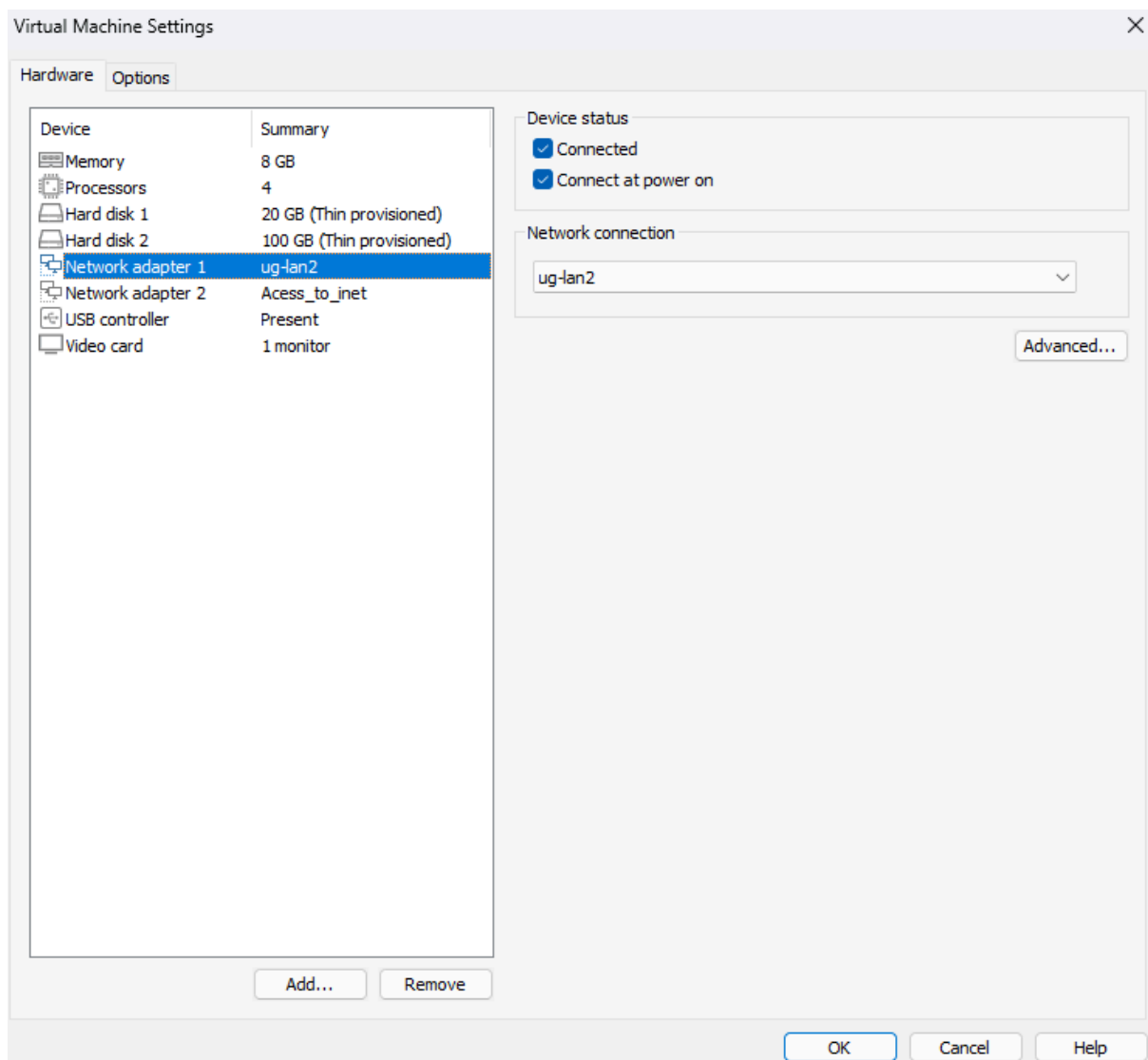


## UserGate NGFW

В данной лабораторной работе необходимо выполнить установку и настройку [UserGate NGFW](#) с дальнейшим подключением к нему клиента под управлением [Windows 10/11](#). В качестве среды виртуализации рекомендуется выбрать [VMWare Workstation](#) (ключи активации для проги можно найти [тут](#)). Необходимо настроить два сетевых адаптера (Bridge + internal) и назначить их Юзергейту, клиенту назначить только интернал адаптер, выход в Интернет и все настройки, он должен получать от Юзергейта.



Первый сетевой адаптер будет относиться Юзергейтом в зону Management, там необходимо указать internal сеть, в качестве второго адаптера указываете свою сеть с выходом в Интернет, через bridge.

Ваш лучший друг в данной работе - [документация](#)! Ну, и нейросети...

Креды для входа в систему UserGate по умолчанию: Admin/usergate

Экран после первого запуска:

```
UGOS NGFW 7.4.0.209490R

Web-administrator GUI: https://127.0.0.1:8001/

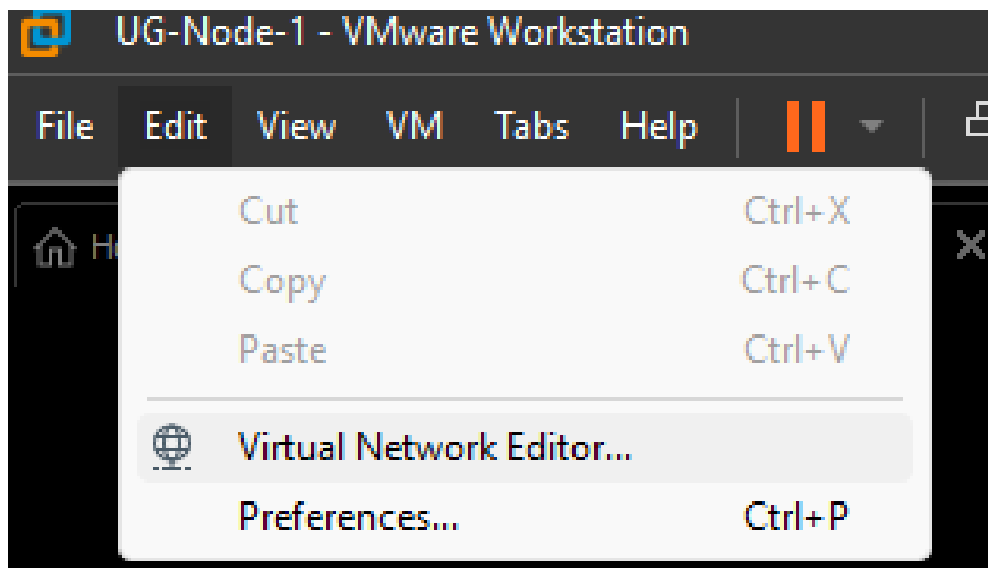
UGOS login: _
```

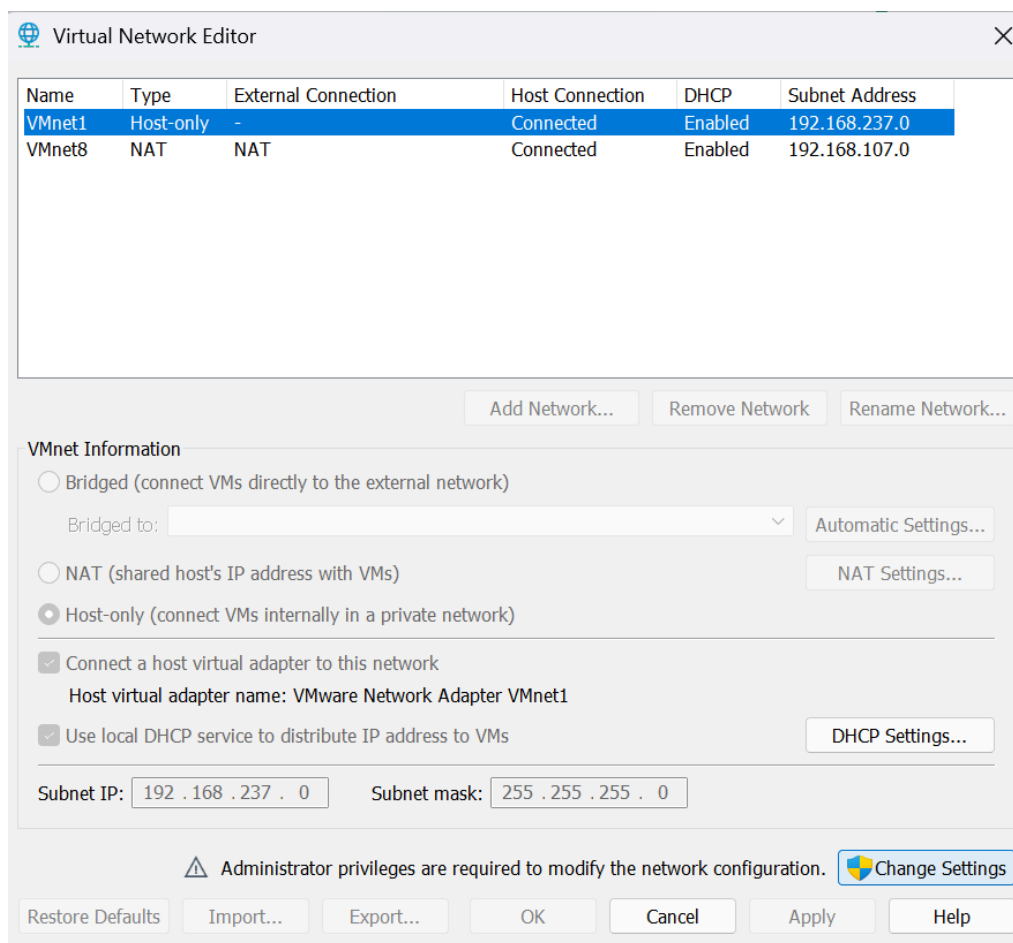
Делаем логичный вывод, что по loopback адресу мы никак не сможем зайти в web-интерфейс для настройки, потому необходимо задать статический адрес для port0, выполнив следующие команды:

```
UGOS NGFW 7.4.0.209490R

Admin@hauwerledoft> configure
Admin@hauwerledoft# set network interface adapter port0 ip-addresses [ 172.16.10.2/26 ] enabled on_
```

Маска и адрес в зависимости от того, какие параметры вы выбрали при настройке internal адаптера в VMWare.





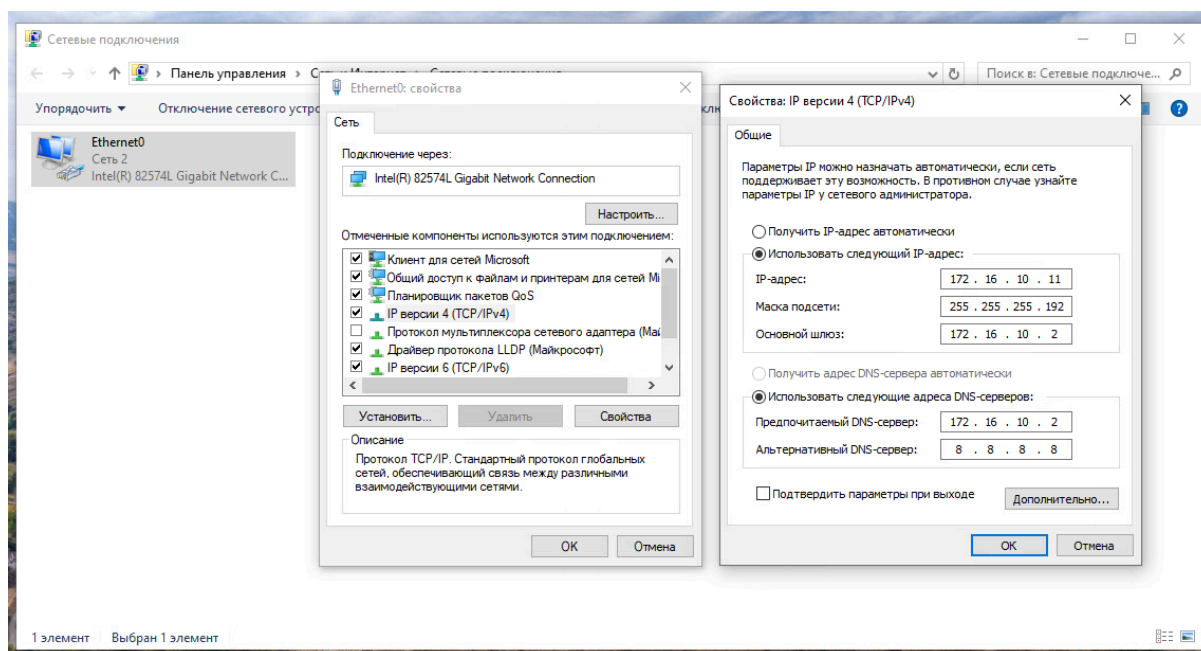
Выбираем Change settings, далее Bridget и выбираем соответствующий адаптер, далее вводим адрес сети и маску. На моих скринах адреса отличаются, потому что настройку выполнял на удаленном сервере, но сути это не меняет. И да, этот шаг необходимо выполнить в первую очередь, до выдачи адреса Юзергейту.

Далее выполним перезагрузку.

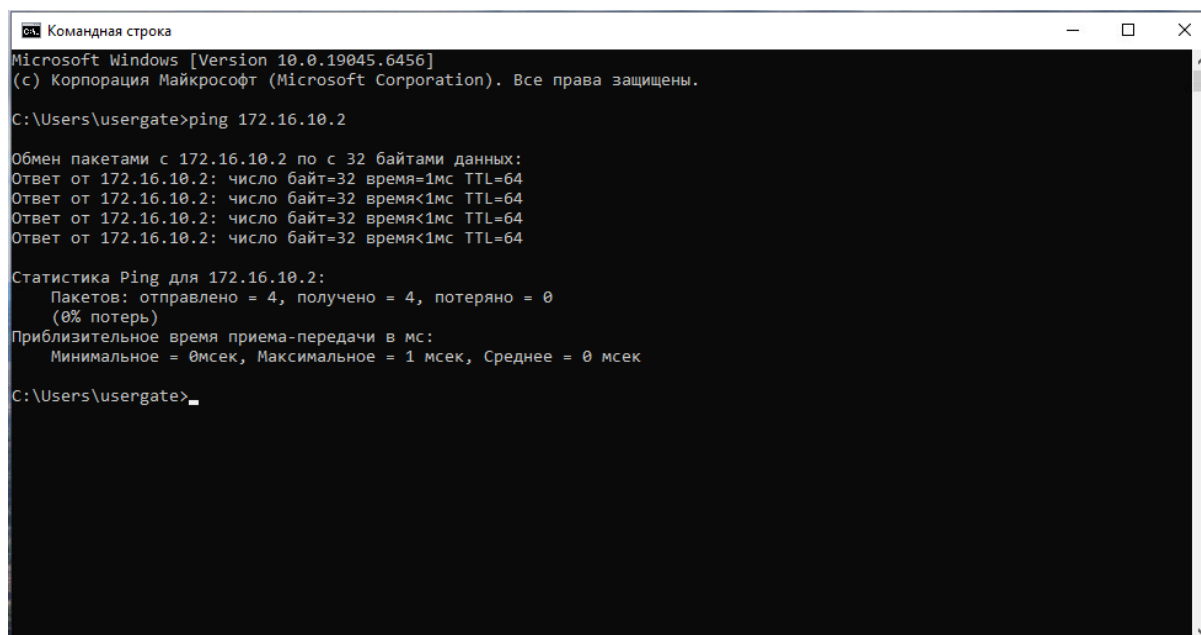
После перезагрузки увидим следующее:

```
UGOS NGFW 7.4.0.209490R
Web-administrator GUI: https://172.16.10.2:8001/
UGOS login:
```

Если все так, то переходим к Виндовой машине, там необходимо ручками задать статический адрес машины, чтобы он был в той же подсети, что и Юзергейт:



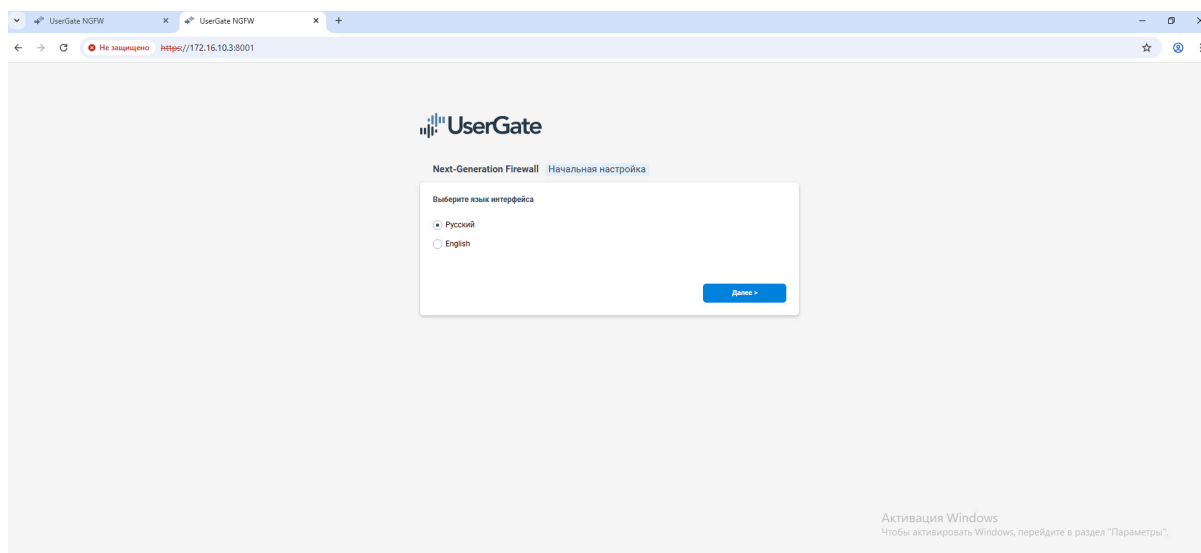
Проверим, что пинги до Юзергейта идут:



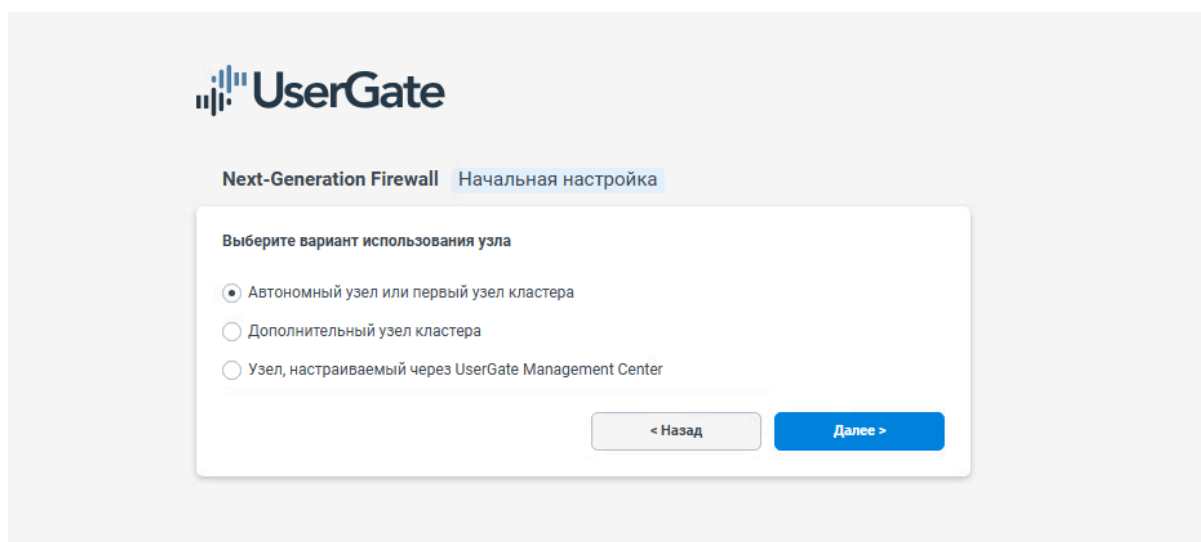
Супер, теперь можем переходить в браузер по адресу:

<https://<ip-usergate>:8001>

Если все сделано верно, то нас встретит окно первоначальной настройки:




Следуем простым шагам, на этапе вариант использования узла выбираем Автономный узел:



Далее придумываем пароль и попадаем в систему.

Далее для доступа юзергейта в Интернет нужно настроить DNS и Шлюз. В качестве шлюза необходимо указать тот, который используется на вашем основном ноутбуке (при условии, что вы используете bridge и ваш основной комп имеет доступ в интернет). Выполним `ipconfig` на основной машине, чтобы узнать необходимые параметры:



Командная строка

Основной шлюз. . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : cloudnetworks.ru  
 Локальный IPv6-адрес канала . . . . : fe80::6fda:474d:ed9e:62bd%15  
 IPv4-адрес. . . . . : 10.63.2.101  
 Маска подсети . . . . . : 255.255.255.128  
 Основной шлюз. . . . . : 10.63.2.1

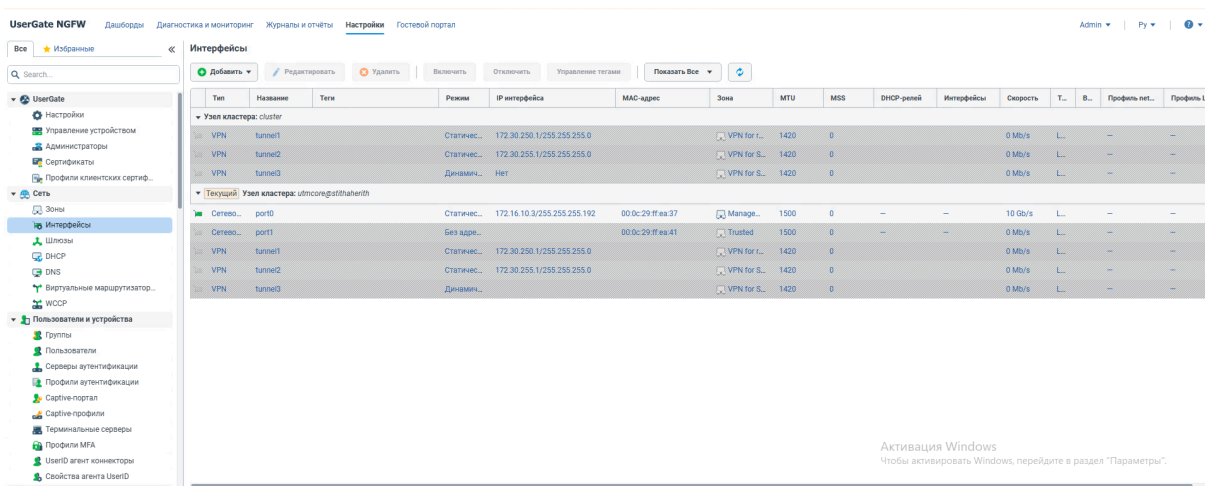
Адаптер Ethernet Сетевое подключение Bluetooth:

Состояние среды. . . . . : Среда передачи недоступна.  
 DNS-суффикс подключения . . . . . :

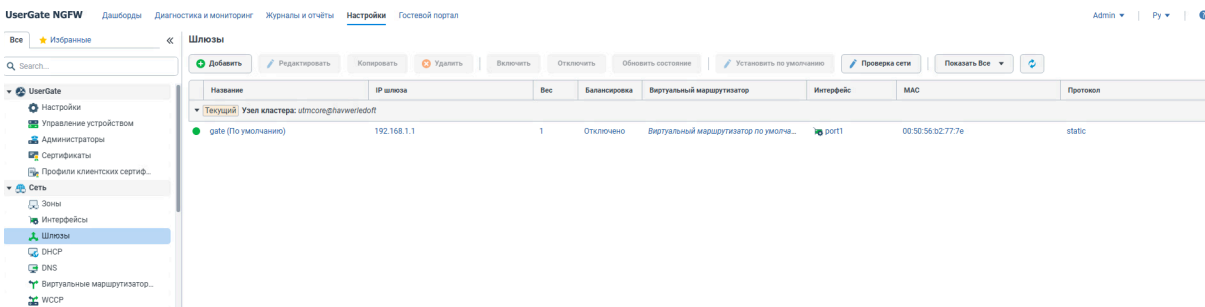
C:\Users\v.chernyj>

В настройках юзергейта необходимо указать данный шлюз и назначить на port1 ip-адрес из той же сети, что и ваш ПК.

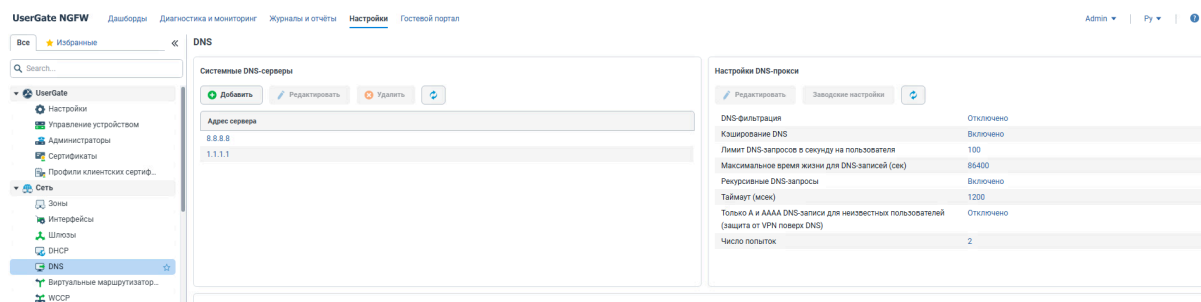
Настройка интерфейсов:



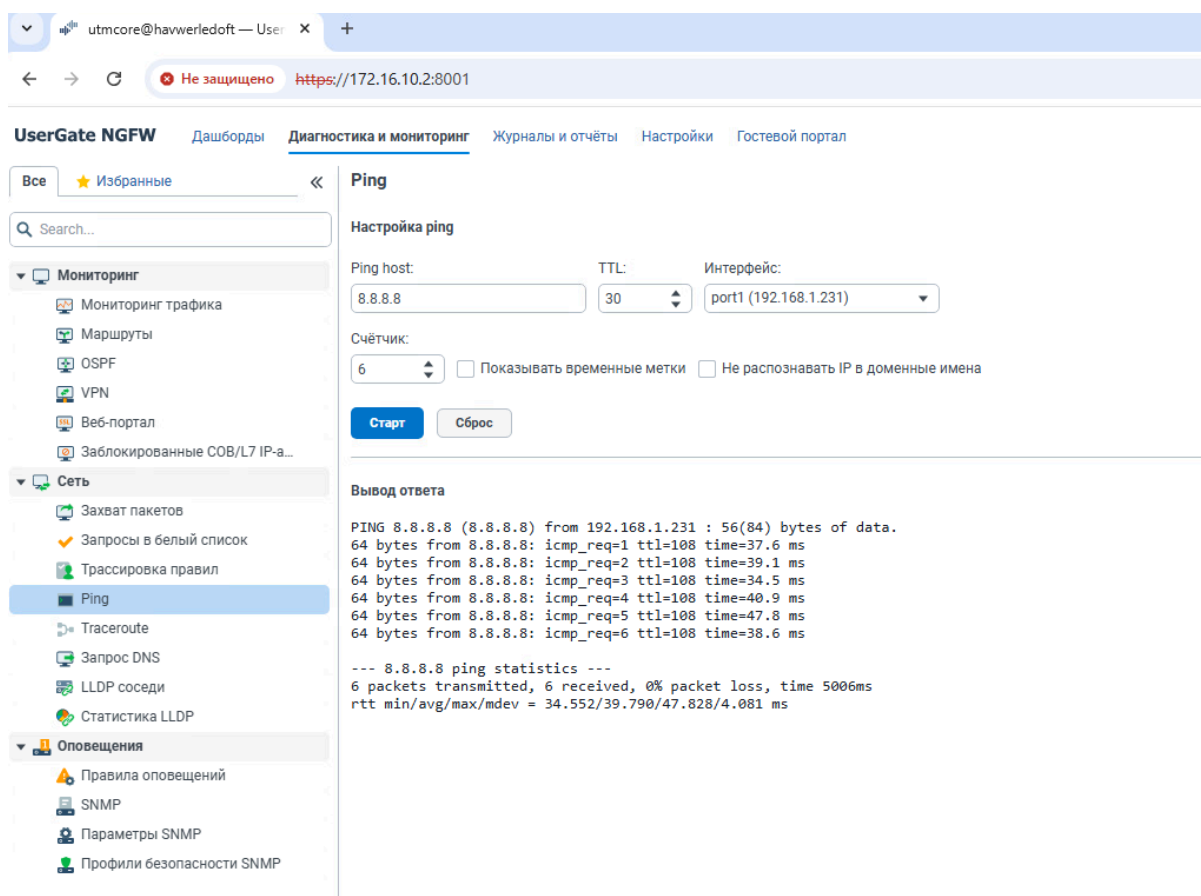
Шлюза:



## DNS:



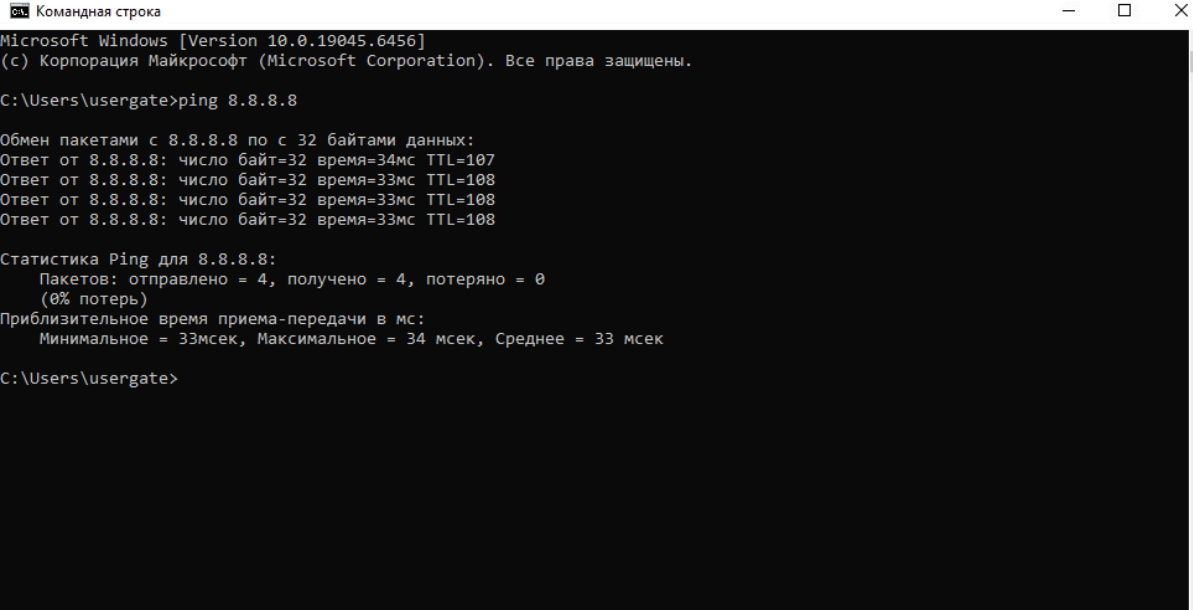
На вкладке Диагностика и мониторинг - Ping, проверьте доступность в Интернет для юзергейта:



Далее необходимо обеспечить клиенту доступ в Интернет, для этого необходимо на юзергейте:

- создать базовое правило NAT;
- создать несколько правил межсетевого экрана - дефолтное запрещающее, которое будет все запрещать и поместить его в самый низ, и правило, которое будет все разрешать, и поместить его наверх.

Проверить доступ в Интернет на клиенте.



```
Командная строка
Microsoft Windows [Version 10.0.19045.6456]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\usergate>ping 8.8.8.8

Обмен пакетами с 8.8.8.8 по 32 байтами данных:
Ответ от 8.8.8.8: число байт=32 время=34мс TTL=107
Ответ от 8.8.8.8: число байт=32 время=33мс TTL=108
Ответ от 8.8.8.8: число байт=32 время=33мс TTL=108
Ответ от 8.8.8.8: число байт=32 время=33мс TTL=108

Статистика Ping для 8.8.8.8:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 33мсек, Максимальное = 34 мсек, Среднее = 33 мсек

C:\Users\usergate>
```

Далее необходимо [замерить скорость интернета](#) на клиенте. Затем искусственно ее замедлить с помощью юзергейта, и сделать повторный замер, сравнить результаты.

Далее создать правило, которое разрешает HTTP/HTTPS подключения, и правило, которое запрещает Any ICMP запросы.

Продемонстрировать результаты.

При сдаче работы быть готовым ответить на вопросы из всего, что вы настраивали, включая: что такое зона? какие зоны бывают? можно ли запретить доступ в интернет по определенному протоколу? и т. п.



\*Задание для получения плюсика:

Необходимо настроить фильтрацию контента и запретить пользователю искать что-либо в поисковике Яндекс. Для этого нужно включить инспекцию SSL, и добавить сертификат CA.der в хранилище корневых доверенных сертификатов на клиенте. Далее необходимо настроить правило для фильтрации контента. Продемонстрировать результат. Ответить на вопросы. Результат должен быть +- таким:

