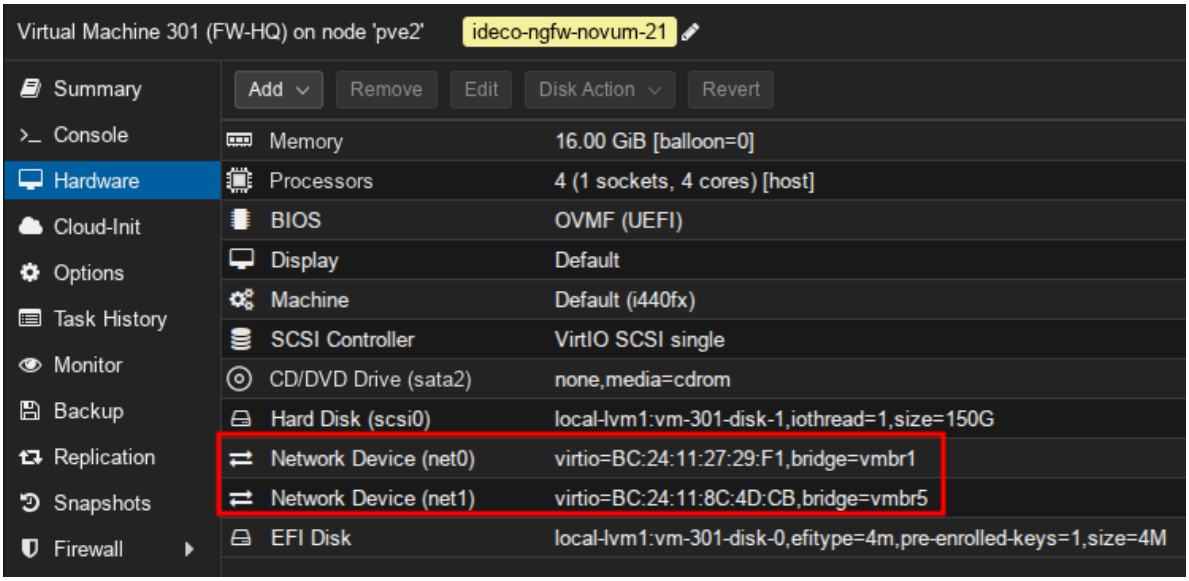
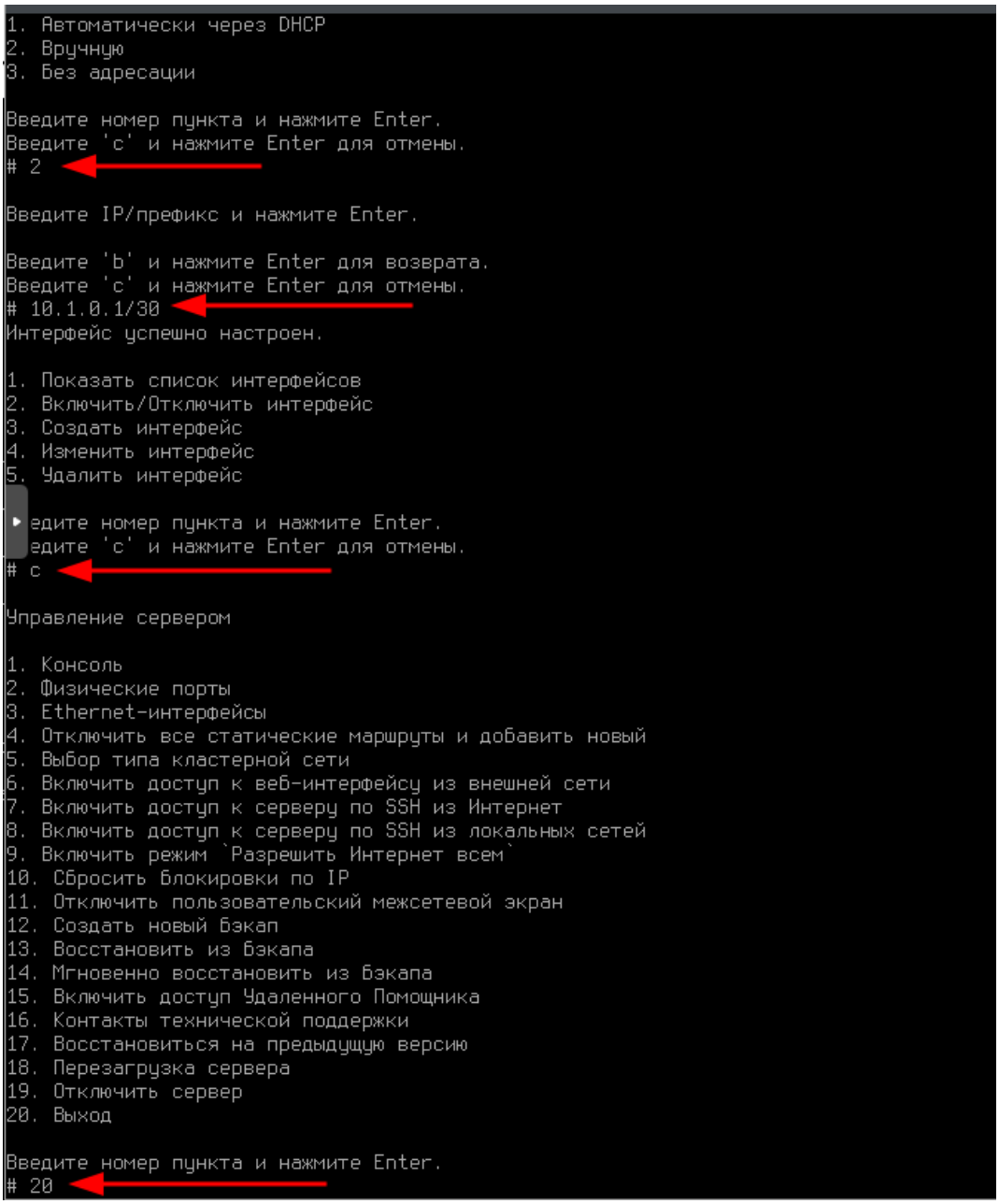
FW-HQ:

- Настройка интерфейса управления, для доступа к веб-интерфейсу с **ADM-HQ**:
  - **vmbr1** - для подключения к провайдеру **ISP**
  - **vmbr5** - для локальной сети (маршрутизация между VLAN)

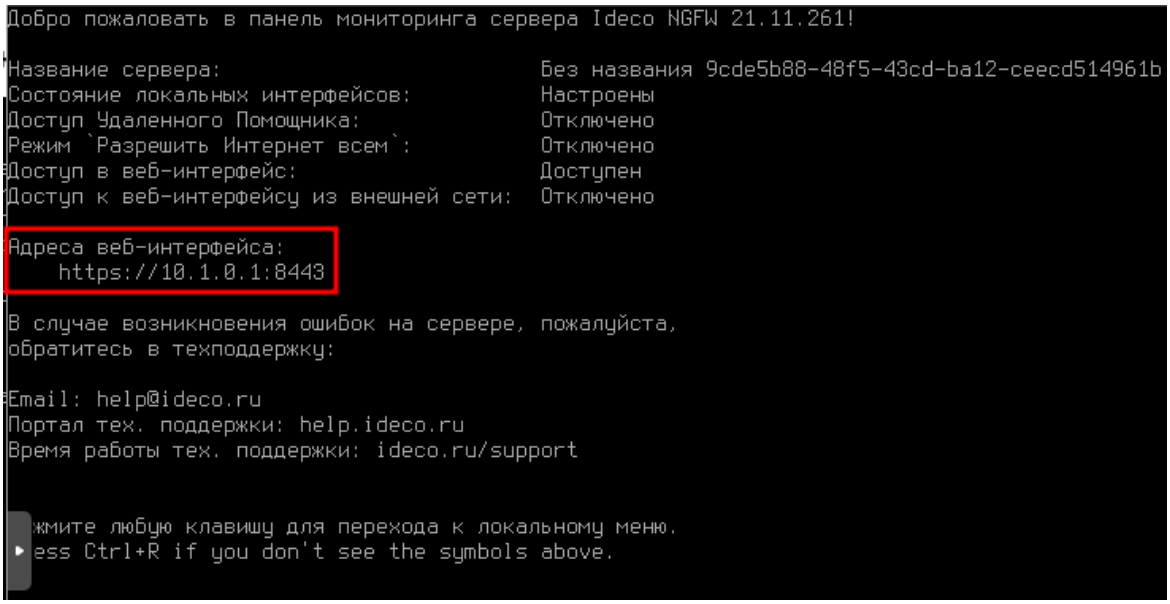


- Создаём **Ethernet-интерфейс** с именем **mgmt** и задаём IP-адрес из произвольной сети:

```
Введите номер пункта и нажмите Enter.
# 3

1. Показать список интерфейсов
2. Включить/Отключить интерфейс
3. Создать интерфейс
4. Изменить интерфейс
5. Удалить интерфейс

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 3

Выберите порт:

-------------------------------------------------------------------------------------------------
  N    |  Порт     |  MAC-адрес          |  Назначение    |  Производитель сетевой карты
-------------------------------------------------------------------------------------------------
  1    |  eth0_f1  |  bc:24:11:27:29:f1  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------
  2    |  eth1_cb  |  bc:24:11:8c:4d:cb  |  Сервис        |  Red Hat, Inc. Virtio network device
-------------------------------------------------------------------------------------------------

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2

Введите имя интерфейса (или оставьте пустым) и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# mgmt

Выберите роль для интерфейса:

1. CP
2. LAN
3. WAN

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2

Выберите VCE:

1. Системный контекст

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 1
```

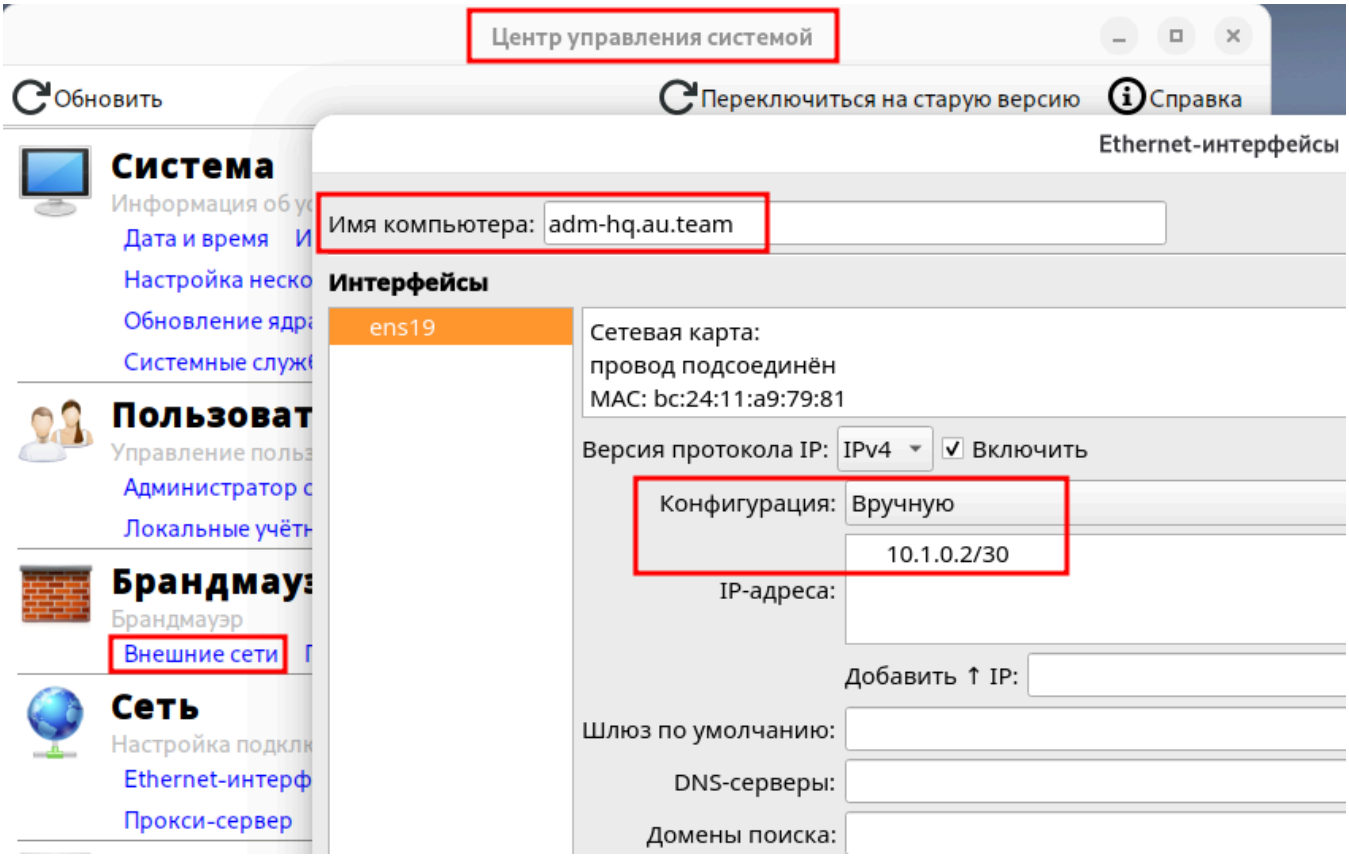

1. Автоматически через DHCP
2. Вручную
3. Без адресации
Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
2
Введите IP/префикс и нажмите Enter.
Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
10.1.0.1/30
Интерфейс успешно настроен.
1. Показать список интерфейсов
2. Включить/Отключить интерфейс
3. Создать интерфейс
4. Изменить интерфейс
5. Удалить интерфейс
едите номер пункта и нажмите Enter.
едите 'c' и нажмите Enter для отмены.
c
Управление сервером
1. Консоль
2. Физические порты
3. Ethernet-интерфейсы
4. Отключить все статические маршруты и добавить новый
5. Выбор типа кластерной сети
6. Включить доступ к веб-интерфейсу из внешней сети
7. Включить доступ к серверу по SSH из Интернет
8. Включить доступ к серверу по SSH из локальных сетей
9. Включить режим `Разрешить Интернет всем`
10. Сбросить блокировки по IP
11. Отключить пользовательский межсетевой экран
12. Создать новый бэкап
13. Восстановить из бэкапа
14. Мгновенно восстановить из бэкапа
15. Включить доступ Удаленного Помощника
16. Контакты технической поддержки
17. Восстановиться на предыдущую версию
18. Перезагрузка сервера
19. Отключить сервер
20. Выход
Введите номер пункта и нажмите Enter.
20

- Результат:

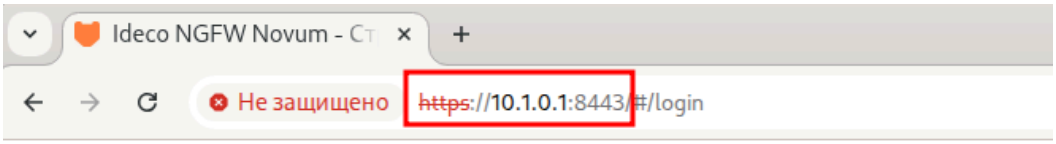

Добро пожаловать в панель мониторинга сервера Ideco NGFW 21.11.261!
Название сервера: Без названия 9cde5b88-48f5-43cd-ba12-ceecd514961b
Состояние локальных интерфейсов: Настроены
Доступ Удаленного Помощника: Отключено
Режим `Разрешить Интернет всем`: Отключено
Доступ в веб-интерфейс: Доступен
Доступ к веб-интерфейсу из внешней сети: Отключено
Адреса веб-интерфейса:
https://10.1.0.1:8443
В случае возникновения ошибок на сервере, пожалуйста,
обратитесь в техподдержку:
Email: help@ideco.ru
Портал тех. поддержки: help.ideco.ru
Время работы тех. поддержки: ideco.ru/support
жмите любую клавишу для перехода к локальному меню.
ess Ctrl+R if you don't see the symbols above.

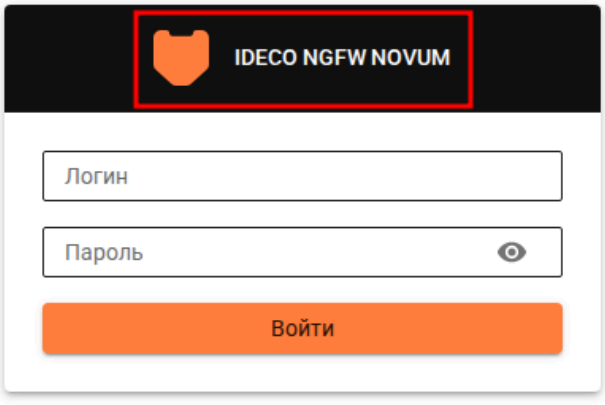
ADM-PC:

- Назначаем имя на устройство в формате FQDN (au.team)
- Назначаем IP-адрес из той же сети что и **FW-HQ**

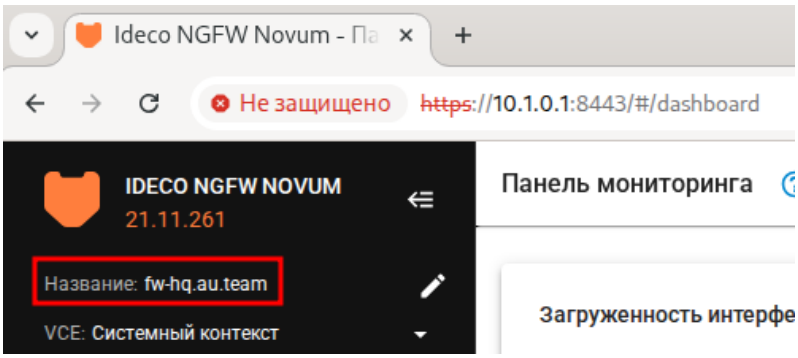


- Переходим в веб-интерфейс управления **FW-HQ**, обращаясь по **https://10.1.0.1:8443**:

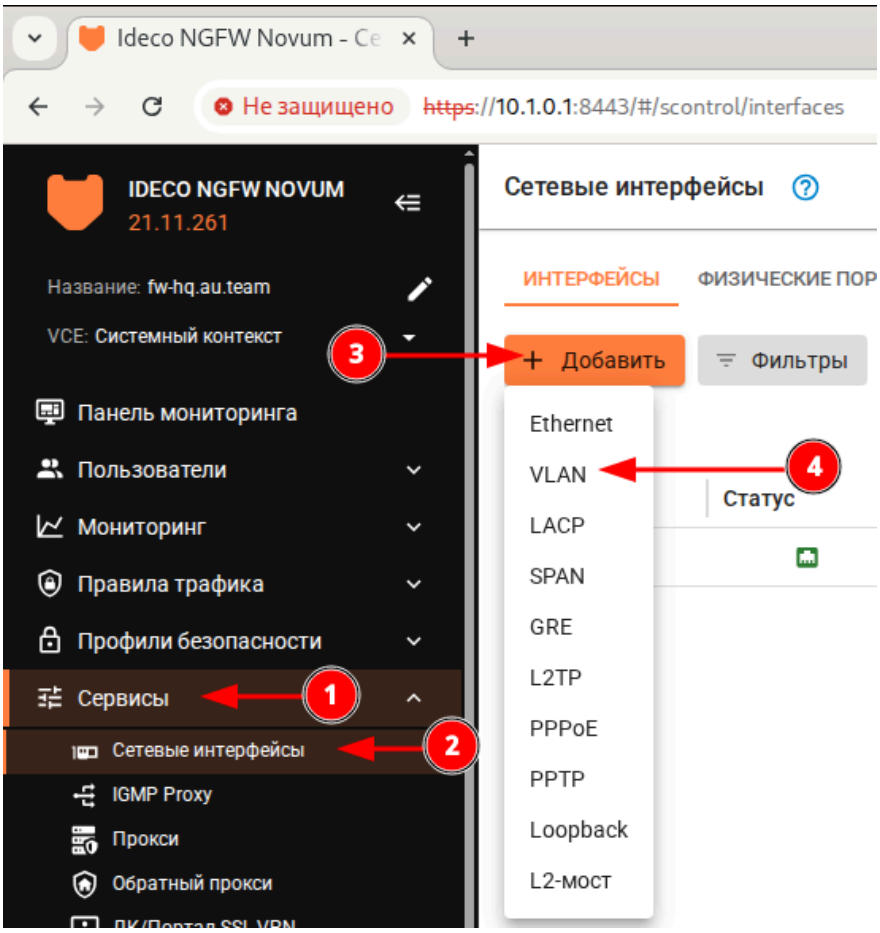




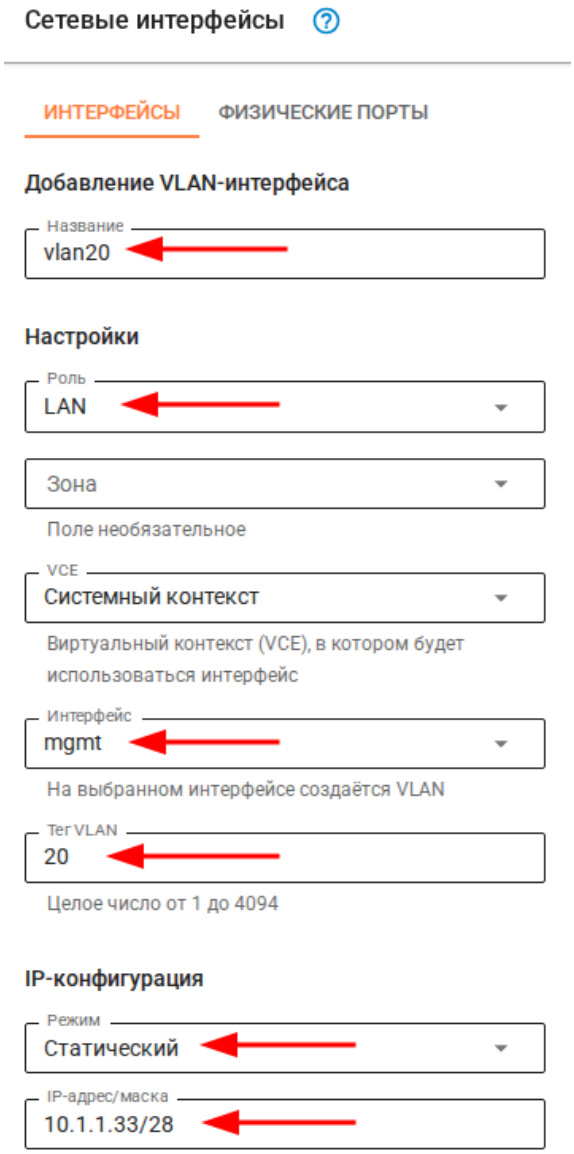
- Назначаем имя на устройство в формате FQDN (au.team)



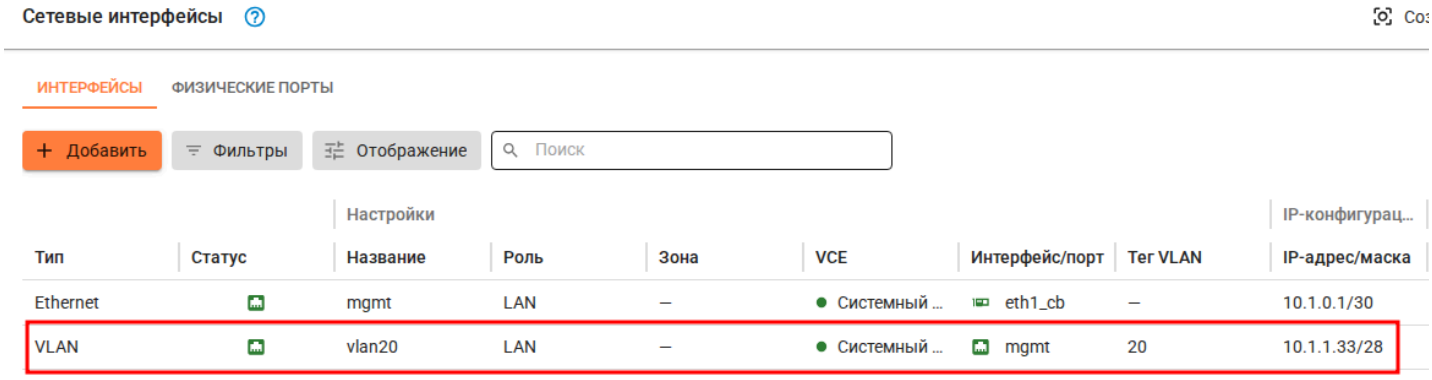
- Создаём VLAN интерфейс на основе физического и указываем VID и IP-адрес в соответствии с L2 и L3:



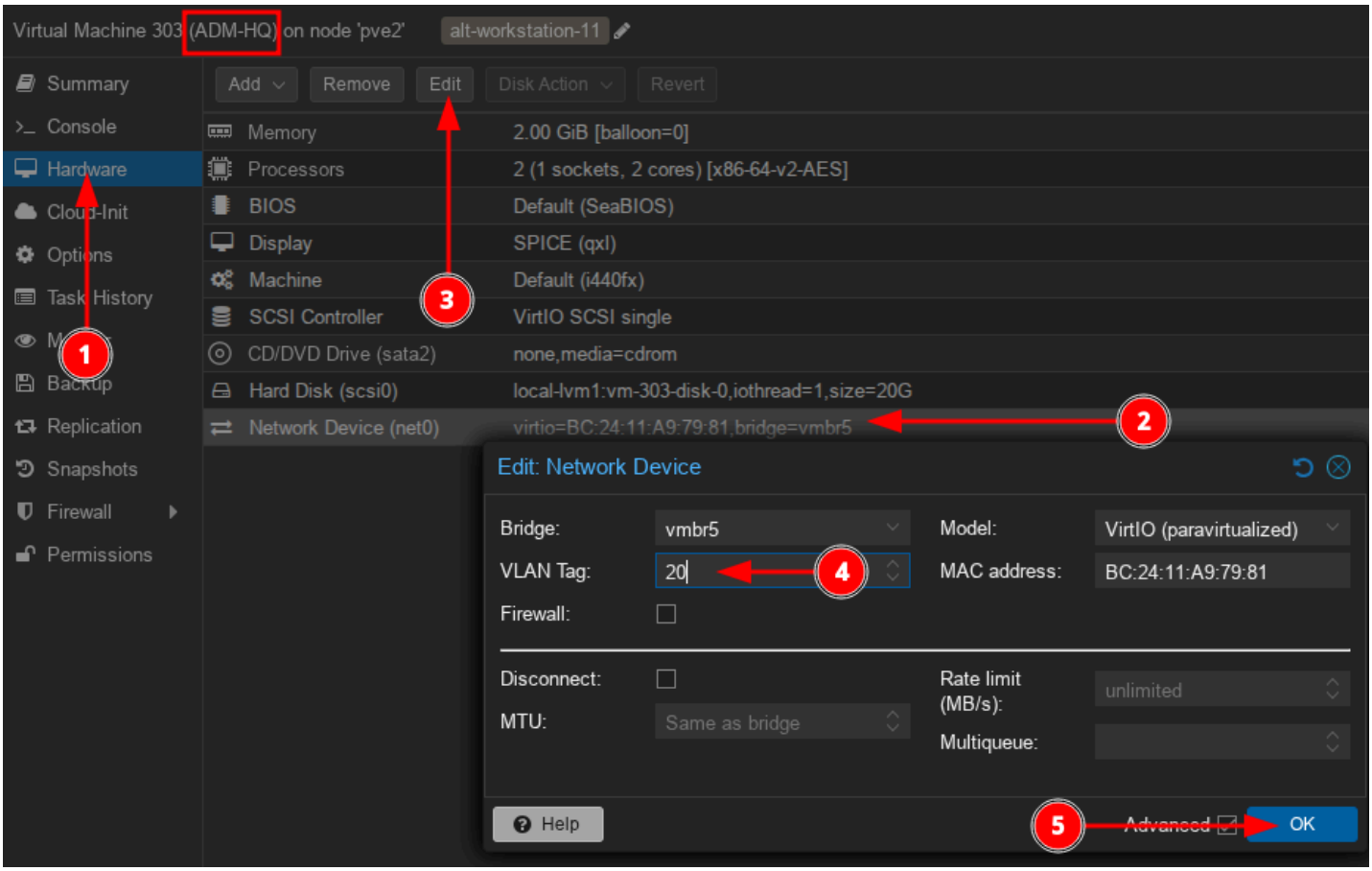
  - заполняем форму создания **VLAN** интерфейса



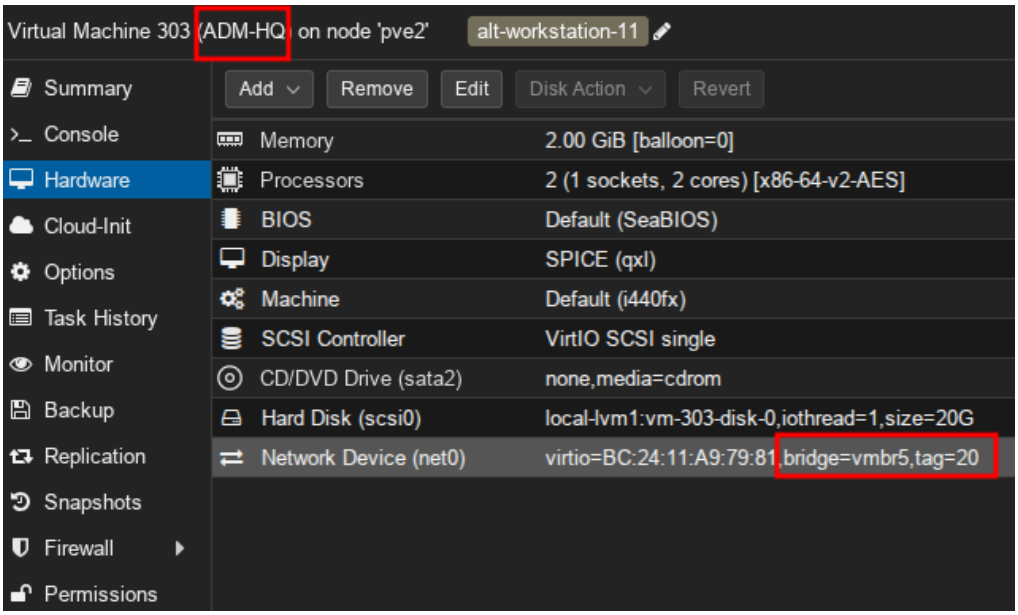
- Результат:



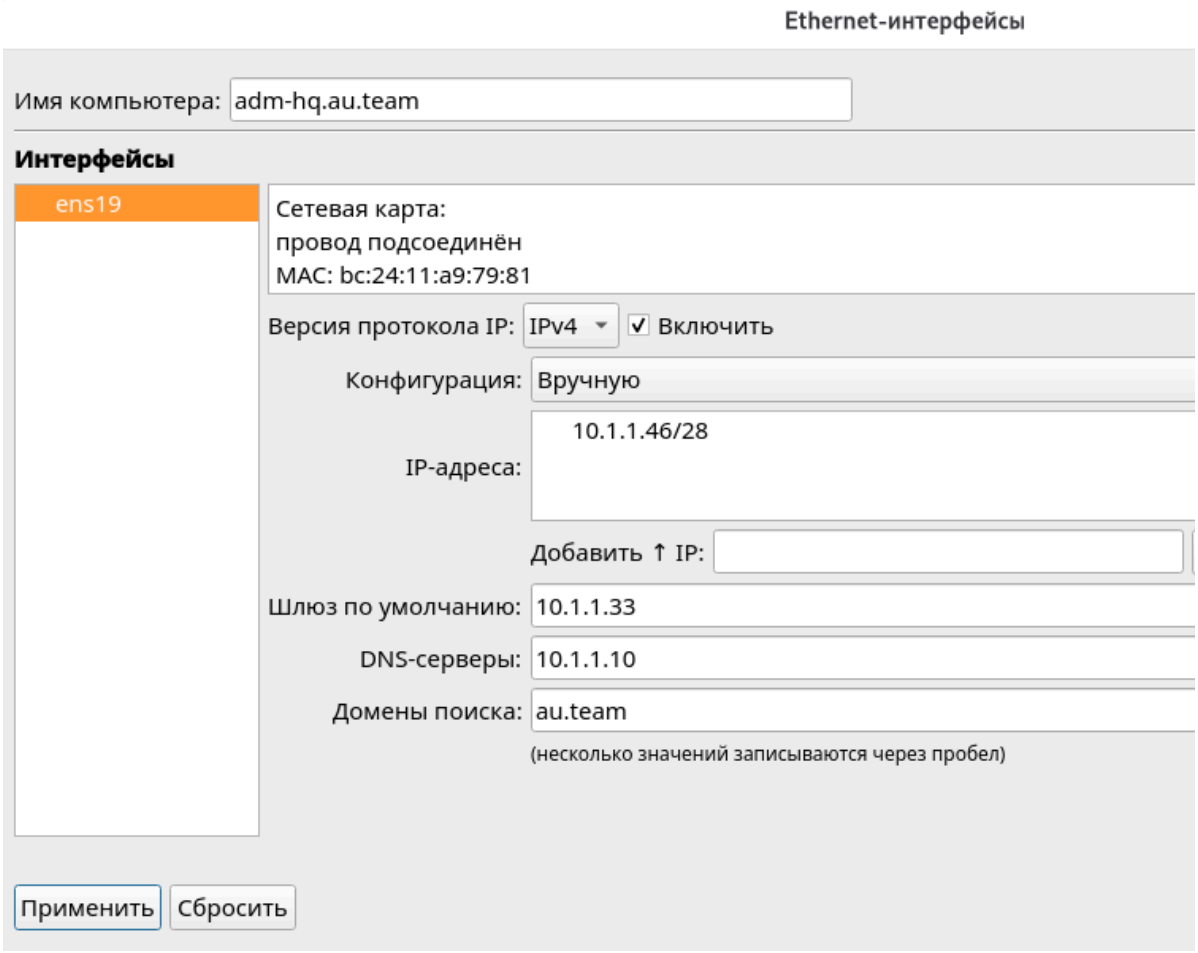
- Выполняем коммутацию для **ADM-HQ** в соответствие с L2:



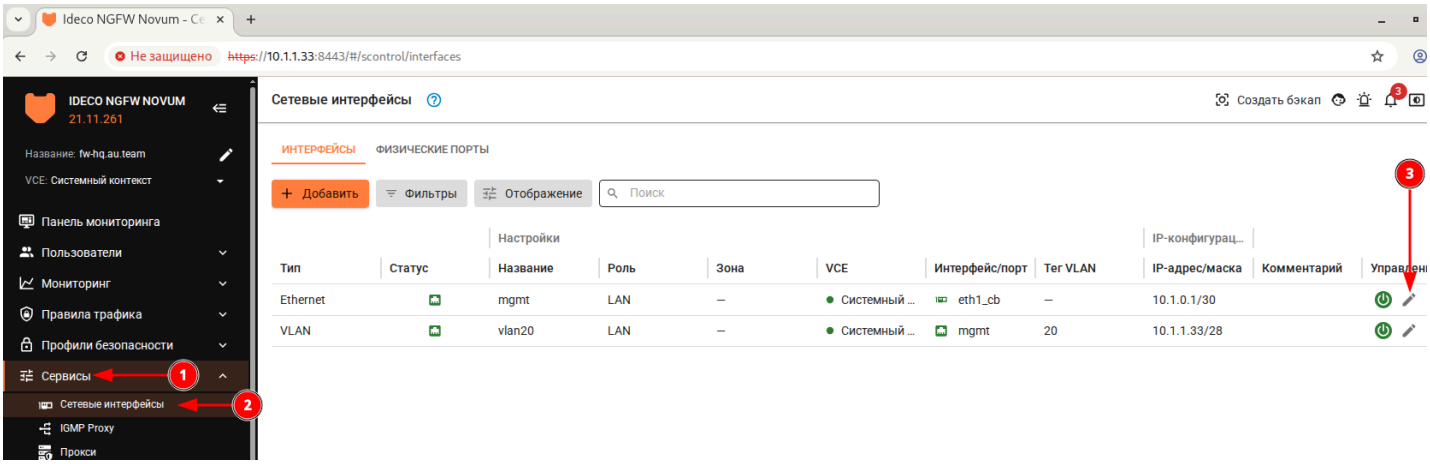
- Результат:

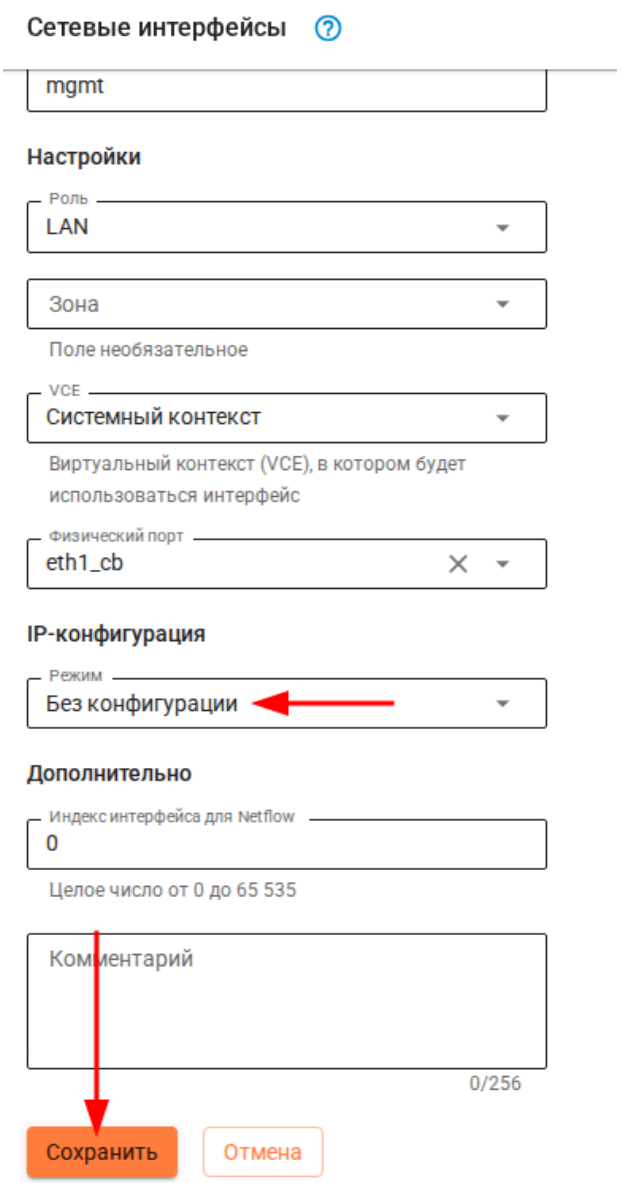


- Перенастраиваем IP-адрес на интерфейсе для **ADM-HQ** в соответствие с L3:

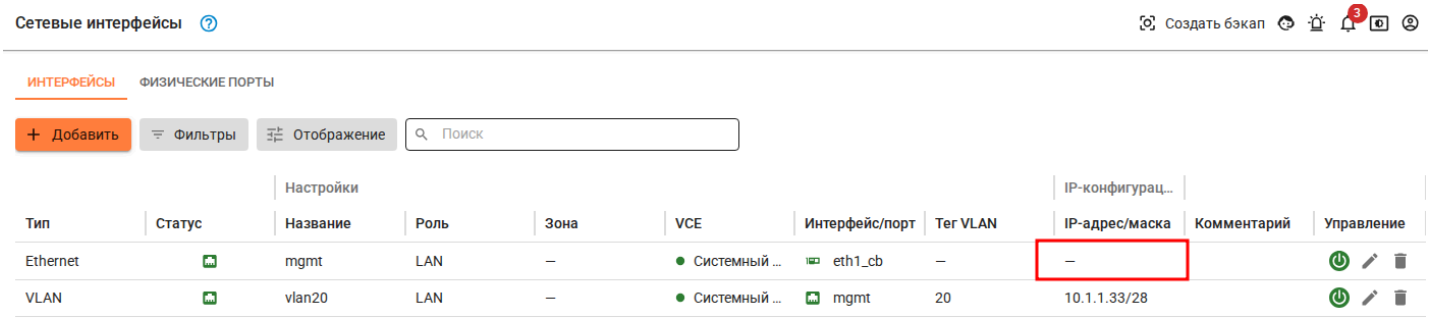


- Теперь доступ в веб-интерфейс управления **FW-HQ**, обращаясь по **https://10.1.1.33:8443**
  - выполняем вход и удаляем IP-адрес с интерфейса **mgmt**
  - НО не удаляем сам интерфейс!

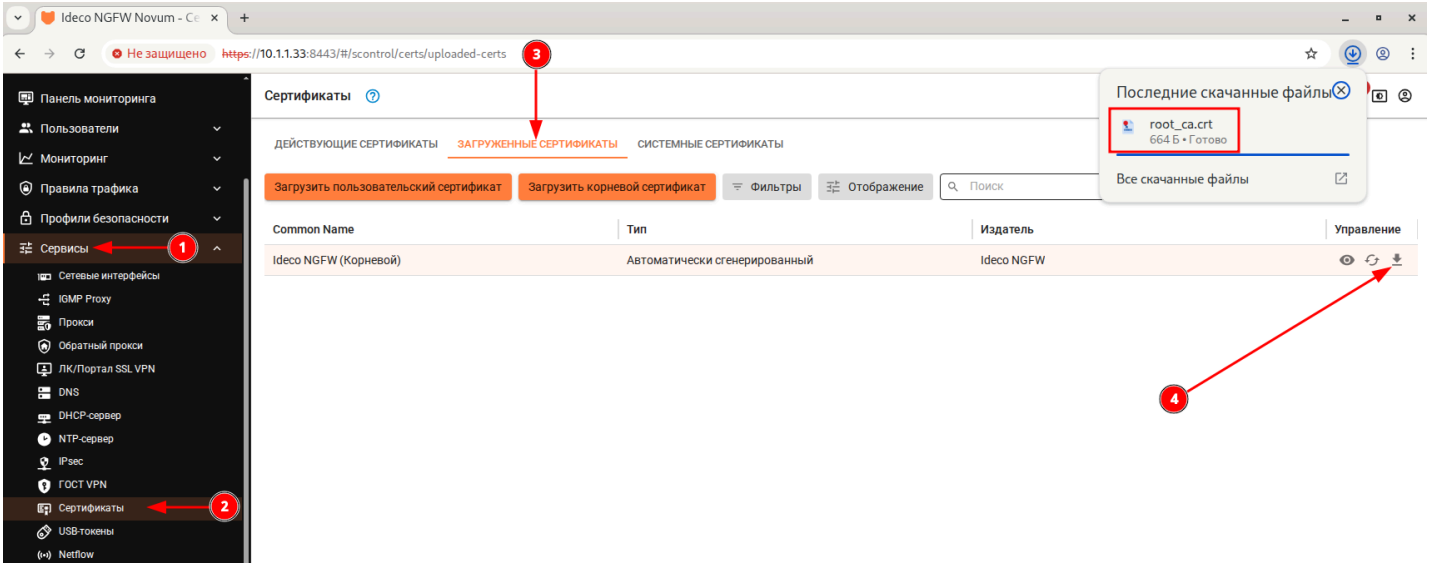




- Результат:
  - теперь есть соответствие как L2, так и L3



- Скачаем корневой сертификат:

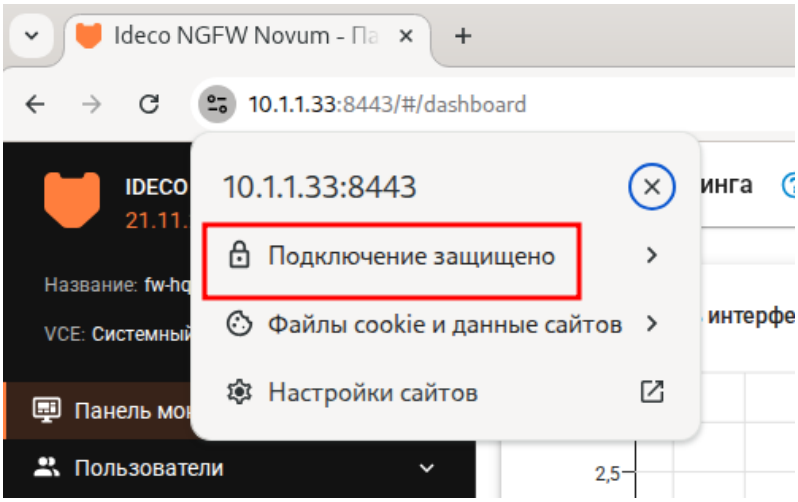


- Добавим в хранилище для **ADM-HQ**:

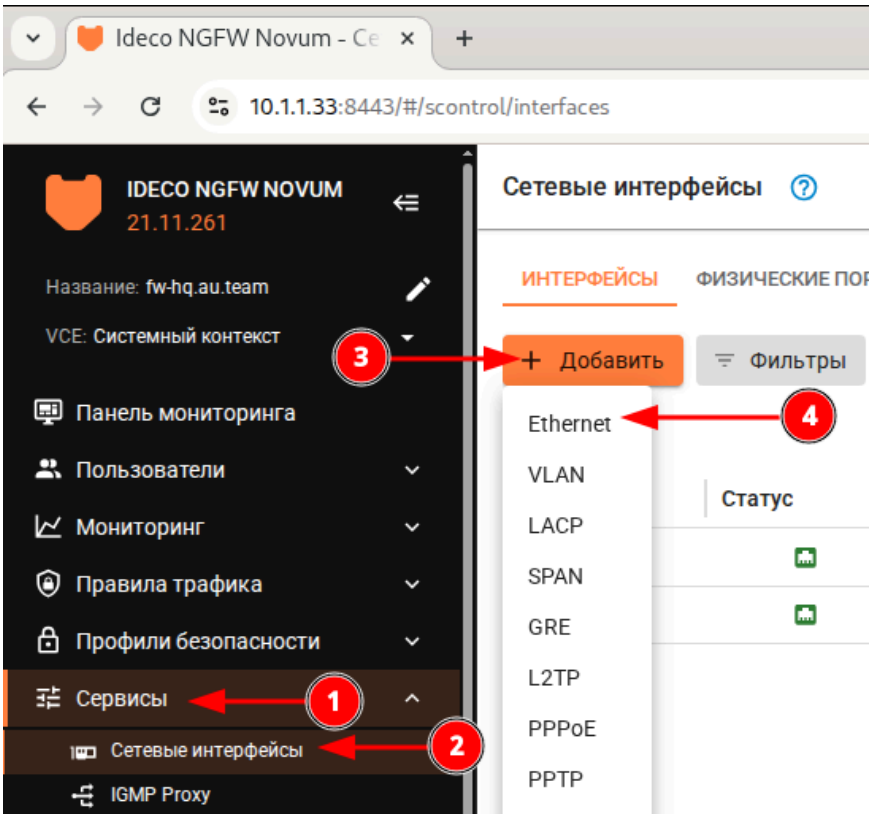
```
su -
```

```
mv /home/user/Загрузки/root_ca.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

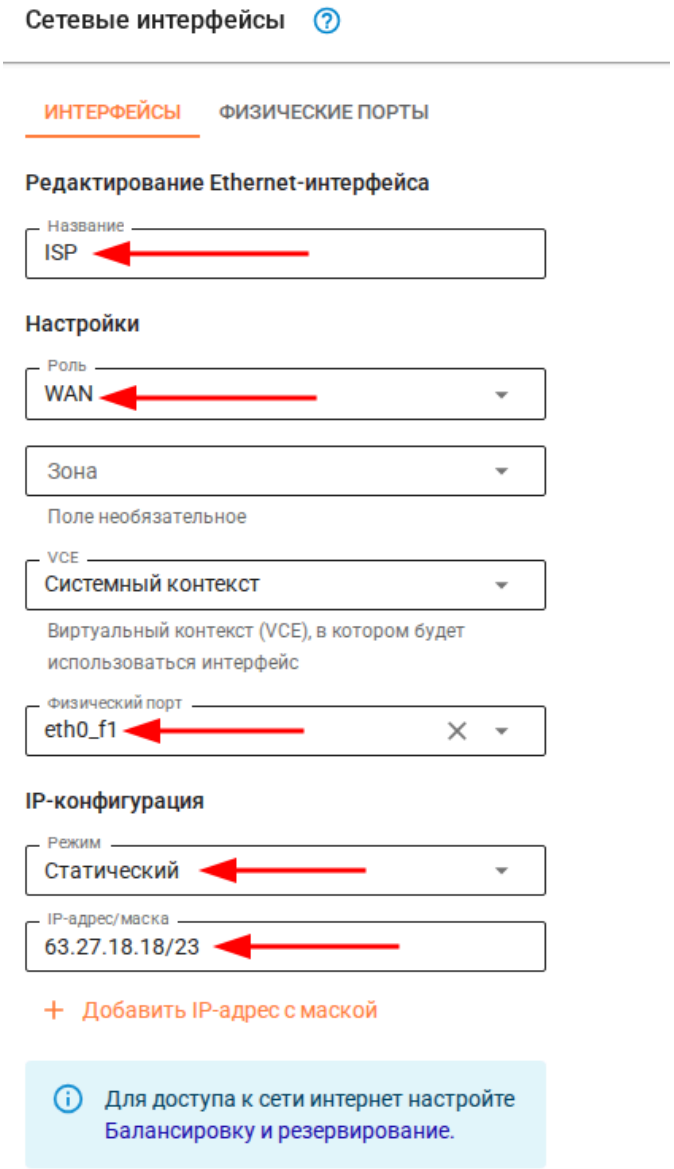
- Результат:
  - предварительно закрыть браузер и открыть по новой



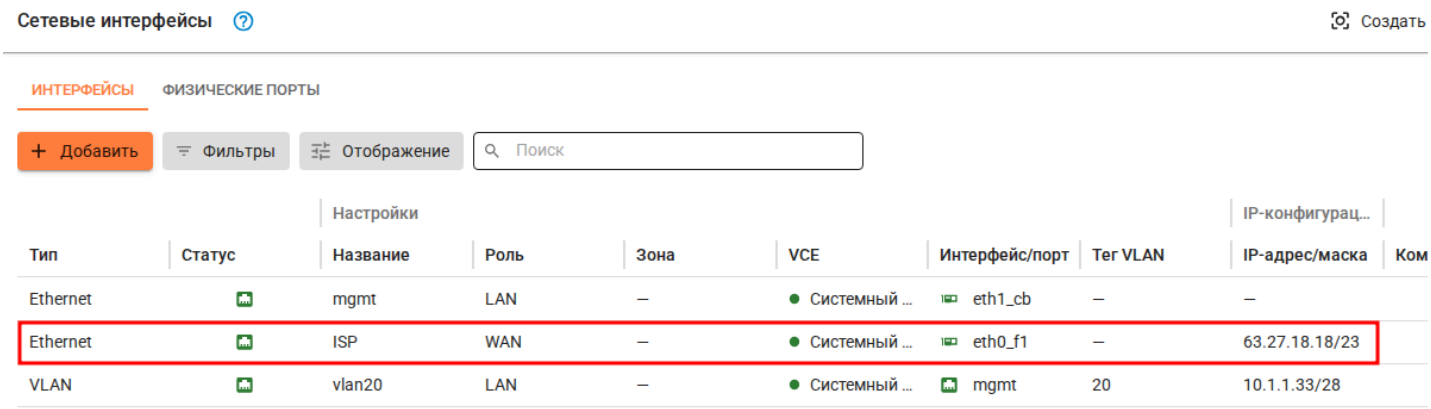
- Выполним добавление Ethernet-интерфейса с ролью WAN
  - для подключения к **ISP** в соответствие с L3



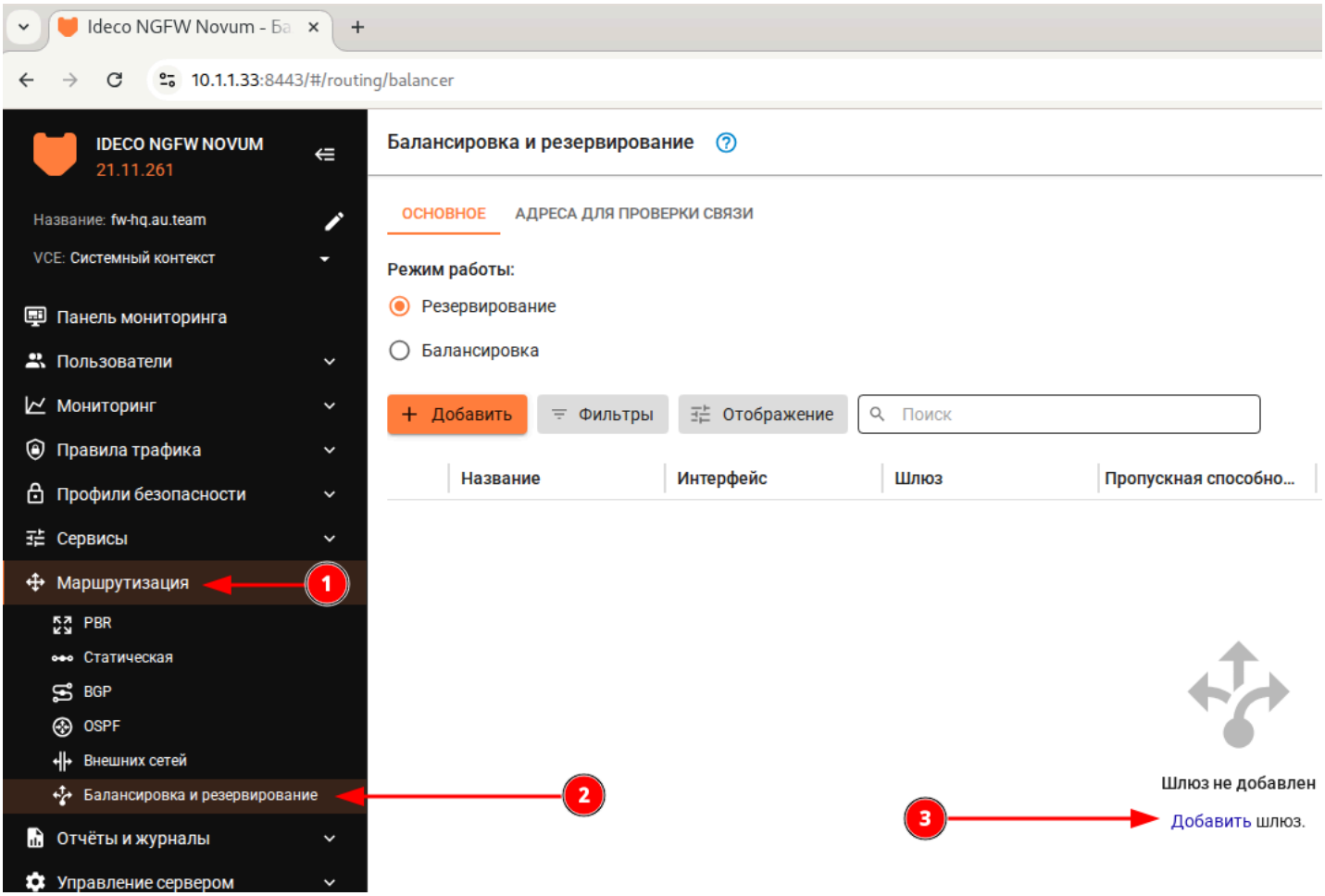
- заполняем форму по добавлению **Ethernet** интерфейса



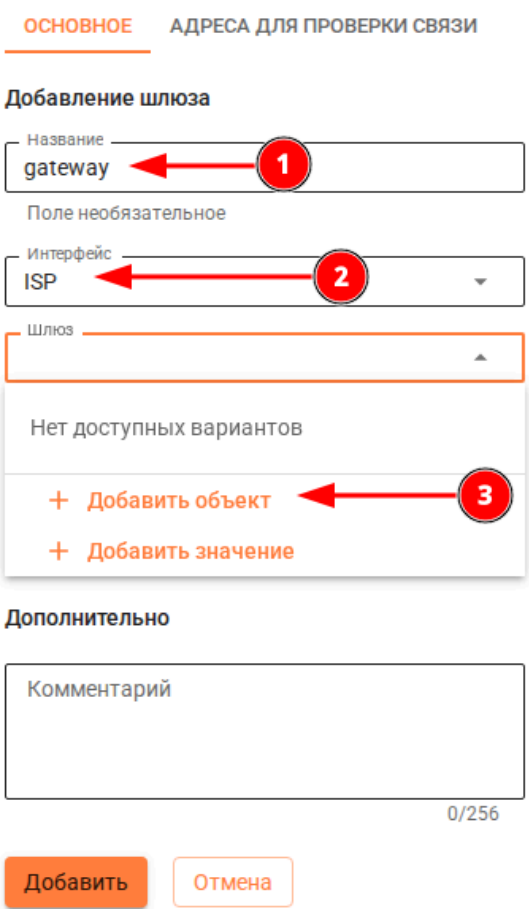
- Результат:



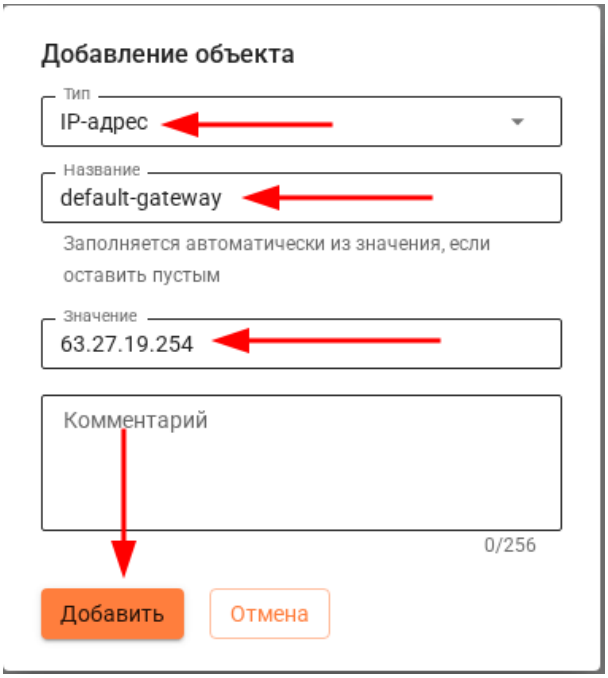
- Для доступа к сети интернет нужно настроить **Балансировку и резервирование**:



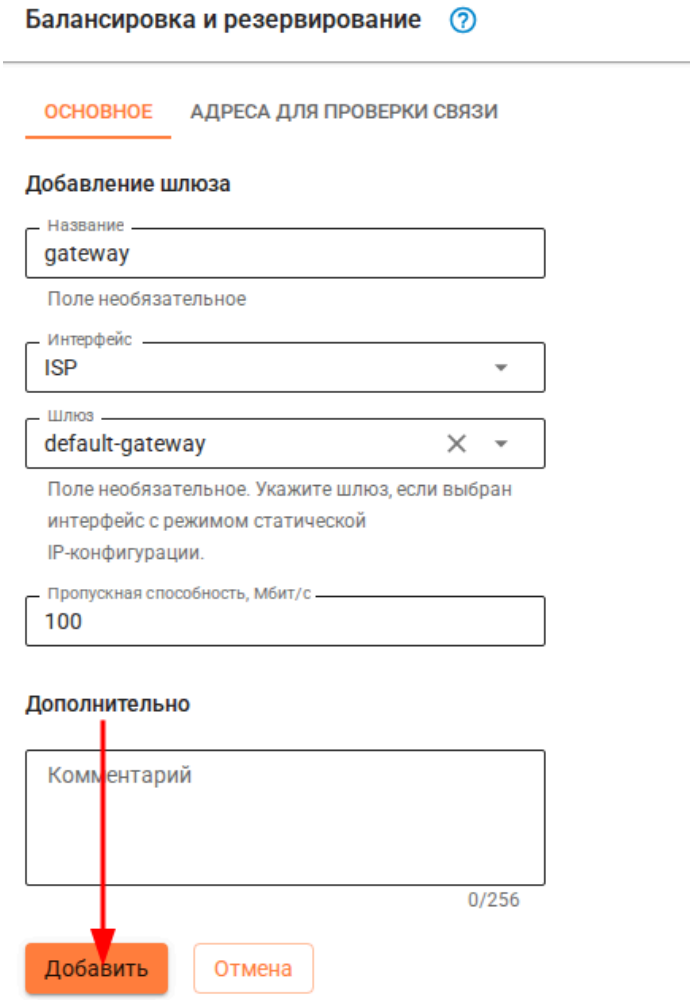
  - заполняем форму **Добавление шлюза**



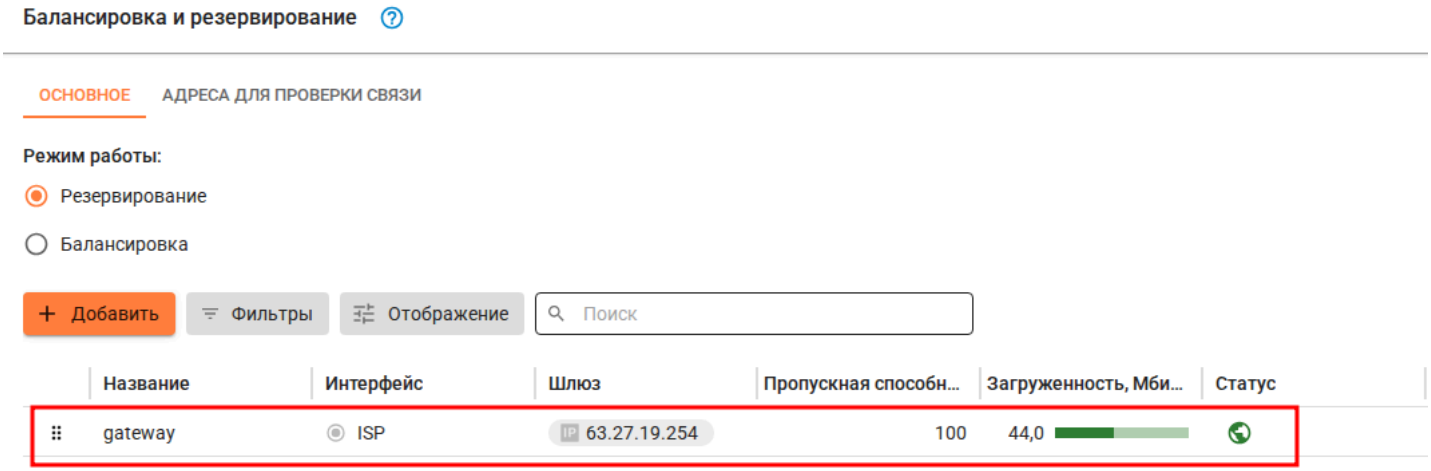
- добавляем объект типа **IP-адрес** и указываем значение IP-адрес, который будет использоваться в качестве шлюза



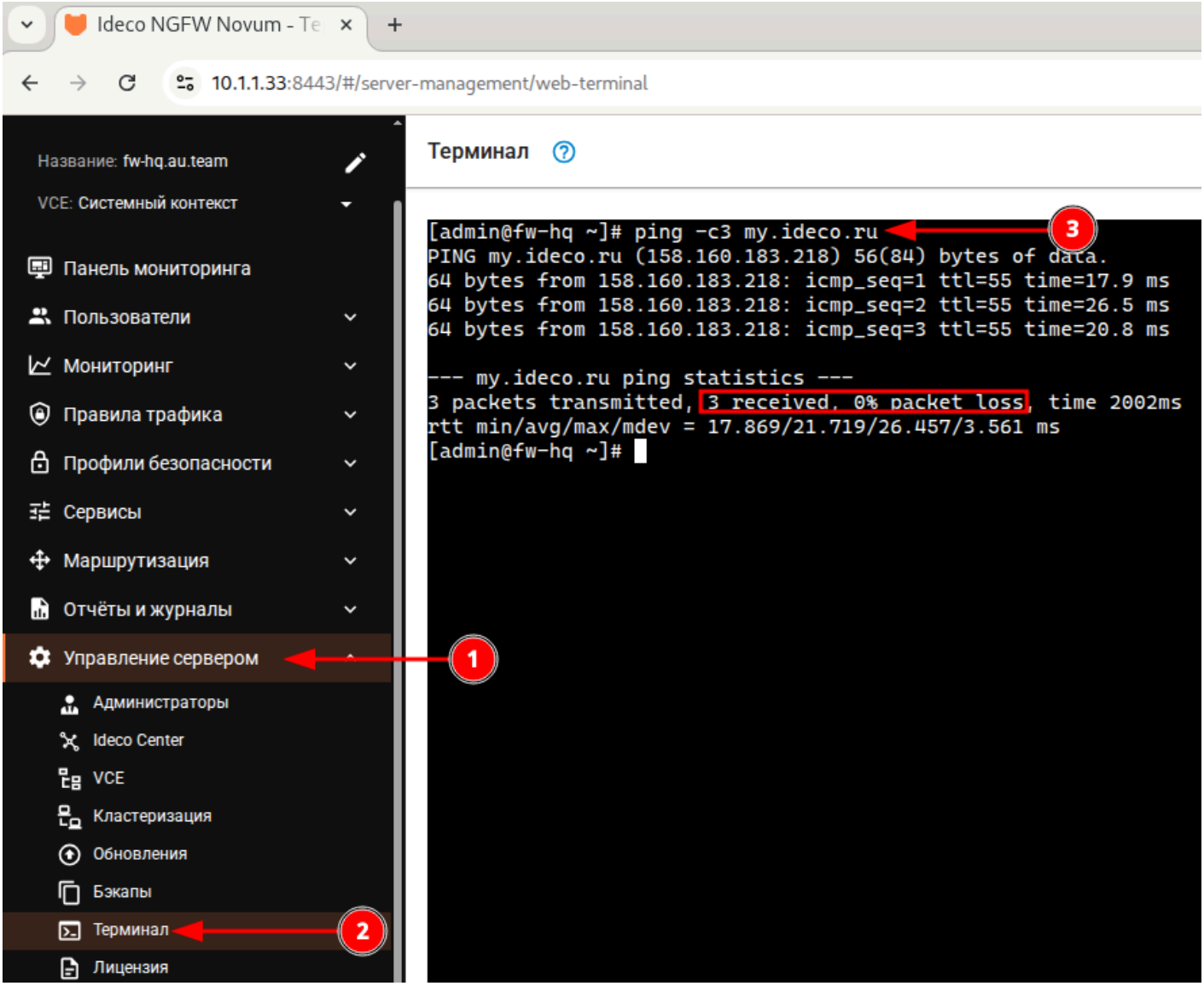
- нажимаем **Добавить**



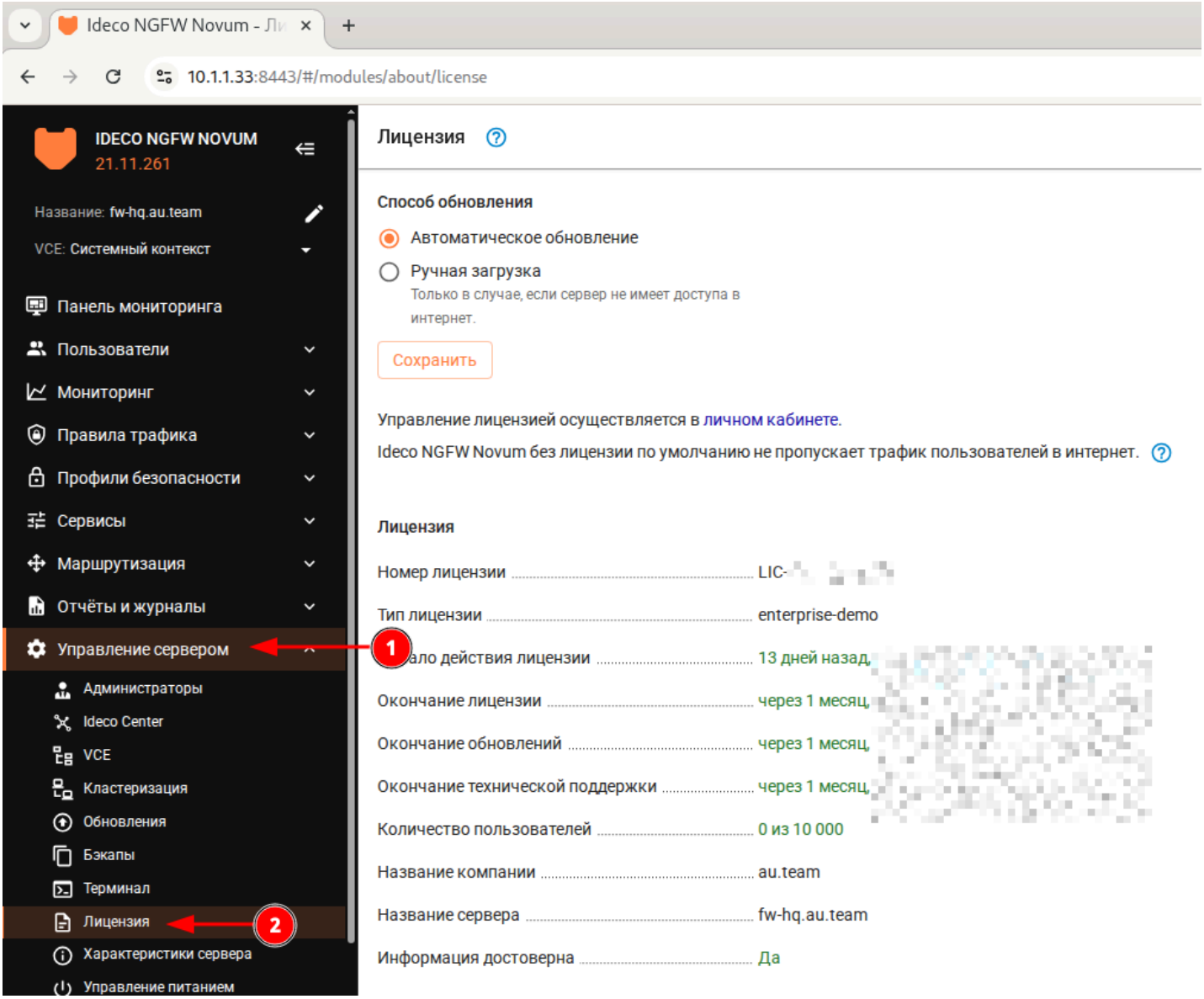
- Результат:



- Проверить доступ в сеть Интернет:



- Проверить наличие лицензии:



- Создать все необходимые VLAN в соответствие с L2 и L3 аналогично как для vlan 20
  - ожидаемый результат

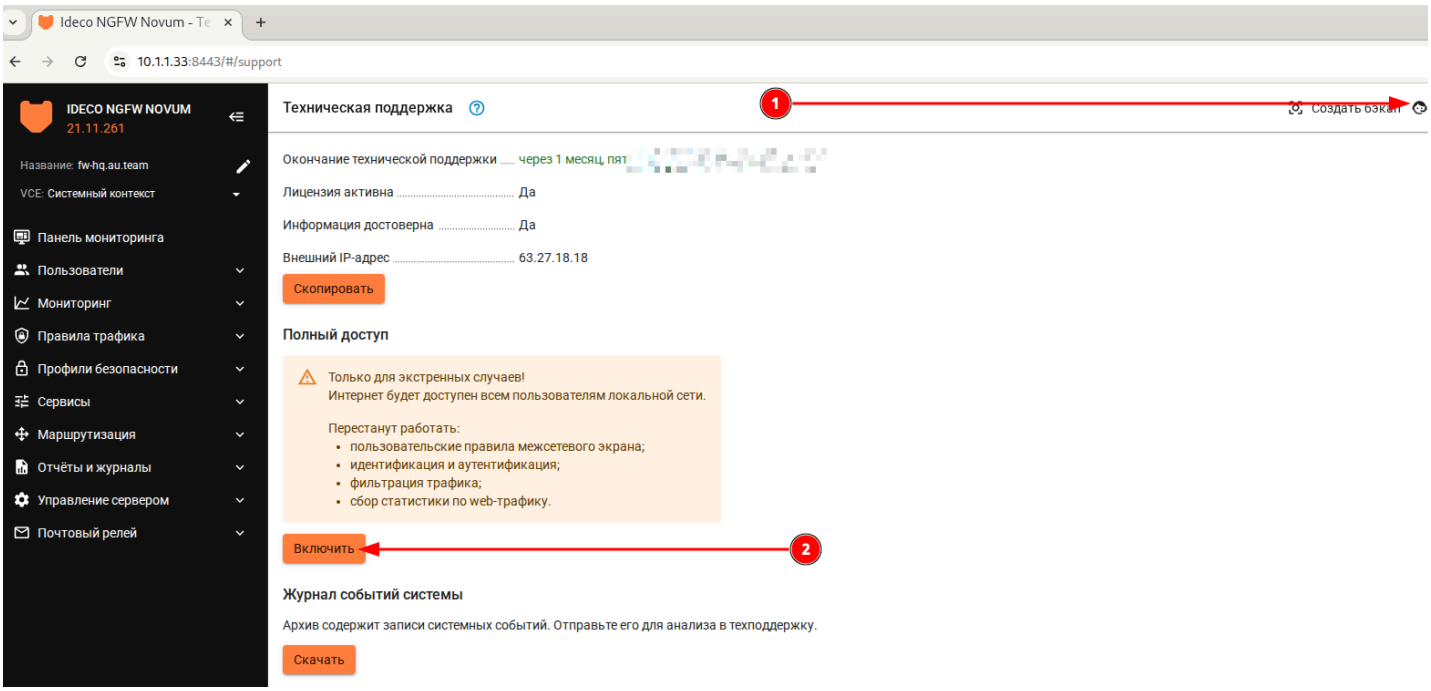
Сетевые интерфейсы

ИНТЕРФЕЙСЫ | ФИЗИЧЕСКИЕ ПОРТЫ

+ Добавить | Фильтры | Отображение | Поиск

		Настройки						IP-конфигурац...
Тип	Статус	Название	Роль	Зона	VCE	Интерфейс/порт	Тег VLAN	IP-адрес/маска
Ethernet		ISP	WAN	–	Системный ...	eth0_f1	–	63.27.18.18/23
Ethernet		mgmt	LAN	–	Системный ...	eth1_cb	–	–
VLAN		vlan10	LAN	–	Системный ...	mgmt	10	10.1.1.1/27
VLAN		vlan20	LAN	–	Системный ...	mgmt	20	10.1.1.33/28
VLAN		vlan30	LAN	–	Системный ...	mgmt	30	10.1.2.1/24

- Так как авторизация по требованию задания подразумевается из-под доменных пользователей
  - временно включим режим "Разрешить интернет всем"
  - для установки и развёртывания домена FreeIPA на SRV-HQ



- Проверить доступ в сеть Интернет:

```
[user@adm-hq ~]$ ping -c3 77.88.8.8
PING 77.88.8.8 (77.88.8.8) 56(84) bytes of data.
64 bytes from 77.88.8.8: icmp_seq=1 ttl=54 time=27.9 ms
64 bytes from 77.88.8.8: icmp_seq=2 ttl=54 time=25.7 ms
64 bytes from 77.88.8.8: icmp_seq=3 ttl=54 time=24.9 ms

--- 77.88.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 24.856/26.137/27.853/1.261 ms
```

- Также стоит отключить перехват пользовательских запросов DNS: