

## 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)

Virtual Machine 301 (FW-HQ) on node 'pve2' ideco-ngfw-novum-21

|              |                       |   |      |             |        |
|--------------|-----------------------|---|------|-------------|--------|
| Summary      | Add                   | Remove  | Edit | Disk Action | Revert |
| Console      | Memory                | 16.00 GiB [balloon=0]   |      |             |        |
| Hardware     | Processors            | 4 (1 sockets, 4 cores) [host]                                   |      |             |        |
| Cloud-Init   | BIOS                  | OVMF (UEFI)   |      |             |        |
| Options      | Display               | Default   |      |             |        |
| Task History | Machine               | Default (i440fx)  |      |             |        |
| Monitor      | SCSI Controller       | VirtIO SCSI single  |      |             |        |
| Backup       | CD/DVD Drive (sata2)  | none,media=cdrom  |      |             |        |
| Replication  | Hard Disk (scsi0)     | local-lvm1:vm-301-disk-1,iothread=1,size=150G                   |      |             |        |
| Snapshots    | Network Device (net0) | virtio=BC:24:11:27:29:F1,bridge=vmbr1                           |      |             |        |
| Firewall     | Network Device (net1) | virtio=BC:24:11:8C:4D:CB,bridge=vmbr5                           |      |             |        |
|              | EFI Disk              | local-lvm1:vm-301-disk-0,efitype=4m,pre-enrolled-keys=1,size=4M |      |             |        |

- 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 'с' 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 'с' и нажмите Enter для отмены.

# 2

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

Введите 'b' и нажмите Enter для возврата.

Введите 'с' и нажмите Enter для отмены.

# mgmt

Выберите роль для интерфейса:

1. CP
2. LAN
3. WAN

Введите номер пункта и нажмите Enter.

Введите 'с' и нажмите Enter для отмены.

# 2

Выберите VCE:

1. Системный контекст

Введите номер пункта и нажмите Enter.

Введите 'с' и нажмите Enter для отмены.

# 1

```
1. Автоматически через DHCP
2. Вручную
3. Без адресации

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

Введите IP/префикс и нажмите Enter.

```
Введите 'b' и нажмите Enter для возврата.
Введите 'с' 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
```

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

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-ceedc514961b
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

Нажмите любую клавишу для перехода к локальному меню.
Press 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

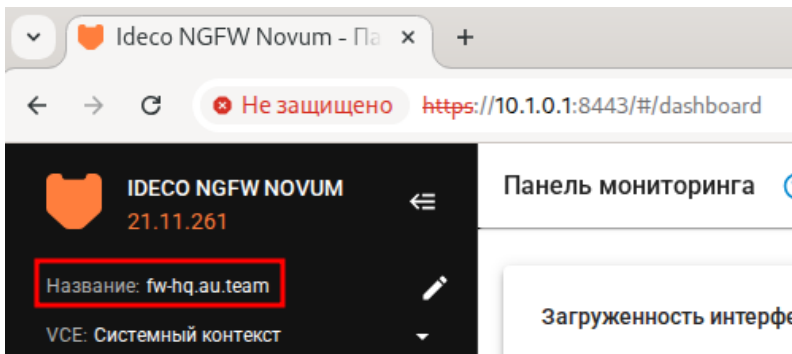
The screenshot shows the 'Ethernet-интерфейсы' (Ethernet interfaces) configuration page in the System Center. The browser title is 'Центр управления системой'. The left sidebar contains navigation links for 'Система', 'Пользователи', 'Брандмауэр', and 'Сеть'. The main content area shows the configuration for the 'ens19' interface. The 'Имя компьютера' (Computer name) is set to 'adm-hq.au.team'. The 'Конфигурация' (Configuration) is set to 'Вручную' (Manual), and the 'IP-адреса' (IP addresses) field contains '10.1.0.2/30'. Other fields like 'Сетевая карта' (Network card), 'MAC', 'Версия протокола IP' (IP protocol version), 'Шлюз по умолчанию' (Default gateway), 'DNS-серверы' (DNS servers), and 'Домены поиска' (Search domains) are also visible.

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

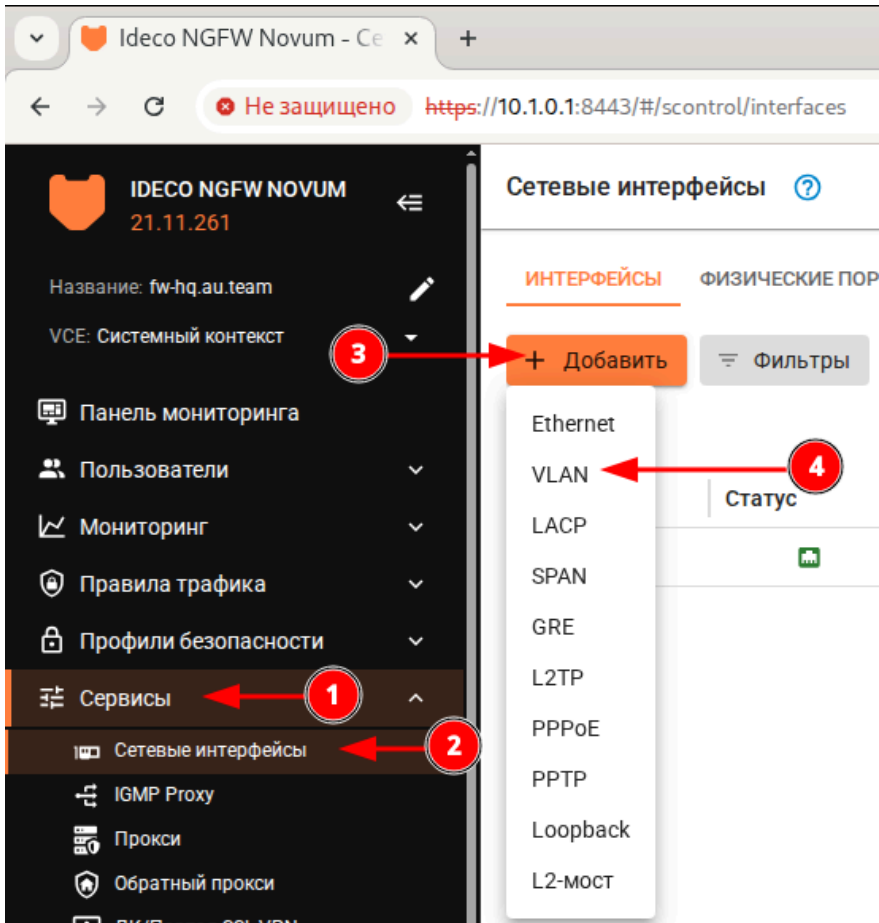
The screenshot shows a web browser window with the address bar containing 'https://10.1.0.1:8443/#/login'. The browser title is 'Ideco NGFW Novum - Ст'. The page content is not fully visible, but the URL indicates it is the login page for the firewall.

The screenshot shows the login page for IDECO NGFW NOVUM. The page has a black header with the IDECO logo and the text 'IDECO NGFW NOVUM'. Below the header, there are two input fields: 'Логин' (Login) and 'Пароль' (Password). The password field has an eye icon to toggle visibility. At the bottom, there is an orange button labeled 'Войти' (Login).

- 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

Добавление VLAN-интерфейса

Название

Настройки

Роль

Зона

Поле необязательное

VCE

Виртуальный контекст (VCE), в котором будет использоваться интерфейс

Интерфейс

На выбранном интерфейсе создаётся VLAN

Тег VLAN

Целое число от 1 до 4094

IP-конфигурация

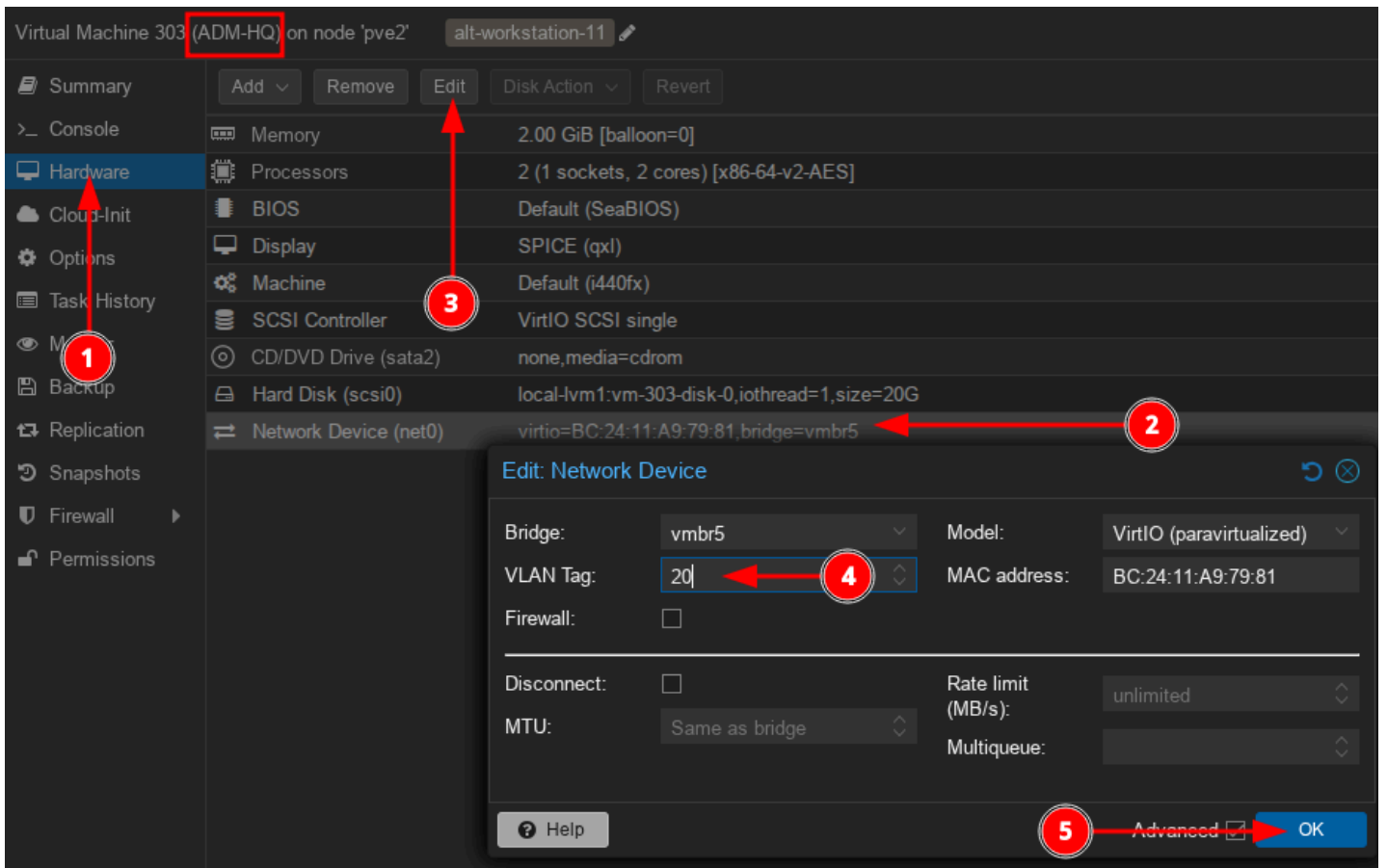
Режим

IP-адрес/маска

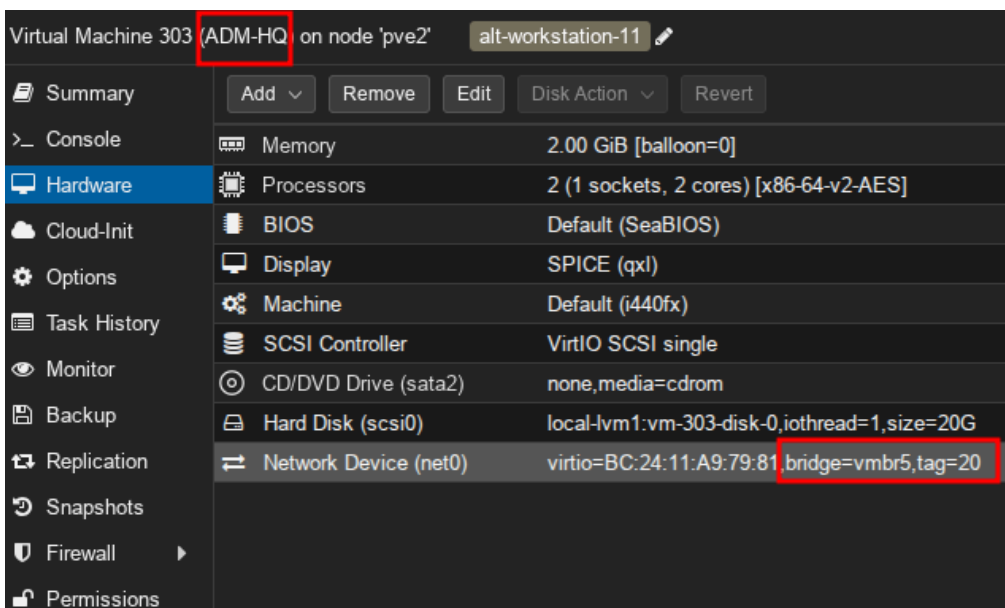
- Результат:

| Тип      | Статус | Настройки |      |      | VCE             | Интерфейс/порт | Тег VLAN | IP-конфигурац... |
|----------|--------|-----------|------|------|-----------------|----------------|----------|------------------|
|          |        | Название  | Роль | Зона |                 |                |          | IP-адрес/маска   |
| Ethernet |        | mgmt      | LAN  | —    | ● Системный ... | eth1_cb        | —        | 10.1.0.1/30      |
| VLAN     |        | vlan20    | LAN  | —    | ● Системный ... | mgmt           | 20       | 10.1.1.33/28     |

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



- Результат:



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

## Ethernet-интерфейсы

Имя компьютера: adm-hq.au.team

### Интерфейсы

ens19

Сетевая карта:  
провод подсоединён  
MAC: bc:24:11:a9:79:81

Версия протокола IP: IPv4  Включить

Конфигурация: Вручную

IP-адреса:  
10.1.1.46/28

Добавить ↑ IP:

Шлюз по умолчанию: 10.1.1.33

DNS-серверы: 10.1.1.10

Домены поиска: au.team

(несколько значений записываются через пробел)

Применить

Сбросить

- 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**
  - **HQ** не удаляем сам интерфейс!

Сетевые интерфейсы

ИНТЕРФЕЙСЫ ФИЗИЧЕСКИЕ ПОРТЫ

+ Добавить Фильтры Отображение Поиск

| Тип      | Статус | Настройки |      |      |               | Интерфейс/порт | Tag VLAN | IP-адрес/маска | Комментарий | Управление |
|----------|--------|-----------|------|------|---------------|----------------|----------|----------------|-------------|------------|
|          |        | Название  | Роль | Зона | VCE           |                |          |                |             |            |
| Ethernet |        | mgmt      | LAN  | -    | Системный ... | eth1_cb        | -        | 10.1.0.1/30    |             |            |
| VLAN     |        | vlan20    | LAN  | -    | Системный ... | mgmt           | 20       | 10.1.1.33/28   |             |            |

## Сетевые интерфейсы ?

mgmt

### Настройки

Роль

LAN

Зона

Поле необязательное

VCE

Системный контекст

Виртуальный контекст (VCE), в котором будет использоваться интерфейс

Физический порт

eth1\_cb

### IP-конфигурация

Режим

Без конфигурации

### Дополнительно

Индекс интерфейса для Netflow

0

Целое число от 0 до 65 535

Комментарий

0/256

Сохранить

Отмена

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

## Сетевые интерфейсы ?

Создать бэкап

### ИНТЕРФЕЙСЫ ФИЗИЧЕСКИЕ ПОРТЫ

+ Добавить

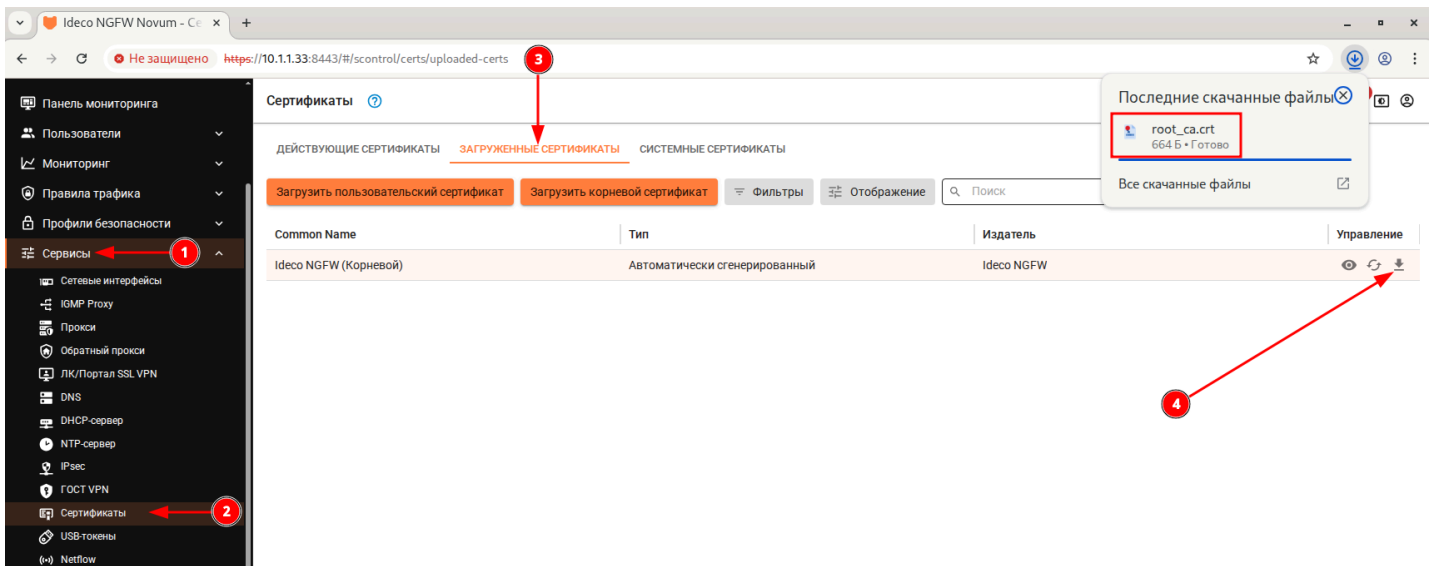
Фильтры

Отображение

Поиск

| Тип      | Статус | Настройки |      |      | IP-конфигурац... |          |                | Комментарий | Управление |
|----------|--------|-----------|------|------|------------------|----------|----------------|-------------|------------|
|          |        | Название  | Роль | Зона | Интерфейс/порт   | Ter VLAN | IP-адрес/маска |             |            |
| Ethernet |        | mgmt      | LAN  | —    | eth1_cb          | —        | —              |             |            |
| VLAN     |        | vlan20    | LAN  | —    | mgmt             | 20       | 10.1.1.33/28   |             |            |

- Скачаем корневой сертификат:

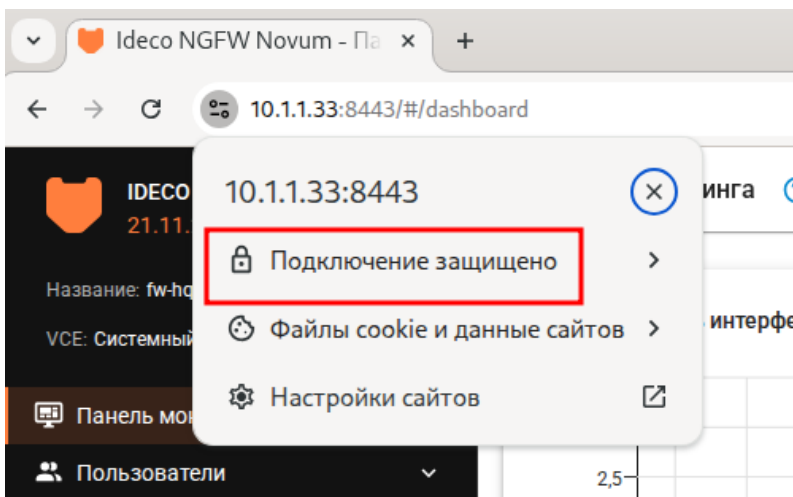


- Добавим в хранилище для ADM-HQ:

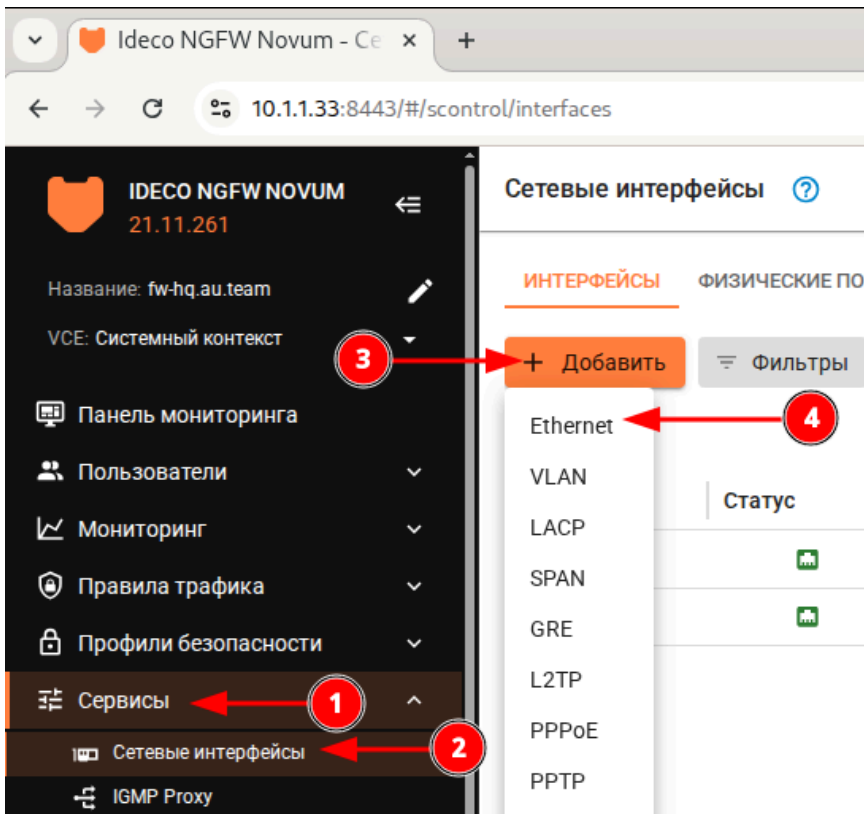
```
su -
```

```
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 соответствии с L3



- заполняем форму по добавлению **Ethernet** интерфейса

## Сетевые интерфейсы ?

**ИНТЕРФЕЙСЫ** ФИЗИЧЕСКИЕ ПОРТЫ

### Редактирование Ethernet-интерфейса

Название

#### Настройки

Роль

Зона

Поле необязательное

VCE

Виртуальный контекст (VCE), в котором будет использоваться интерфейс

Физический порт

#### IP-конфигурация

Режим

IP-адрес/маска

[+ Добавить IP-адрес с маской](#)

**i** Для доступа к сети интернет настройте Балансировку и резервирование.

- Результат:

ИНТЕРФЕЙСЫ   ФИЗИЧЕСКИЕ ПОРТЫ

[+](#) Добавить   [≡](#) Фильтры   [≡](#) Отображение  

| Тип      | Статус | Настройки |      |      |                 | Интерфейс/порт | Тег VLAN | IP-конфигурац... |     |
|----------|--------|-----------|------|------|-----------------|----------------|----------|------------------|-----|
|          |        | Название  | Роль | Зона | VCE             |                |          | IP-адрес/маска   | Ком |
| Ethernet |        | mgmt      | LAN  | —    | ● Системный ... | eth1_cb        | —        | —                |     |
| Ethernet |        | ISP       | WAN  | —    | ● Системный ... | eth0_f1        | —        | 63.27.18.18/23   |     |
| VLAN     |        | vlan20    | LAN  | —    | ● Системный ... | mgmt           | 20       | 10.1.1.33/28     |     |

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

Идеco NGFW Novum - Ба x   +

← → ↻

**ИДЕСО NGFW NOVUM**  
21.11.2017

- Название: fw-hq.au.team
- VCE: Системный контекст
- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Профили безопасности
- Сервисы
- Маршрутизация** 1
- PBR
  - Статическая
- BGP
- OSPF
- Внешних сетей
- Балансировка и резервирование** 2
- Отчёты и журналы
- Управление сервером

### Балансировка и резервирование [?](#)

**ОСНОВНОЕ**   АДРЕСА ДЛЯ ПРОВЕРКИ СВЯЗИ

Режим работы:

Резервирование

Балансировка

[+](#) Добавить   [≡](#) Фильтры   [≡](#) Отображение  

| Название         | Интерфейс | Шлюз | Пропускная способно... |
|------------------|-----------|------|------------------------|
| Шлюз не добавлен |           |      |                        |

3 → [Добавить шлюз.](#)

- заполняем форму **Добавление шлюза**

### Добавление шлюза

Название  ← 1  
Поле необязательное

Интерфейс  ← 2

Шлюз

Нет доступных вариантов

+ Добавить объект ← 3  
+ Добавить значение

### Дополнительно

Комментарий

0/256

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

**Добавление объекта**

Тип  ←

Название  ←  
Заполняется автоматически из значения, если оставить пустым

Значение  ←

Комментарий

0/256

- нажимаем **Добавить**

## Балансировка и резервирование ?

**ОСНОВНОЕ** АДРЕСА ДЛЯ ПРОВЕРКИ СВЯЗИ

### Добавление шлюза

Название

Поле необязательное

Интерфейс

Шлюз

Поле необязательное. Укажите шлюз, если выбран интерфейс с режимом статической IP-конфигурации.

Пропускная способность, Мбит/с

### Дополнительно

Комментарий

0/256

**Добавить**

Отмена

- Результат:

## Балансировка и резервирование ?

**ОСНОВНОЕ** АДРЕСА ДЛЯ ПРОВЕРКИ СВЯЗИ

Режим работы:

Резервирование

Балансировка

+ Добавить

Фильтры

Отображение

Поиск

|   | Название | Интерфейс                            | Шлюз            | Пропускная способн... | Загруженность, Мби...                | Статус |
|---|----------|--------------------------------------|-----------------|-----------------------|--------------------------------------|--------|
| ⋮ | gateway  | <input checked="" type="radio"/> ISP | IP 63.27.19.254 | 100                   | 44,0 <div style="width: 44%;"></div> |        |

- Проверить доступ в сеть Интернет:

Идеко NGFW Novum - Те x +

10.1.1.33:8443/#/server-management/web-terminal

Терминал ?

Название: fw-hq.au.team  
VCE: Системный контекст

- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Профили безопасности
- Сервисы
- Маршрутизация
- Отчёты и журналы
- Управление сервером**
- Администраторы
- Ideco Center
- VCE
- Кластеризация
- Обновления
- Бэкапы
- Терминал**
- Лицензия

```
[admin@fw-hq ~]# ping -c3 my.ideco.ru
PING my.ideco.ru (158.160.183.218) 56(84) bytes of data:
64 bytes from 158.160.183.218: icmp_seq=1 ttl=55 time=17.9 ms
64 bytes from 158.160.183.218: icmp_seq=2 ttl=55 time=26.5 ms
64 bytes from 158.160.183.218: icmp_seq=3 ttl=55 time=20.8 ms

--- my.ideco.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 17.869/21.719/26.457/3.561 ms
[admin@fw-hq ~]#
```

- Проверить наличие лицензии:

Идеco NGFW Novum - Ли x +

10.1.1.33:8443/#/modules/about/license

**ИДЕСО NGFW NOVUM**  
21.11.261

Название: fw-hq.au.team

VCE: Системный контекст

- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Профили безопасности
- Сервисы
- Маршрутизация
- Отчёты и журналы
- Управление сервером
- Администраторы
- Ideco Center
- VCE
- Кластеризация
- Обновления
- Бэкапы
- Терминал
- Лицензия
- Характеристики сервера
- Управление питанием

## Лицензия ?

**Способ обновления**

Автоматическое обновление

Ручная загрузка

Только в случае, если сервер не имеет доступа в интернет.

Сохранить

Управление лицензией осуществляется в [личном кабинете](#).

Идеco NGFW Novum без лицензии по умолчанию не пропускает трафик пользователей в интернет. ?

**Лицензия**

|                                 |                 |
|---------------------------------|-----------------|
| Номер лицензии                  | LIC-            |
| Тип лицензии                    | enterprise-demo |
| Остаток действия лицензии       | 13 дней назад   |
| Окончание лицензии              | через 1 месяц   |
| Окончание обновлений            | через 1 месяц   |
| Окончание технической поддержки | через 1 месяц   |
| Количество пользователей        | 0 из 10 000     |
| Название компании               | au.team         |
| Название сервера                | fw-hq.au.team   |
| Информация достоверна           | Да              |

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

### Сетевые интерфейсы ?

Co

ИНТЕРФЕЙСЫ    ФИЗИЧЕСКИЕ ПОРТЫ

+ Добавить    Фильтры    Отображение   

| Тип      | Статус                               | Настройки  |      |      | VCE             | Интерфейс/порт | Tag VLAN | IP-конфигурац... |
|----------|--------------------------------------|------------|------|------|-----------------|----------------|----------|------------------|
|          |                                      | Название ↑ | Роль | Зона |                 |                |          | IP-адрес/маска   |
| Ethernet | <span style="color: green;">■</span> | ISP        | WAN  | —    | ● Системный ... | eth0_f1        | —        | 63.27.18.18/23   |
| Ethernet | <span style="color: green;">■</span> | mgmt       | LAN  | —    | ● Системный ... | eth1_cb        | —        | —                |
| VLAN     | <span style="color: green;">■</span> | vlan10     | LAN  | —    | ● Системный ... | mgmt           | 10       | 10.1.1.1/27      |
| VLAN     | <span style="color: green;">■</span> | vlan20     | LAN  | —    | ● Системный ... | mgmt           | 20       | 10.1.1.33/28     |
| VLAN     | <span style="color: green;">■</span> | 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

The screenshot shows the IDECO NGFW NOVUM web interface. The left sidebar contains a navigation menu with items like 'Панель мониторинга', 'Пользователи', 'Мониторинг', 'Правила трафика', 'Профили безопасности', 'Сервисы', 'Маршрутизация', 'Отчёты и журналы', 'Управление сервером', and 'Почтовый релей'. The main content area is titled 'Техническая поддержка' and shows the status of technical support: 'Окончание технической поддержки ... через 1 месяц, пять дней'. It also displays license information and an external IP address (63.27.18.18). A warning box indicates that internet access will be available to all local network users, but some services will stop working. A red arrow labeled '1' points to the 'Создать заявку' button, and another red arrow labeled '2' points to the 'Включить' button.

- 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:

The screenshot shows the IDECO NGFW NOVUM web interface for DNS settings. The left sidebar has 'Сервисы' highlighted with a red arrow labeled '1', and 'DNS' highlighted with a red arrow labeled '2'. The main content area is titled 'DNS' and shows the status 'Работает'. There are tabs for 'ВНЕШНИЕ DNS-СЕРВЕРЫ', 'MASTER-ЗОНЫ', 'FORWARD-ЗОНЫ', and 'DDNS'. Under 'Настройки', there are several options: 'Перехват пользовательских DNS-запросов' (checked), 'Логировать DNS-запросы', 'DNS security', 'Блокировать запросы на DNS-резолвинг при недействительной лицензии на DNS security', 'Безопасный поиск', and 'Шифрование DNS over TLS'. A red arrow labeled '3' points to the 'Перехват пользовательских DNS-запросов' toggle. At the bottom, there are buttons for '+ Добавить', 'Отображение', and a search box. Below the settings is a table with columns for 'Тип', 'Адрес DNS-сервера', and 'Подключение'.