168.1.136:8090
ugutm login: _



В веб-консоли продолжаем установку, нам нужно выбирать язык интерфейса (на данный момент это русский или английский язык), часовой пояс, далее читаем и соглашаемся с лицензионным соглашением. Задаем логин и пароль для входа в веб-интерфейс управления.

3. Настройка

После установки вот так выглядит окно веб интерфейса управления платформой:



Затем необходимо настроить сетевые интерфейсы. Для этого в разделе "Интерфейсы" нужно включить их, установить корректные IP-адреса и назначить соответствующие зоны.

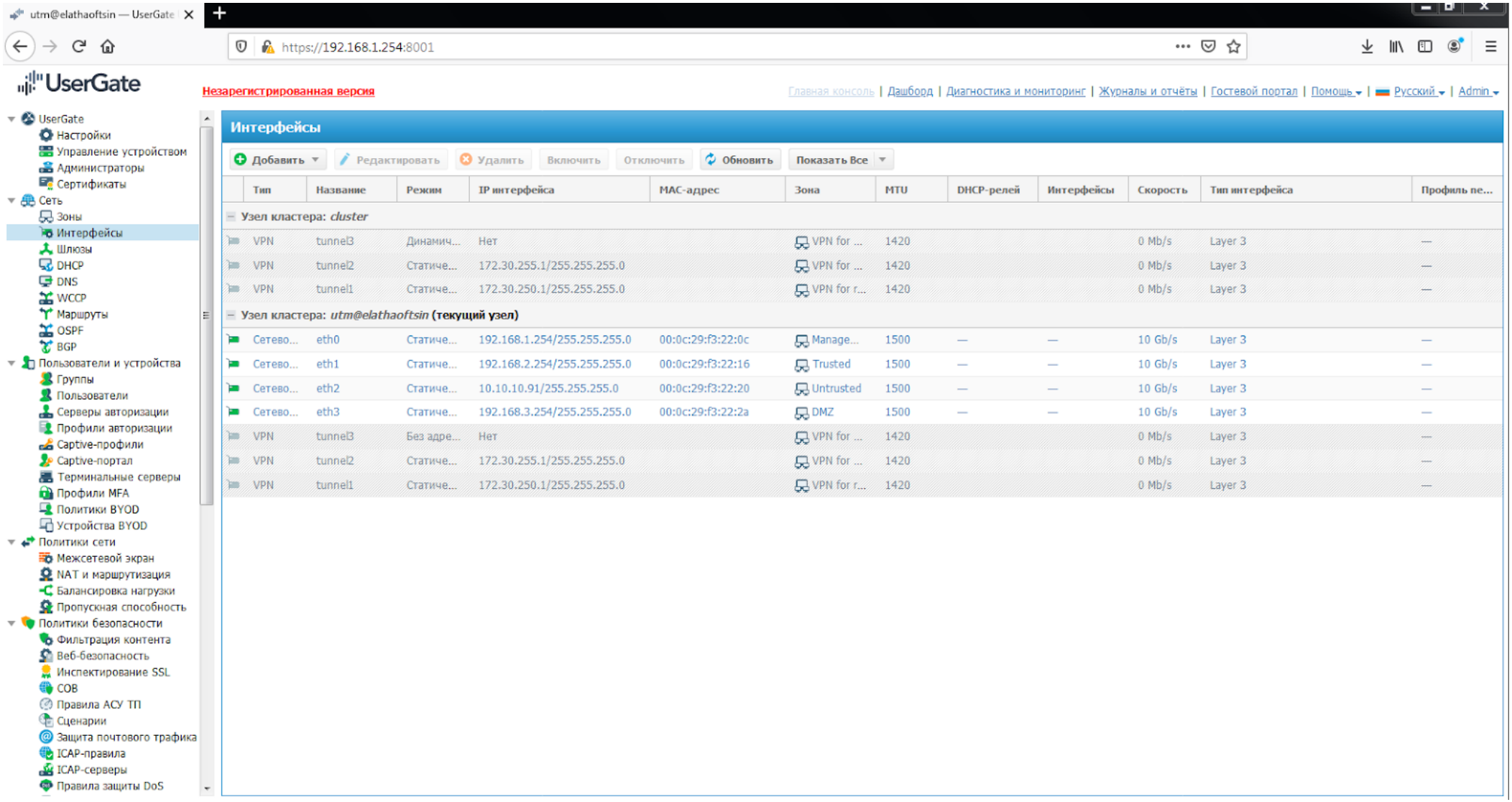
Раздел "Интерфейсы" отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN-интерфейсы. Еще он показывает все интерфейсы каждого узла кластера. Настройки интерфейсов специфичны для каждого из узлов, то есть не глобальны.

В свойствах интерфейса:

- Включить или отключить интерфейс
- Указать тип интерфейса - Layer 3 или Mirror
- Назначить зону интерфейсу
- Назначить профиль Netflow для отправки статистических данных на Netflow коллектор
- Изменить физические параметры интерфейса - MAC-адрес и размер MTU
- Выбрать тип присвоения IP-адреса - без адреса, статический IP-адрес или полученный по DHCP
- Настроить работу DHCP-релея на выбранном интерфейсе.

Кнопка "Добавить" позволяет добавить следующие типы логических интерфейсов:

- VLAN
- Бонд
- Мост
- PPPoE
- VPN
- Туннель


utm@elathaoftsin — UserGate
https://192.168.1.254:8001
UserGate
Незарегистрированная версия
Главная консоль | Дашборд | Диагностика и мониторинг | Журналы и отчёты | Гостевой портал | Помощь | Русский | Admin
UserGate
Настройки
Управление устройством
Администраторы
Сертификаты
Сеть
Зоны
Интерфейсы
Шлюзы
DHCP
DNS
WCCP
Маршруты
OSPF
BGP
Пользователи и устройства
Группы
Пользователи
Серверы авторизации
Профили авторизации
Captive-профили
Captive-портал
Терминальные серверы
Профили MFA
Политики BYOD
Устройства BYOD
Политики сети
Межсетевой экран
NAT и маршрутизация
Балансировка нагрузки
Пропускная способность
Политики безопасности
Фильтрация контента
Веб-безопасность
Инспектирование SSL
СОВ
Правила АСУ ТП
Сценарии
Защита почтового трафика
ICAP-правила
ICAP-серверы
Правила защиты DoS
Интерфейсы
Добавить
Редактировать
Удалить
Включить
Отключить
Обновить
Показать Все
Тип
Название
Режим
IP интерфейса
MAC-адрес
Зона
MTU
DHCP-релей
Интерфейсы
Скорость
Тип интерфейса
Профиль пе...
Узел кластера: cluster
VPN tunnel3 Динамич... Нет VPN for ... 1420 0 Mb/s Layer 3 —
VPN tunnel2 Статиче... 172.30.255.1/255.255.255.0 VPN for ... 1420 0 Mb/s Layer 3 —
VPN tunnel1 Статиче... 172.30.250.1/255.255.255.0 VPN for r... 1420 0 Mb/s Layer 3 —
Узел кластера: utm@elathaoftsin (текущий узел)
Сетево... eth0 Статиче... 192.168.1.254/255.255.255.0 00:0c:29:f3:22:0c Manage... 1500 — — 10 Gb/s Layer 3 —
Сетево... eth1 Статиче... 192.168.2.254/255.255.255.0 00:0c:29:f3:22:16 Trusted 1500 — — 10 Gb/s Layer 3 —
Сетево... eth2 Статиче... 10.10.10.91/255.255.255.0 00:0c:29:f3:22:20 Untrusted 1500 — — 10 Gb/s Layer 3 —
Сетево... eth3 Статиче... 192.168.3.254/255.255.255.0 00:0c:29:f3:22:2a DMZ 1500 — — 10 Gb/s Layer 3 —
VPN tunnel3 Без адре... Нет VPN for ... 1420 0 Mb/s Layer 3 —
VPN tunnel2 Статиче... 172.30.255.1/255.255.255.0 VPN for ... 1420 0 Mb/s Layer 3 —
VPN tunnel1 Статиче... 172.30.250.1/255.255.255.0 VPN for r... 1420 0 Mb/s Layer 3 —

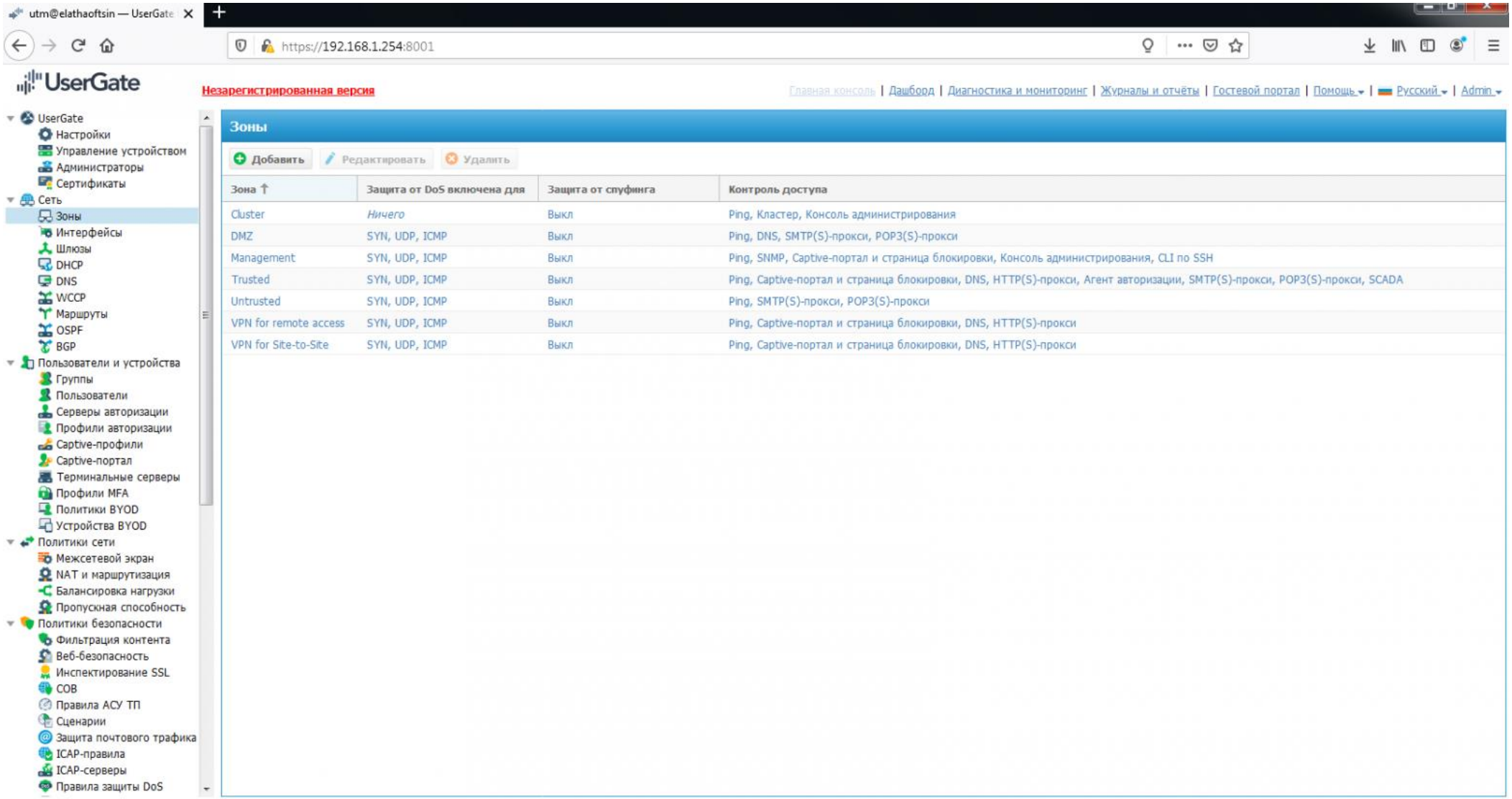
Помимо перечисленных ранее зон, с которыми поставляется образ Usergate, есть еще три типа предопределенных:

Cluster - зона для интерфейсов, используемых для работы кластера

VPN for Site-to-Site - зона, в которую помещаются все клиенты типа Офис-Офис, подключаемые к UserGate по VPN

VPN for remote access - зона, в которую помещаются все мобильные пользователи, подключенные к UserGate по VPN

Администраторы UserGate могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны, но как сказано в руководстве к версии 5, можно создать не более 15 зон. Для изменения или создания их нужно перейти в раздел зоны. Для каждой зоны можно установить порог отбрасывания пакетов, поддерживается SYN, UDP, ICMP. Также настраивается контроль доступа к сервисам Usergate, и включается защита от спуфинга.


utm@elathaoftsin — UserGate
https://192.168.1.254:8001
UserGate
Незарегистрированная версия
Главная консоль | Дашборд | Диагностика и мониторинг | Журналы и отчёты | Гостевой портал | Помощь | Русский | Admin
UserGate
Настройки
Управление устройством
Администраторы
Сертификаты
Сеть
Зоны
Интерфейсы
Шлюзы
DHCP
DNS
WCCP
Маршруты
OSPF
BGP
Пользователи и устройства
Группы
Пользователи
Серверы авторизации
Профили авторизации
Captive-профили
Captive-портал
Терминальные серверы
Профили MFA
Политики BYOD
Устройства BYOD
Политики сети
Межсетевой экран
NAT и маршрутизация
Балансировка нагрузки
Пропускная способность
Политики безопасности
Фильтрация контента
Веб-безопасность
Инспектирование SSL
СОВ
Правила АСУ ТП
Сценарии
Защита почтового трафика
ICAP-правила
ICAP-серверы
Правила защиты DoS
Зоны
Добавить
Редактировать
Удалить
Зона
Защита от DoS включена для
Защита от спуфинга
Контроль доступа
Cluster
Ничего
Выкл
Ping, Кластер, Консоль администрирования
DMZ
SYN, UDP, ICMP
Выкл
Ping, DNS, SMTP(S)-прокси, POP3(S)-прокси
Management
SYN, UDP, ICMP
Выкл
Ping, SNMP, Captive-портал и страница блокировки, Консоль администрирования, CLI по SSH
Trusted
SYN, UDP, ICMP
Выкл
Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Агент авторизации, SMTP(S)-прокси, POP3(S)-прокси, SCADA
Untrusted
SYN, UDP, ICMP
Выкл
Ping, SMTP(S)-прокси, POP3(S)-прокси
VPN for remote access
SYN, UDP, ICMP
Выкл
Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси
VPN for Site-to-Site
SYN, UDP, ICMP
Выкл
Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси

После настройки интерфейсов необходимо в разделе "Шлюзы" настроить маршрут по умолчанию. Т.е. для подключения UserGate к интернету необходимо указать IP-адрес одного или нескольких шлюзов. Если для подключения к интернету используется несколько провайдеров, то необходимо указать несколько шлюзов. Настройка шлюза уникальна для каждого из узлов кластера. Если задано два или более шлюзов возможны 2 варианта работы:

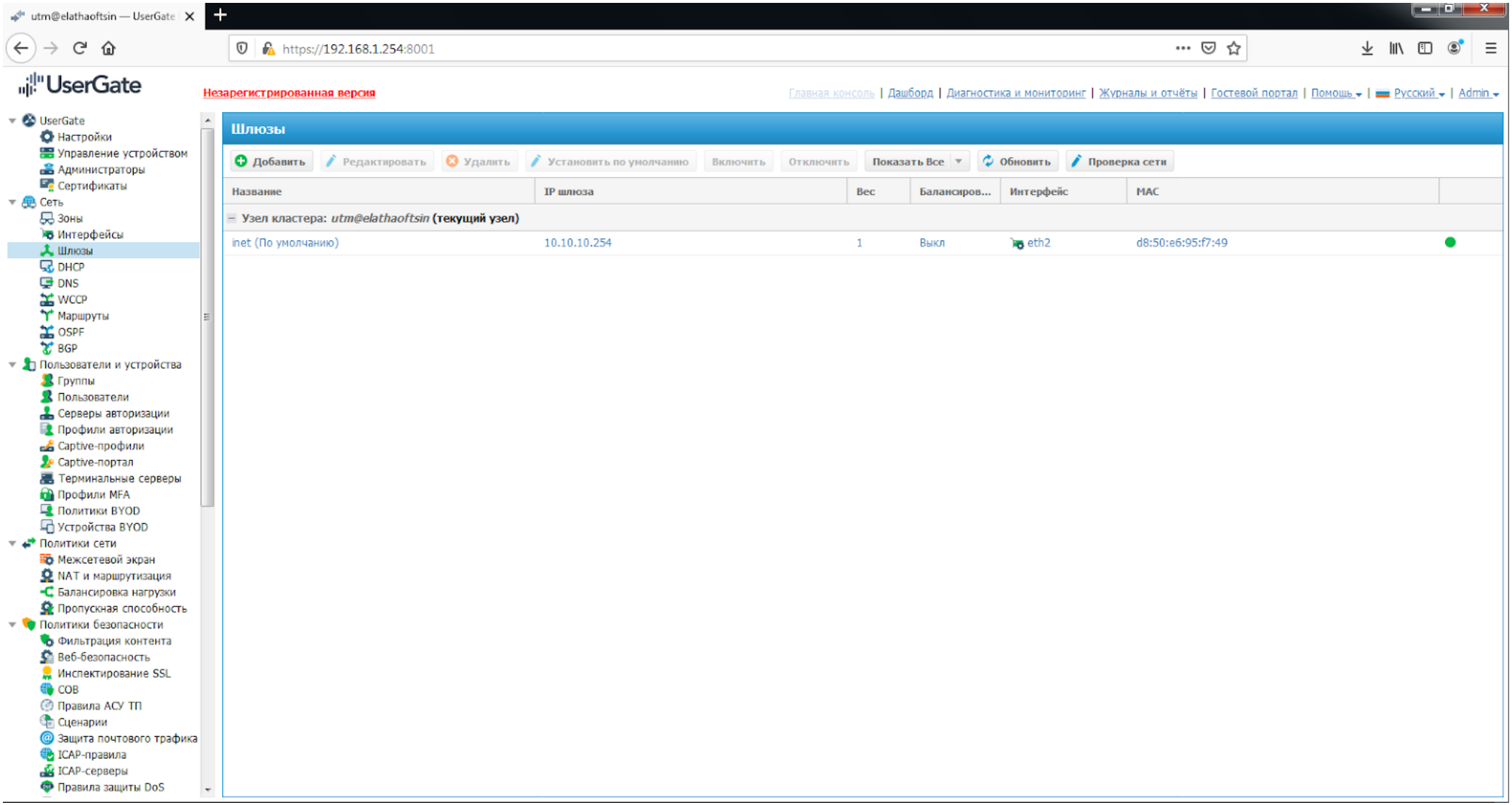
1. Балансировка трафика между шлюзами.
2. Основной шлюз с переключением на запасной.

Состояние шлюза (доступен – зеленый, недоступен – красный) определяется следующим образом:

1. Проверка сети отключена – шлюз считается доступным, если UserGate может получить его MAC-адрес с помощью ARP-запроса. Проверка наличия доступа в интернет через этот шлюз не производится. Если MAC-адрес шлюза не может быть определен, шлюз считается недоступным.
2. Проверка сети включена - шлюз считается доступным, если:

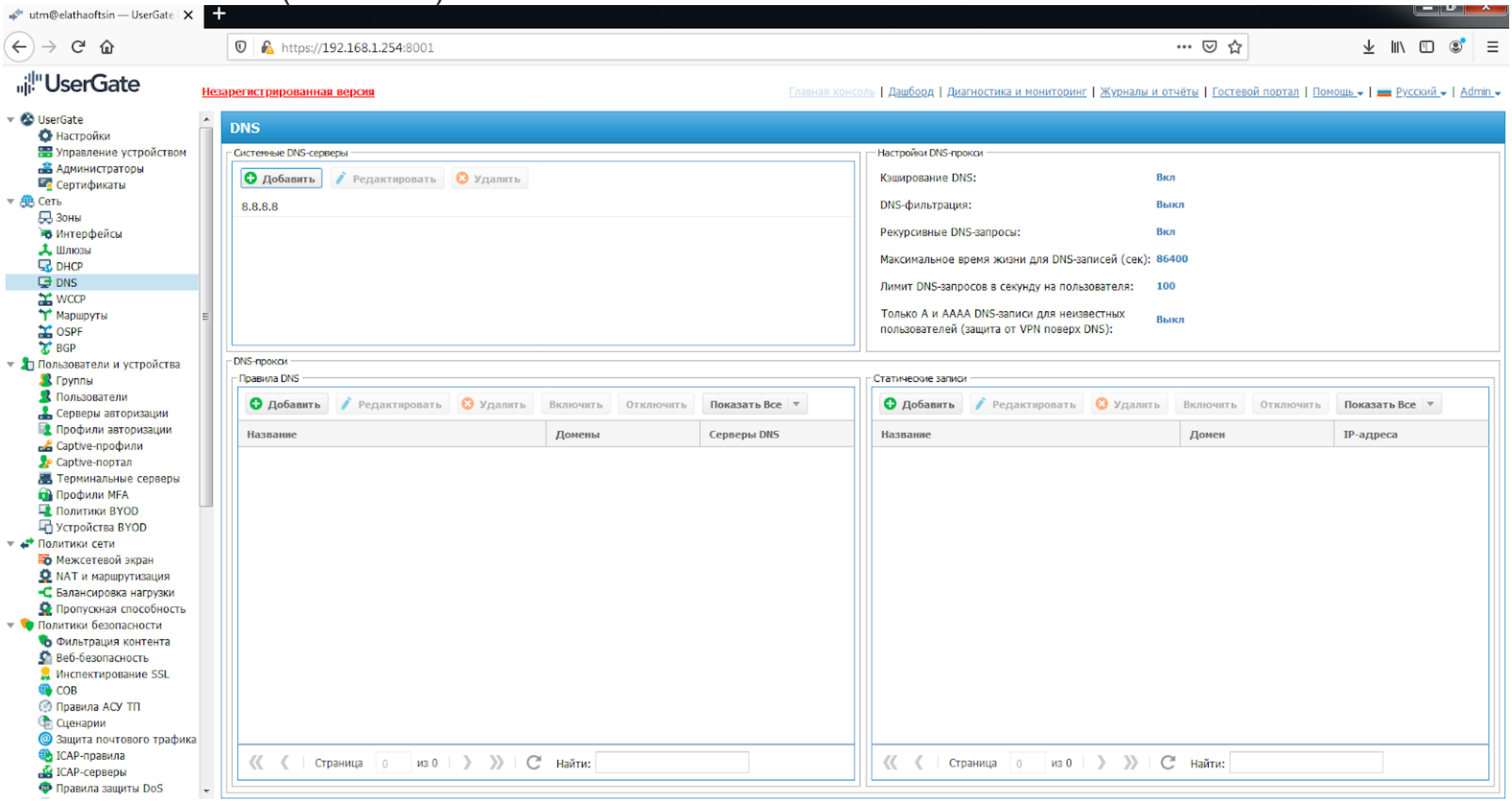
- UserGate может получить его MAC-адрес с помощью ARP-запроса.
- Проверка наличия доступа в интернет через этот шлюз завершилась успешно.

В противном случае шлюз считается недоступным.



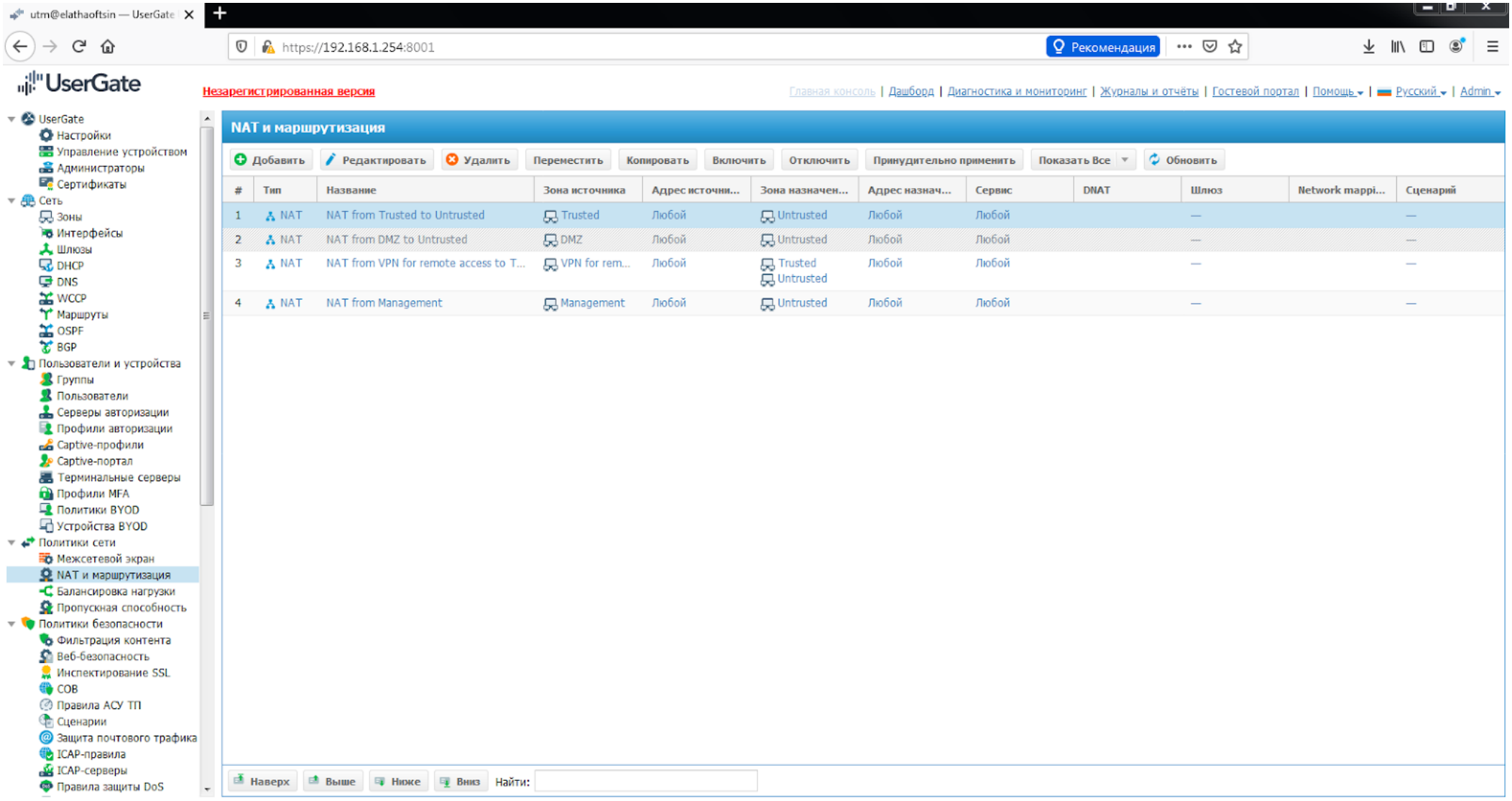
В разделе "DNS" необходимо добавить DNS сервера, которые будет использовать UserGate. Данная настройка указывается в области Системные DNS-серверы. Ниже находятся настройки по управлению DNS-запросами от пользователей. UserGate позволяет использовать DNS-прокси. Сервис DNS-прокси позволяет перехватывать DNS-запросы от

пользователей и изменять их в зависимости от нужд администратора. С помощью правил DNS-прокси можно указать серверы DNS, на которые пересылаются запросы на определенные домены. Кроме этого, с помощью DNS-прокси можно задавать статические записи типа host (A-запись).



В разделе "NAT и Маршрутизация" нужно создать необходимые правила NAT. Для доступа в интернет пользователей сети Trusted правило NAT уже создано - «Trusted-->Untrusted», остается его только включить. Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. UserGate рекомендует создавать общие правила NAT, например, правило NAT из локальной сети (обычно зона Trusted) в интернет (обычно зона Untrusted), а разграничение доступа по пользователям, сервисам, приложениям осуществлять с помощью правил межсетевого экрана.

Также есть возможность создать правила DNAT, порт-форвардинг, Policy-based routing, Network mapping.



После этого в разделе "Межсетевой экран" необходимо создать правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети Trusted правило межсетевого экрана так же уже создано - «Internet for Trusted» и его необходимо включить. С помощью правил межсетевого экрана администратор может разрешить или запретить

любой тип транзитного сетевого трафика, проходящего через UserGate. В качестве условий правила могут выступать зоны и IP-адреса источника/назначения, пользователи и группы, сервисы и приложения. Правила применяются также как и в разделе "NAT и Маршрутизация", т.е. сверху вниз. Если не создано ни одного правила, то любой транзитный трафик через UserGate запрещен.