Kaspersky SD-WAN

Руководство по развертыванию демонстрационного стенда Kaspersky SD-WAN в среде VMware

Часть 1

kaspersky

Содержание

1. **Kaspersky SD-WAN.**

Решение Kaspersky SD-WAN используется для построения программно-определяемых распределенных сетей (англ. Software Defined WAN или SD-WAN) для маршрутизации сетевого трафика по каналам сети передачи данных с применением технологии SDN (Software Defined Networking). В сетях SD-WAN наиболее эффективные пути маршрутизации трафика определяются автоматически.

Технология SDN подразумевает разделение уровня управления сетью (англ. Control Plane) и уровня передачи данных (англ. Data Plane). Уровень управления контролирует передачу пакетов по сети через телекоммуникационное оборудование, установленное на площадке клиента (англ. Customer Premises Equipment, или устройства CPE). Передача пакетов через устройства CPE осуществляется на уровне передачи данных.

В сетях, построенных с применением технологии SDN, уровень управления переносится в централизованный контроллер SD-WAN. Данный контроллер взаимодействует с устройствами CPE, составляющими уровень передачи данных, а также с SD-WAN оркестратором, который используется для управления сетью SD-WAN с помощью веб-интерфейса.

Решение Kaspersky SD-WAN предназначено для операторов связи, компаний, имеющих крупную филиальную сеть, и используется для замены стандартных маршрутизаторов в распределенных сетях.

Решение Kaspersky SD-WAN обладает следующими основными характеристиками:

- Работа на основе проводных и беспроводных сетей любого типа.
- Использование несколько виртуальных каналов для обеспечения высокой доступности сети и балансировки трафика.
- Коррекция ошибок при передаче данных.
- Интеллектуальное управление трафиком.
- Автоматическая настройка устройств CPE с использованием концепции Zero Trust Provisioning (ZTP).
- Централизованное управление и мониторинг.

1.1. **Архитектура решения Kaspersky SD-WAN.**

Краткое описание основных компонентов решения Kaspersky SD-WAN:

- SD-WAN оркестратор. Предоставляет единый графический веб-интерфейс управления, отвечает за управление сервисами SD-WAN сети и содержит инвентаризационную базу CPE устройств.
- SD-WAN контроллер. Управляет наложенной сетью (англ. Overlay Network), обеспечивает построение топологии сети и создание транспортных сервисов внутри наложенных туннелей. Поддерживает транспортные сервисы L2 Point-to-Point (P2P), Point-to-Multipoint (P2M), Multipoint-to-Multipoint (M2M) и L3 VPN. Управляет устройствами CPE и шлюзами SD-WAN по протоколу OpenFlow. Определяет распределение трафика между туннелями, выполняет мониторинг качества соединения и автоматическое переключение трафика на резервный туннель в случае возникновения проблем на основном. Контроллер находится под управлением SD-WAN оркестратора.
- SD-WAN шлюзы. Объединяют CPE устройства в единую сеть. Наложенные туннели терминируются на SD-WAN шлюзах, после чего трафик передается дальше в соответствии с топологией сети.
- CPE устройства или Kaspersky Edge Service Router (KESR). Телекоммуникационное оборудование, которое подключается к шлюзам SD-WAN с помощью наложенных туннелей и образует SDN-фабрику в виде наложенной сети.

Архитектура решения Kaspersky SD-WAN представлена на рисунке 1.

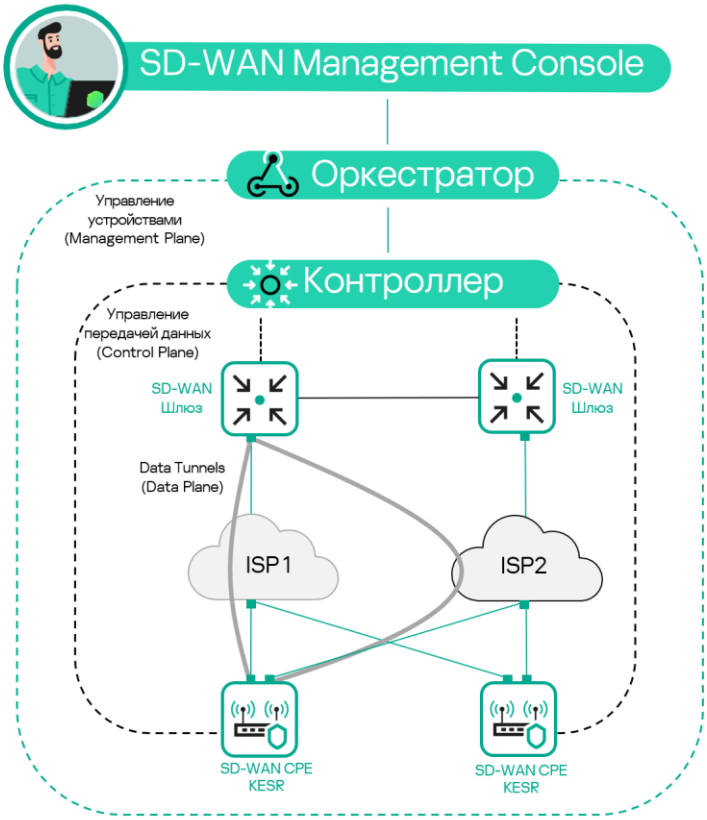


Рисунок 1. Архитектура решения Kaspersky SD-WAN.

2. **Описание схемы демонстрационного стенда Kaspersky SD-WAN.**

Все компоненты демонстрационного стенда Kaspersky SD-WAN развернуты в среде виртуализации VMware.

На виртуальном хосте orc1 развернуты Docker контейнеры решения Kaspersky SD-WAN, включая оркестратор, контролер и систему мониторинга Zabbix.

Логическая схема демонстрационного стенда Kaspersky SD-WAN представлена на рисунке 2. Демонстрационный стенд включает в себя:

- Площадка DC с сетевыми сегментами dc-lan1 и oob, подключенными к маршрутизатору R13. Виртуальная машина SD-WAN оркестратора orc1 размещена в сегменте oob, сервер srv1 с WWW службой размещен в сегменте dc-lan1.
- На границе DC размещены два маршрутизатора R11 и R12, за которыми размещены два SD-WAN шлюза: vGW-11 и vGW-12. Внутренние (lan) интерфейсы R13, vGW-11 и vGW-12 подключены к сетевому сегменту dc-perim.
- Маршрутизаторы R11 и R12 выполняют функцию Source Network Address Translation (SNAT) для vGW-11 и vGW-12 и Destination Network Address Translation (DNAT) для портов, указанных в Таблице №1.
- Маршрутизатор R14 выполняет SNAT, роль шлюза по умолчанию для R13, и выход в Интернет для хоста orc1. R14 выполняет DNAT для хоста orc1 для портов, указанных в Таблице №1 для Docker контейнеров SD-WAN оркестратора и SD-WAN контроллера.
- Хост ISP эмулирует подключение к сети Интернет / операторам связи ISP1 – ISP8.
- Для подключения CPE устройств SD-WAN шлюзы должны быть доступны по определённому набору портов, перечисленных в Таблице №1.
- Устройство vCPE-3 представляет собой пример подключения удаленной площадки с одним CPE устройством, подключенным к двум операторам связи.
- Устройство vCPE-4 представляет собой пример будущего, не рассматриваемой в рамках текущего стенда, подключения удаленной площадки с универсальным uCPE устройством.
- Шлюзы vCPE-51 и vCPE-52 представляют собой пример подключения удаленной площадки с двумя CPE устройствами для отказоустойчивости, решение поддерживает использование протокола VRRP, в рамках данного демонстрационного стенда его использование не рассматривается.

2.1. **Схема демонстрационного стенда.**

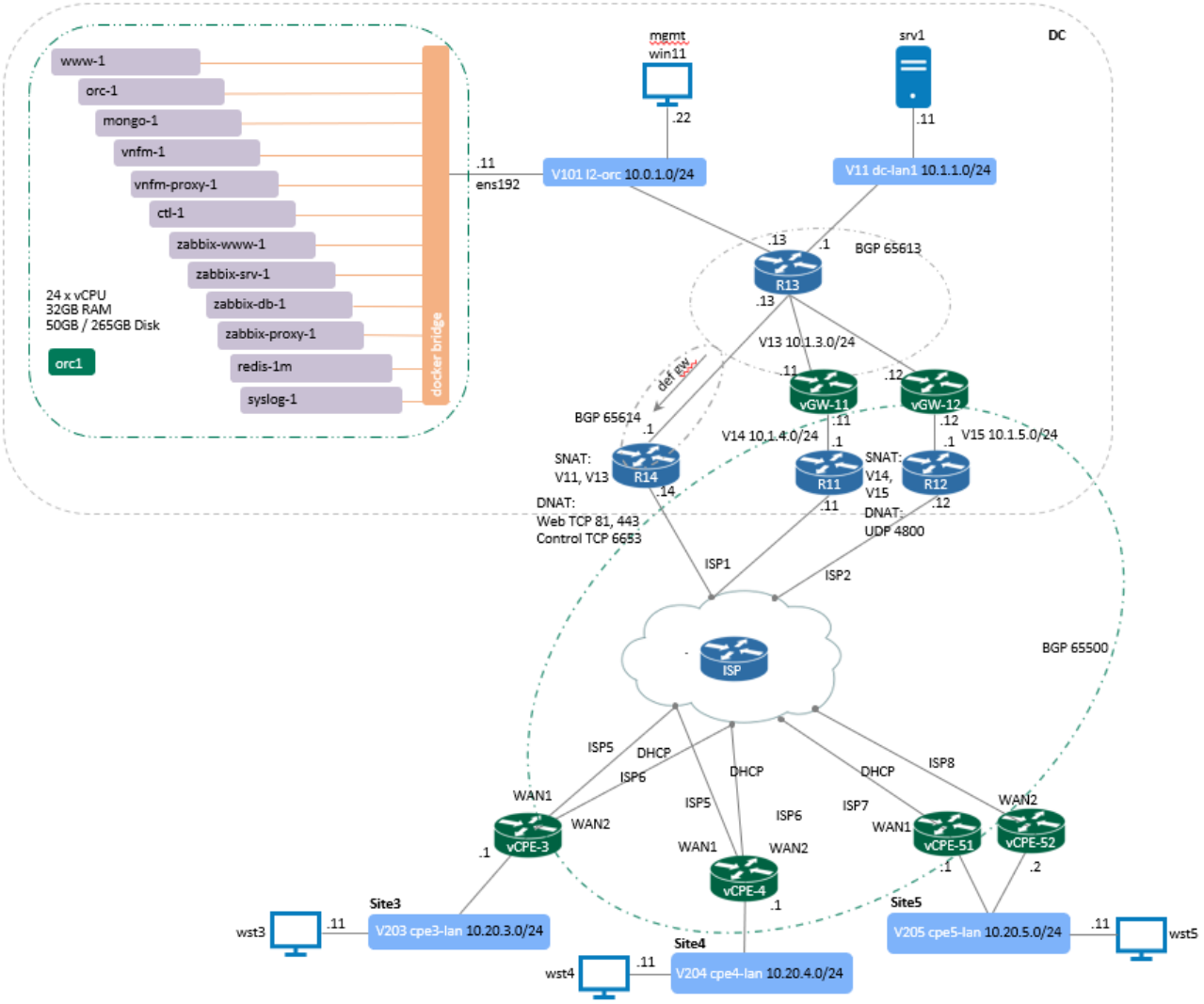


Рисунок 2 – Демонстрационный стенд Kaspersky SD-WAN 2.0

2.2. **Сетевые порты, используемые центральными компонентами решения.**

Компонент	**Порт**	**Назначение**
SD-WAN оркестратор	TCP 82 TCP 85 TCP 443	Доступ к веб- интерфейсу CPE через веб-интерфейс оркестратора. Доступ к веб- интерфейсу Zabbix. Доступ к веб- интерфейсу оркестратора.
SD-WAN контроллер	TCP 6653-6656	Подключение SD-WAN шлюзов и CPE устройств к контроллеру по TLS. CPE устройство подключается каждым wan интерфейсом к отдельному порту контроллера: • sdwan0 - 6653 • sdwan1 - 6654 • и т.д.
SD-WAN шлюзы	UDP 4800	Дата трафик.

Таблица 1. – Сетевые порты для взаимодействия SD-WAN шлюзов и CPE устройств с центральными компонентами решения, и доступ к веб- интерфейсу оркестратора для администрирования решения.

2.3. **План IP адресации.**

Данный IP план соответствует схеме из пункта 2.1. в случае использования других адресов требуется изменить план и все настройки SD-WAN в дальнейших шагах.

Имя	Операционная система	IP адрес	Назначение	Минимальные ресурсы
orc1	Ubuntu 20.04.06 LTS Server	10.0.1.11	На хосте развернуты Docker контейнеры: www-1, orc-1, redis-1m, mongo-1, vnfm-1, vnfm-proxy-1, ctl, zabbix-www-1, zabbix-srv-1, zabbix-prx-1, zabbix-db-1, syslog-1	24 x vCPU, 32 GB RAM
vGW-11	CPEOS	wan 10.1.4.11 lan 10.1.3.11	SD-WAN шлюз	4 x vCPU, 2 GB RAM
vGW-12	CPEOS	wan 10.1.5.12 lan 10.1.3.12	SD-WAN шлюз	4 x vCPU, 2 GB RAM
vCPE-3	CPEOS	wan DHCP lan 10.20.3.1	CPE	4 x vCPU, 2 GB RAM
vCPE-4	CPEOS	wan DHCP lan 10.20.4.1	CPE	4 x vCPU, 2 GB RAM
vCPE-51	CPEOS	wan DHCP lan 10.20.5.1	CPE	4 x vCPU, 2 GB RAM
vCPE-52	CPEOS	wan DHCP lan 10.20.5.2	CPE	4 x vCPU, 2 GB RAM
R11	CentOS 7	wan 10.50.1.11 lan 10.1.4.1	Пограничный маршрутизатор DC	2 x vCPU, 2 GB RAM
R12	CentOS 7	wan 10.50.2.12 lan 10.1.5.1	Пограничный маршрутизатор DC	2 x vCPU, 2 GB RAM
R13	CentOS 7	dc-perim 10.1.3.13 oob 10.0.1.13 dc-lan1 10.1.1.1	Маршрутизатор ядра DC	2 x vCPU, 2 GB RAM
R14	CentOS 7	wan 10.50.1.14 lan 10.1.3.1	Пограничный маршрутизатор DC, NAT	2 x vCPU, 2 GB RAM

kaspersky

Имя	Операционная система	IP адрес	Назначение	Минимальные ресурсы
ISP	CentOS 7	isp1 10.50.1.1 isp2 10.50.2.1 isp5 10.50.5.1 isp6 10.50.6.1 isp7 10.50.7.1 isp8 10.50.8.1	Эмуляция ISP1 – ISP8	2 x vCPU, 2 GB RAM
srv1	CentOS 7	10.1.1.11	Сервер WWW/DC	2 x vCPU, 4 GB RAM
wst3	CentOS 7	10.20.3.11	Рабочая станция Site3	2 x vCPU, 4 GB RAM
wst4	CentOS 7	10.20.4.11	Рабочая станция Site4	2 x vCPU, 4 GB RAM
wst5	CentOS 7	10.20.5.11	Рабочая станция Site5	2 x vCPU, 4 GB RAM
mgmt	Windows 11	10.0.1.10 10.1.1.10 10.1.3.10 10.50.1.10 10.20.3.10 10.20.4.10 10.20.5.10	Рабочая станция для управления демо стендом.	6 x vCPU, 6 GB RAM

2.4. **Версии программного обеспечения.**

Таблица №3 – Версии программного обеспечения Kaspersky SD-WAN, используемого в данном демонстрационном стенде:

Компонент SD-WAN	**Версия**
www	knaas-www:2.23.07.release.81.amd64_en-US_ru-RU
orc	knaas-orc:2.23.07.release.88.amd64_en-US_ru-RU
mongo	mongo:5.0.7.amd64
ctl	knaas-ctl:2.23.07.release.39.amd64_en-US_ru-RU
vnfm	knaas-vnfm:2.23.07.release.8.amd64_en-US_ru-RU
vnfm-proxy	knaas-vnfm-proxy:2.23.07.release.2.amd64_en-US_ru-RU
redis	redis:6.2.7.amd64
zabbix-www	zabbix-web-nginx-mysql:5.0.32.amd64
zabbix-proxy	zabbix-proxyr-mysql:5.0.32.amd64
zabbix-srv	zabbix-server-mysql:5.0.32.amd64
zabbix-db	mariadb:10.4.28.amd64
syslog	syslog-ng:3.30.1.amd64
vCPE	knaas-cpe_2.23.07.release.23.combined.amd64-legacy.qcow2
Хост orc1	Ubuntu 20.04.06 LTS Server
installer	knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU.tar.gz

2.5. **Требования к аппаратным ресурсам решения Kaspersky SD-WAN.**

Таблица №4 - Требования к аппаратным ресурсам для управления до 50 CPE устройств.

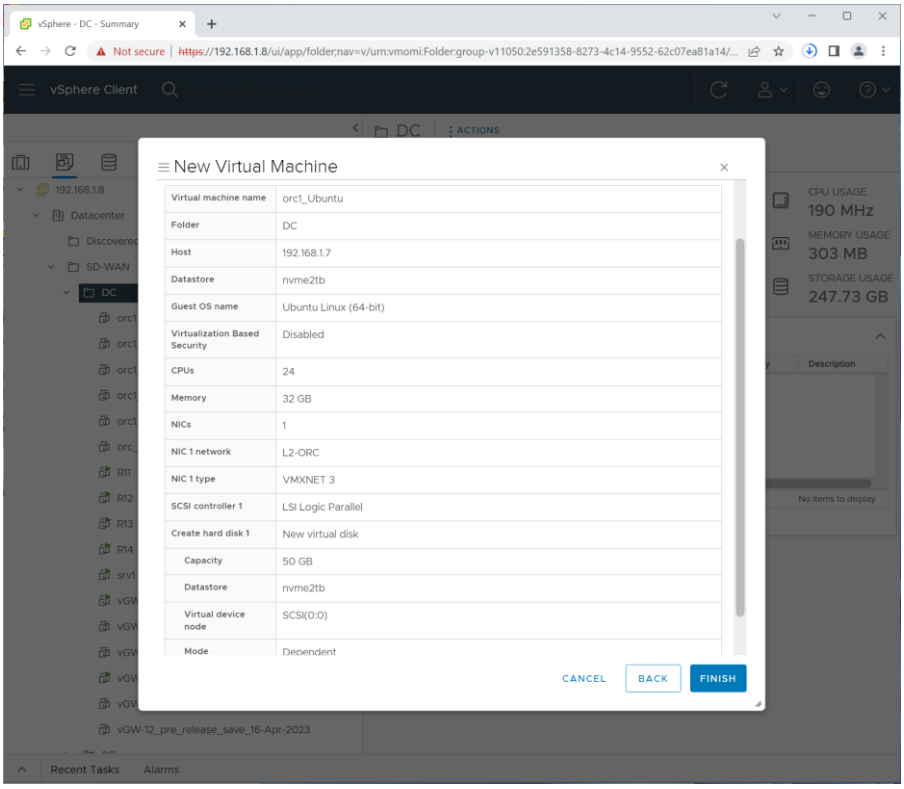
Хост	**CPU (hyper-threading), cores**	**RAM, GB**	**Disk, GB, SSD** Используется в данной конфигурации/ Рекомендуется
orc1	24	32	50 / 265

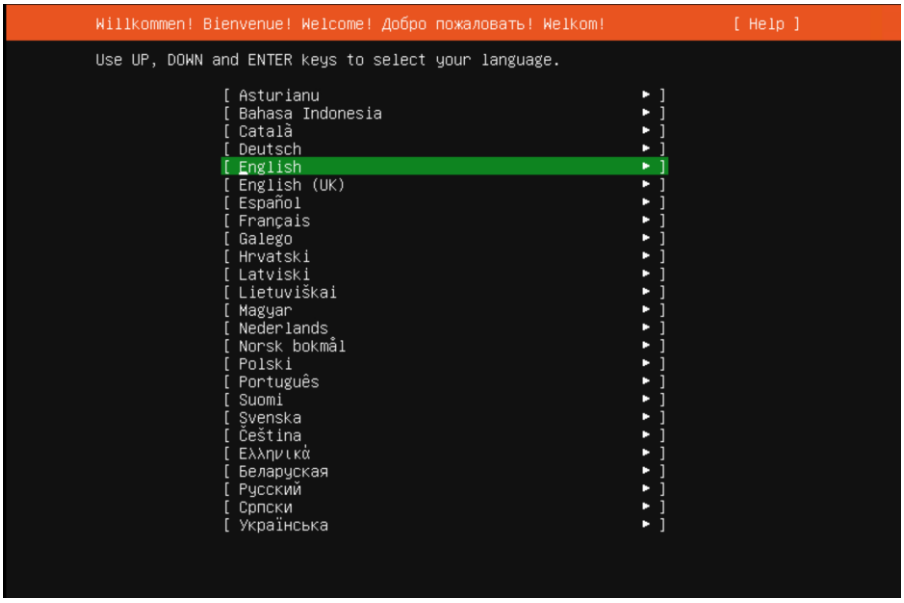
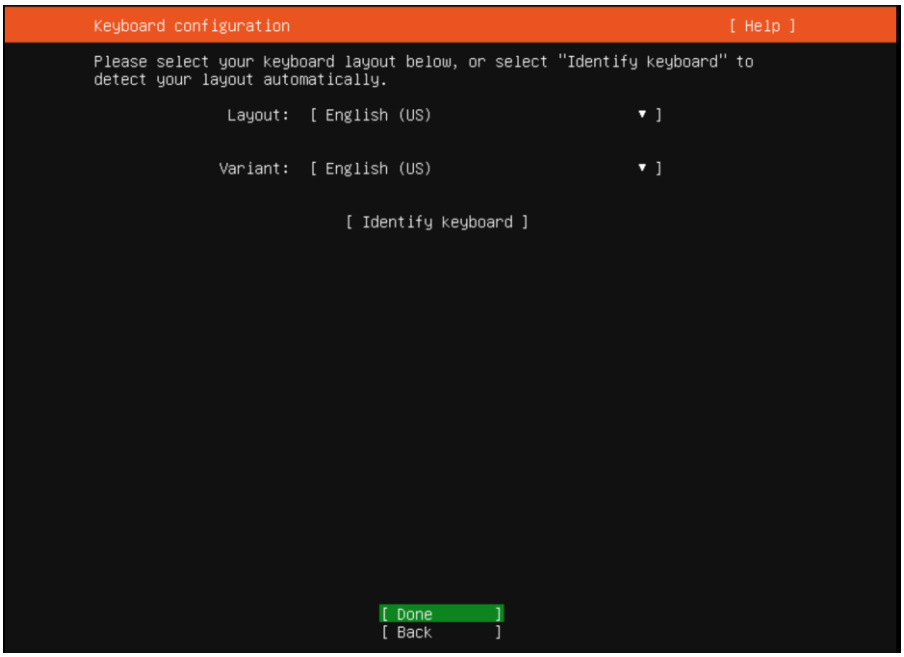
3. **Установка и настройка компонентов решения Kaspersky SD-WAN.**

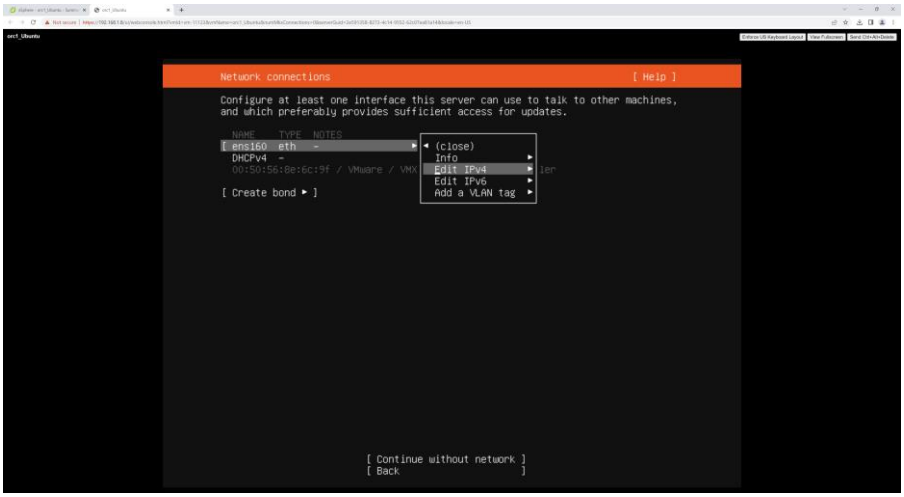
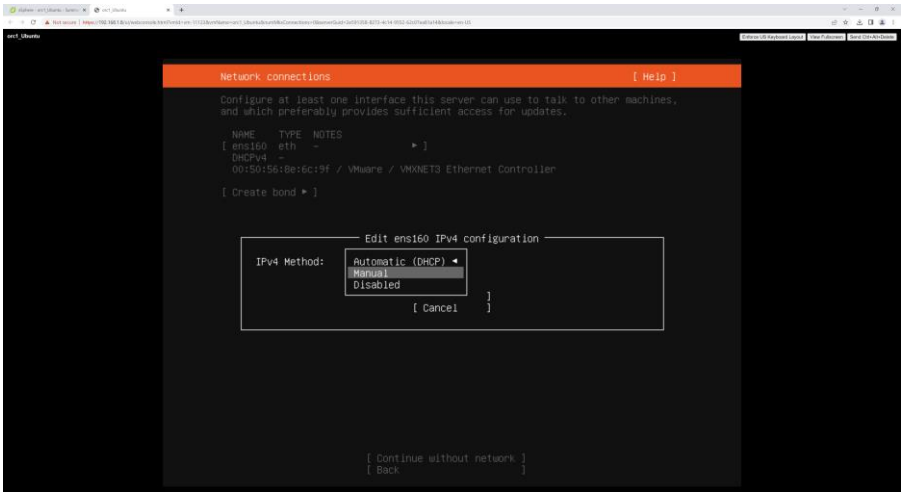
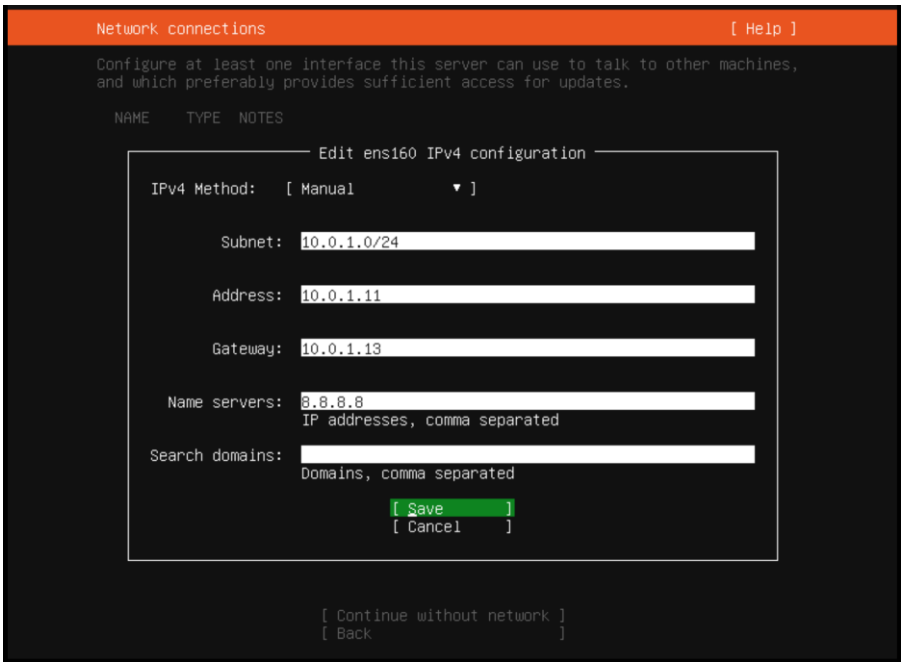
Для развертывания решения SD-WAN необходимо создать виртуальную машину (в данном руководстве имя хоста задано как orc1) и установить операционную систему Ubuntu 20.04.06 LTS Server. Если виртуальная машина уже готова, то перейти к пункту 3.2.

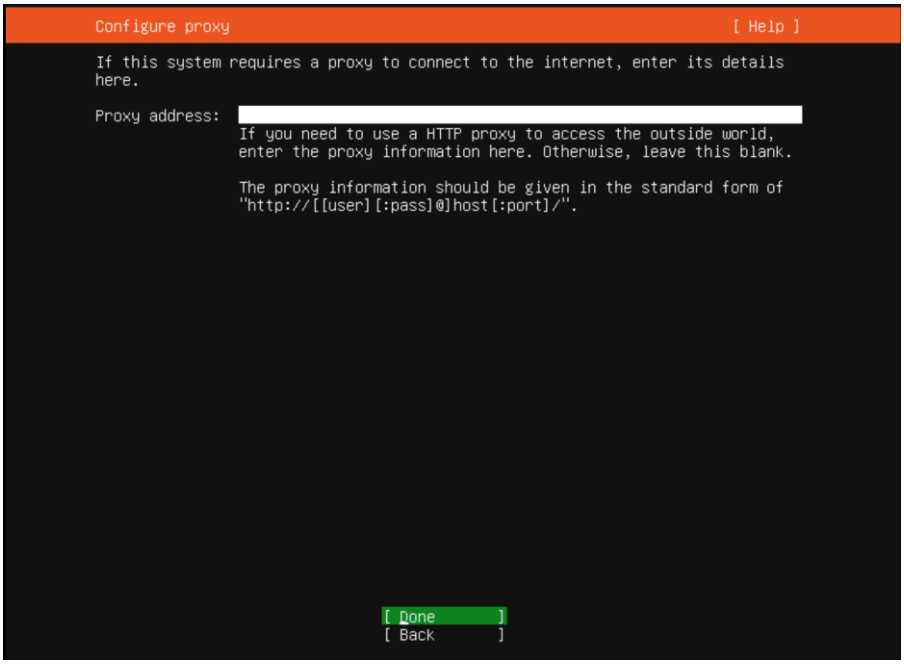
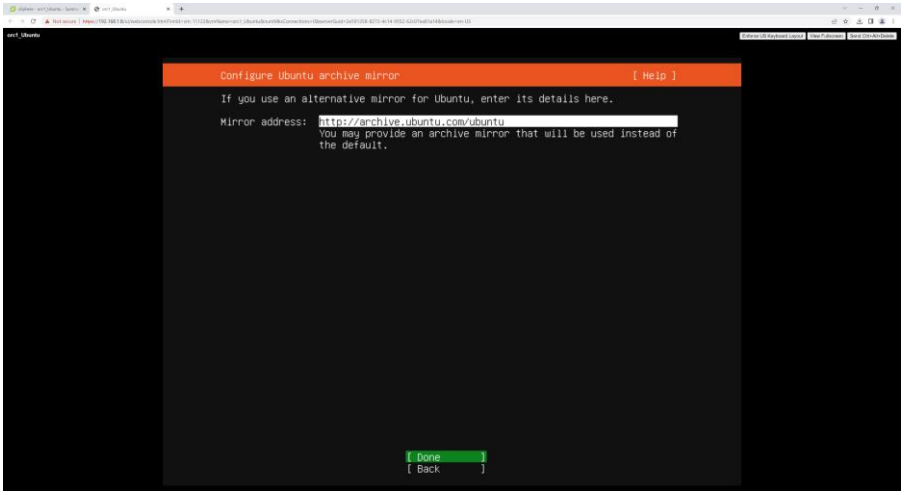
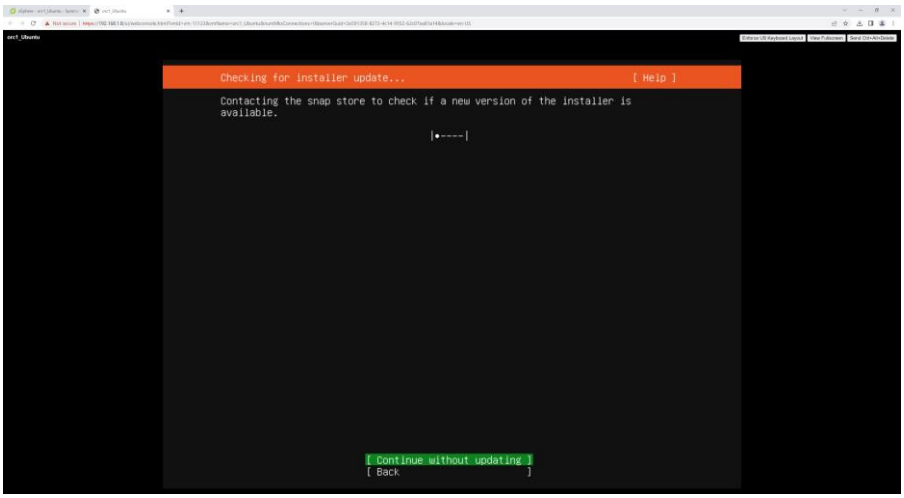
Для установки используется дистрибутив Linux Ubuntu 20.04.06 LTS Server: https://releases.ubuntu.com/20.04.6/ubuntu-20.04.6-live-server-amd64.iso

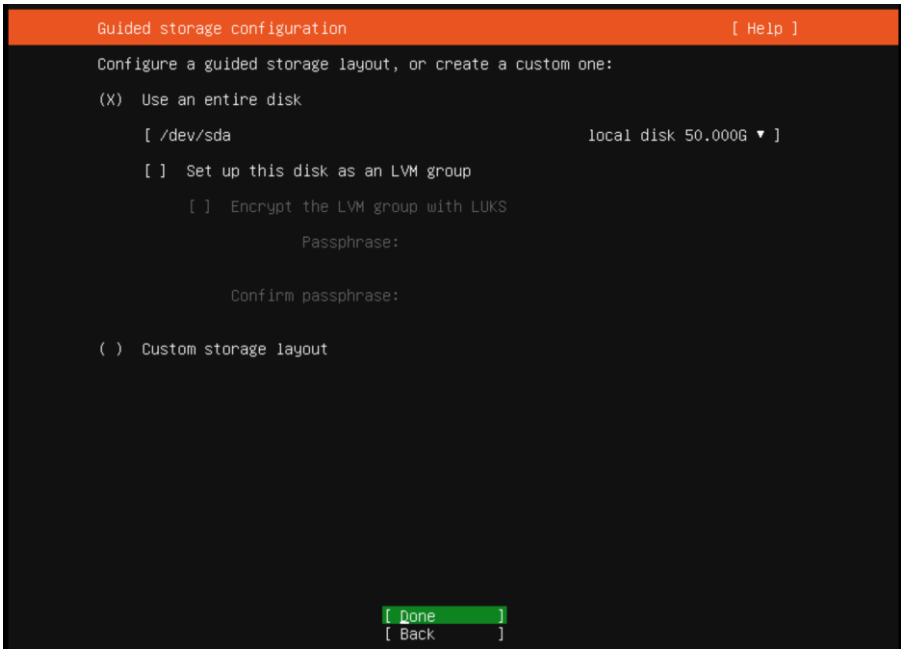
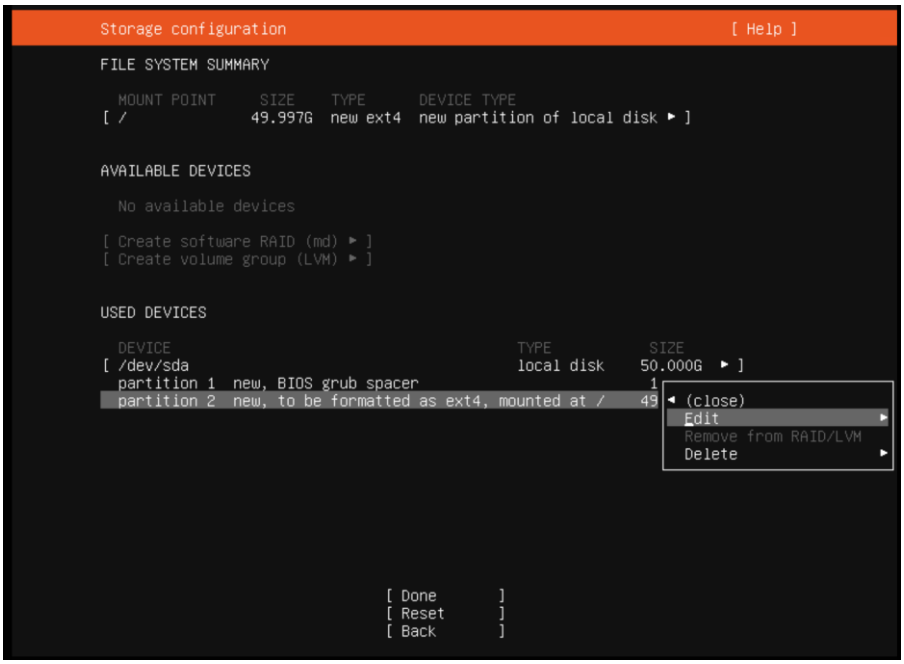
3.1. **Установка операционной системы хоста**

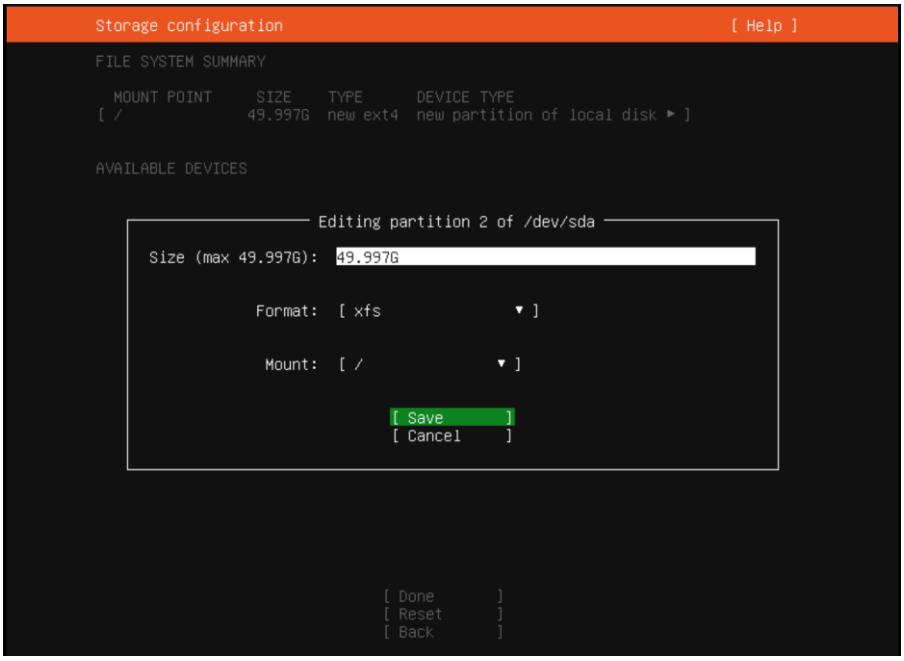
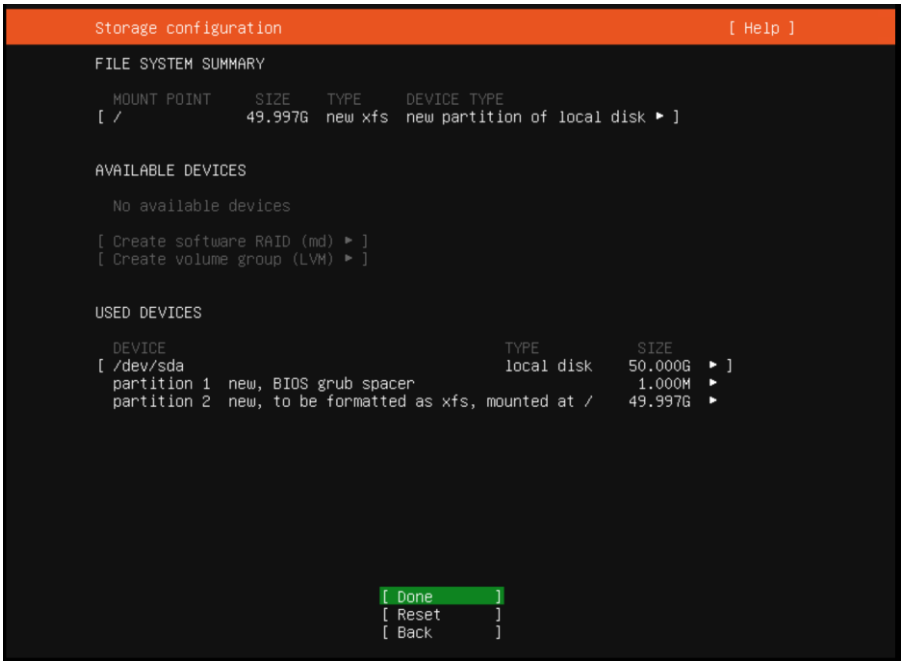
3.1.1. Создать виртуальную машину для хоста orc1. Ресурсы CPU, RAM, Disk задать в соответствии с таблицей №4.	

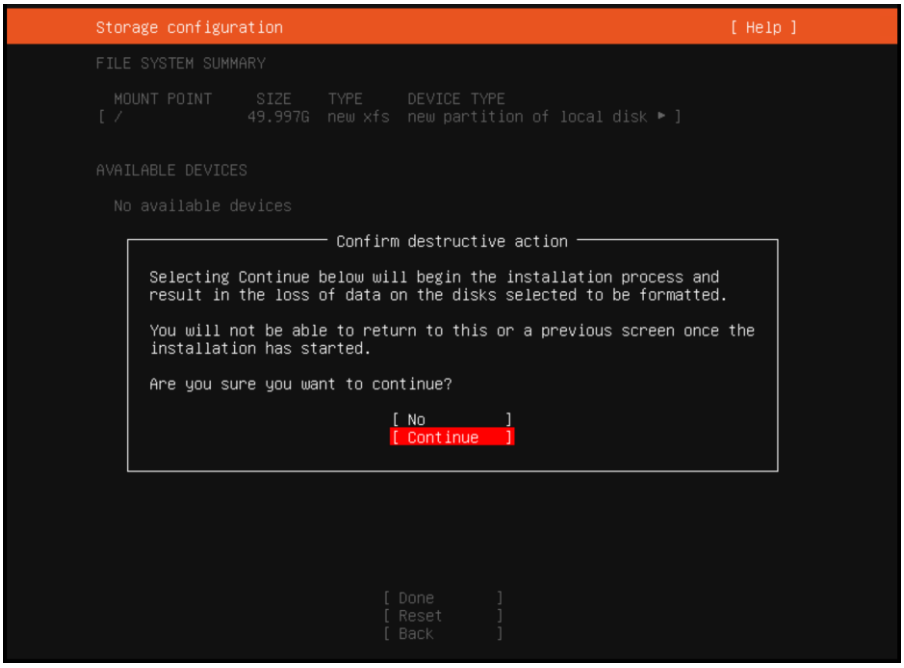
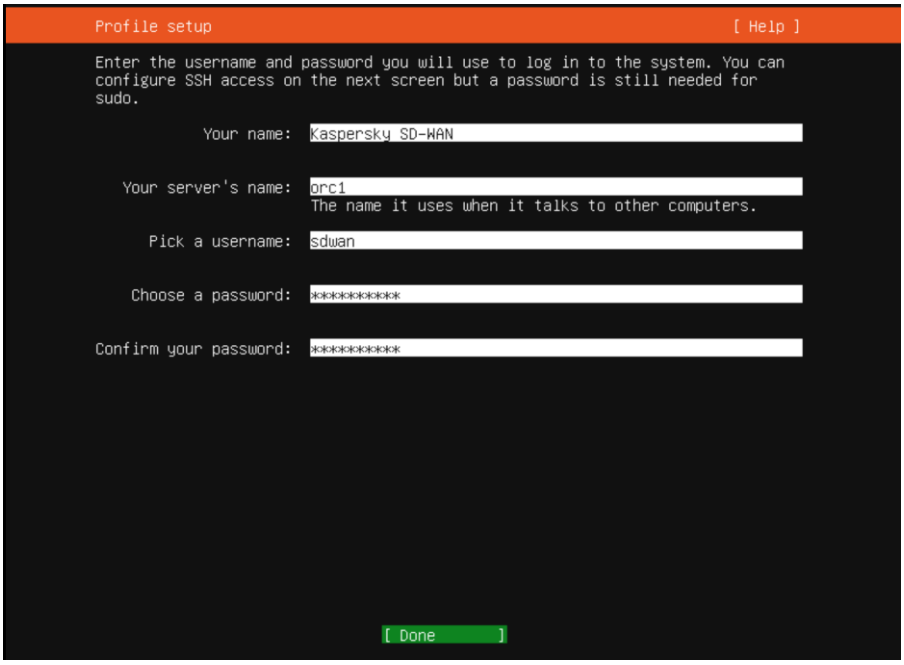
3.1.2. Загрузка с установочного образа *Ubuntu 20.04.06 LTS Server*. Выбрать язык: *English (оставить значение по умолчанию).*	
3.1.3. Выбрать раскладку клавиатуры: *US/US (оставить значение по умолчанию)*.	

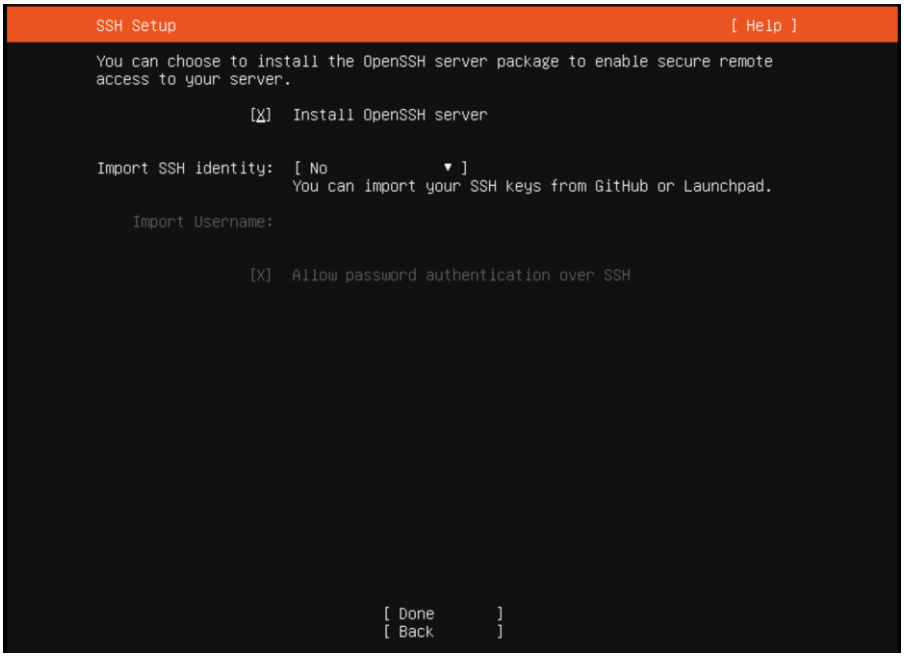
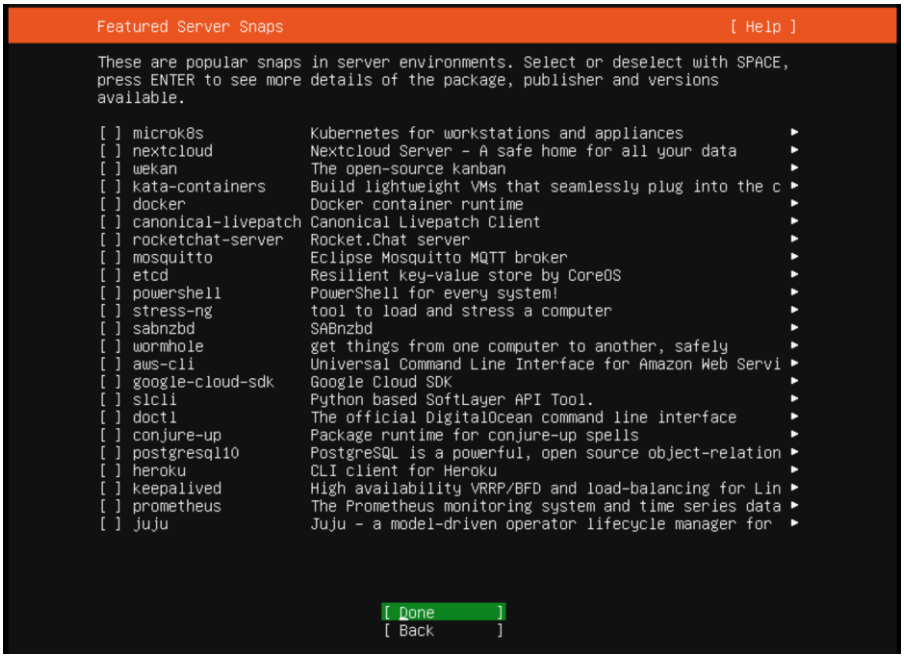
3.1.4. Выбрать редактирование настроек IPv4 сетевого интерфейса (в примере *ens160*).	
3.1.5. Выбрать ручную настройку IPv4 (*Manual*).	
3.1.6. Настроить параметры IPv4 сетевого интерфейса согласно плану адресации, нажать *Save*.	

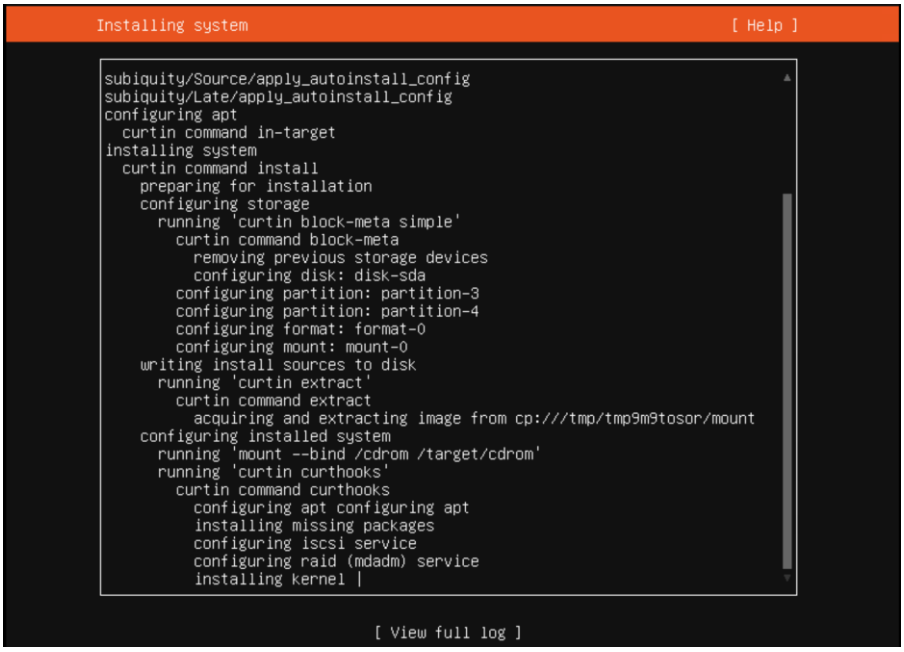
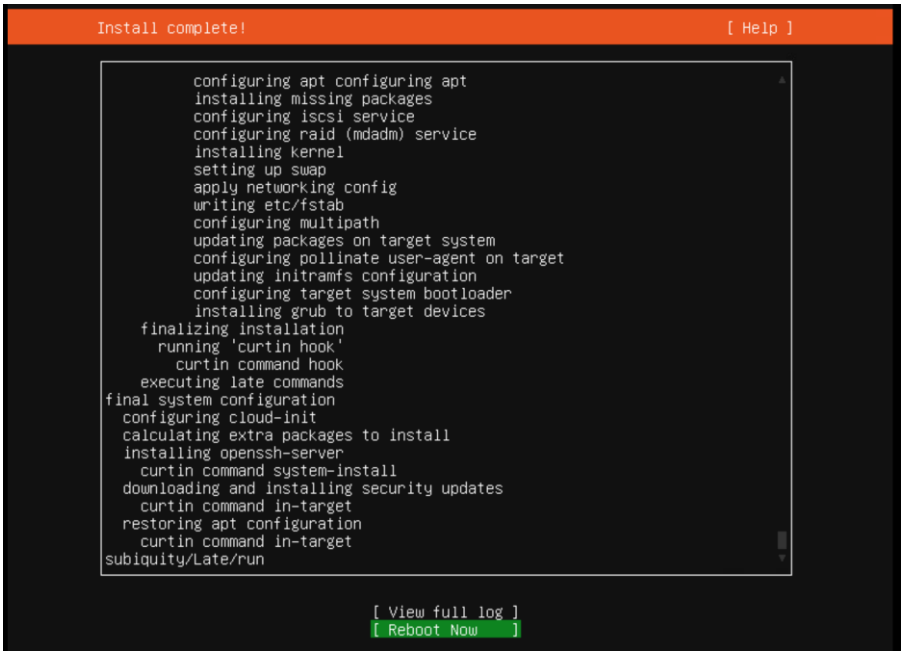
3.1.7. Пропустить (выполнить при необходимости) настройку прокси-сервера, выбрать *Done.*	
3.1.8. Настроить параметры зеркала архивов для Ubuntu (оставить значение по-умолчанию) и нажать *Done.*	
3.1.9. Выбрать *Continue without updating.*	

3.1.10. Выбрать использование всего диска для установки, в данном примере без создания логических групп.	
3.1.11. Выбрать раздел корневой раздел для редактирования (*partition 2 – Edit*).	

3.1.12. Указать формат файловой системы: XFS, нажать *Save.* При разработке данного документа используется диск 50GB, рекомендуемые значения для использования 50xCPE – 265GB.	
3.1.13. Сохранить изменения –нажать *Done.*	

3.1.14. Подтвердить начало установки – выбрать *Continue.*	
3.1.15. Создать служебного пользователя с именем “sdwan”, используется при развертывании системы управления Kaspersky SD-WAN. Задать имя сервера (*orc1*).	

3.1.16. Добавить установку службы *OpenSSH*, нажать *Done.*	
3.1.17. Пропустить установку дополнительных пакетов, нажать *Done* (необходимые пакеты будут установлены позднее).	

3.1.18. Дождатся начала установки системы до появления подтверждающих сообщений.	
3.1.19. Выбрать *Reboot Now* для перезагрузки системы и завершения установки.	

3.2. **Настройка операционной системы хоста и установка компонентов системы управления Kaspersky SD-WAN.**

3.2.1. Проверить работу NTP.

Время должно быть синхронизировано:

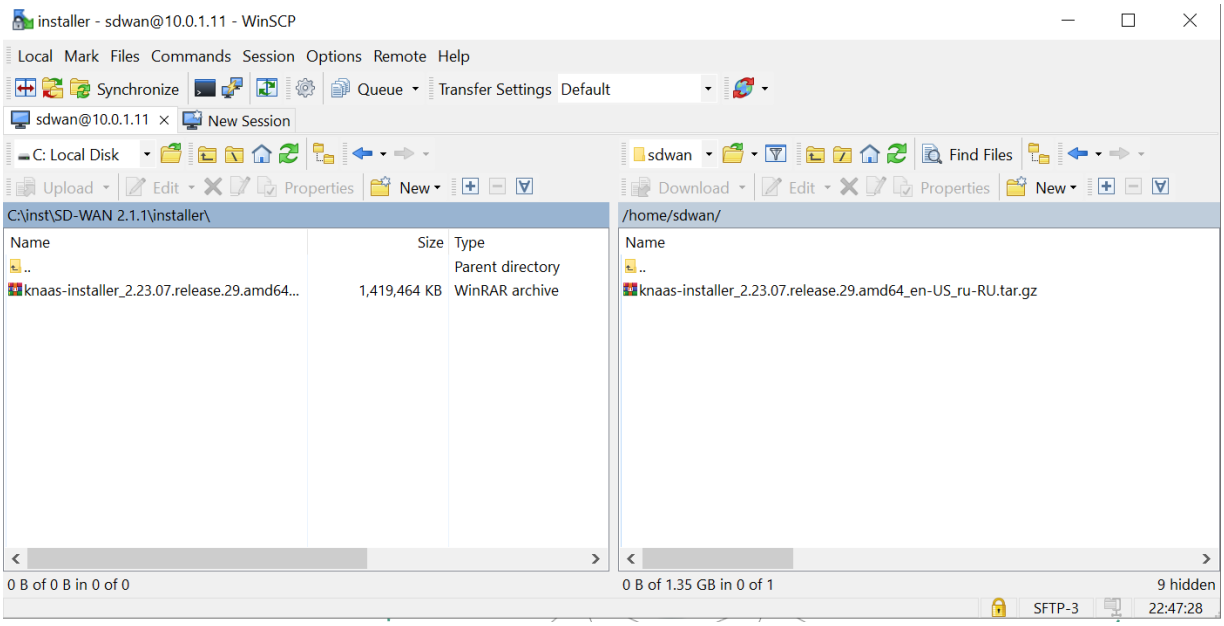
[sdwan@orc1] # timedatectl status

System clock synchronized: yes

3.2.2. Загрузить архив *knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU.tar.gz* с плейбуками установки компонентов системы управления Kaspersky SD-WAN в домашний каталог пользователя sdwan на хост orc1.

Загрузить образы контейнеров системы управления Kaspersky SD-WAN в каталог images.

Для установки используется пользователь sdwan, созданный в пункте 3.1.15, в случае использования другого пользователя необходимо использовать соответствующий каталог.

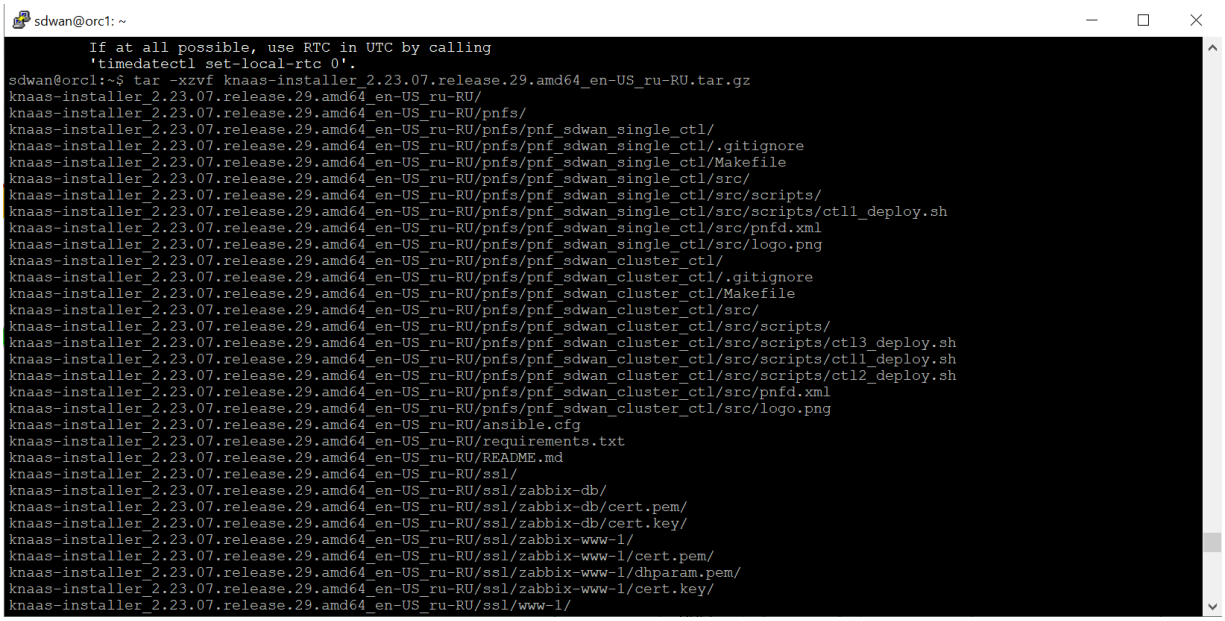


3.2.3. Распаковать установочный архив в каталог пользователя sdwan:

sdwan@orc1:~$ tar -xzvf knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU.tar.gz

Перейти в директорию инсталлятора:

sdwan@orc1:~$ cd knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU



3.2.4. Обновление списков и версий установленных пакетов.

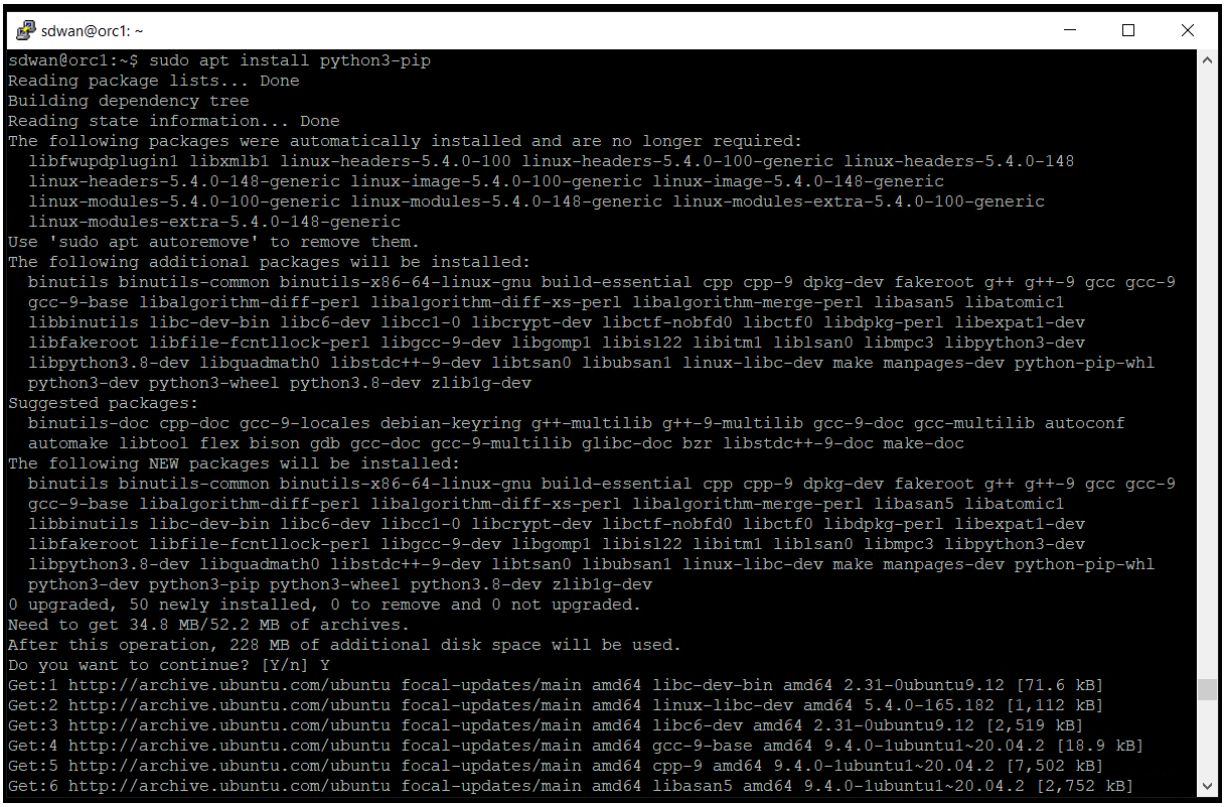
Выполнить команду ниже.

sdwan@orc1:~$ sudo apt update && sudo apt upgrade --yes

3.2.5. Установка необходимых пакетов перед запуском плейбуков установки.

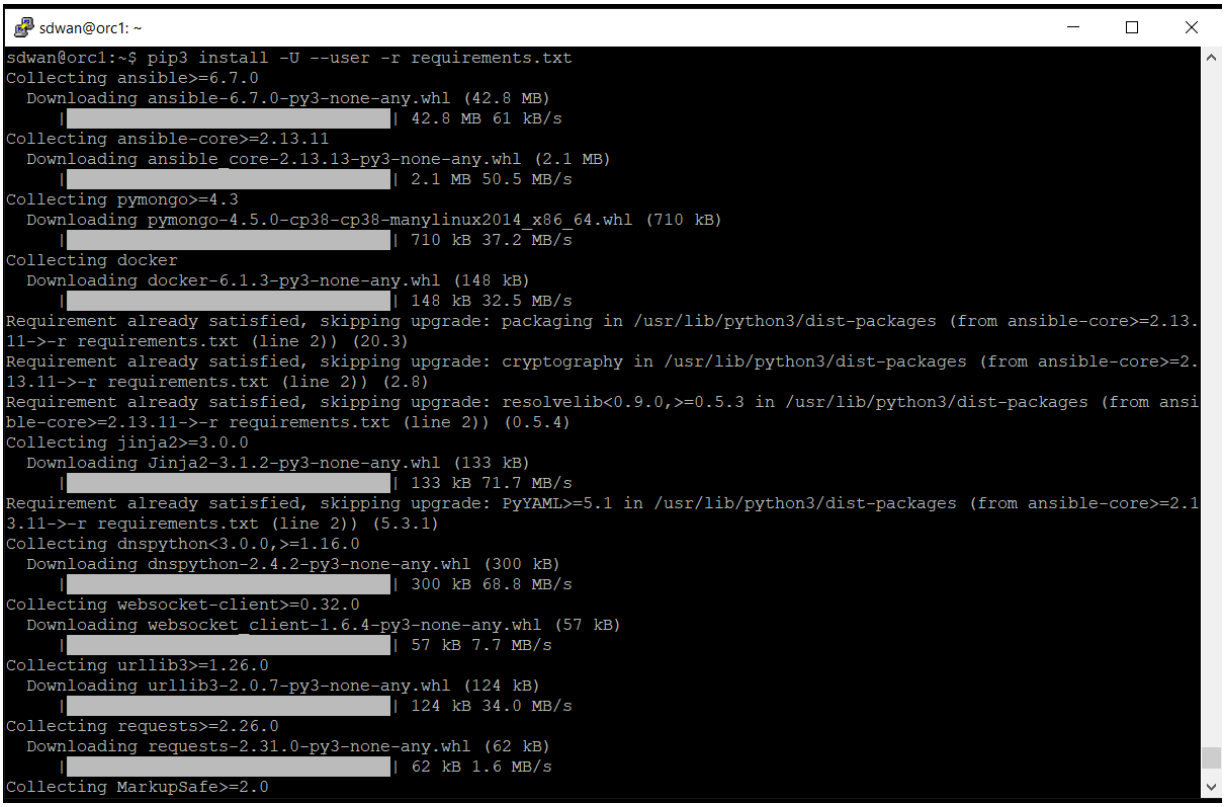
Установить PIP. Выполнить команду ниже.

sdwan@orc1:~$ sudo apt install python3-pip --yes



Установить требуемые пакеты с помощью PIP (Ansible, PyMongo, Docker).

sdwan@orc1:~$ pip3 install -U --user -r requirements.txt



Добавить *$HOME/.local/bin* в переменную PATH(необходимо для корректной работы Ansible).

sdwan@orc1:~$ echo 'export PATH=$PATH:$HOME/.local/bin' >> ~/.bashrc
sdwan@orc1:~$ source ~/.bashrc

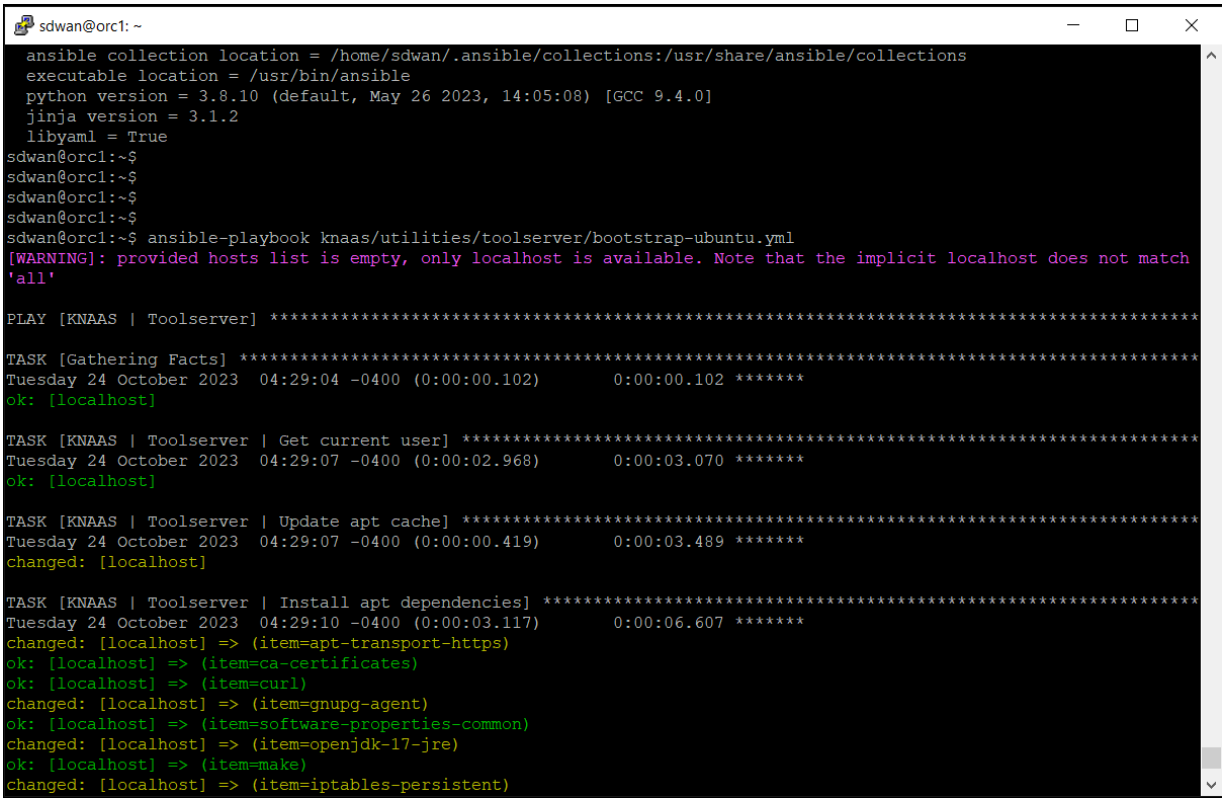
Проверить, что Ansible запускается корректно.

sdwan@orc1:~$ ansible --version

3.2.6. Подготовить хост к установке с использованием плейбука bootstrap-ubuntu.yml (будут установлены необходимые пакеты).

Выполнить:

sdwan@orc1:~$ ansible-playbook knaas/utilities/toolserver/bootstrap-ubuntu.yml

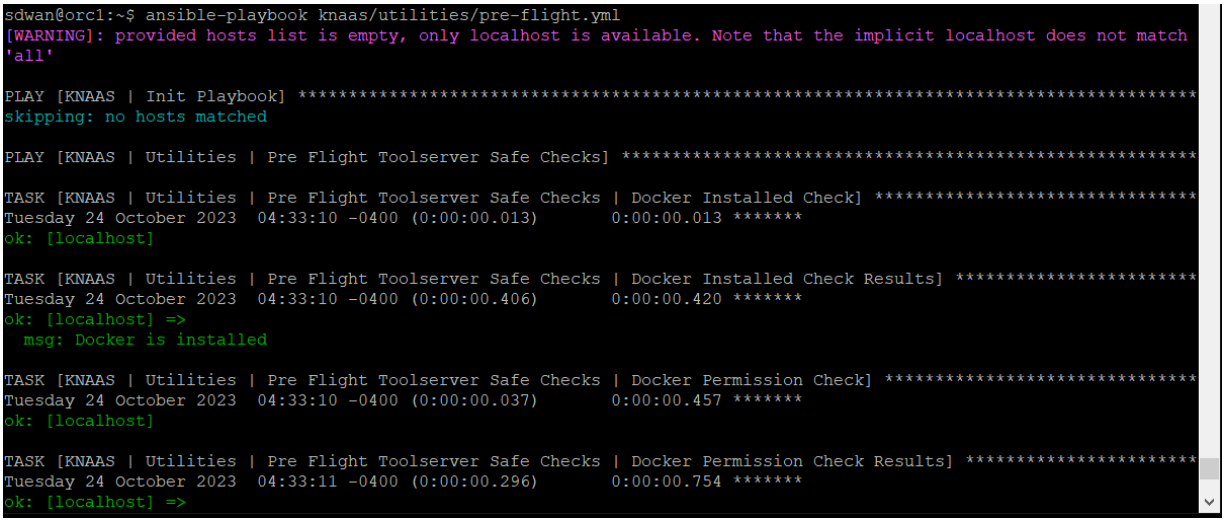


3.2.7. Добавить пользователя *sdwan* в группу *docker*.

sdwan@orc1:~$ sudo usermod -aG docker sdwan
sdwan@orc1:~$ su sdwan

3.2.8. Выполнить проверку перед установкой решения Kasperksy SD-WAN с использованием плейбука pre-flight.

sdwan@orc1:~$ ansible-playbook knaas/utilities/pre-flight.yml



3.2.9. Настроить параметры установки системы управления Kaspersky SD-WAN.

Скопировать базовый файл с переменными (в данном руководстве будет использоваться файл aio.yml):

*sdwan@orc1:~$ cp inventory/external/pnf/aio/variables.yml /home/sdwan/*aio.yml

Открыть для редактирования конфигурационный файл aio.yml:

*sdwan@orc1:~$ vi /home/sdwan/*aio.yml:

Задать следующие основные параметры установки:

- Сеть для контейнеров knaas_os_man base (10.11.13)
- Внутренний и публичный IP адреса хоста orc1: ip_private и ip_public (10.0.1.11 и 10.50.1.14).
- Доменное имя хоста orc1(будет использовано в генерации сертификатов): dn_public (sdwan.local как пример)
- Путь для сохранения сгенерированных паролей от баз данных и vault: vault_password_dirname (/home/sdwan/passwords/)
- Путь для сохранения сертификатов: ssl: path_local (/home/sdwan/ssl)
- Проверить версии контейнеров в соответствии с таблицей 2.4 (параметр tag).

Для установки в плейбуке используется пользователь sdwan, созданный в пункте 3.1.15, в случае использования другого пользователя необходимо изменить настройки на новые значения.

3.2.10. Запуск плейбука установки компонентов системы управления Kaspersky SD-WAN.

Запустить процесс установки системы управления Kaspersky SD-WAN, в ходе которого будут настроены правила межсетевого экранирования iptables, сгенерированы сертификаты удостоверяющего центра и компонентов решения, запущены контейнеры системы управления Kaspersky SD-WAN.

Задать параметр согласия с EULA:

sdwan@orc1:~$ export KNAAS_EULA_AGREED="true"

Для запуска плейбука установки Kaspersky SD-WAN необходимо выполнить команду *ansible-playbook*:

sdwan@orc1:~$ ansible-playbook -e ansible_become_pass=пароль sudo пользователя -i inventory/generic -e "@/home/sdwan/aio.yml" knaas/knaas-install.yml

```
sdwan@orc1: ~
sdwan@orc1:~$
sdwan@orc1:~$
sdwan@orc1:~$
sdwan@orc1:~$
sdwan@orc1:~$
sdwan@orc1:~$ export KNAAS_EULA_AGREED="true"
sdwan@orc1:~$
sdwan@orc1:~$
sdwan@orc1:~$ ansible-playbook -e ansible_become_pass=net543Nsd[  -i inventory/generic -e "@/home/sdwan/poc_aio.yml" k
naas/knaas-install.yml

PLAY [KNAAS | Init Playbook] ***************************************************************************************

TASK [KNAAS | Init Playbook | KNaaS EULA Agreed] *******************************************************************
Tuesday 24 October 2023  04:55:39 -0400 (0:00:00.041)       0:00:00.041 *******
ok: [ctl-1 -> localhost] => changed=false
  msg: All assertions passed

TASK [KNAAS | Init Playbook | Provision Enabled Group] *************************************************************
Tuesday 24 October 2023  04:55:39 -0400 (0:00:00.067)       0:00:00.109 *******
skipping: [ctl-1] => (item=ctl-2)
skipping: [ctl-1] => (item=ctl-3)
skipping: [ctl-1] => (item=orc-2)
skipping: [ctl-1] => (item=www-2)
skipping: [ctl-1] => (item=vnfm-2)
skipping: [ctl-1] => (item=vnfm-proxy-2)
skipping: [ctl-1] => (item=mockpnf-2)
skipping: [ctl-1] => (item=mockpnf-3)
skipping: [ctl-1] => (item=zabbix-srv-2)
skipping: [ctl-1] => (item=zabbix-db-2)
skipping: [ctl-1] => (item=zabbix-proxy-2)
skipping: [ctl-1] => (item=zabbix-www-2)
skipping: [ctl-1] => (item=syslog-2)
skipping: [ctl-1] => (item=syslog-3)
skipping: [ctl-1] => (item=mongo-2)
skipping: [ctl-1] => (item=mongo-3)
skipping: [ctl-1] => (item=redis-2m)
```

После запуска дождаться окончания работы плейбука установки Kaspersky SD-WAN (Ansible playbook).

```
sdwan@orc1: ~
ctl-1                      : ok=32   changed=23   unreachable=0    failed=0    skipped=32   rescued=0    ignored=0
mockpnf-1                  : ok=16   changed=10   unreachable=0    failed=0    skipped=30   rescued=0    ignored=0
mongo-1                    : ok=27   changed=16   unreachable=0    failed=0    skipped=25   rescued=0    ignored=0
orc-1                      : ok=24   changed=18   unreachable=0    failed=0    skipped=26   rescued=0    ignored=0
redis-1m                   : ok=16   changed=10   unreachable=0    failed=0    skipped=33   rescued=0    ignored=0
syslog-1                   : ok=16   changed=10   unreachable=0    failed=0    skipped=30   rescued=0    ignored=0
vnfm-1                     : ok=21   changed=16   unreachable=0    failed=0    skipped=28   rescued=0    ignored=0
vnfm-proxy-1               : ok=17   changed=13   unreachable=0    failed=0    skipped=29   rescued=0    ignored=0
www-1                      : ok=17   changed=13   unreachable=0    failed=0    skipped=29   rescued=0    ignored=0
zabbix-db-1                : ok=21   changed=13   unreachable=0    failed=0    skipped=28   rescued=0    ignored=0
zabbix-proxy-1             : ok=22   changed=14   unreachable=0    failed=0    skipped=27   rescued=0    ignored=0
zabbix-srv-1               : ok=21   changed=14   unreachable=0    failed=0    skipped=28   rescued=0    ignored=0
zabbix-www-1               : ok=23   changed=15   unreachable=0    failed=0    skipped=26   rescued=0    ignored=0

Tuesday 24 October 2023  04:58:32 -0400 (0:00:01.576)       0:02:53.322 *******
===============================================================================
KNAAS | PREPARE | Fetch Docker Images | Load Docker Images Remote ------------------------------------------ 46.12s
KNAAS | INSTALL | SSL | Zabbix WWW Generate Diffie-Hellman parameters ---------------------------------------- 28.24s
zabbix_srv_install : KNAAS | INSTALL | Zabbix | Deploy Server ----------------------------------------------- 12.21s
KNAAS | PREPARE | Fetch Docker Images | Copy Docker Images ------------------------------------------------ 8.65s
zabbix_www_install : KNAAS | INSTALL | Zabbix | Deploy Zabbix WWW ------------------------------------------- 5.06s
zabbix_proxy_install : KNAAS | INSTALL | Zabbix | Deploy Proxy ----------------------------------------------- 4.32s
KNAAS | PREPARE | SSL | Generate Host Private Keys ---------------------------------------------------------- 3.73s
KNAAS | PREPARE | Provision iptables | Open external tcp ports ------------------------------------------- 2.69s
KNAAS | INSTALL | KNaaS Orchestrator | Deploy Orchestrator ------------------------------------------------ 2.55s
KNAAS | INSTALL | KNaaS Controller | Deploy Controller ---------------------------------------------------- 2.23s
zabbix_db_install : KNAAS | INSTALL | Zabbix | Deploy MariaDB ---------------------------------------------- 2.09s
KNAAS | INSTALL | KNaaS VNFM Proxy | Deploy VNFM Proxy ------------------------------------------------- 2.02s
KNAAS | PREPARE | SSL | Generate CA Private Key -------------------------------------------------------- 1.91s
KNAAS | INSTALL | MongoDB | Config | Create ReplicaSet ------------------------------------------------ 1.78s
KNAAS | PREPARE | SSL | Generate CA Certificate -------------------------------------------------------- 1.76s
KNAAS | INSTALL | Deploy | Syslog ------------------------------------------------------------------------ 1.73s
KNAAS | INSTALL | MongoDB | Config | Create MongoDB ---------------------------------------------------- 1.72s
KNAAS | INSTALL | KNaaS VNFM | Deploy VNFM ------------------------------------------------------------- 1.69s
KNAAS | INSTALL | KNaaS Orchestrator | Embed PKCS12 TrustStore CA ---------------------------------------- 1.66s
KNAAS | INSTALL | Redis | Deploy Redis ------------------------------------------------------------------ 1.60s
sdwan@orc1:~$
```

В ходе установки будут сгенерированы пароли для баз данных и сертификатов. По умолчанию они будут сохранены в /home/sdwan/passwords/keystore.yml и зашифрованы с помощью ansible-vault. Пароль для vault также будет сгенерирован и сохранен в /home/sdwan/passwords/vault_password.txt.

Сохраните файлы и пароль vault для дальнейшего использования!

3.2.11. Очистить историю команд.

sdwan@orc1:~$ history -c && history -w

3.2.12. При необходимости повторного запуска программы установки Kaspersky SD-WAN необходимо произвести удаление установленных компонентов. Для этого необходимо запустить плейбук *knaas-teardown.yml*

sdwan@orc1:~$ ansible-playbook -i inventory/generic -e "@/home/sdwan/aio.yml" -e "ansible_become_password=пароль sudo пользователя" knaas/knaas-teardown.yml

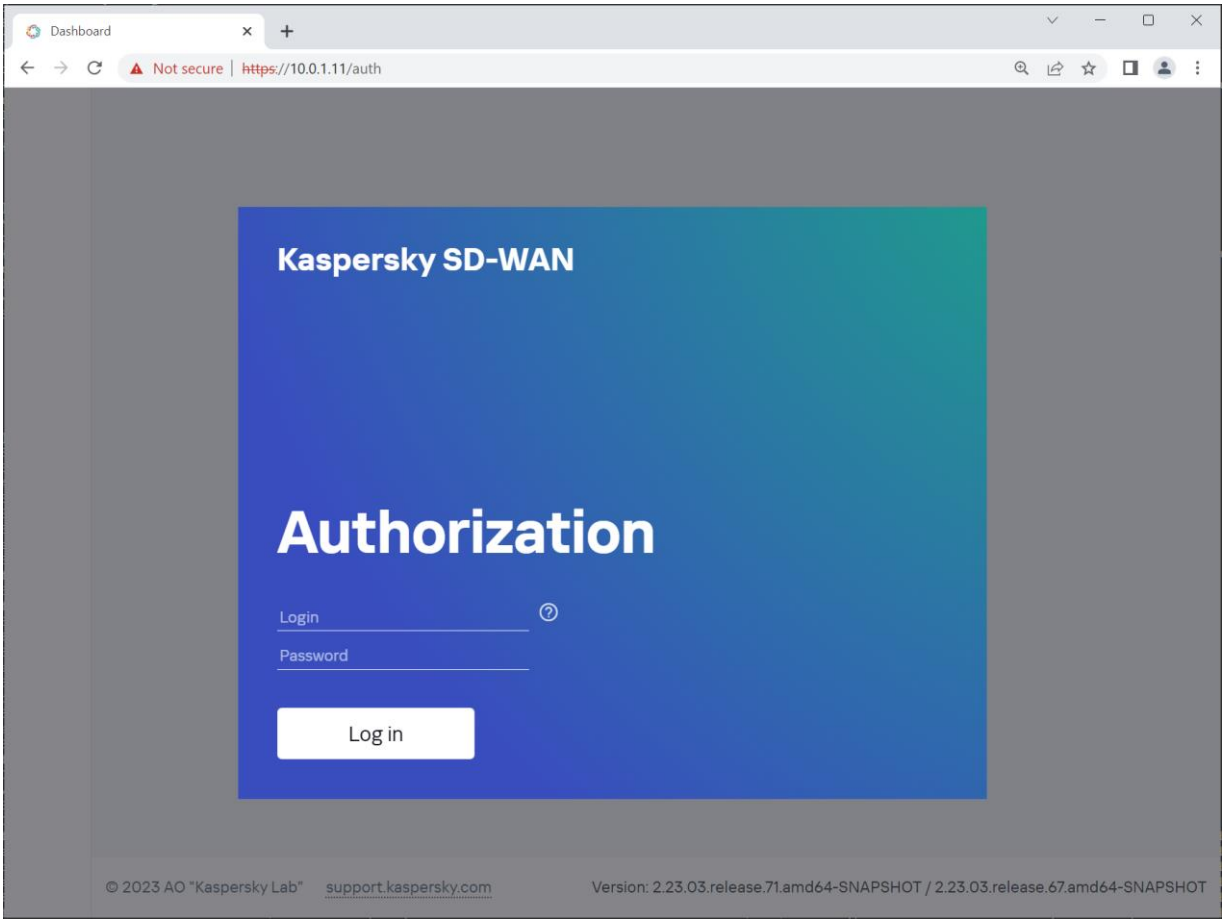
3.3. **Подключение к консоли управления Kaspersky SD-WAN.**

3.3.1. Вход в Kaspersky SD-WAN.

Данные для входа:

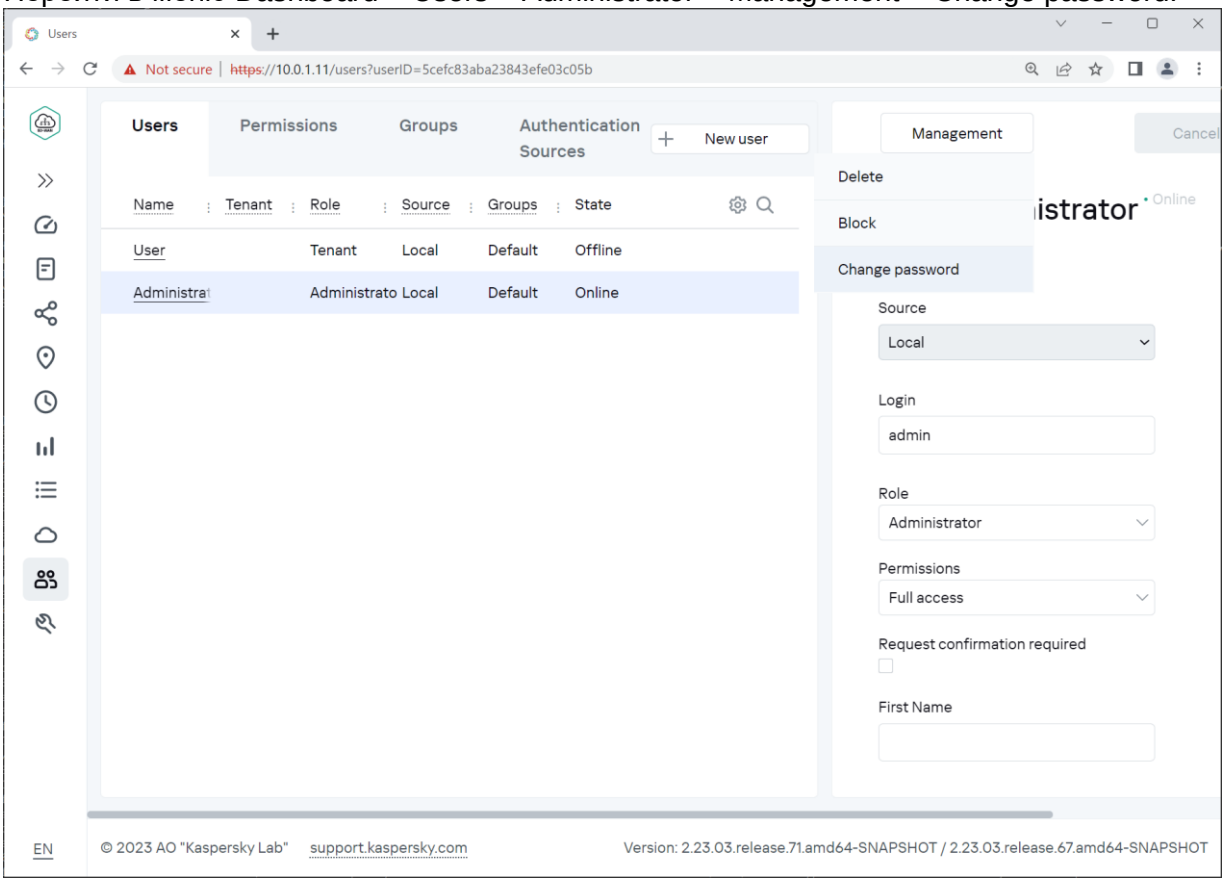
- Логин и пароль «по умолчанию»: admin & admin
- https://10.0.1.11

При изменении IP плана из пункта 2.3 использовать новый IP адрес хоста orc1.



3.3.2. Сменить пароль пользователя admin.

Перейти в меню Dashboard > Users > Administrator > Management > Change password:

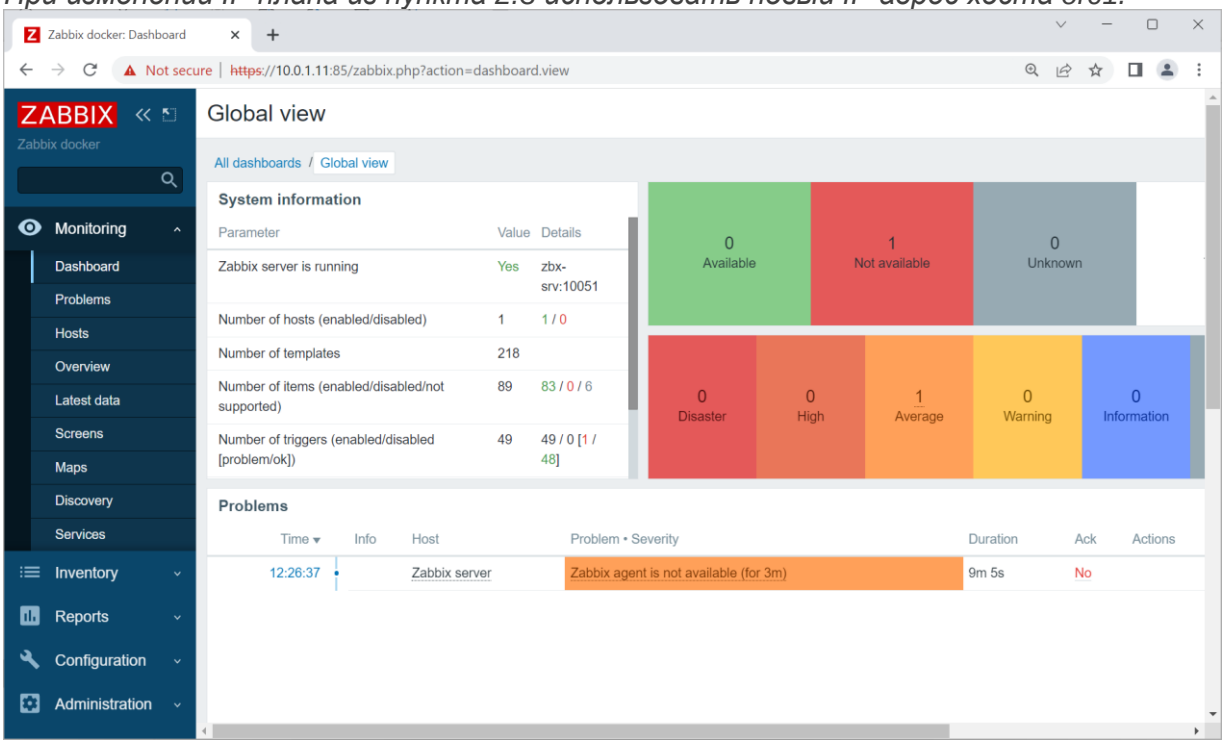


3.4. **Подключение к веб- консоли управления и настройка системы мониторинга Zabbix.**

3.4.1. Для подключения к веб- консоли управления Zabbix необходимо перейти по ссылке: https://10.0.1.11:85

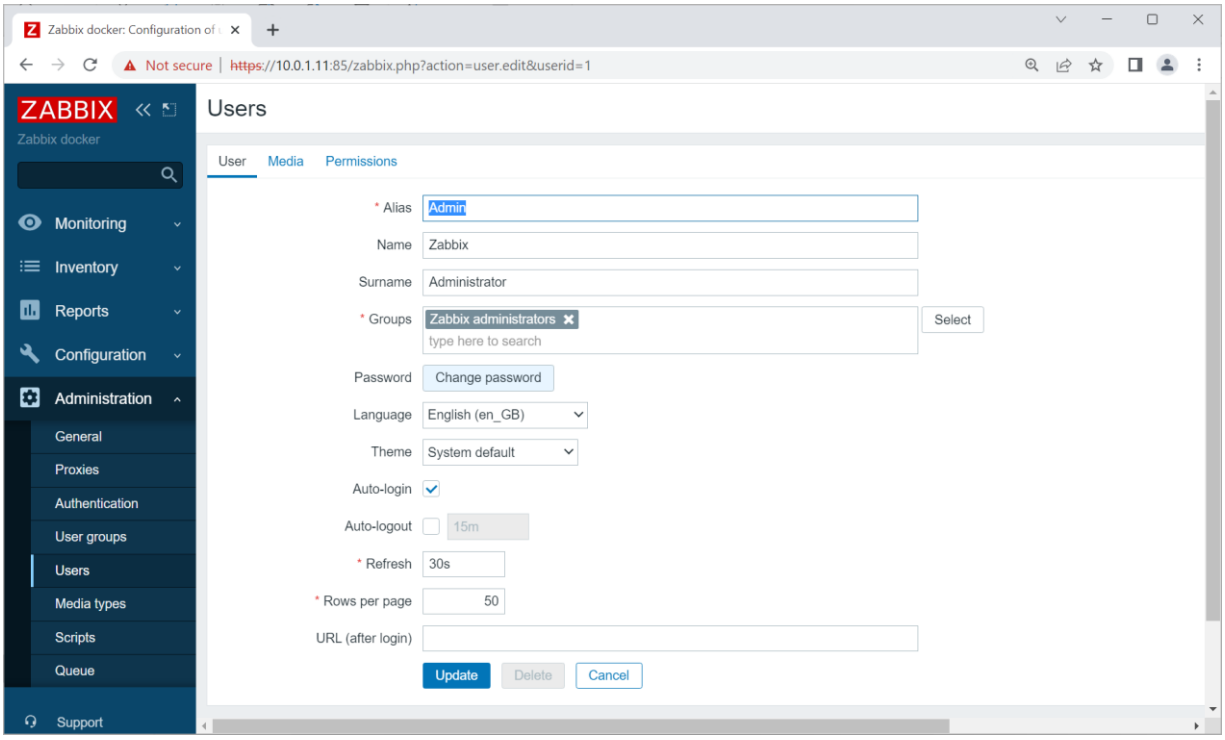
Пароль по умолчанию: Admin & zabbix.

При изменении IP плана из пункта 2.3 использовать новый IP адрес хоста orc1.



3.4.2. Сменить пароль пользователя Admin.

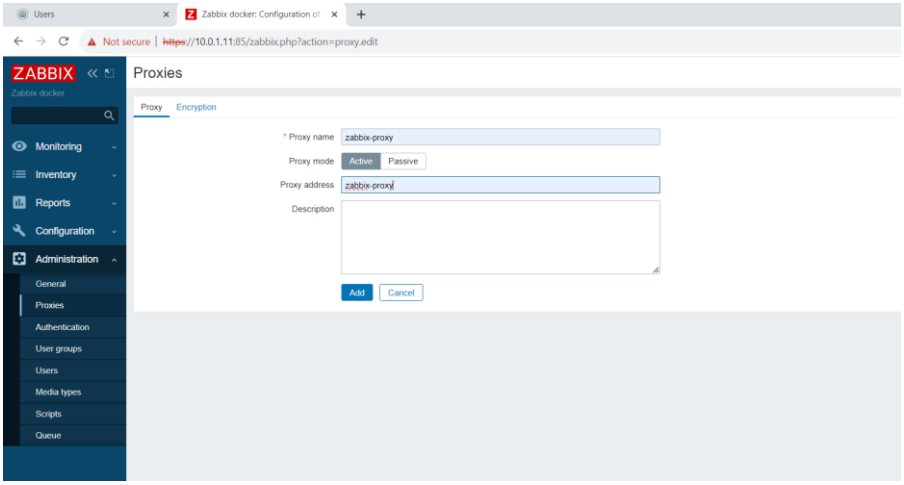
Перейти в меню Administration > Users >Admin > Change password.

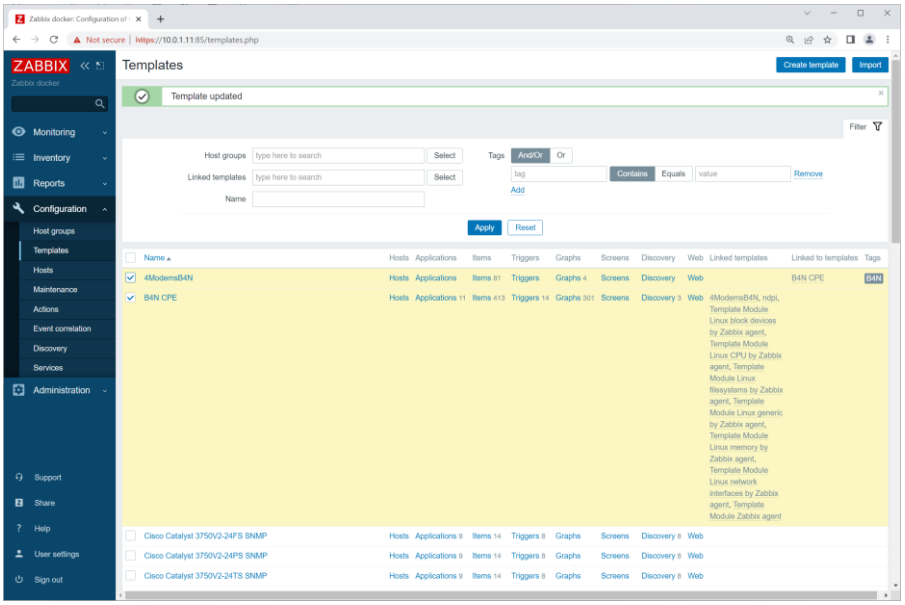


3.4.3. Добавить Zabbix Proxy.

Перейти в меню Administration > Proxies, нажать Create Proxy.

В поле Proxy name и Proxy address ввести: zabbix-proxy и нажать Add.



3.4.4. Перейти в меню Configuration > Templates, нажать Import и импортировать шаблоны: “4ModemsB4N” и “B4N CPE”.	

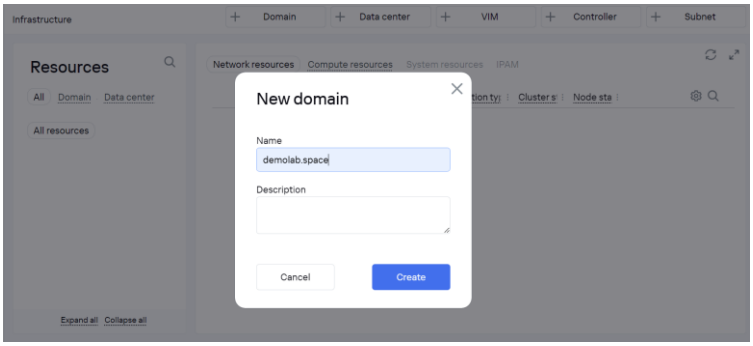
4. **Базовая настройка Kaspersky SD-WAN**

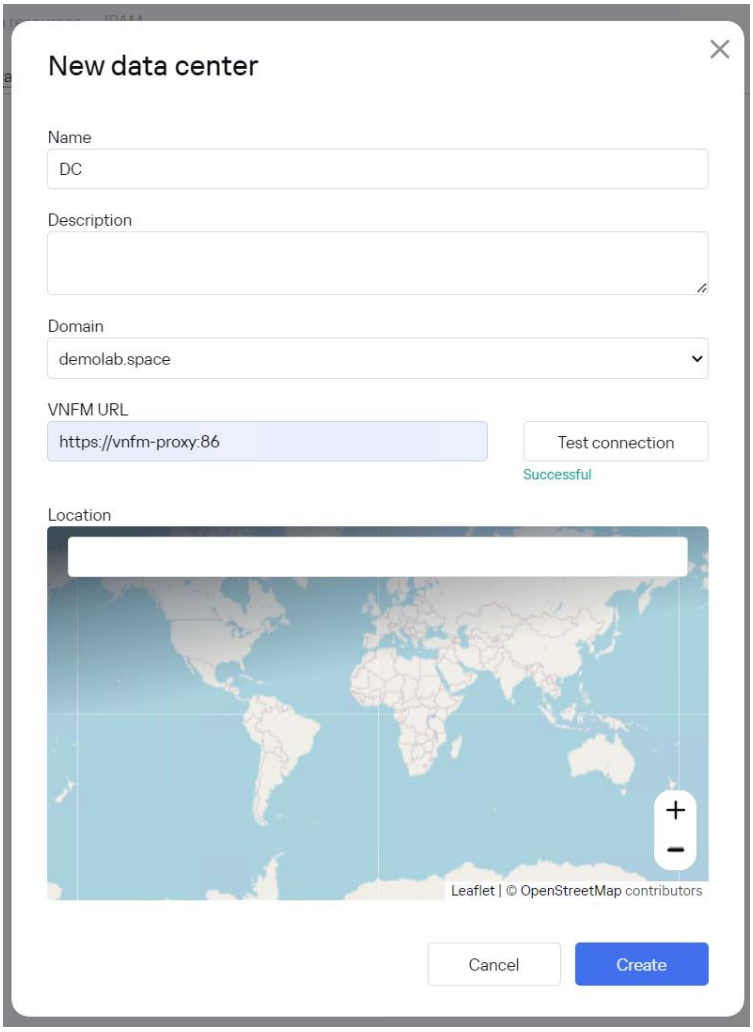
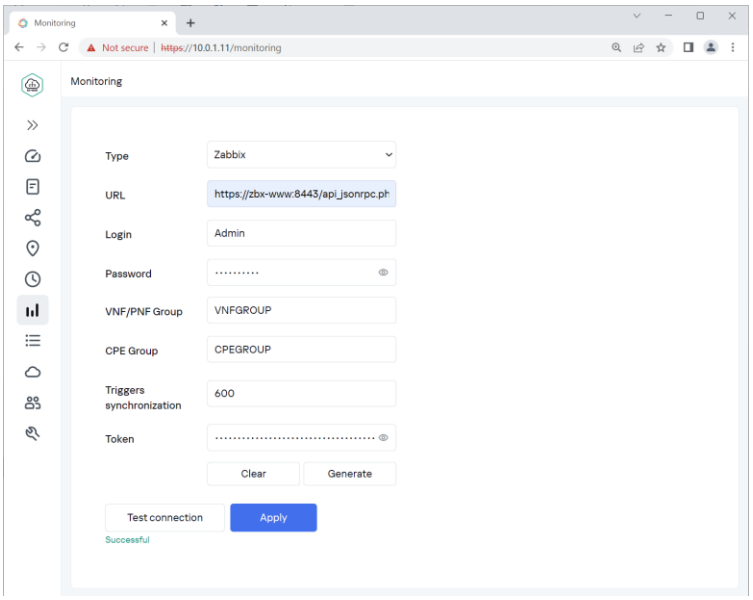
4.1. **Создание домена и центра обработки данных**

Оркестратор управляет сетевыми и вычислительными ресурсами, которые могут принадлежать разным доменам (Domain) и центрам обработки данных (Data Center).

Домен - логическая группа ресурсов под единым административным управлением.

Центр обработки данных - логическая сущность, позволяющая группировать сетевые и вычислительные ресурсы.

4.1.1. Создать домен и вложенный центр обработки данных. В разделе “Infrastructure” использовать кнопку “+Domain”. При создании домена необходимо ввести его имя и, опционально, комментарий.	

4.1.2. Создать Data Center. В разделе “Infrastructure” использовать кнопку “+Data Center”. В поле VNF URL ввести: https://vnfm-proxy:86 Нажать Test Connection и Create.	
4.1.3. Подключение к серверу мониторинга. Перейти в меню “Monitoring”. Type – выбрать Zabbix. URL – задать URL к Zabbix API: https://zbx-www:8443/api_jsonrpc.php Login – имя пользователя для подключения к Zabbix API (с правами read/write в группах, где будут создаваться CPE для мониторинга). Login: Admin Password: net543Nsd[	

VNF/PNF Group: VNFGROUP CPE Group: CPEGROUP Нажать кнопку “Generate”, чтобы сгенерировать токен для подключения к серверу Zabbix. Нажать “Test connection”, для проверки доступности сервера Zabbix (т.е. правильность введенных настроек). Нажать Apply.	

4.1.4. Настройка системных ресурсов.

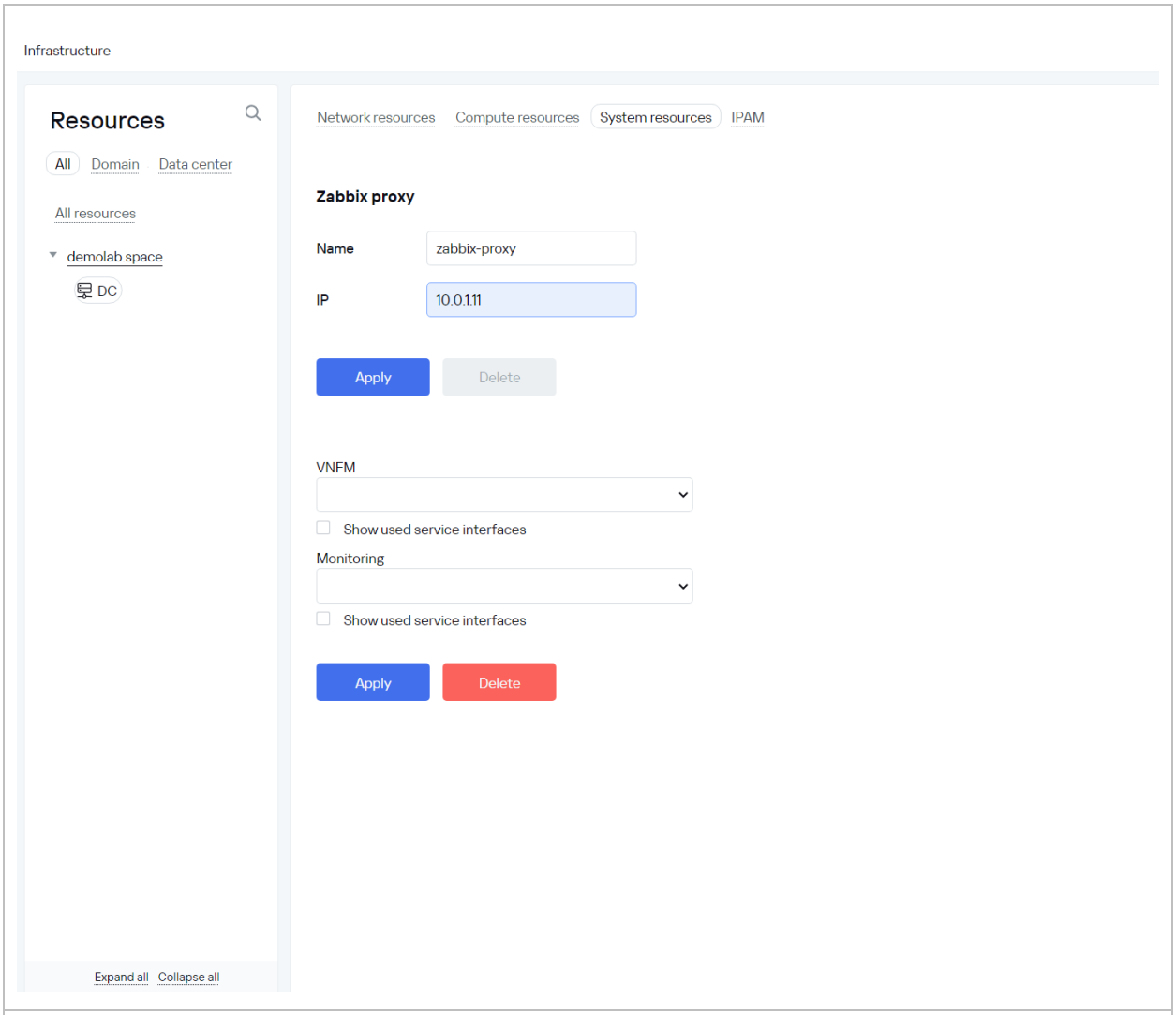
В основном меню справа выбрать раздел “Infrastructure”, далее в дереве ресурсов выбрать DC и перейти на вкладку “System Resources”.

Указать информацию для подключения к серверу Zabbix Proxy:

- Имя Zabbix Proxy (должно совпадать с именем, указанным в настройках Zabbix Server): zabbix-proxy
- IP адрес: 10.0.1.11

При изменении IP плана из пункта 2.3 использовать новый IP адрес хоста orc1.

Нажать Apply.



4.1.5. Добавление пула IP адресов для сети управления.

Настроить пулы IP адресов для CPE устройств.

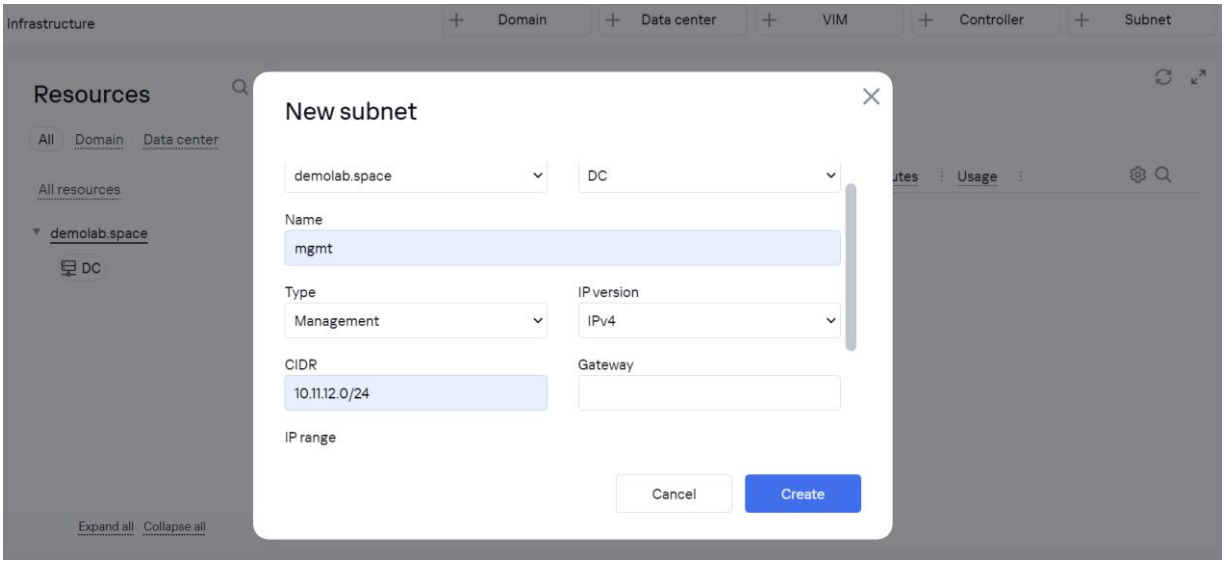
Для каждого DC выделяются один или несколько диапазонов адресов IPAM (IP Address Management).

Перейти на вкладку Infrastructure > Domain > DC > IPAM и нажать кнопку ‘+Subnet”.
Указать необходимую информацию:

- Name: mgmt
- CIDR: 10.11.12.0/24
- IP Range: 10.11.12.13 – 10.11.12.253

Нажать Create.

Если требуется использовать другую подсеть, то необходимо изменить соответствующие адреса в шаблонах vGW и маршруты на R13.



4.1.6. Подготовить PNF дескриптор для SD-WAN контроллера.

Пример дескриптора PNF находится в архиве с плейбуками установки по пути:
pnfs/pnd_sdwan_single_ctl/src/

Скопировать файлы дескриптора из архива и внести изменения в дескриптор pnfd.xml

Задать адрес оркестратора в переменной orc_ip: ввести IP адрес шлюза из сети Docker knaas_os_man (заданной в пункте 3.2.9): 10.11.13.1.
Данный адрес будет использоваться для связи контроллера с оркестратором.
При изменении этой сети изменить адрес на другой.

Задать публичный IP адрес SD-WAN контроллера в переменной ctl1_external_ip.

Содержание файла pnfd.xml:

```
<?xml version="1.0" encoding="UTF-8" ?>
<pnfd>
   <name>SD-WAN CTL PNF</name>
   <description>Kaspersky SD-WAN Solution</description>
   <provider>AO Kaspersky Lab</provider>
   <version>2.23.07.0</version>
   <connection-points>
      <external>
            <connection-point>
            <name>WAN-CTL1</name>
            <description>WAN-CTL1</description>
            <ip>AUTO</ip>
            <mask>AUTO</mask>
         </connection-point>
      </external>
   </connection-points>
   <configurations>
      <configuration>
         <name>deploy_containers1</name>
         <filename>ctl1_deploy.sh</filename>
         <executor>/bin/ash</executor>
         <authentication>password</authentication>
         <stage>initialization</stage>
      </configuration>
```

```
</configurations>
<user-configuration>
<tabs>
   <tab>
      <name>Orchestrator</name>
      <variables>
         <variable>
            <name>orc_ip</name>
            <description>Orchestrator's API IP</description>
            <input-type>input</input-type>
            <required>true</required>
            <type>string</type>
            <default-value>10.11.13.1</default-value>
            <example>10.11.13.1</example>
         </variable>
         <variable>
            <name>orc_port</name>
            <description>Orchestrator's API Port</description>
            <input-type>input</input-type>
            <required>true</required>
            <type>string</type>
            <default-value>443</default-value>
            <example>443</example>
         </variable>
         <variable>
            <name>orc_proto</name>
            <description>Protocol for Orchestrator API</description>
            <input-type>input</input-type>
            <required>true</required>
            <type>string</type>
            <default-value>https</default-value>
            <example>https</example>
         </variable>
      </variables>
   </tab>
   <tab>
      <name>CTL1</name>
      <variables>
         <variable>
            <name>ctl1_ip</name>
            <description>Internal ip of the second interface of the ctl</description>
            <input-type>input</input-type>
            <required>true</required>
            <type>string</type>
            <default-value>10.11.11.97</default-value>
            <example>172.17.9.228</example>
         </variable>
         <variable>
            <name>ctl1_port</name>
            <description>SD-WAN Ctl port</description>
            <input-type>input</input-type>
            <required>true</required>
            <type>string</type>
            <default-value>6653</default-value>
            <example>6653</example>
         </variable>
         <variable>
            <name>ctl1_external_ip</name>
            <description>External ip of the ctl</description>
            <input-type>input</input-type>
            <required>true</required>
            <type>string</type>
            <default-value>10.50.1.14</default-value>
            <example>172.17.9.228</example>
         </variable>
      </variables>
   </tab>
</tabs>
</user-configuration>
<flavours>
```

```
    <flavour>
      <name>Standard</name>
      <description>Standard SD-WAN</description>
      <position>1</position>
      <management>
      </management>
      <vdus>
        <vdu>
          <name>ctl</name>
          <start-order>1</start-order>
          <ssh-port>22022</ssh-port>
          <zabbix_template>Template OS Linux by Zabbix agent</zabbix_template>
          <monitoring-type>agent</monitoring-type>
          <configurations>
            <configuration-name-ref>deploy_containers1</configuration-name-ref>
          </configurations>
          <def-user>root</def-user>
          <def-password>samplePassword</def-password>
          <password-authentication>yes</password-authentication>
          <network-interfaces>
            <interface>
              <name>Management</name>
              <type>management</type>
              <description>1</description>
            </interface>
            <interface>
              <name>2</name>
              <type>data</type>
              <description>WAN-CTL1</description>
              <connection-point-ref>WAN-CTL1</connection-point-ref>
            </interface>
          </network-interfaces>
        </vdu>
      </vdus>
    </flavour>
  </flavours>
</pnfd>
```

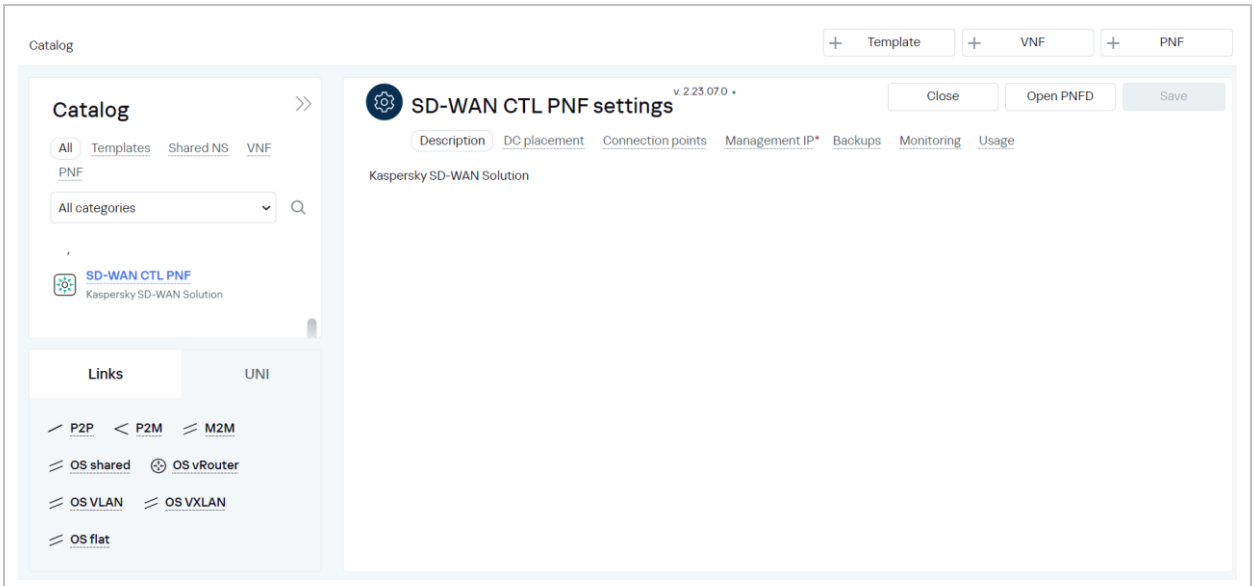
После внесения изменений упаковать файлы в архив pnf_sdwan_single_ctl.2.23.07.1.zip.

Также для создания архива можно воспользоваться утилитой *make*:

Выполнить make из папки pnfs/pnd_sdwan_single_ctl/.

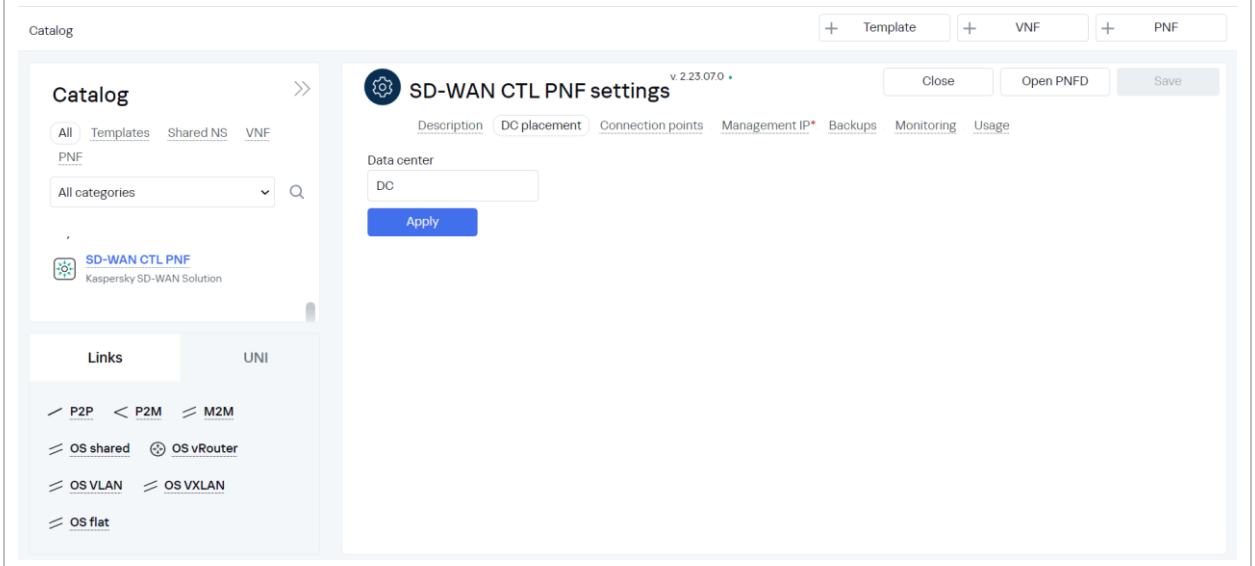
4.1.7. Импортировать PNF CTL в Catalog:

- В меню слева выбрать Catalog, нажать кнопку добавления PNF («+PNF»).
- Указать путь и выбрать готовый для загрузки архив pnf_sdwan_single_ctl.2.23.07.1.zip
- Дождаться загрузки PNF в каталог.



4.1.8. Перейти на вкладку PNF. Нажать на Physical Network Function > SD-WAN-CTL-PNF.

Перейти на закладку DC Placement, выбрать DC, нажать Apply.



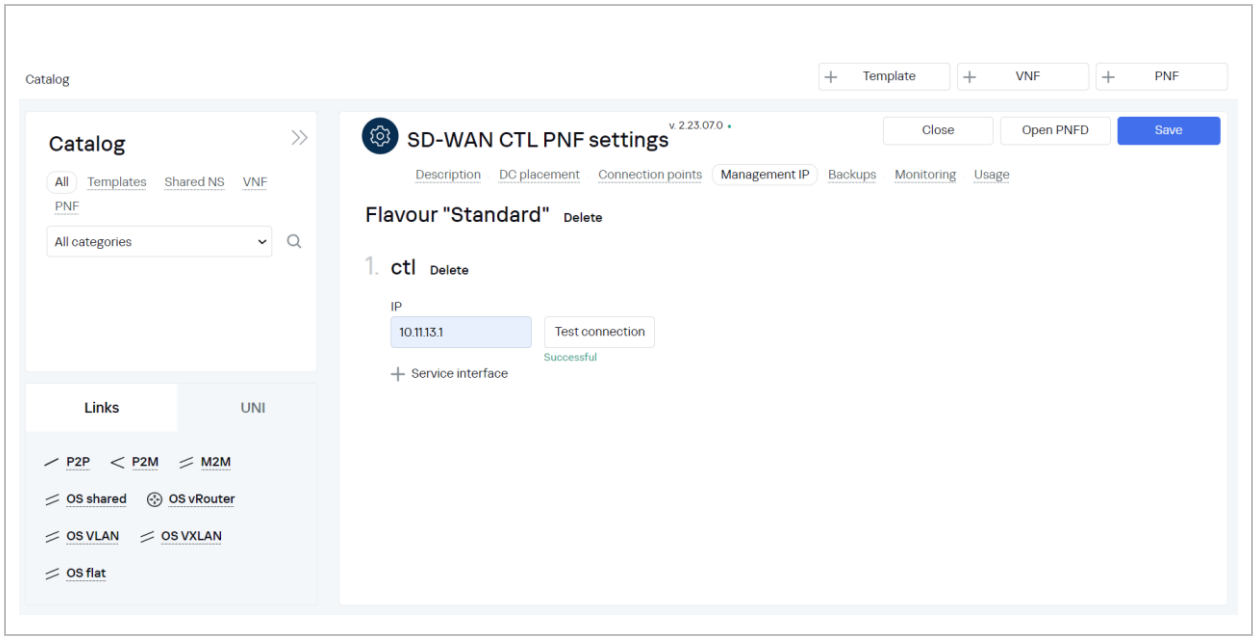
4.1.9. Перейти на закладку Management IP.

Дважды нажать Add для добавления IP адреса SD-WAN контроллера.

Ввести начальный IP адрес из сети knaas_os_man (заданной в пункте 3.2.9): 10.11.13.1. При изменении этой сети изменить адрес на другой.

Нажать Test Connection (в случае успешной проверки появится надпись Successful).

Нажать Save.


Catalog
Template
VNF
PNF
Catalog
All
Templates
Shared NS
VNF
PNF
All categories
Links
UNI
P2P
P2M
M2M
OS shared
OS vRouter
OS VLAN
OS VXLAN
OS flat
SD-WAN CTL PNF settings
v. 2.23.07.0
Close
Open PNFD
Save
Description
DC placement
Connection points
Management IP
Backups
Monitoring
Usage
Flavour "Standard"
Delete
1. ctl
Delete
IP
10.11.13.1
Test connection
Successful
Service interface

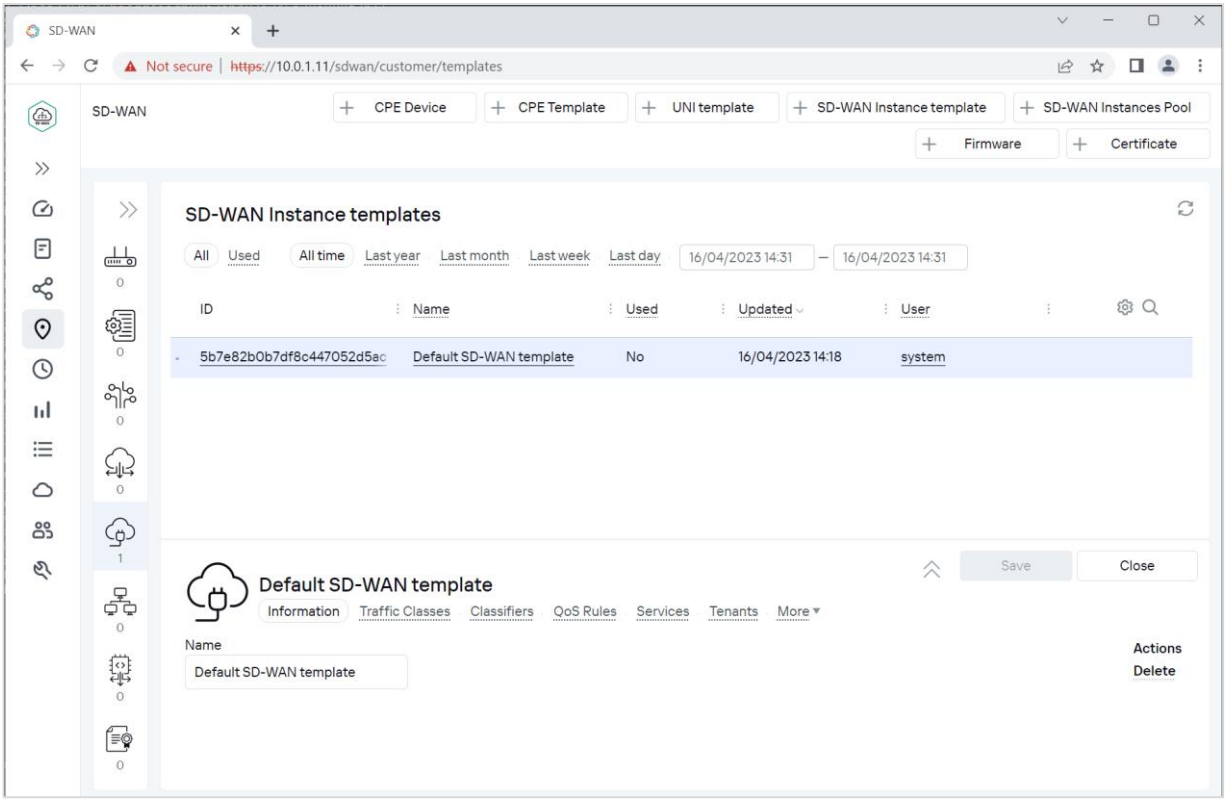
4.2. **Создание шаблона экземпляра SD-WAN.**

Шаблон экземпляра SD-WAN (англ. SD-WAN Instance template) содержит параметры наложенной SDN-сети. Применяется к контроллеру SD-WAN после развертывания сервиса SD-WAN. Для добавления шаблона экземпляра SD-WAN необходимо перейти в раздел SD-WAN веб-интерфейса оркестратора, после чего перейти в подраздел SD-WAN Instance template.

4.2.1. Настройка шаблона SD-WAN Instance.

Перейти в раздел SD-WAN > SD-WAN Instance templates и открыть для редактирования шаблон Default SD-WAN Instance template.

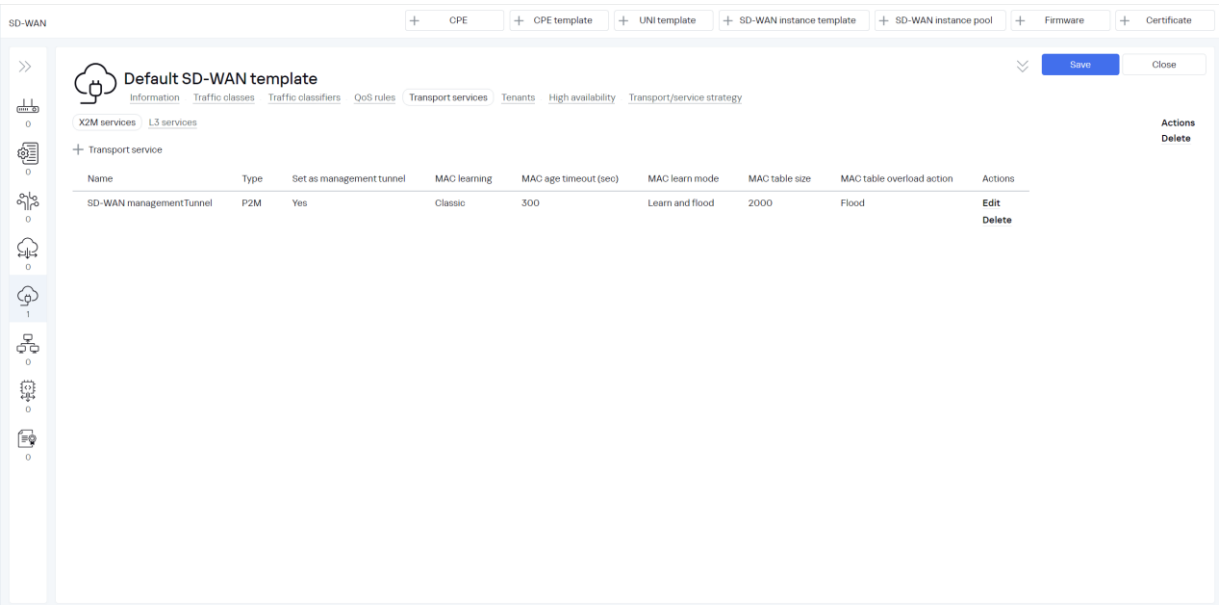
В поле Name задать имя или оставить значение «по умолчанию».



4.2.2. Перейти на вкладку Transport Services.

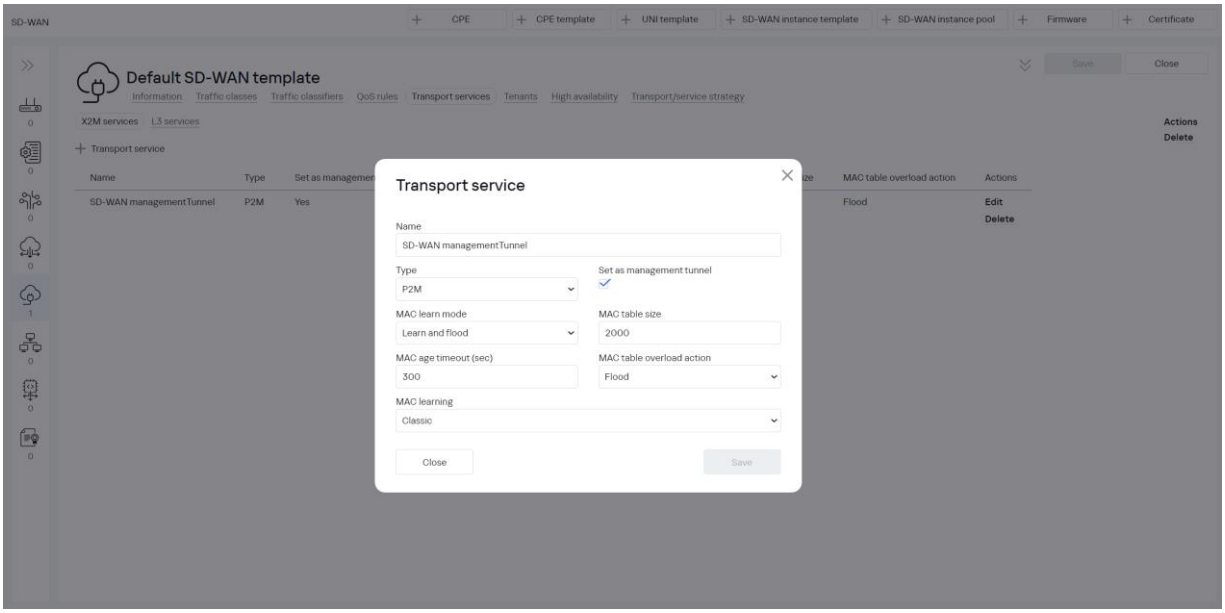
Удалить сервис SD-WAN P2M Data.

Оставить только SD-WAN managementTunnel.



4.2.3. Нажать Edit для редактирования параметров SD-WAN managementTunnel.

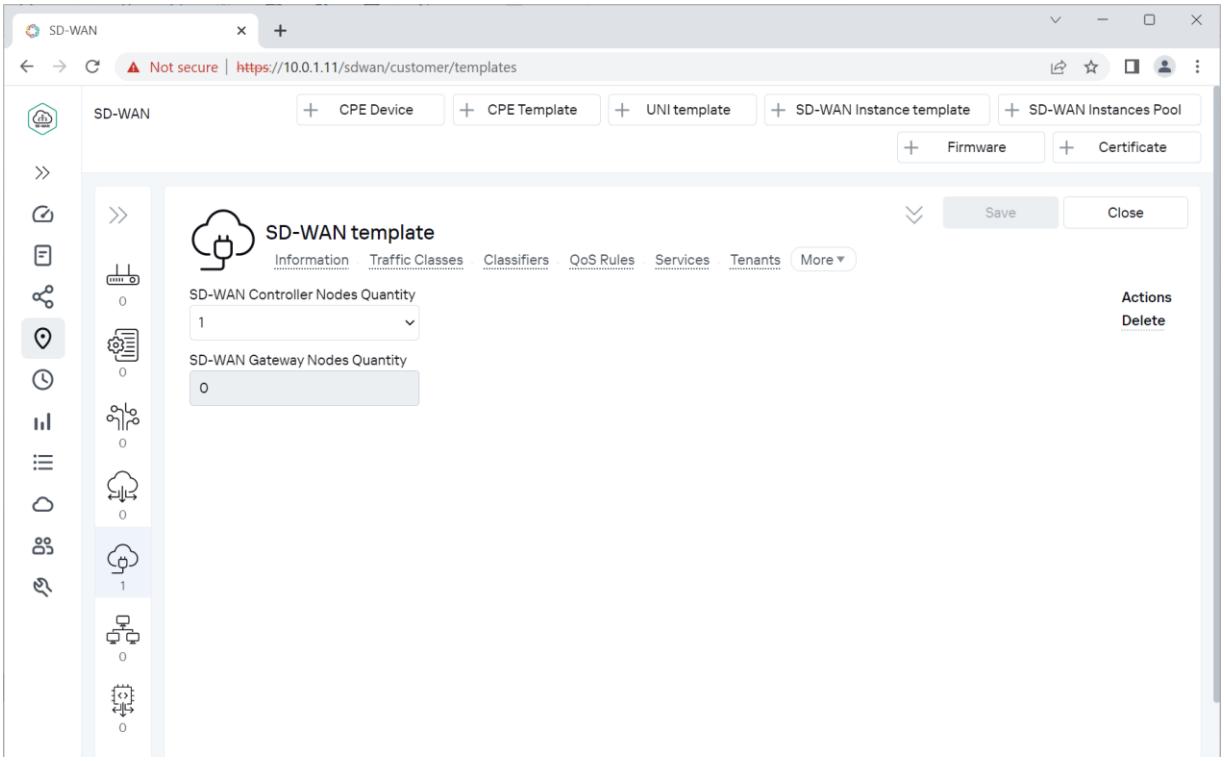
Настройки «по умолчанию» соответствуют информации на снимке экрана.



4.2.4. Перейти на вкладку High Availability.

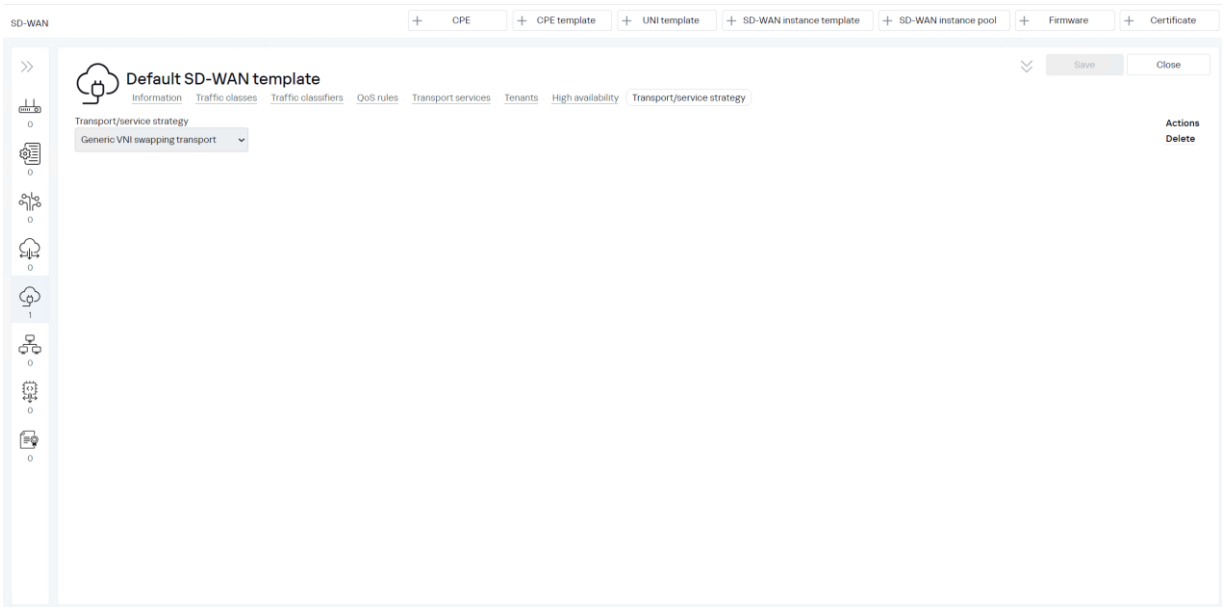
Значения по умолчанию:

- SD-WAN Controller Nodes Quantity: 1
- SD-WAN Gateway Nodes Quantity: 0



4.2.5. Перейти на вкладку Transport/Service Strategy.

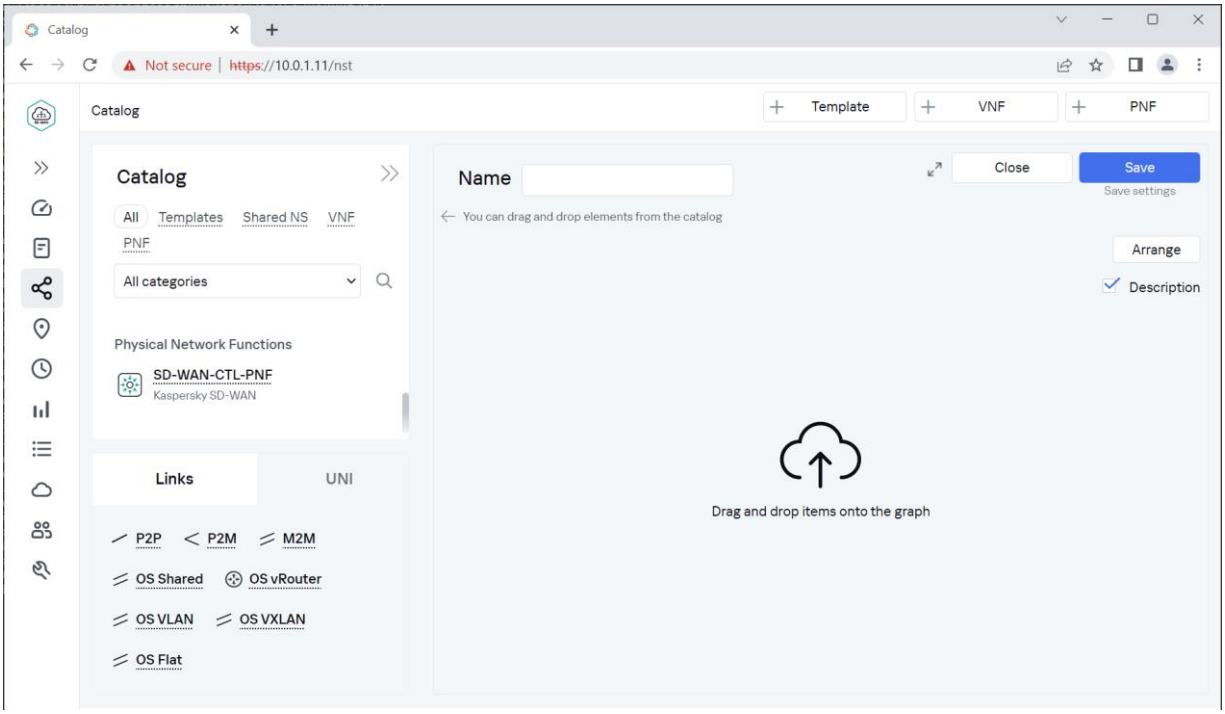
Значение: Generic VNI Swapping Transport означает решение SD-WAN.



4.3. **Создание шаблона сервиса SD-WAN.**

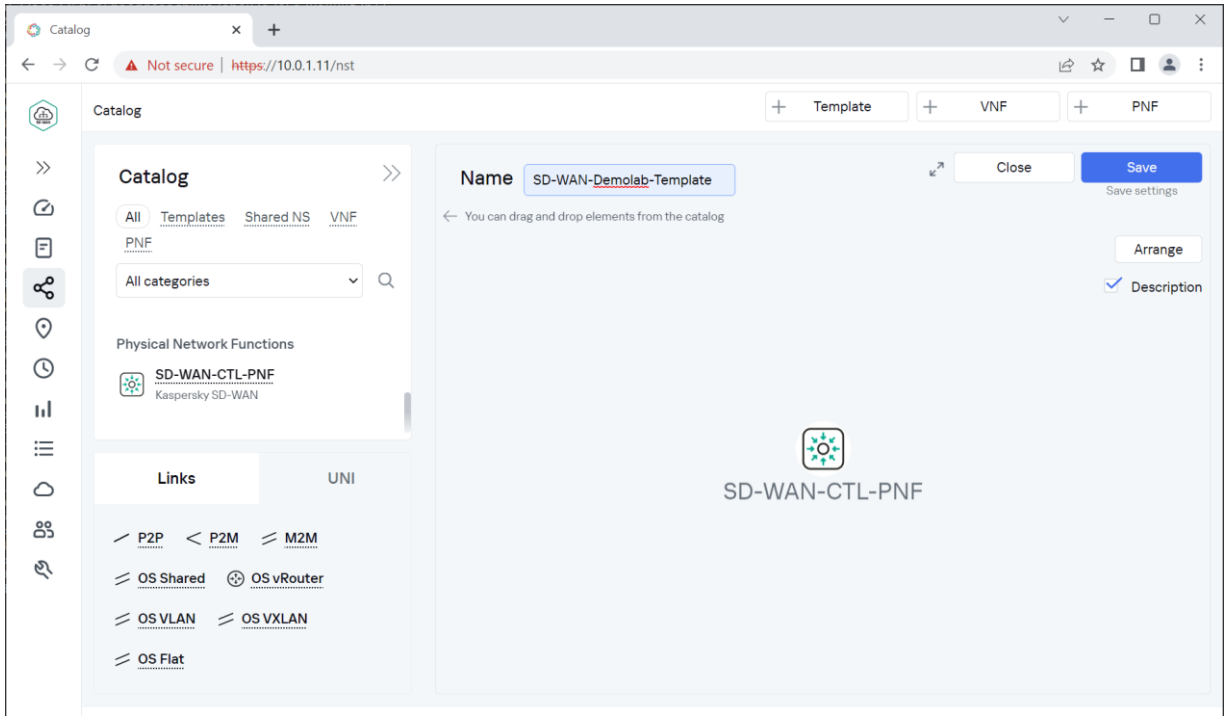
4.3.1. Создание шаблона сервиса SD-WAN.

Перейти в меню Catalog, нажать кнопку добавления шаблона сетевого сервиса “+Template”.

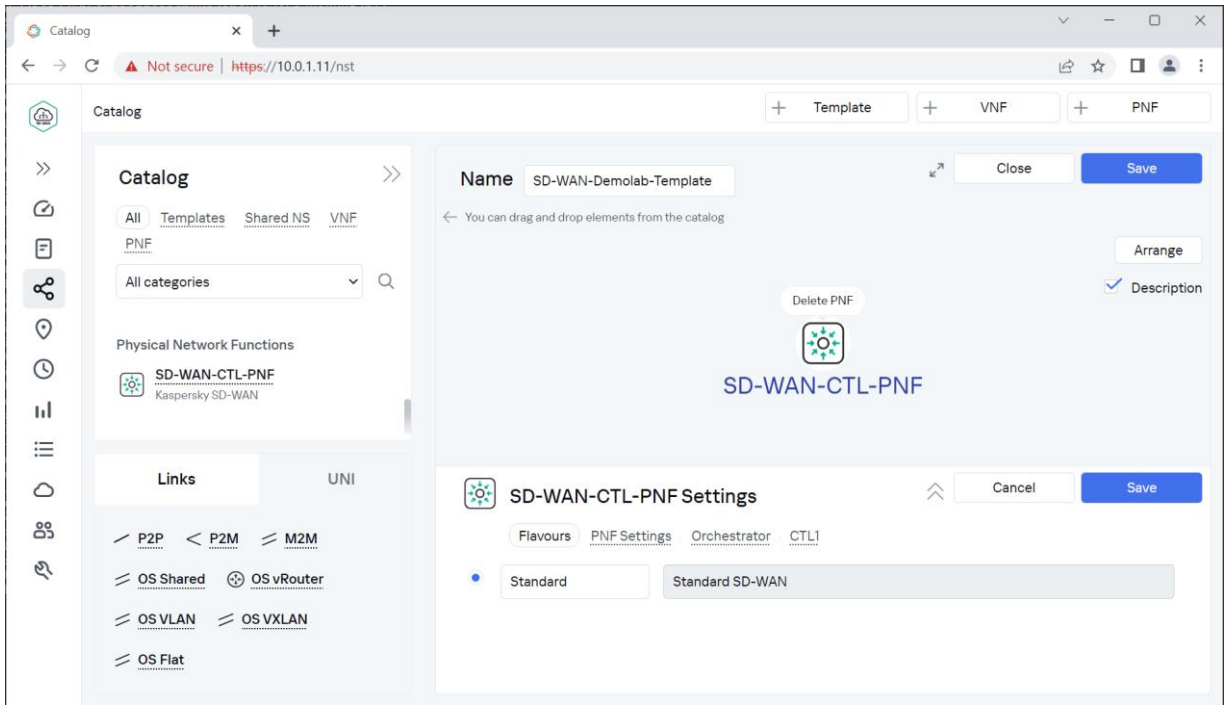


4.3.2. Перетащить с помощью мыши в окно конструктора SD-WAN контроллер в виде PNF(SD-WAN-CTL-PNF).

Задать имя шаблона и нажать Save.

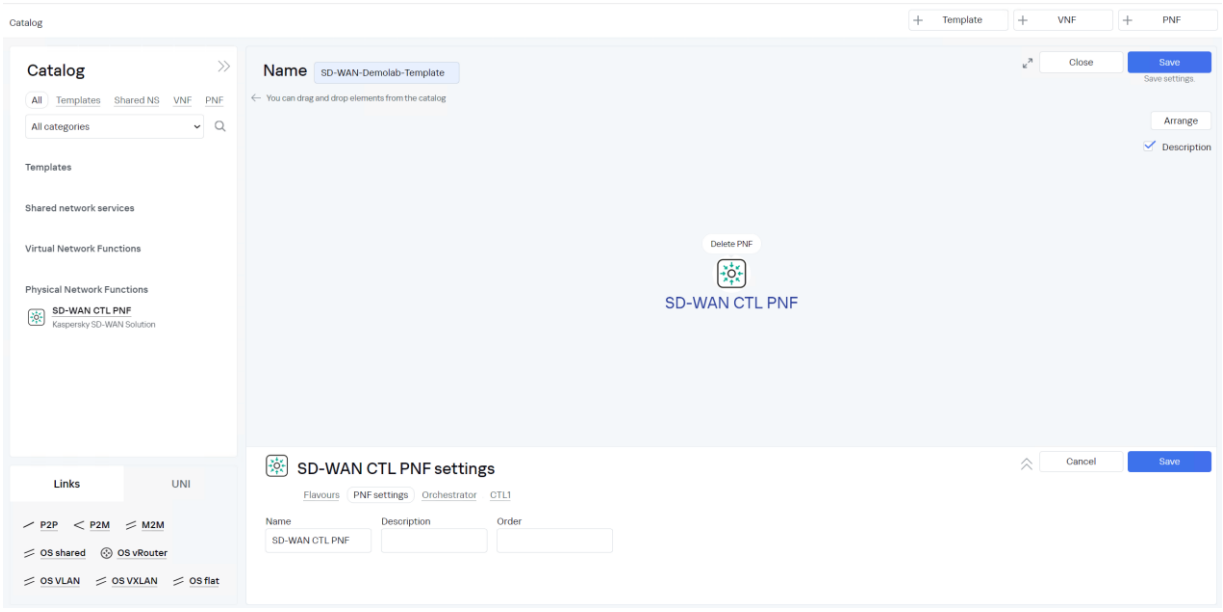


4.3.3. Нажать на объект SD-WAN-CTL-PNF.



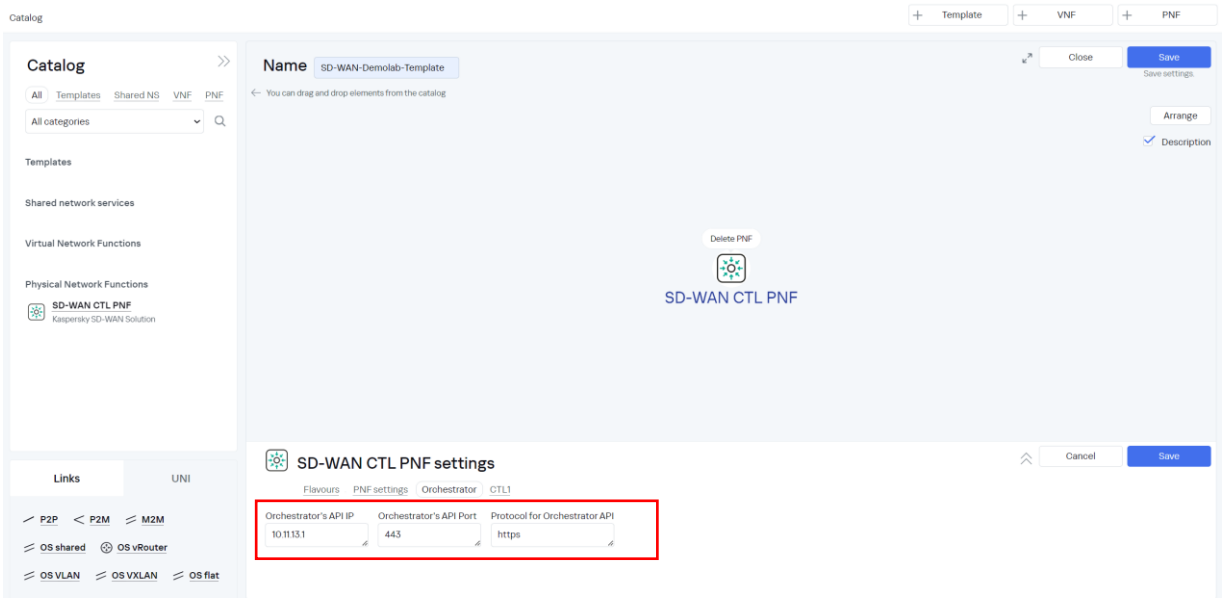
4.3.4. Перейти на закладку PNF Settings.

Задать имя SD-WAN контроллера.



4.3.5. Перейти на закладку Orchestrator.

Задать адрес оркестратора: ввести начальный IP адрес из сети knaas_os_man (заданной в пункте 3.2.9): 10.11.13.1.
При изменении этой сети изменить адрес на другой.

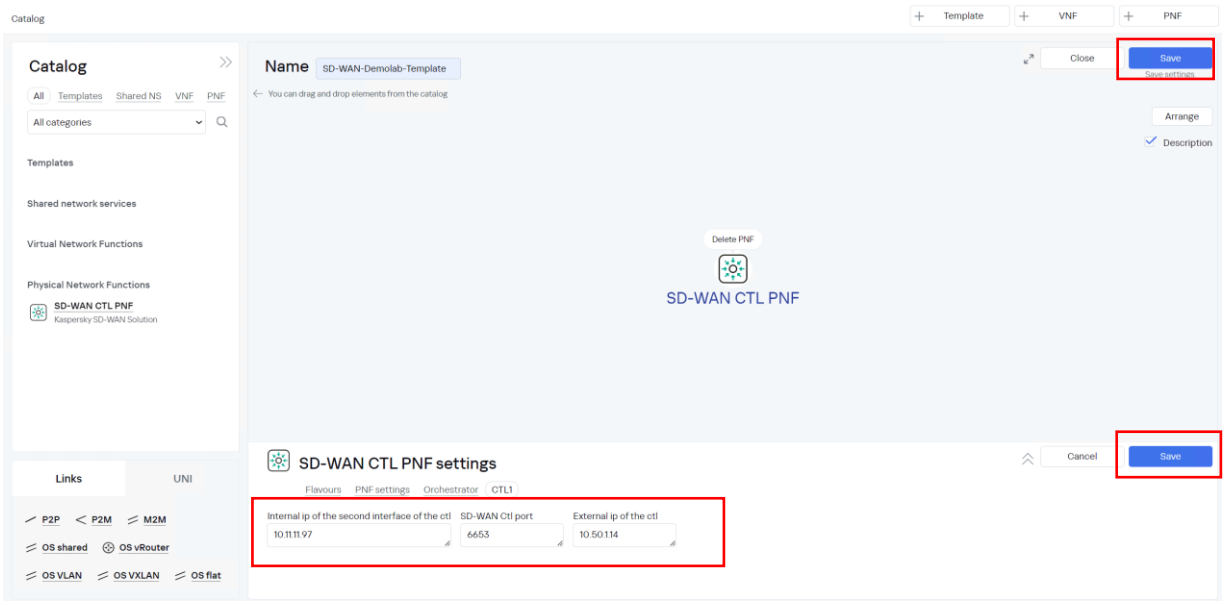


4.3.6. Перейти на вкладку CTL1.

В качестве внутреннего IP адреса задать IP адрес контейнера контроллера: 10.11.11.97

В качестве внешнего IP адреса задать публичный IP адрес R14: 10.50.1.14, на котором настроен DNAT порта 6653 на orc.
При изменении IP плана из пункта 2.3 использовать новый публичный IP адрес.

Нажать Save в настройках контроллера, затем нажать Save в настройках шаблона.



4.4. **Создание Tenant и развертывание сервиса SD-WAN.**

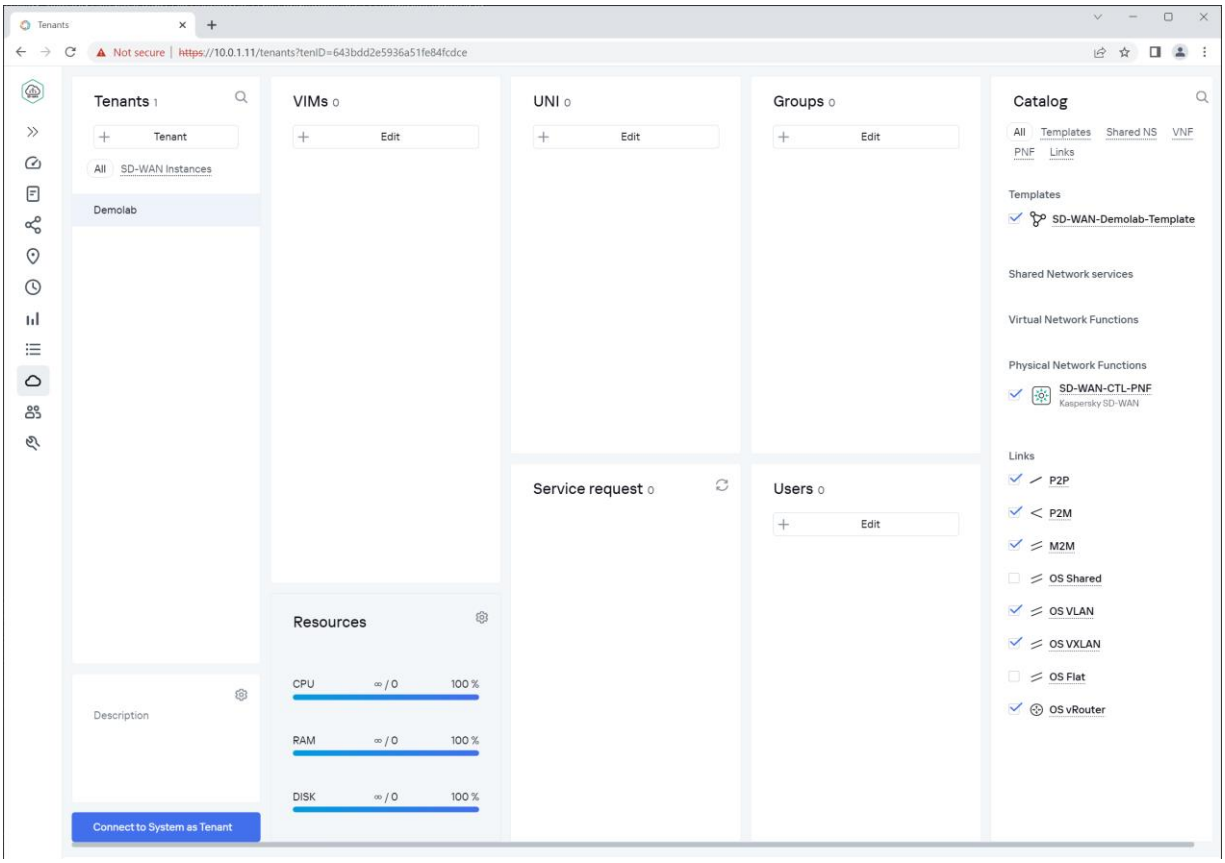
4.4.1. Перейти в меню Tenants.

Нажать кнопку “+Tenant” и ввести имя tenant.

Важно: не используйте “.” и специальные символы в названии.

В области Catalog отметить / выбрать все: Templates и Physical Network Functions.

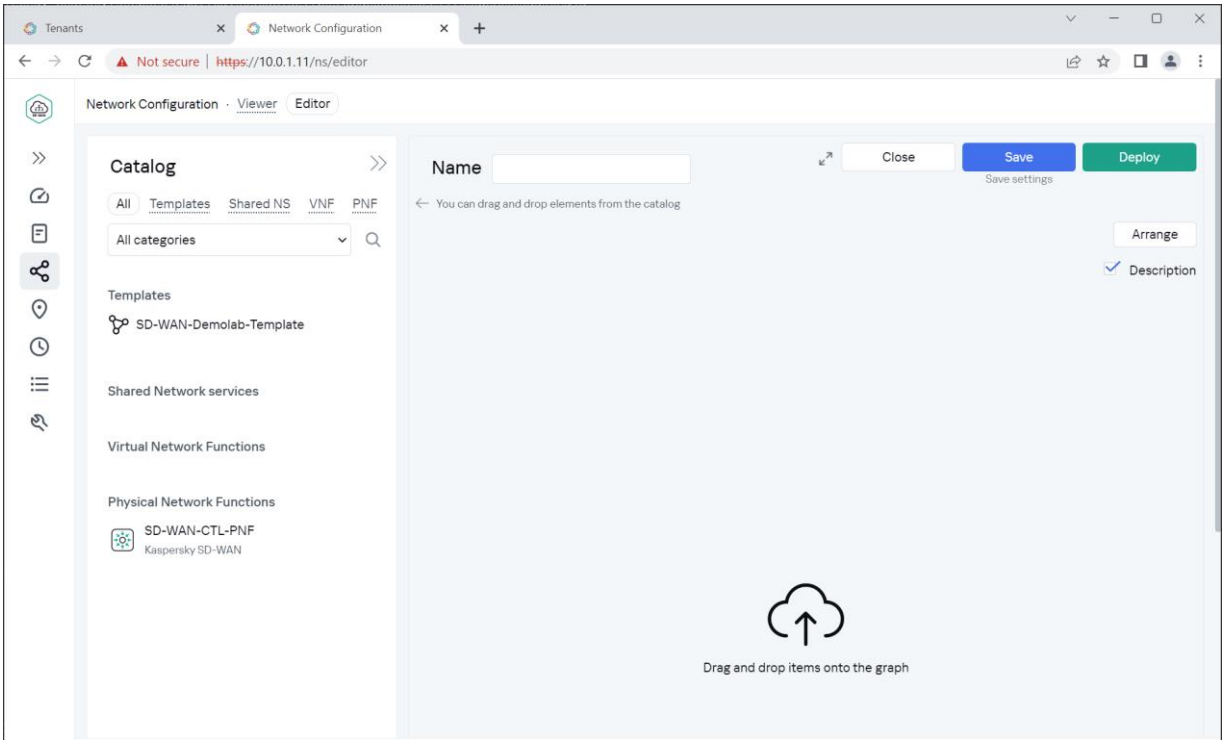
Опционально - назначить администратора tenant, предварительно создав для этого учетную запись в разделе Users с ролью Tenant.



4.4.2. Развертывание сетевого сервиса SD-WAN из шаблона SD-WAN.

Нажать кнопку Connect to System as Tenant или подключиться к SD-WAN оркестратору администратором Tenant.

В меню Catalog > Services нажать кнопку Add a Service.

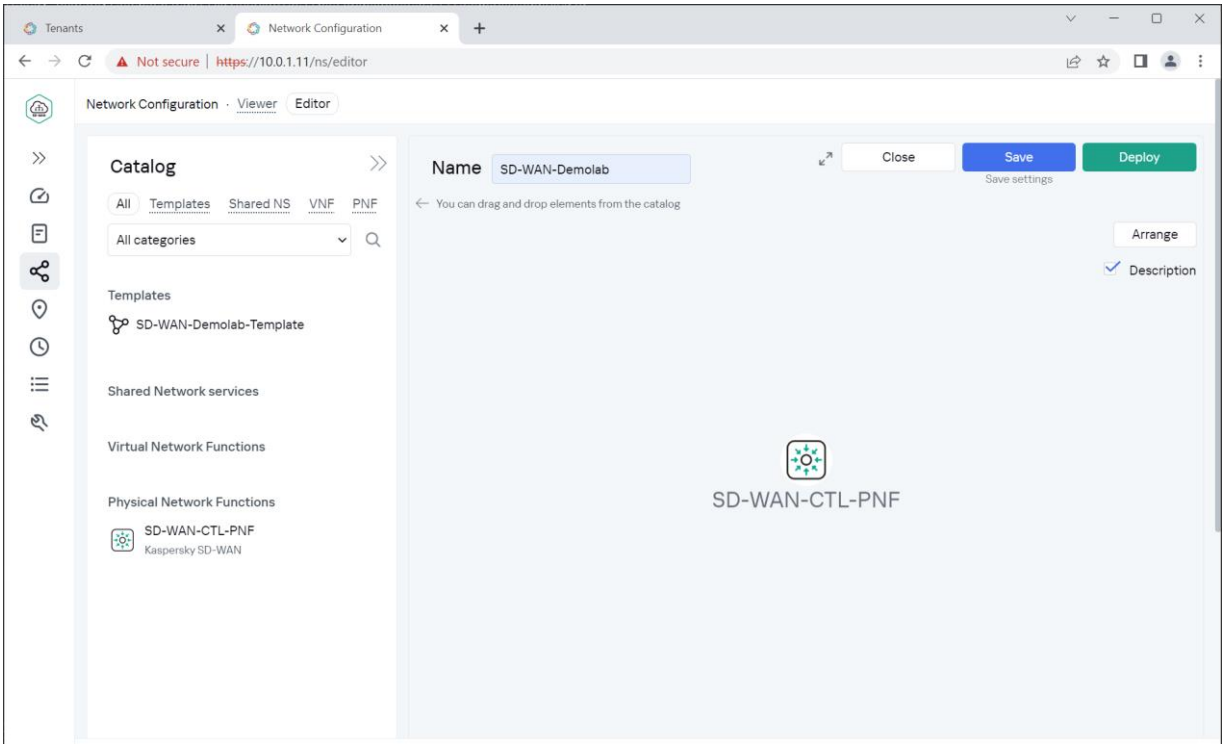


4.4.3. В области Templates выбрать созданный ранее шаблон SD-WAN и перетащить в окно конструктора сервисов.

Задать имя сервиса SD-WAN.

Нажать Save.

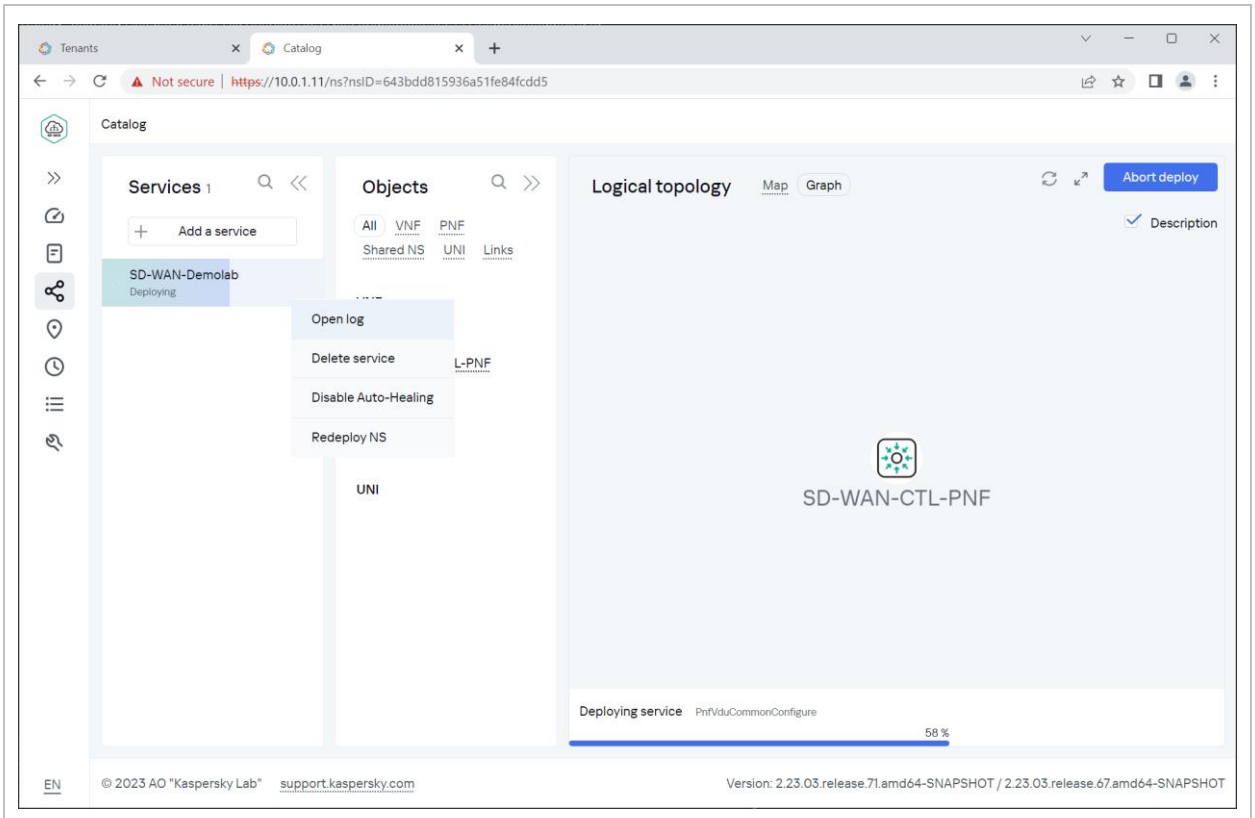
Нажать кнопку Deploy.

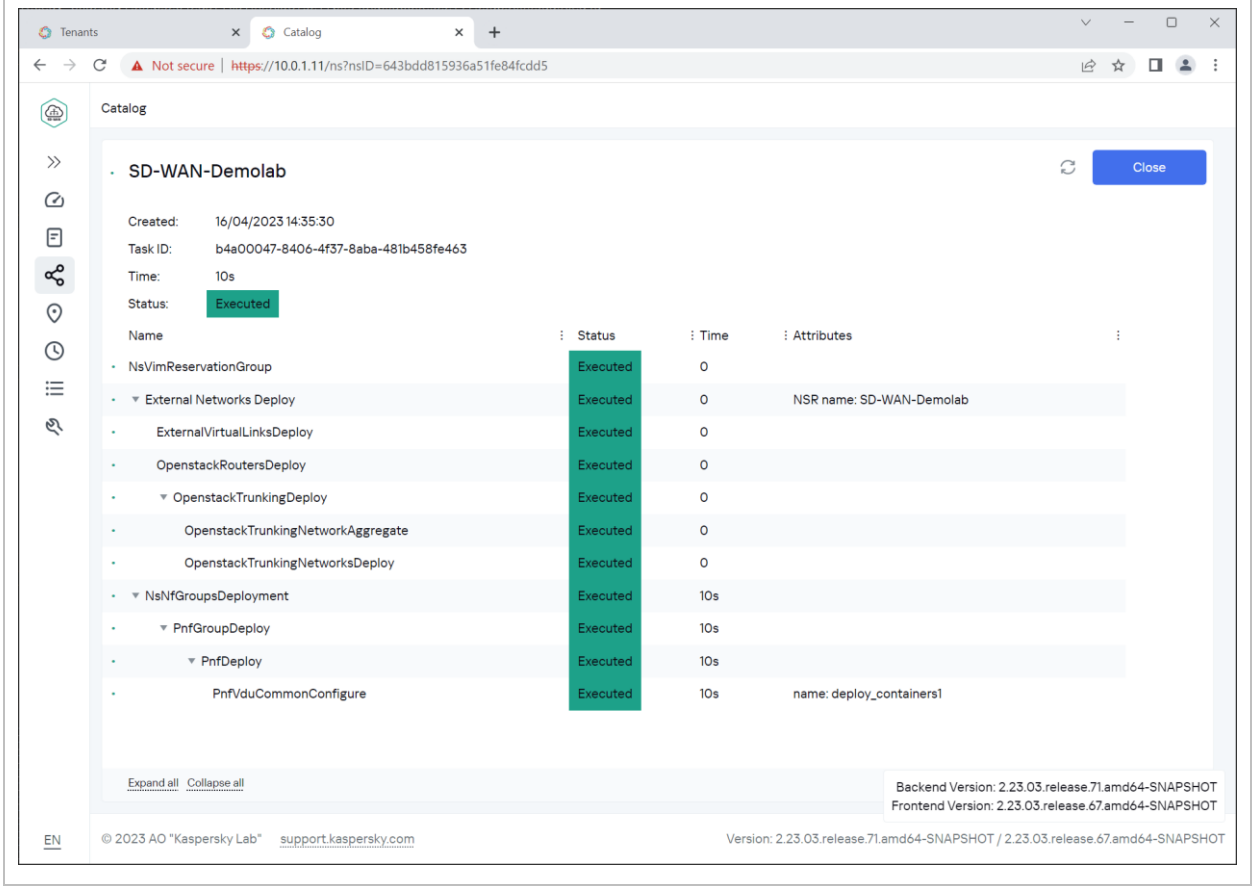


4.4.4. Система автоматически переходит в режим просмотра, отображается статус развёртывания сервиса SD-WAN.

Для наблюдения за статусом развертывания компонентов сервиса нажать кнопку настройки сервиса (шестеренка) и выбрать “Open log”.

Дождаться окончания развертывания сервиса SD-WAN. В области Services сервис SD-WAN должен быть отмечен зеленым индикатором с статусом “Running”.

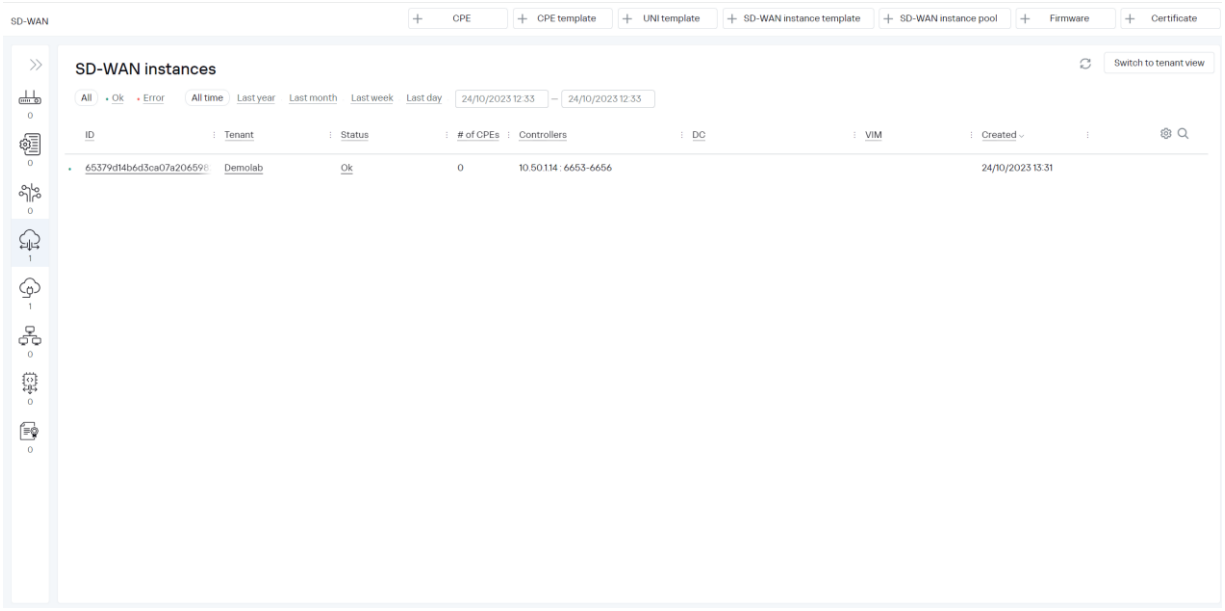

Tenants
Catalog
Not secure | https://10.0.1.11/ns?nsID=643bdd815936a51fe84fcdd5
Catalog
Services 1
Add a service
SD-WAN-Demolab
Deploying
Open log
Delete service
Disable Auto-Healing
Redeploy NS
Objects
All VNF PNF
Shared NS UNI Links
L-PNF
UNI
Logical topology
Map Graph
Abort deploy
Description
SD-WAN-CTL-PNF
Deploying service PnfVduCommonConfigure
58 %
EN
© 2023 AO "Kaspersky Lab" support.kaspersky.com
Version: 2.23.03.release.71.amd64-SNAPSHOT / 2.23.03.release.67.amd64-SNAPSHOT


Tenants
Catalog
Not secure | https://10.0.1.11/ns?nsID=643bdd815936a51fe84fcdd5
Catalog
SD-WAN-Demolab
Close
Created: 16/04/2023 14:35:30
Task ID: b4a00047-8406-4f37-8aba-481b458fe463
Time: 10s
Status: Executed
Name | Status | Time | Attributes
NsVimReservationGroup | Executed | 0
External Networks Deploy | Executed | 0 | NSR name: SD-WAN-Demolab
ExternalVirtualLinksDeploy | Executed | 0
OpenstackRoutersDeploy | Executed | 0
OpenstackTrunkingDeploy | Executed | 0
OpenstackTrunkingNetworkAggregate | Executed | 0
OpenstackTrunkingNetworksDeploy | Executed | 0
NsNfGroupsDeployment | Executed | 10s
PnfGroupDeploy | Executed | 10s
PnfDeploy | Executed | 10s
PnfVduCommonConfigure | Executed | 10s | name: deploy_containers1
Expand all Collapse all
Backend Version: 2.23.03.release.71.amd64-SNAPSHOT
Frontend Version: 2.23.03.release.67.amd64-SNAPSHOT
EN
© 2023 AO "Kaspersky Lab" support.kaspersky.com
Version: 2.23.03.release.71.amd64-SNAPSHOT / 2.23.03.release.67.amd64-SNAPSHOT

4.4.5. Проверка запуска экземпляра сети SD-WAN.

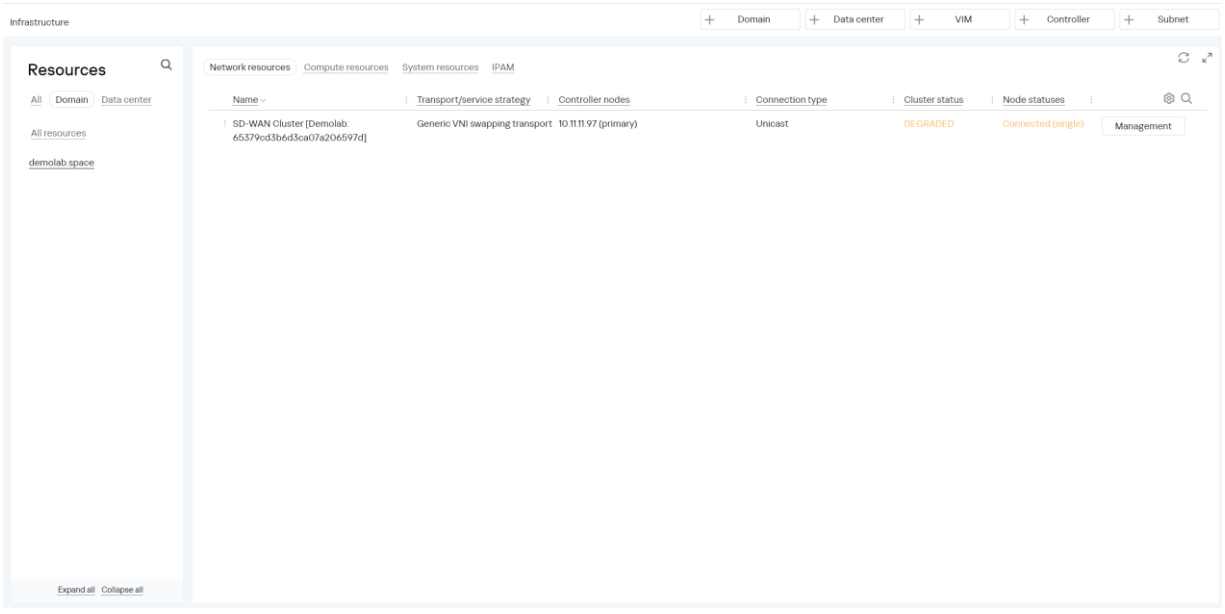
После успешного запуска сервиса на стороне Tenant необходимо убедиться в успешном завершении конфигурации сервиса (Для этого надо подключится как администратор. Повторить 3.3.1 или перейти на предыдущее окно браузера).

Перейти в меню SD-WAN > SD-WAN Instances.
Перед ID SD-WAN сервиса должен отображаться индикатор зеленого цвета.



4.4.6. Перейти в меню Infrastructure > Domain > DC.

Проверить статус SD-WAN контроллера. Degraded – означает, что контроллер один, без отказоустойчивости.



4.4.7. Удаление временного контейнера mockpnf.
При развёртывании сервиса SD-WAN и настройке контроллера оркестратор подключается к контроллеру через контейнер mockpnf с временным паролем. После развертывание сервиса требуется удалить временный контейнер.
Выполнить на хосте orc1 команду:

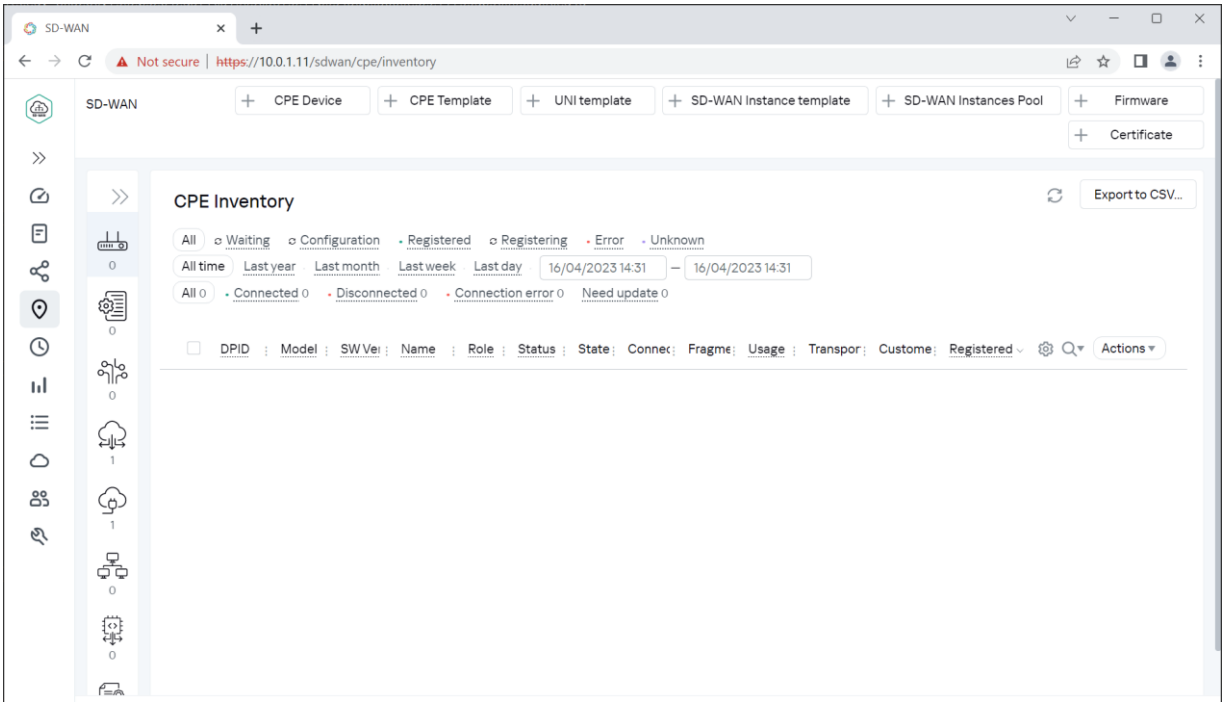
sdwan@orc1:~$ docker rm -f mockpnf-1

4.5. **Создание шаблонов SD-WAN шлюзов.**

Шаблон SD-WAN шлюза содержит параметры, которые применяются при его регистрации и его перезагрузке.

4.5.1. Для SD-WAN шлюзов используется шаблон CPE.

Перейти в меню SD-WAN > CPE templates.



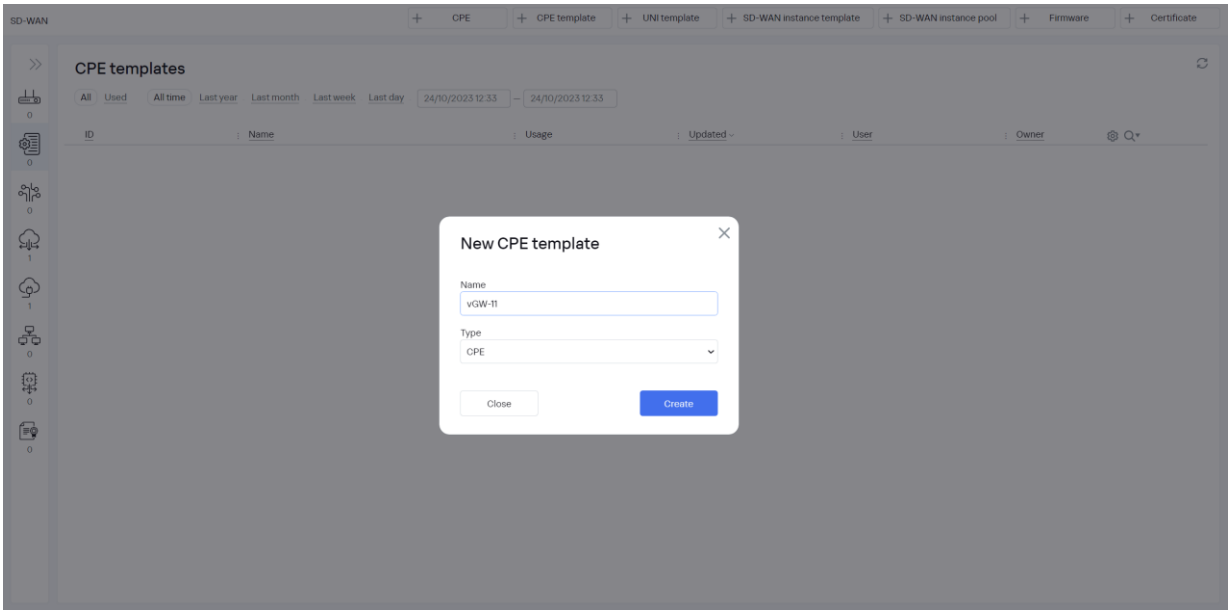
4.5.2. Нажать кнопку “+CPE Template”.

В поле Name задать имя шлюза: vGW-11.

Установить значение Type: CPE.

Нажать Create.

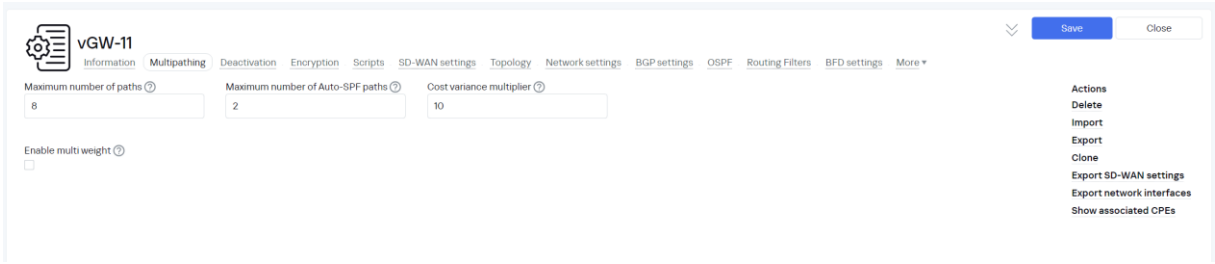
Для шлюза vGW-12 будет создан отдельный шаблон.



4.5.3. Перейти на вкладку Multipathing.

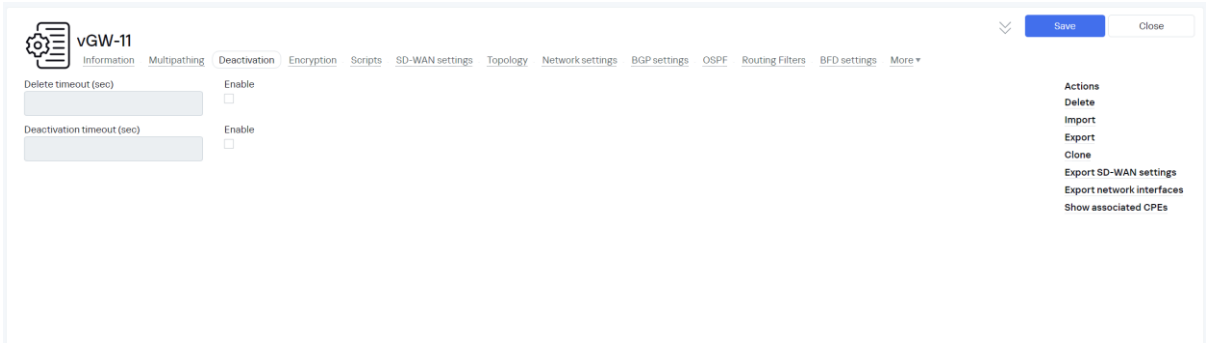
Оставить параметры по «умолчанию»: 8/2/10.

Выключить параметр Enable Multi Weight.



4.5.4. Перейти на вкладку Deactivation.

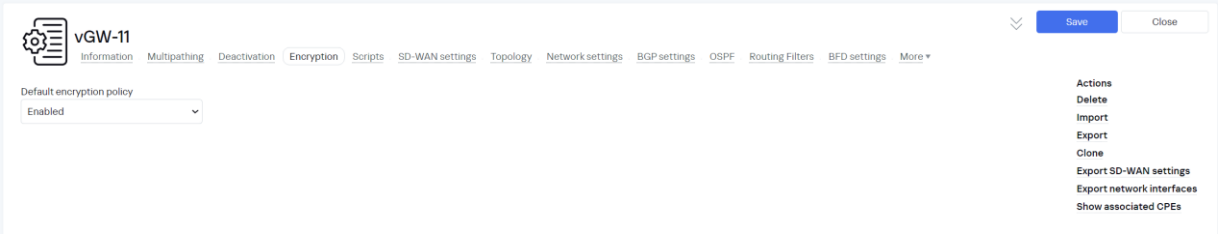
Оставить параметры по «умолчанию».



4.5.5. Перейти на вкладку Encryption.

Включить шифрование: Enabled.

Нажать Save.



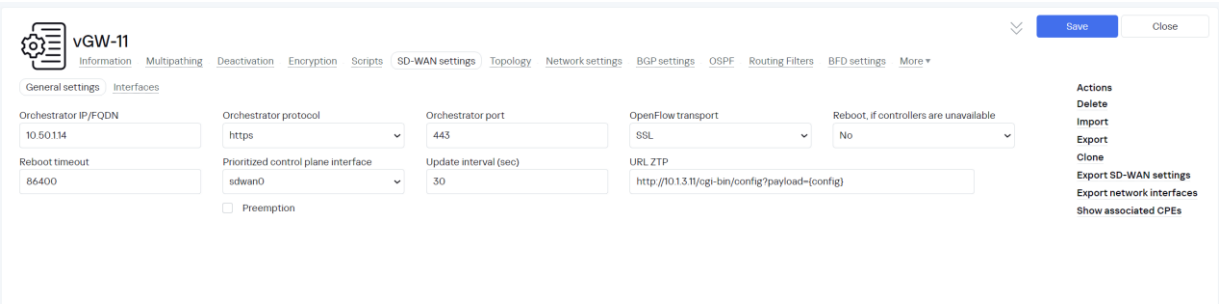
4.5.6. Перейти на вкладку SD-WAN Settings > Globals.

SD-WAN Orchestrator IP/FQDN: 10.50.1.14
При изменении IP плана из пункта 2.3 использовать новый публичный IP адрес хоста orc1.

SD-WAN Orchestrator Port: 443
Openflow Transport: ssl.

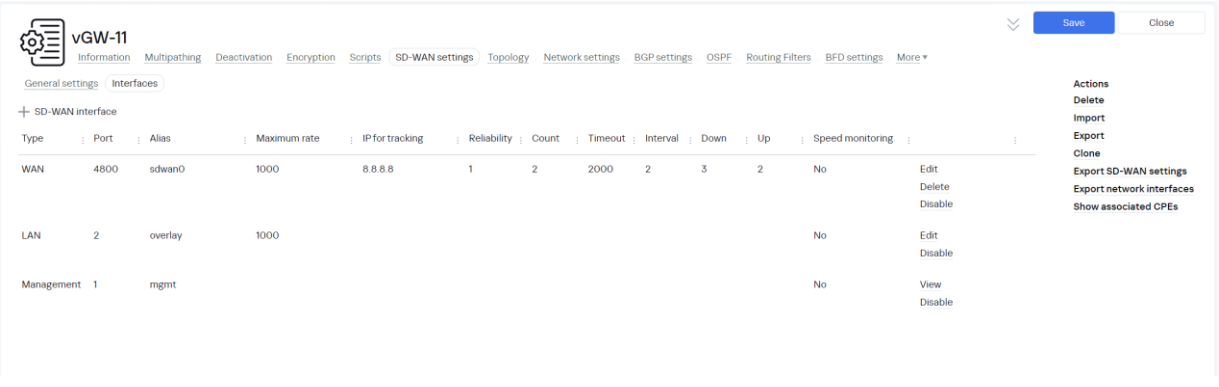
Prioritized Control-Plane Interface: sdwan0.

Изменить IP адрес 192.168.7.1 в URL ZTP на 10.1.3.11



4.5.7. Перейти на вкладку SD-WAN Settings > Interfaces.

В рамках данного демонстрационного стенда у шлюза один внешний сетевой интерфейс, необходимо убрать (Delete) сетевой интерфейс sdwan1.



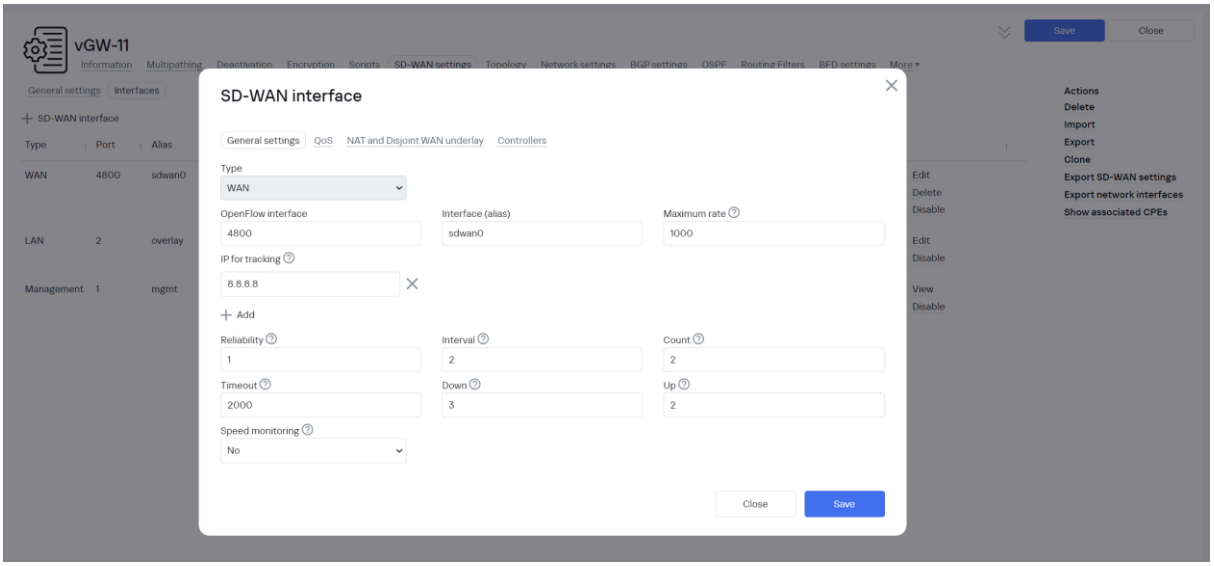
4.5.8. Параметры сетевого интерфейса sdwan0.

Открыть для редактирования сетевой интерфейс sdwan0.

Задать IP адрес для tracking, например, IP адрес шлюза по умолчанию или 8.8.8.8.

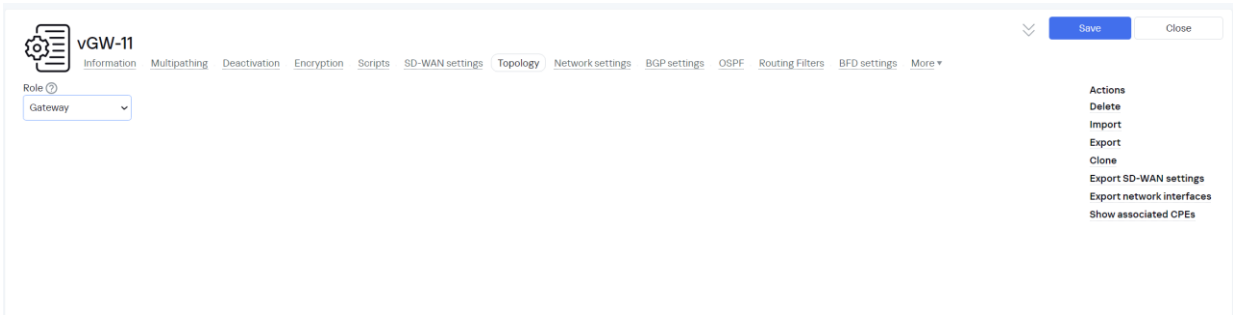
Нажать Save.

Если не доступен tracking IP, SD-WAN шлюз и CPE устройства считают сетевой интерфейс не работоспособным и не будут строить через него туннели.



4.5.9. Перейти на вкладку Topology.

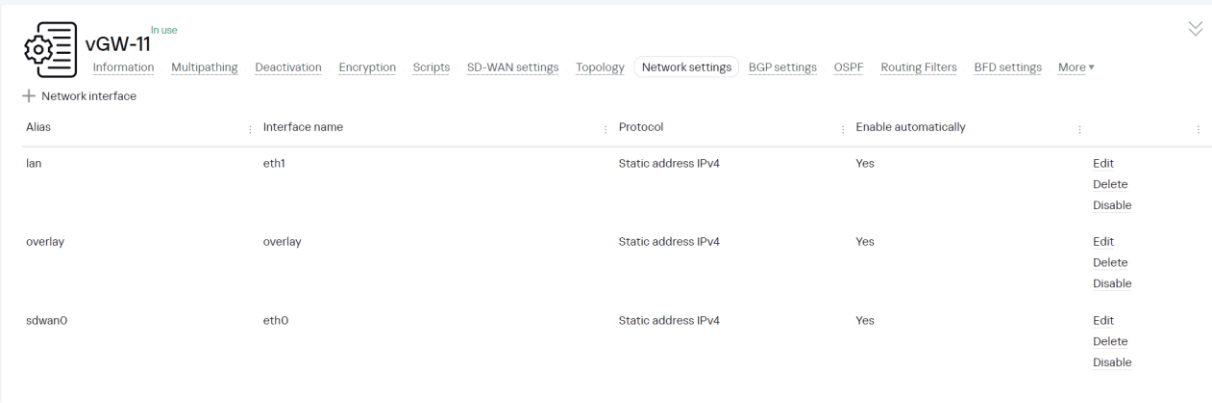
Задать роль: Gateway.



4.5.10. Перейти на вкладку Network Settings.

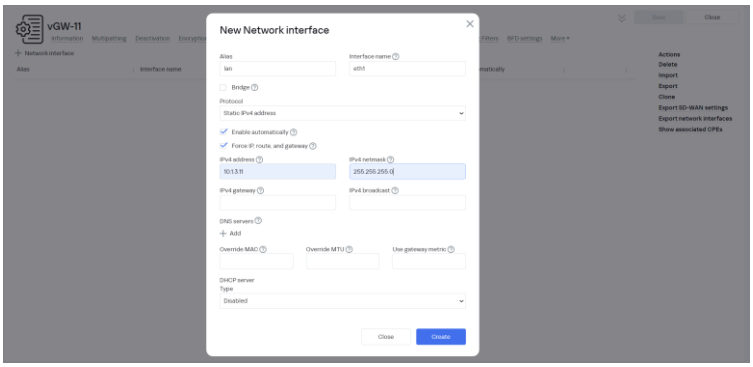
Создать сетевые интерфейсы:

- sdwan0: eth0
- lan: eth1
- overlay: overlay



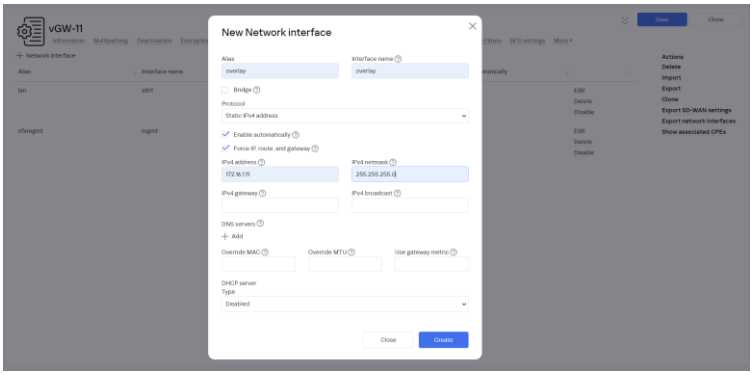
4.5.11. Добавить сетевой интерфейс lan:

- Alias: lan
- Interface Name: eth1
- IP адрес шлюза vGW-11: 10.1.3.11/24



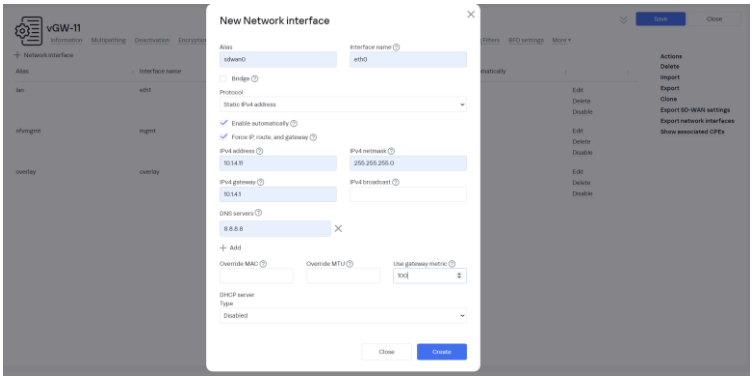
4.5.12. Добавить сетевой интерфейс overlay:

- Alias: overlay
- Interface Name: overlay
- IP адрес шлюза vGW-11: 172.16.1.11/24



4.5.13. Добавить сетевой интерфейс sdwan0:

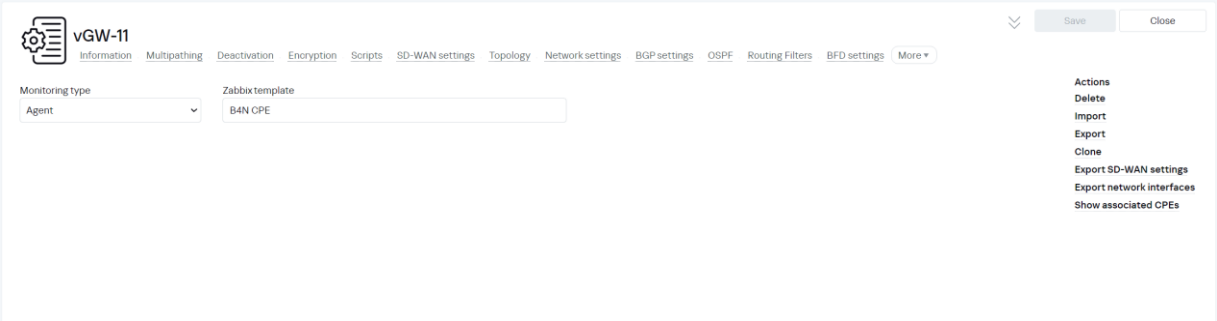
- Alias: sdwan0
- Interface Name: eth0
- IP адрес шлюза vGW-11: 10.1.4.11/24
- IPv4 gateway: 10.1.4.1
- Use custom DNS: 8.8.8.8
- Use gateway metric: 100



4.5.14. Перейти на вкладку Monitoring.

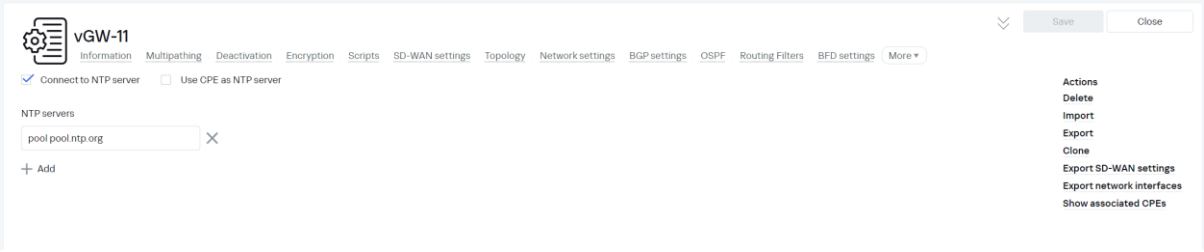
Задать:

- Monitoring type: Agent
- Zabbix template: B4N CPE



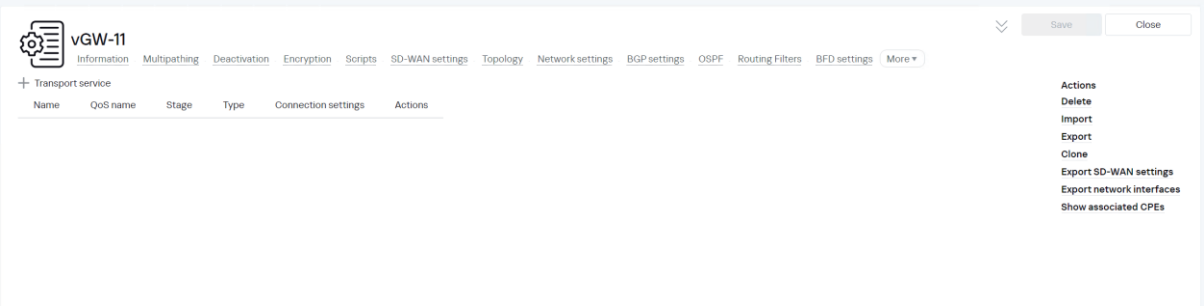
4.5.15. Перейти на вкладку NTP.

По умолчанию включен NTP клиент и настроен пул pool.ntp.org.



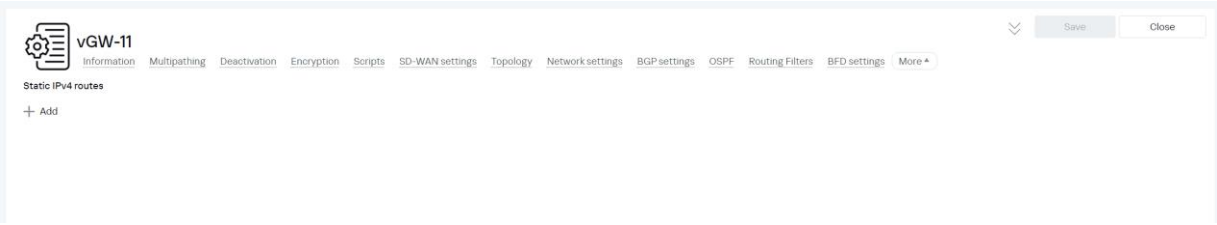
4.5.16. Перейти на вкладку Transport service.

Оставить параметры «по умолчанию».



4.5.17. Перейти на вкладку Static Routes.

Статические маршруты не заданы.



4.5.18. Создание Prefix List для SD-WAN шлюза.

Перейти на вкладку Routing filters > Prefix lists.

Нажать “+Prefix List”.

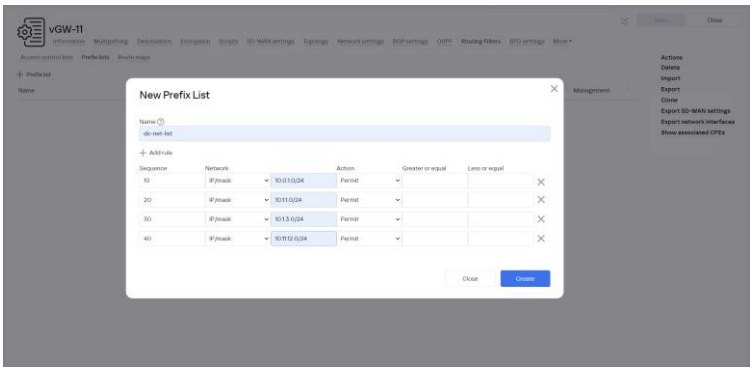
Name: dc-net-list.

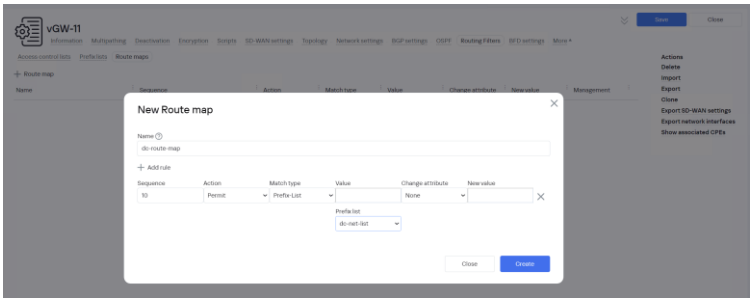
Нажать “+Add Rule”.
Добавить сети:

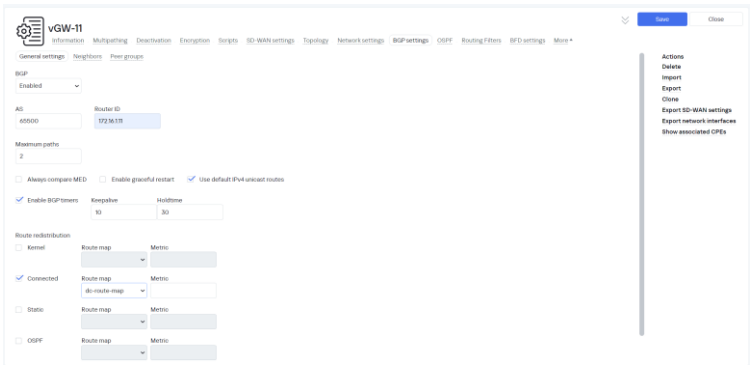
- Seq 10 10.0.1.0/24
- Seq 20 10.1.1.0/24
- Seq 30 10.1.3.0/24
- Seq 40 10.11.12.0/24

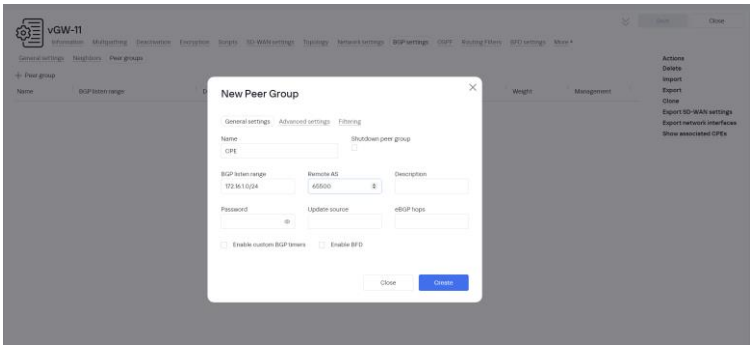
При изменении подсети mgmt в пункте 4.1.5 требуется поменять подсеть в Seq 40 на актуальную.

Нажать Create.



4.5.19. Создание Route Map для SD-WAN шлюза. Перейти на вкладку Routing filters > Route maps. Нажать “+Route Map”. Задать Name: dc-route-map Нажать Add Rule: • Sequence: 10 • Action: Permit • Match Type: Prefix-list • Match Value: dc-net-list Нажать Create.	

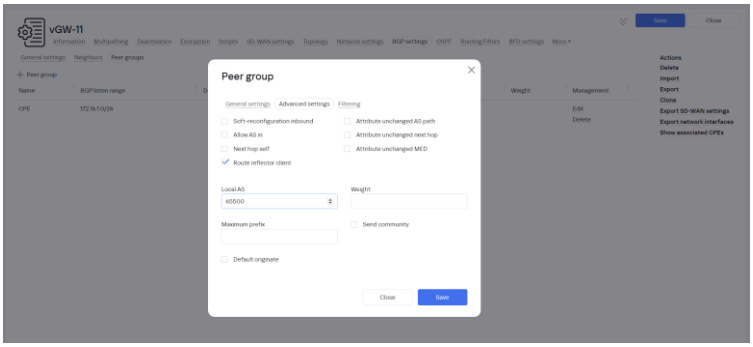
4.5.20. Перейти на вкладку BGP Settings > General settings.
 	
Задать параметры BGP:
• BGP: Enabled
• AS: 65500
• Router ID: 172.16.1.11 (IP адрес сетевого интерфейса overlay).
• Maximum Paths: 2
• Graceful Restart
• Default IPv4 Unicast
• Enable BGP Timers:
  • Keepalive: 10
  • Hold: 30
  •
Назначить Route Map: dc-route-map к Connected маршрутам.
 	
Нажать Save.
	

4.5.21. Открыть BGP Settings и перейти на вкладку Peer Groups. Нажать “+ Peer Group”. Задать параметры: • Name: CPE • BGP Listen Range: 172.16.1.0/24 (сеть overlay) • Remote AS: 65500	

4.5.22. Открыть созданную группы для редактирования (нажать Edit) и перейти на вкладку Advanced Settings.

Включить: Route Reflector Client.
Local AS: 65500.

Нажать Save.



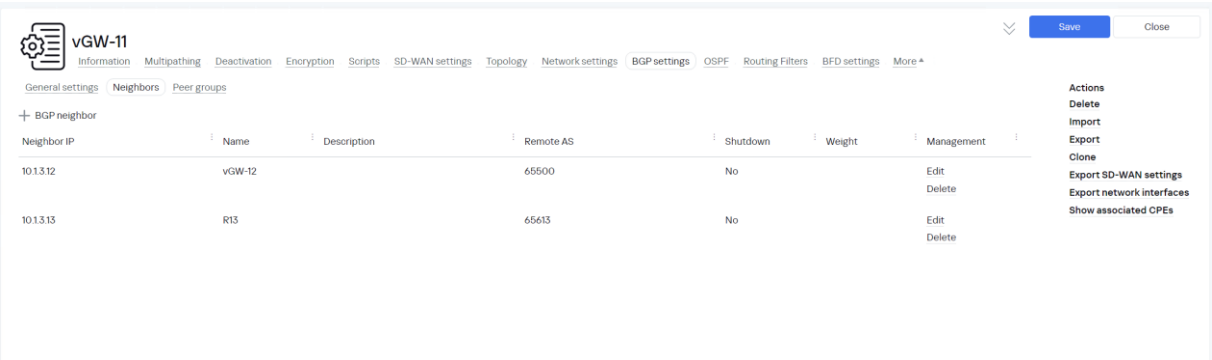
4.5.23. Перейти на вкладку Neighbors и нажать “+BGP Neighbor”.

Задать параметры:

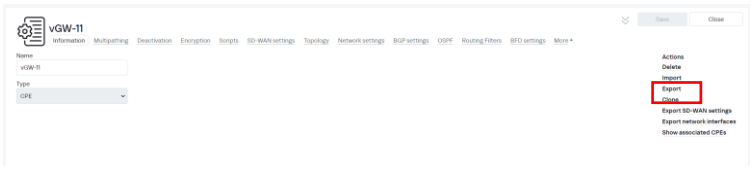
- Name: R13
- Neighbor Address: 10.1.3.13
- Remote AS: 65613

- Name: vGW-12
- Neighbor Address: 10.1.3.12
- Remote AS: 65500

Нажать Create.

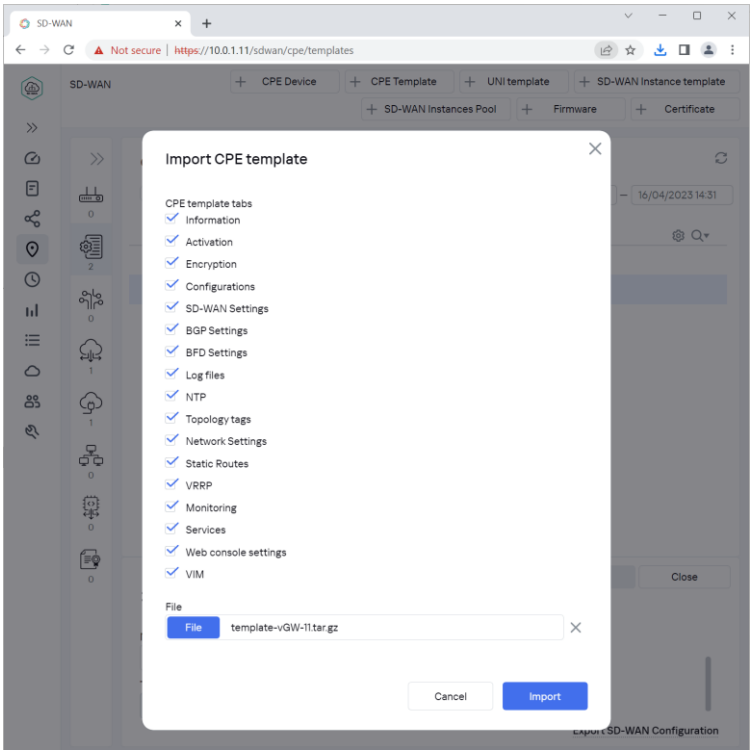
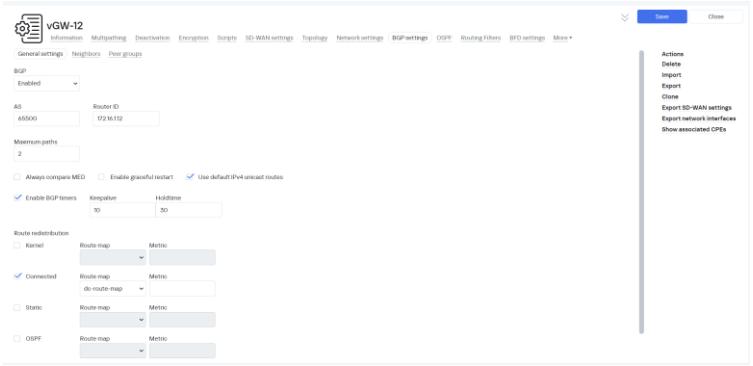


4.5.24. Выполнить экспорт шаблона SD-WAN шлюза vGW-11.



4.5.25. Создать шаблон для SD-WAN шлюза vGW-12.

Выполнить шаги 4.5.1 –4.5.24 или выполнить в него импорт шаблона vGW-11.

Создать шаблон vGW-12, затем внутри щаблона нажать Import и выбрать файл: *vGW-11-template.tag.gz* Нажать Import.	
4.5.26. Адаптировать шаблон для шлюза vGW-12. Во вкладке SD-WAN settings > Globals изменить IP адрес 192.168.7.1 в URL ZTP на 10.1.3.12 Во вкладке Network Settings изменить параметры сетевых интерфейсов: • sdwan0: 10.1.5.12/24, шлюз – 10.1.5.1 • lan: 10.1.3.12/24 • overlay: 172.16.1.12/24 *При изменении подсети mgmt в пункте 4.1.5 требуется поменять IP адрес nfvmgmt на актуальный.* Во вкладке BGP Settings изменить параметры BGP: • Router ID: 172.16.1.12 • Neighbors: R13 и vGW-11	

4.6. **Импорт сертификата CA для CPE устройств.**

4.6.1. Для предотвращения MITM-атак (англ. Man in the middle) при обращении к оркестратору устройство CPE проверяет, можно ли доверять сертификату оркестратора. По умолчанию на устройствах CPE установлены корневые сертификаты публичных центров сертификации. Если для оркестратора используется сертификат, подписанный публичным центром сертификации, установка дополнительного сертификата на устройства CPE не требуется. В противном случае необходимо добавить используемый оркестратором публичный корневой сертификат на устройства CPE, загрузив сертификат в веб-интерфейсе оркестратора.

Более подробно в SD-WAN Online Help > Установка сертификата оркестратора на устройствах CPE: https://support.kaspersky.com/help/SD-WAN/2.0/ru-RU/248730.htm

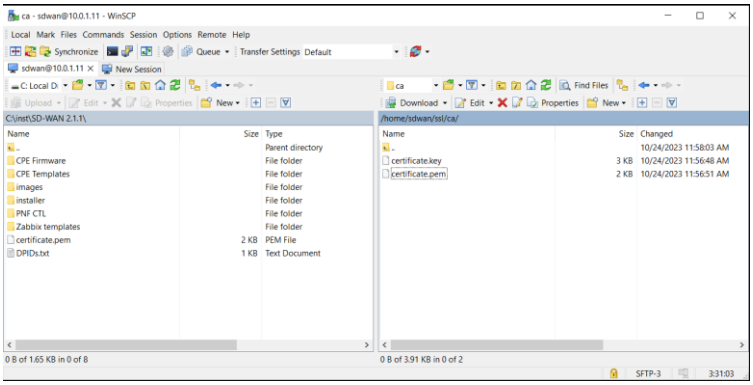
В процессе установки системы управления SD-WAN корневой сертификат CA был сохранен в файл:

/home/sdwan/ssl/ca/certificate.pem

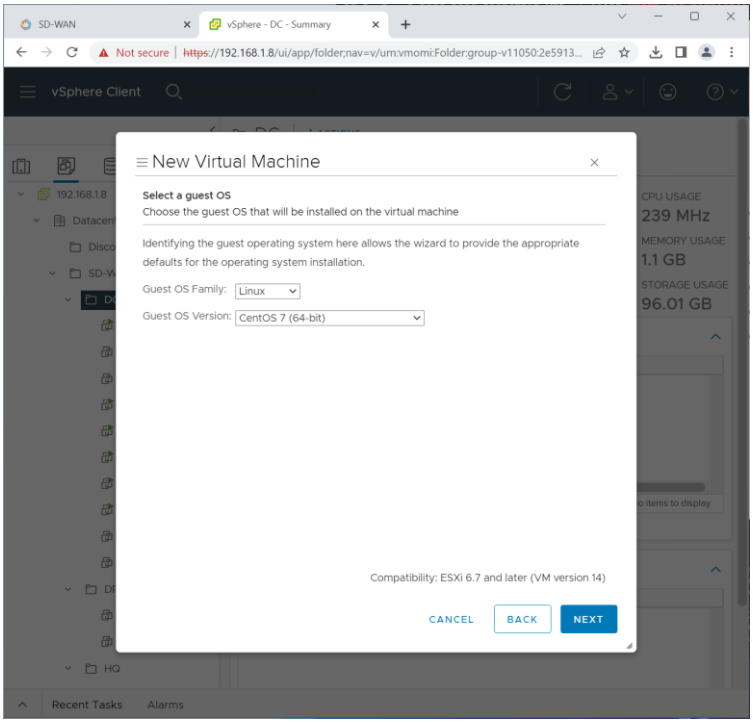
Скачать сертификат с хоста orc1, например, с использованием WinSCP.

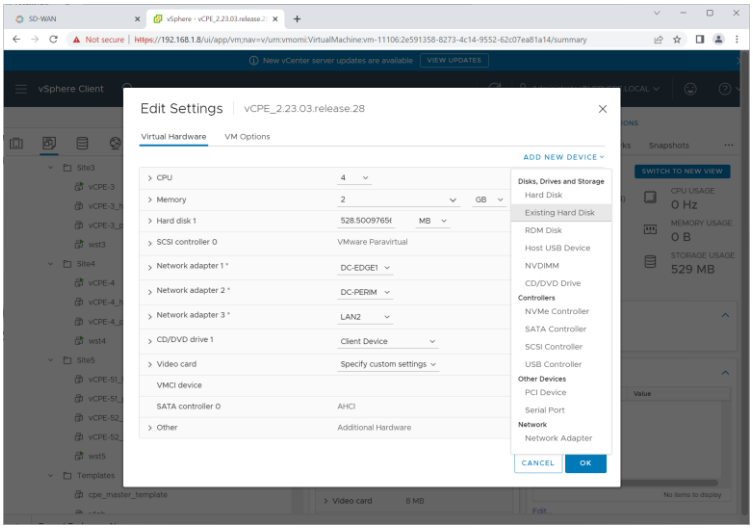
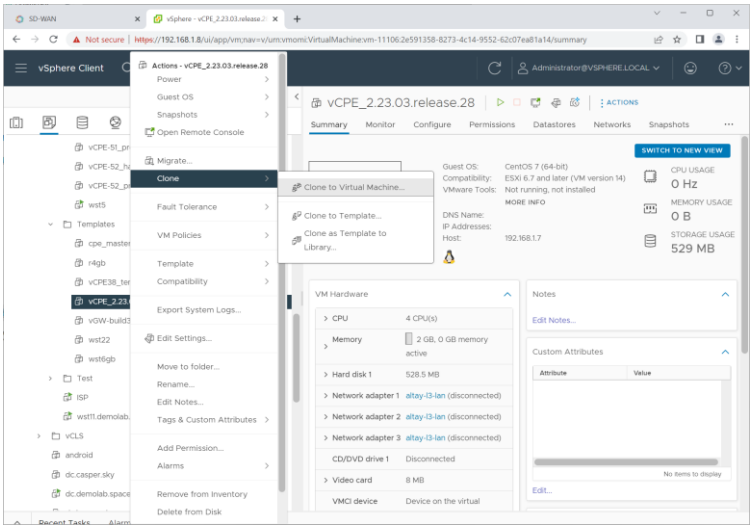
Перейти в меню SD-WAN > Certificates.

Нажать +Certificate, выбрать .pem файл сертификата CA.



4.7. **Подготовка SD-WAN шлюзов.**

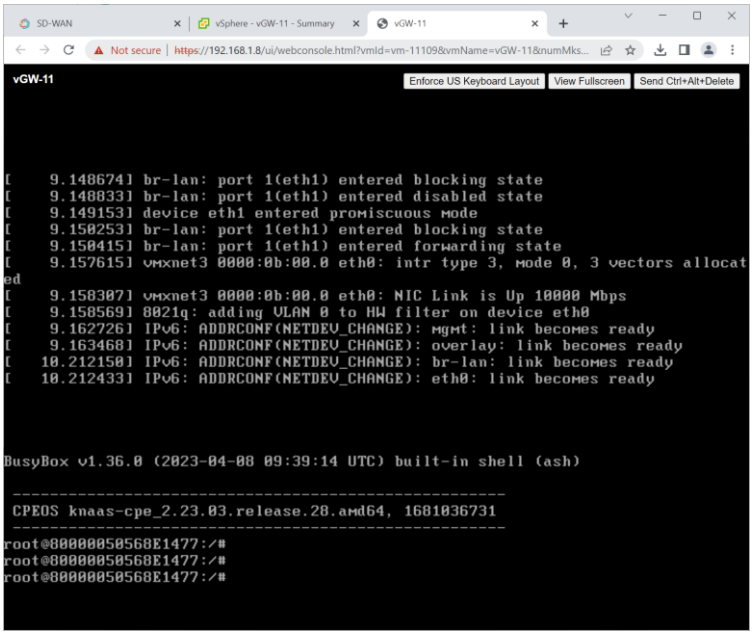
4.7.1. Загрузить единый образ CPE устройства / SD-WAN шлюза. Конвертировать qcow2 диск в vmdk: *# qemu-img convert -p -f qcow2 -O vmdk knaas- knaas-cpe_2.23.07.release.22.combined.amd64-legacy.qcow2 knaas-cpe_2.23.07.release.22.combined.amd64-legacy.vmdk*	
4.7.2. Создать новую виртуальную машину для шаблона CPE устройства. Guest OS Family / Version: CentOS 7.	

4.7.3. Ресурсы виртуальной машины для шаблона CPE устройства: • 4 x CPU • 2 GB RAM • Добавить второй сетевой интерфейс. • Добавить предварительно загруженный на storage ESXi хоста диск CPE устройства в формате vmdk и удалить первый диск.	
4.7.4. Клонировать SD-WAN шлюзы vGW-11 и vGW-12 из созданного на предыдущем этапе шаблона CPE устройства.	

4.7.5. Подключение к SD-WAN шлюзам.

На SD-WAN шлюзе установлен текстовый редактор **vi**:

- Нажать клавишу **i**, редактор перейдёт в режим ввода текста.
- Нажать клавишу **Esc** для возврата в командный режим.
- Команда **:wq** - для записи внесенных изменений и выхода.
- Команда **:q!** - для выхода без записи изменений.



4.7.6. Настройка сетевого интерфейса Lan.

Открыть конфигурационный файл:
 # vi /etc/config/network

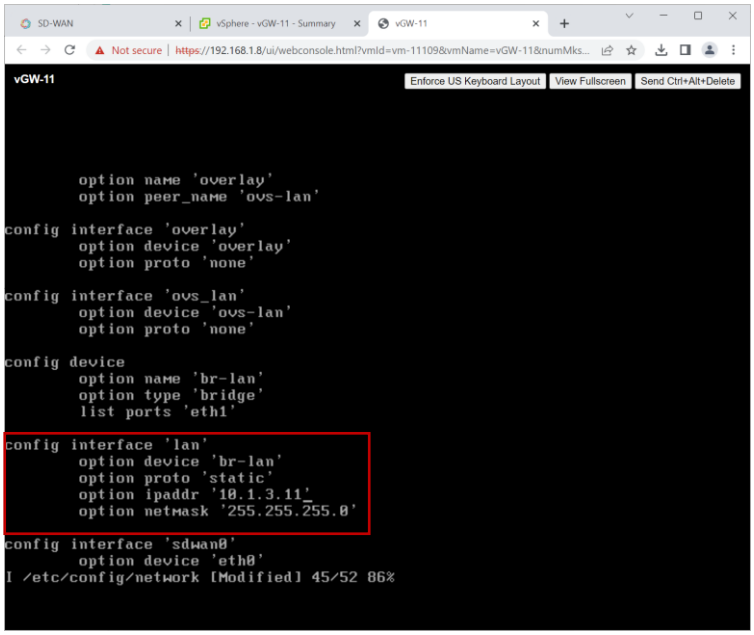
На скриншоте пример vGW-11.

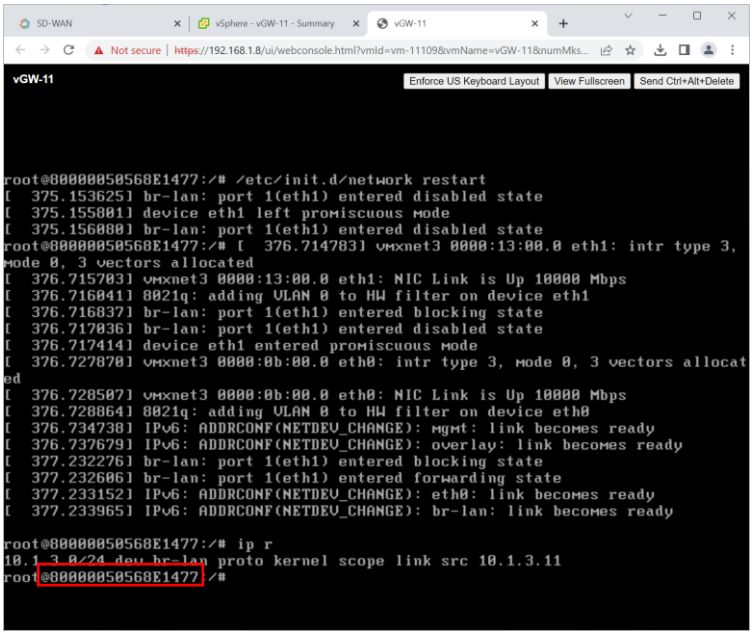
Требуется только настройка lan сетевого интерфейса для выполнения ZTP URL.

Перезагрузить сетевую службу:
 # /etc/init.d/network restart

Проверить примененные настройки
 # ip a

После регистрации (выполнения ZTP URL в пункте 4.8) SD-WAN шлюз получит и заменит сетевые настройки в соответствии настройками в пункте 4.8.5).




SD-WAN
vSphere - vGW-11 - Summary
vGW-11
Not secure
https://192.168.1.8/ui/webconsole.html?vmId=vm-11109&vmName=vGW-11&numMks...
vGW-11
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
root@80000050568E1477:/# /etc/init.d/network restart
[375.153625] br-lan: port 1(eth1) entered disabled state
[375.155801] device eth1 left promiscuous mode
[375.156080] br-lan: port 1(eth1) entered disabled state
root@80000050568E1477:/# [376.714783] vmxnet3 0000:13:00.0 eth1: intr type 3,
mode 0, 3 vectors allocated
[376.715703] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[376.716041] 8021q: adding VLAN 0 to HW filter on device eth1
[376.716837] br-lan: port 1(eth1) entered blocking state
[376.717036] br-lan: port 1(eth1) entered disabled state
[376.717414] device eth1 entered promiscuous mode
[376.727870] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 3 vectors allocat
ed
[376.728507] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[376.728864] 8021q: adding VLAN 0 to HW filter on device eth0
[376.734738] IPv6: ADDRCONF(NETDEV_CHANGE): mgmt: link becomes ready
[376.737679] IPv6: ADDRCONF(NETDEV_CHANGE): overlay: link becomes ready
[377.232276] br-lan: port 1(eth1) entered blocking state
[377.232606] br-lan: port 1(eth1) entered forwarding state
[377.233152] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[377.233965] IPv6: ADDRCONF(NETDEV_CHANGE): br-lan: link becomes ready
root@80000050568E1477:/# ip r
10.1.3.0/24 dev br-lan proto kernel scope link src 10.1.3.11
root@80000050568E1477:/#

4.8. **Регистрация SD-WAN шлюзов.**

4.8.1. Добавить правила iptables на хосте orc1 для связи контейнеров vnfm и Zabbix с сетью mgmt.

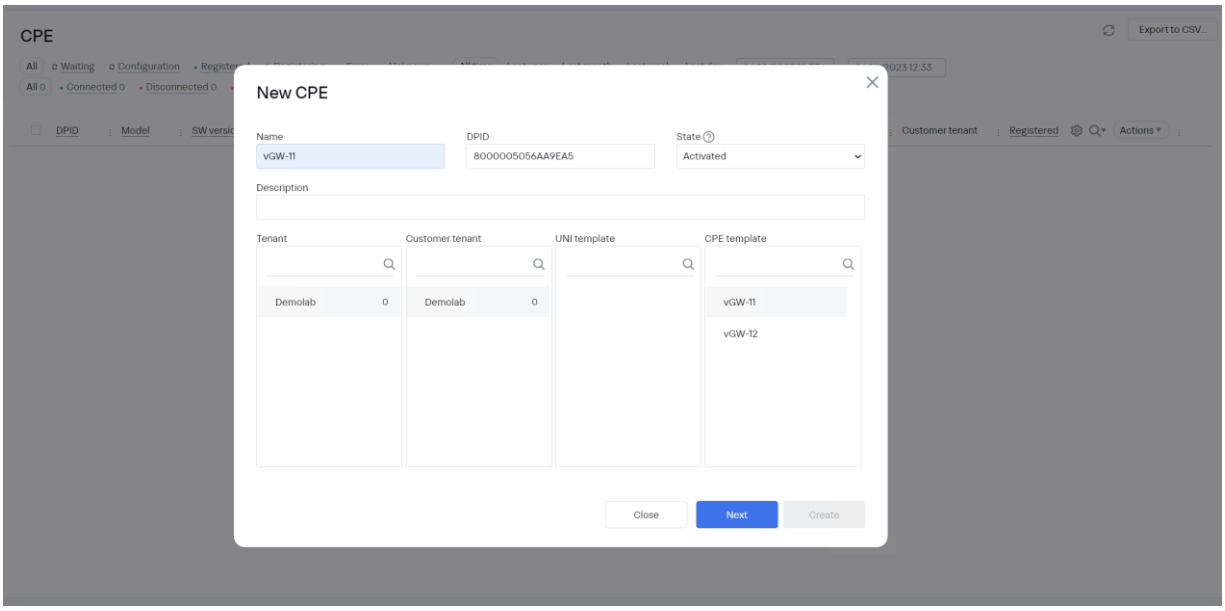
```
sdwan@orc1:~$ sudo iptables -I DOCKER-USER 12 -s 10.11.11.0/24 -d 10.11.12.0/24 -j ACCEPT
sdwan@orc1:~$ sudo iptables -I DOCKER-USER 12 -s 10.11.12.0/24 -d 10.11.11.0/24 -j ACCEPT
sdwan@orc1:~$ sudo iptables-save
```

При изменении подсети mgmt в пункте 4.1.5 требуется поменять IP адреса сетей на актуальные.

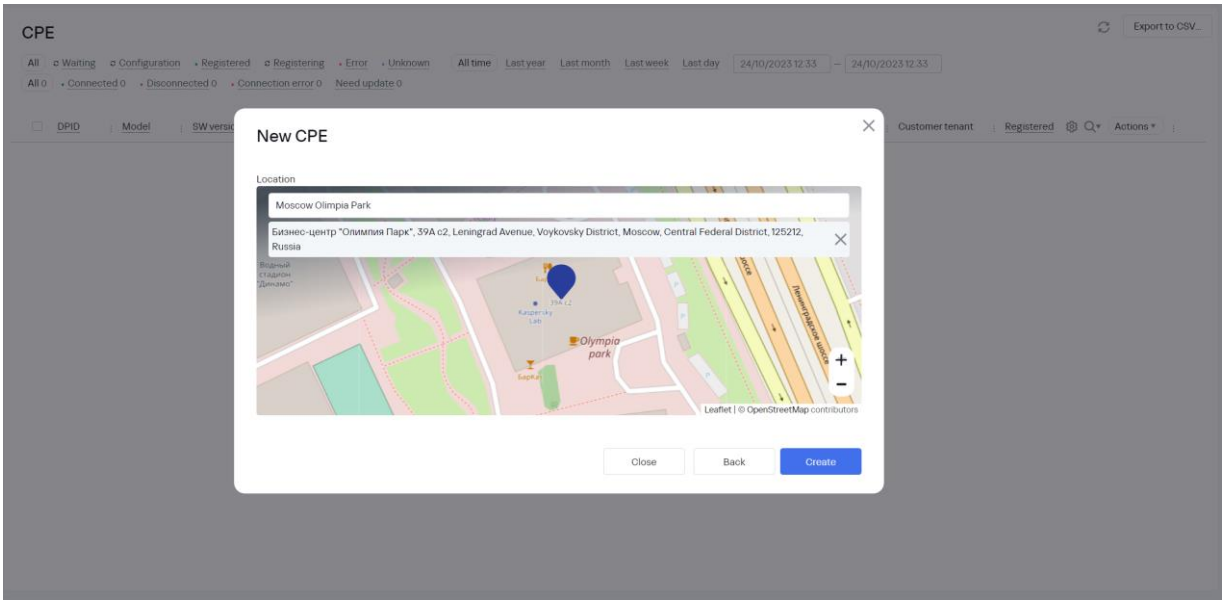
4.8.2. Перейти в меню SD-WAN > CPE.

Нажать +CPE.

Ввести имя SD-WAN шлюза, DPID устройства, выбрать тенанта и шаблон.
DPID устройства отображается в командой строке CPE устройства.



4.8.3. Задать расположение устройства.

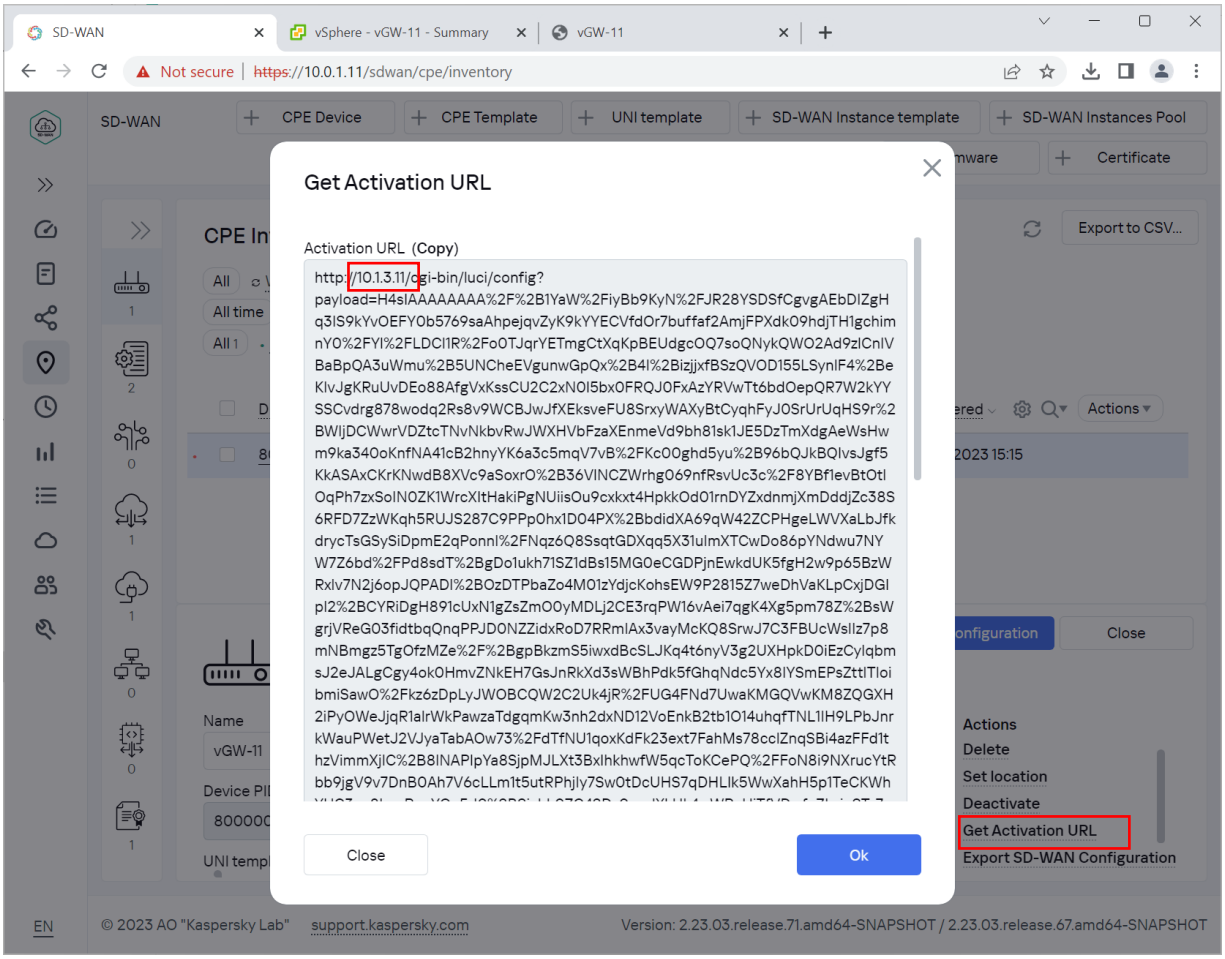


4.8.4. Регистрация SD-WAN шлюза vGW-11.

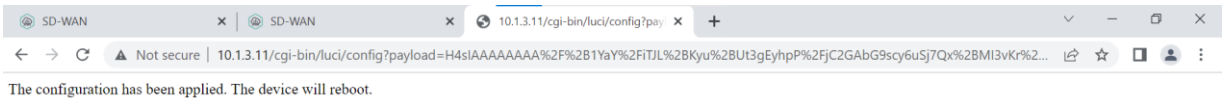
Сгенерировать ZTP URL для активации устройства.

Перейти в меню SD-WAN > CPE > выбрать SD-WAN шлюз и нажать Get Activation URL.

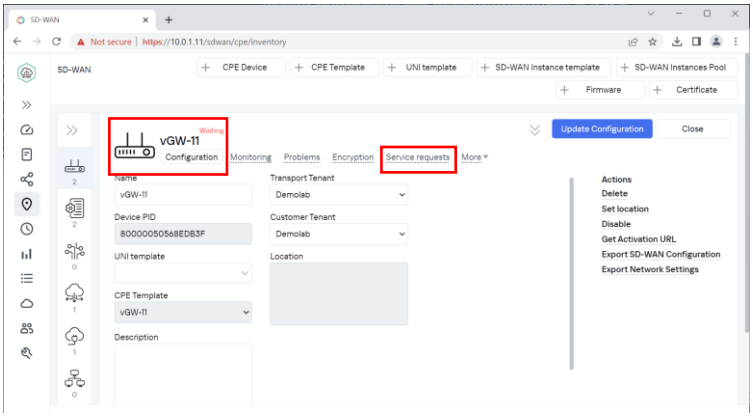
Скопировать ссылку (нажать Copy).



4.8.5. Выполнить регистрацию SD-WAN шлюза vGW-11. Для этого открыть скопированную ссылку в адресной строке браузера.



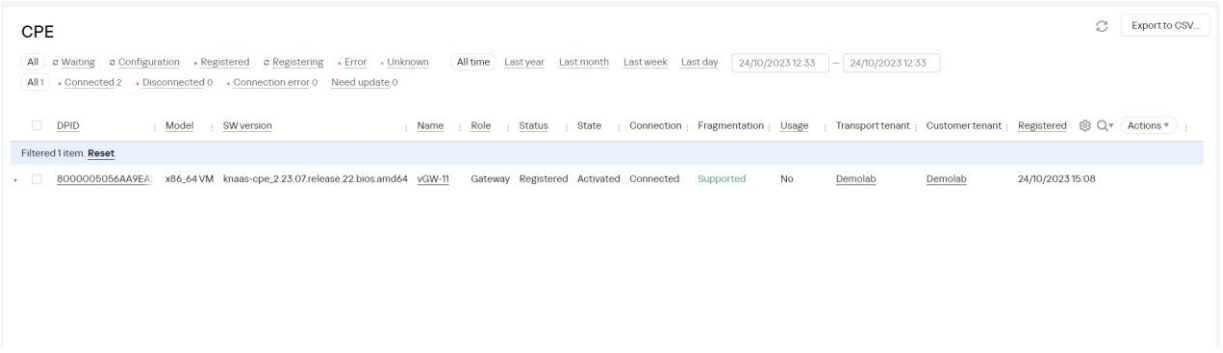
4.8.6. Статус регистрации Waiting.



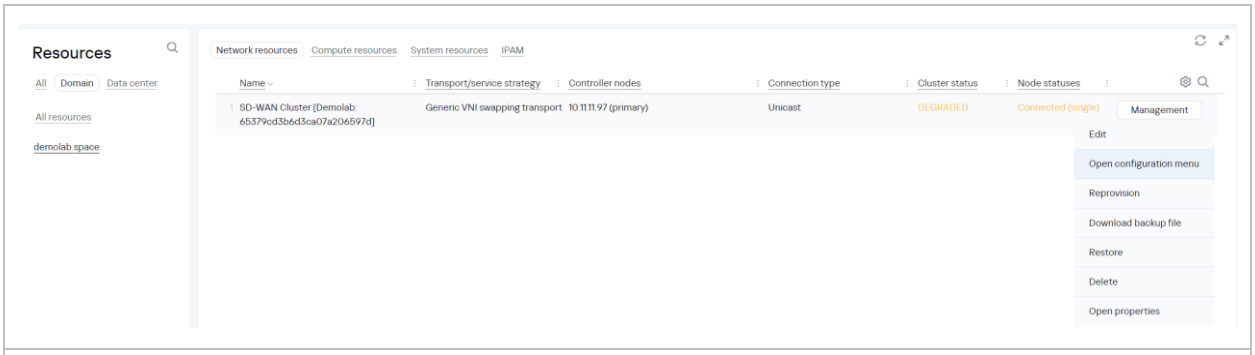
4.8.7. Появилась вкладка “Service Request”.

Для получения деталей регистрации нажать на Task ID задачи.

4.8.8. Настройка SD-WAN шлюза успешно завершена.

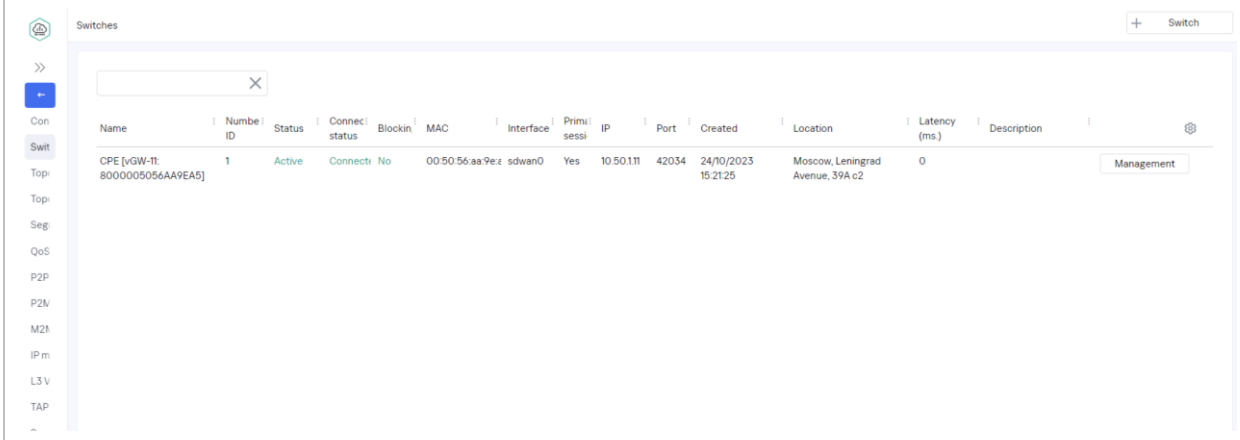


4.8.9. Перейти в меню Infrastructure > Network Resources > SD-WAN контроллер > нажать Management > Open configuration menu.



4.8.10. Перейти в меню Switches.

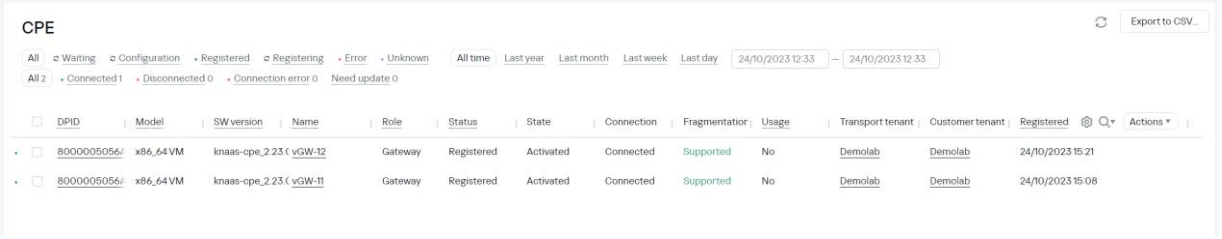
Проверить статус подключения шлюза vGW-11.



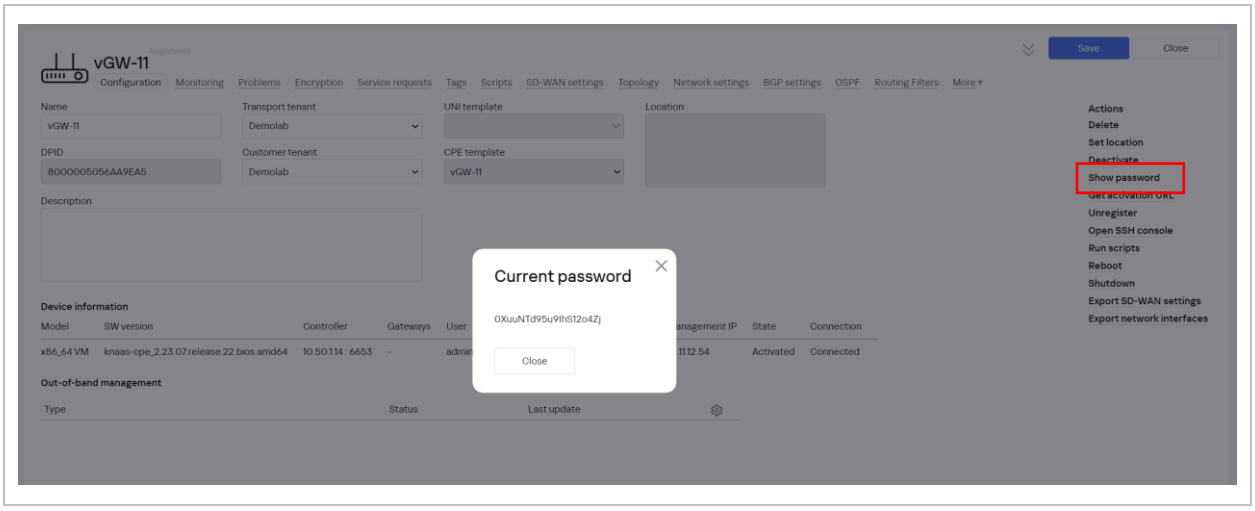
4.8.11. Регистрация шлюза vGW-12.

Выполнить шаги 4.8.2 -4.8.5.

Регистрация SD-WAN шлюзов успешно завершена.



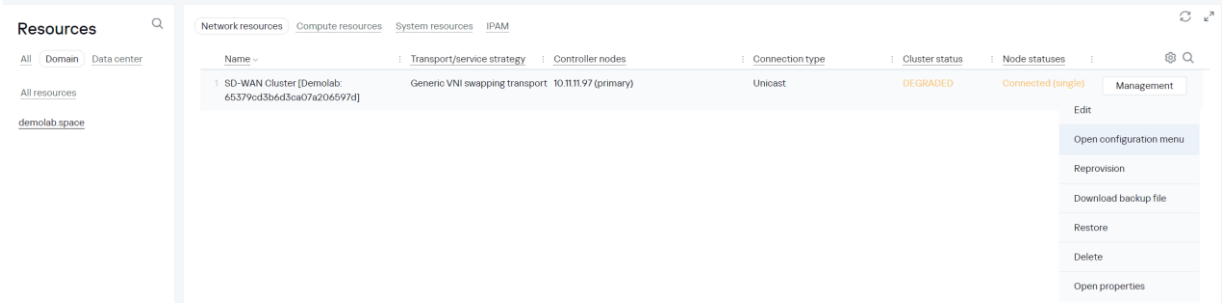
4.8.12. Подключение к шлюзам через SSH.
После регистрации шлюзов оркестратор сменит пароли на устройствах. Для просмотра нового пароля требуется выбрать шлюз и затем нажать Show password.


vGW-11
Registered
Save
Close
Configuration
Monitoring
Problems
Encryption
Service requests
Tags
Scripts
SD-WAN settings
Topology
Network settings
BGP settings
OSPF
Routing Filters
More
Name
vGW-11
Transport tenant
Demolab
UNI template
Location
DPID
8000005056AA9EA5
Customer tenant
Demolab
CPE template
vGW-11
Description
Actions
Delete
Set location
Deactivate
Show password
Get activation URL
Unregister
Open SSH console
Run scripts
Reboot
Shutdown
Export SD-WAN settings
Export network interfaces
Current password
0XuuNTd95u9IlhS12o4Zj
Close
Device information
Model
SW version
Controller
Gateways
User
State
Connection
x86_64 VM
knaas-cpe_2.23.07.release.22.bios.amd64
10.50.114 : 6653
-
admin
Activated
Connected
Out-of-band management
Type
Status
Last update

4.9. **Настройка транспортного сервиса Management P2M.**

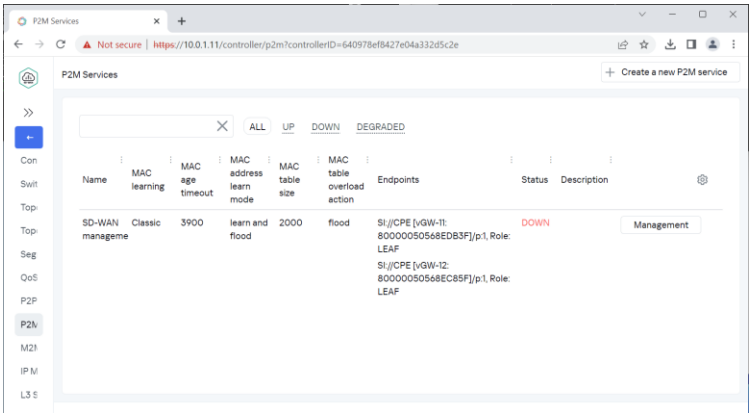
4.9.1. Перейти в меню Infrastructure > Domain > Data Center > Network Resources.

Выбрать SD-WAN контроллер > нажать Management > Open configuration menu.

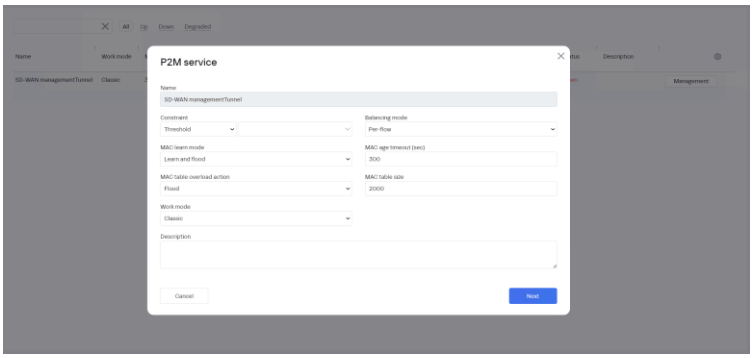


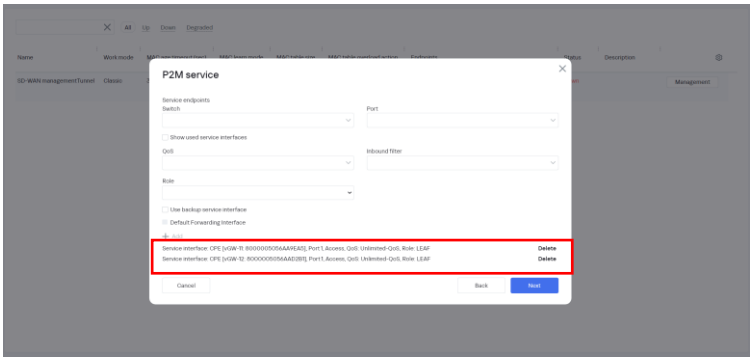
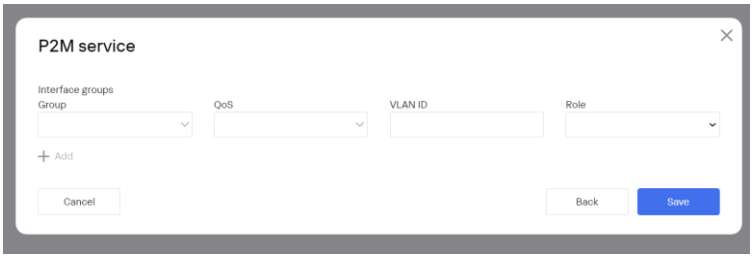
4.9.2. Слева в меню перейти в P2M.

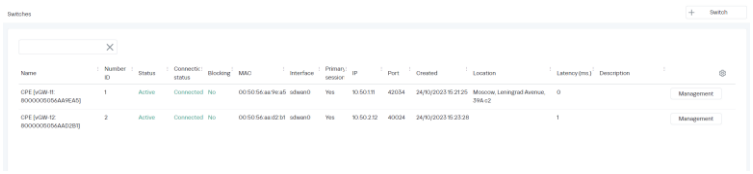
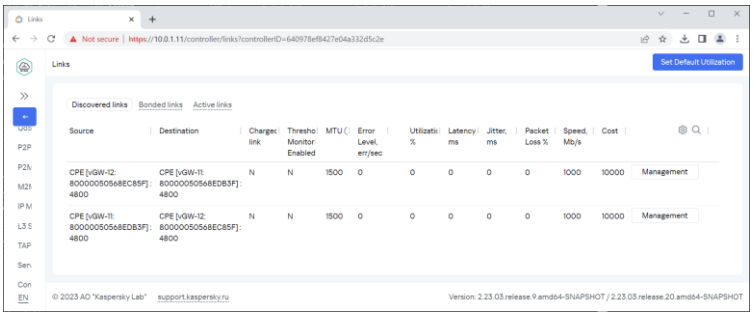
Выбрать SD-WAN managementTunnel > нажать Management > Edit.



4.9.3. Нажать Next.

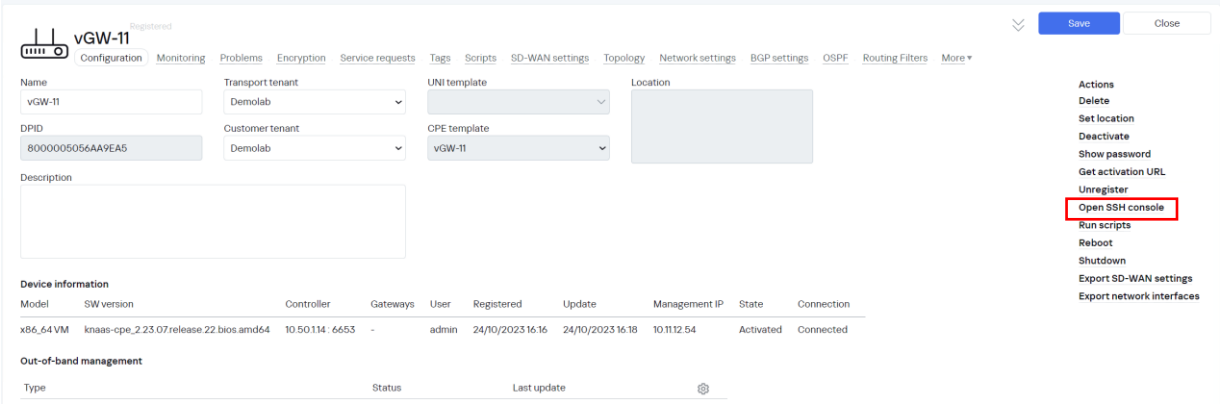


4.9.4. Удалить сервисные интерфейсы (SI) SD-WAN шлюзов с ролью Leaf. Нажать Confirm.	
4.9.5. Добавить сервисные интерфейсы шлюзов с ролью ROOT. Параметры vGW-11: • Switch: CPE [vGW-11]. • Port: Port 1. • QoS: Unlimited QoS. • Role: Root. Нажать Add. Параметры vGW-12: • Switch: CPE [vGW-12]. • Port: Port 1. • QoS: Unlimited QoS. • Role: Root. Нажать Add. Нажать Next.	
4.9.6. Нажать Save.	
4.9.7. Настройка транспортного сервиса Management P2M завершена.	

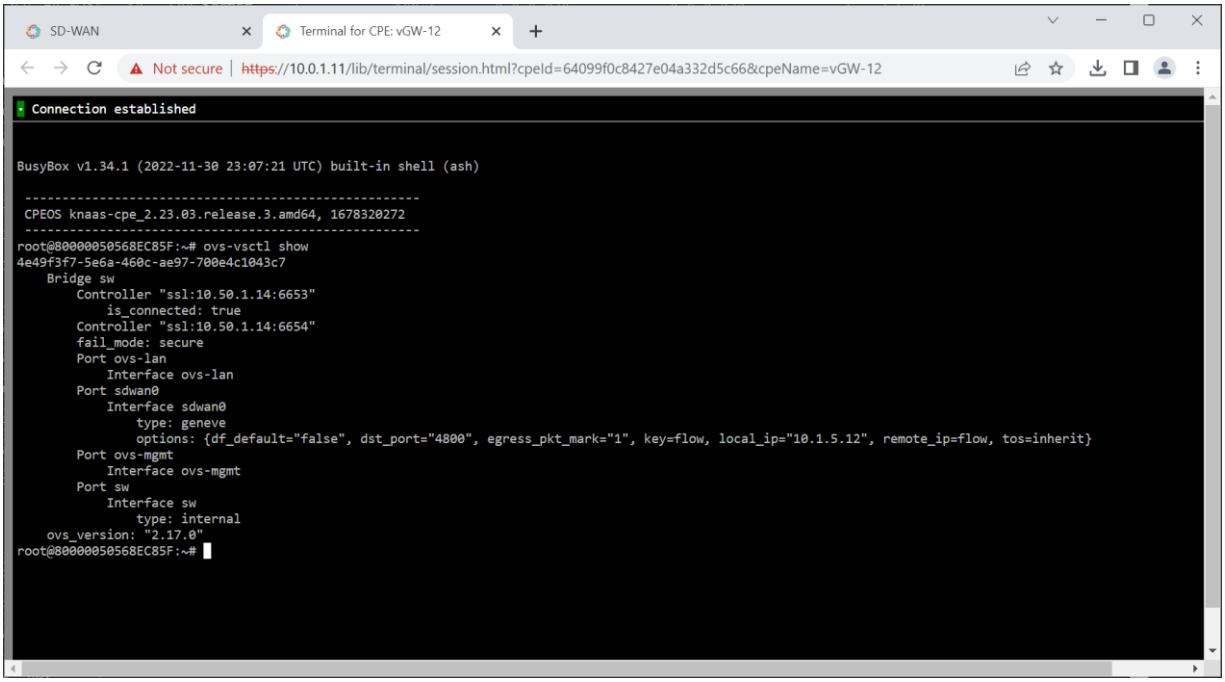
4.9.8. Перейти в раздел Switches и проверить статус OVS (Open vSwitch) коммутаторов на SD-WAN шлюзах.	
4.9.9. Перейти в раздел Tunnels и проверить туннели межу SD-WAN шлюзами.	

4.9.10. Проверка работы доступа к cli консоли SD-WAN шлюза из веб- интерфейса оркестратора.

В меню CPE выбрать SD-WAN шлюз, нажать Open SSH Console.



4.9.11. CLI консоль.



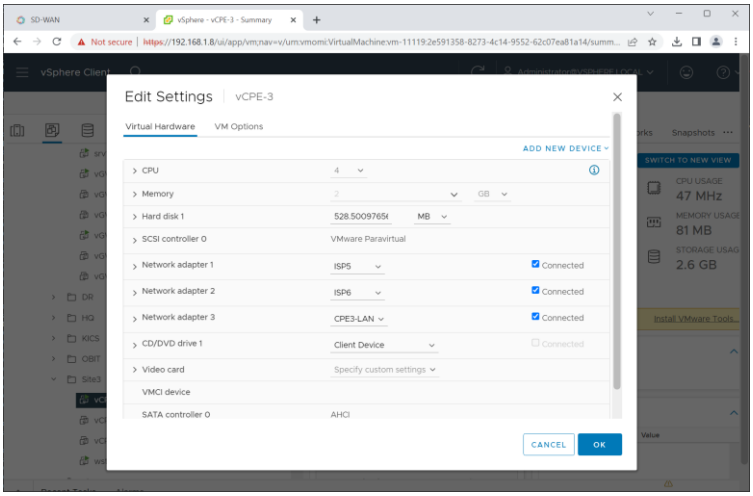
4.9.12. Проверить работу подсистемы мониторинга.

Перейти в меню CPE, выбрать SD-WAN шлюз и открыть вкладку Monitoring.

4.10. **Подготовка CPE устройств.**

4.10.1. Создать виртуальную машину для CPE устройства.

Добавить три сетевых интерфейса: 2 x wan + lan.



4.10.2. Настроить lan интерфейс.

Открыть конфигурационный файл:
 # vi /etc/config/network

Задать сетевой интерфейс eth2 для br-lan, т.к. eth0 и eth1 используются для sdwan0 и sdwan1.

На mgmt рабочей станции win11 есть сетевой интерфейс в сети site3-lan 10.20.3.0/24.

Задать IP адрес для lan: 10.20.3.1/24, будет использоваться для ZTP URL с рабочей станции win11.

Перезапустить сетевую службу:
 # /etc/init.d/network restart

```
config globals 'globals'
        option ula_prefix 'fd6f:d886:3301::/48'

config device
        option type 'veth'
        option name 'mgmt'
        option peer_name 'ovs-mgmt'

config interface 'mgmt'
        option device 'mgmt'
        option proto 'none'

config interface 'ovs_mgmt'
        option device 'ovs-mgmt'
        option proto 'none'

config device
        option type 'veth'
        option name 'overlay'
        option peer_name 'ovs-lan'

config interface 'overlay'
        option device 'overlay'
        option proto 'none'

config interface 'ovs_lan'
        option device 'ovs-lan'
        option proto 'none'

config interface 'lan'
        option type 'bridge'
        option proto 'static'
        option ipaddr '10.20.4.1'
        option netmask '255.255.255.0'
        option ifname 'eth2'
        option auto '1'
        option force_link '1'

config interface 'sdwan0'
        option device 'eth0'
        option proto 'dhcp'
        option metric '100'
```

4.10.3. Задать пароль пользователя root.

 # passwd

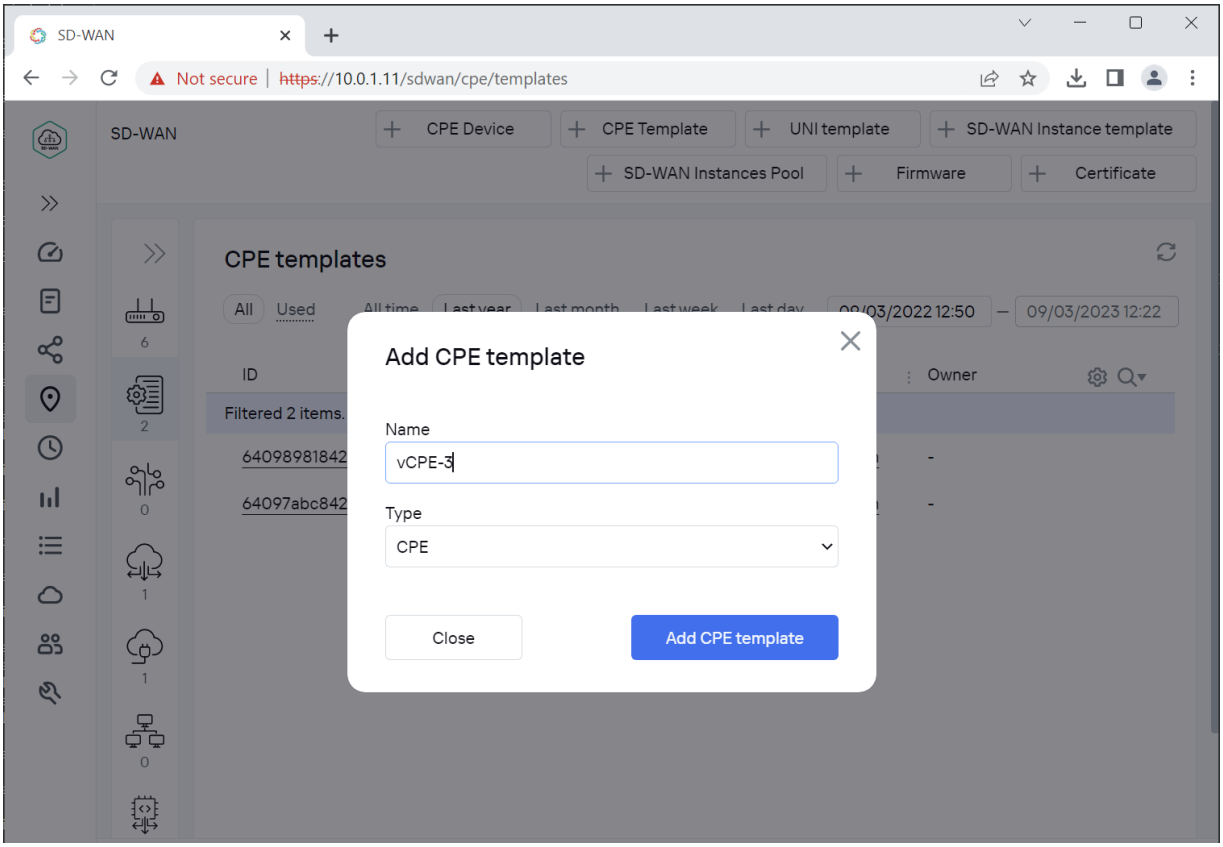
4.11. **Создание шаблонов для CPE устройств.**

4.11.1. Создать шаблон для CPE устройства.

Перейти в меню SD-WAN > CPE Templates.

Нажать “+CPE Template”.

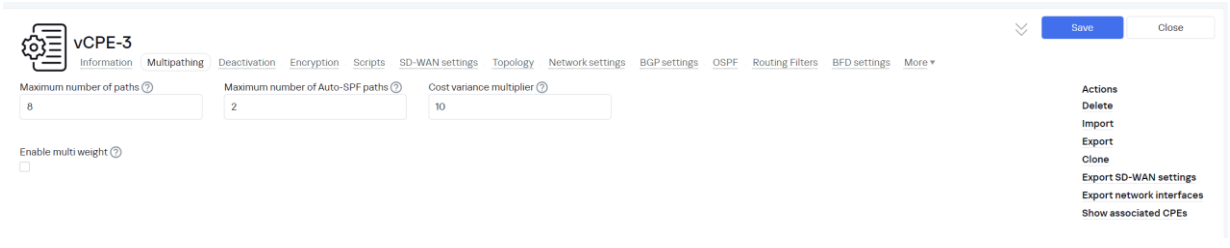
Задать имя: vCPE-3.



4.11.2. Перейти на вкладку Multipathing.

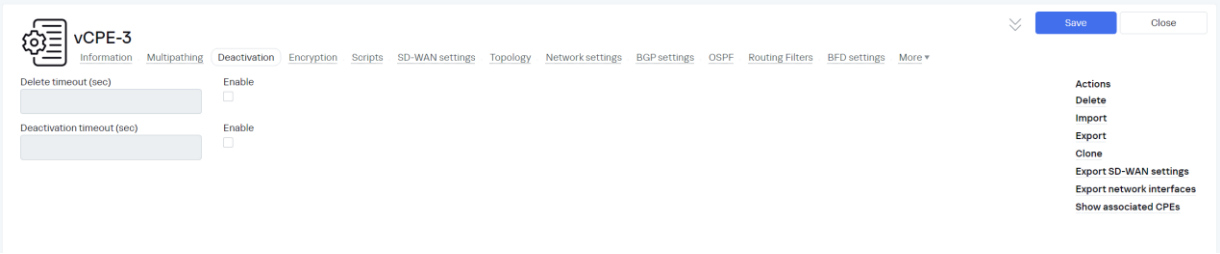
Оставить преднастроенные параметры «по умолчанию»: 8/2/10.

Выключить параметр Enable Multi Weight.



4.11.3. Перейти на вкладку Deactivation.

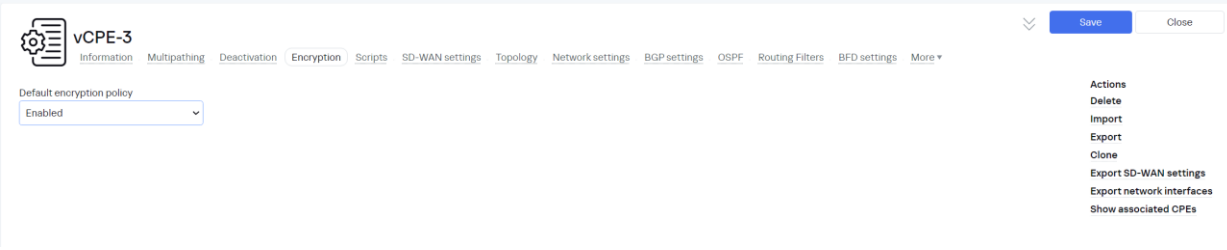
Оставить преднастроенные параметры «по умолчанию».



4.11.4. Перейти на вкладку Encryption.

Включить шифрование: Enabled.

Нажать Save.



4.11.5. Перейти на вкладку SD-WAN Settings.

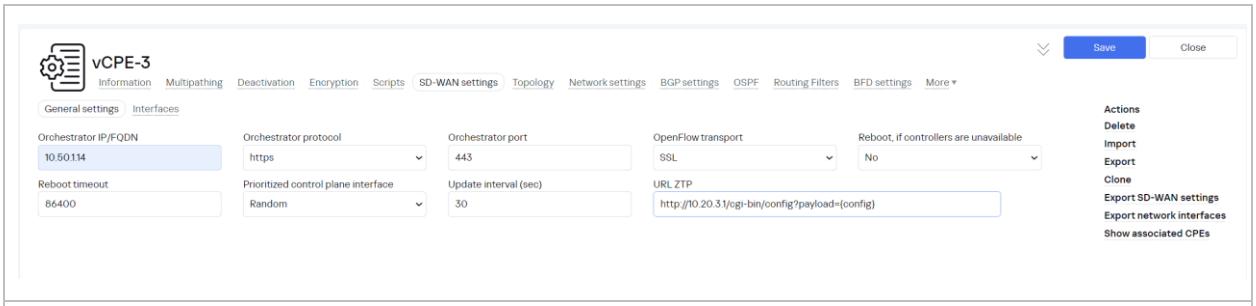
Задать:

- SD-WAN Orchestrator IP/FQDN: 10.50.1.14
- Openflow Transport: ssl
- SD-WAN Orchestrator Port: 443
-

При изменении IP плана из пункта 2.3 использовать новый публичный IP адрес хоста orc1.

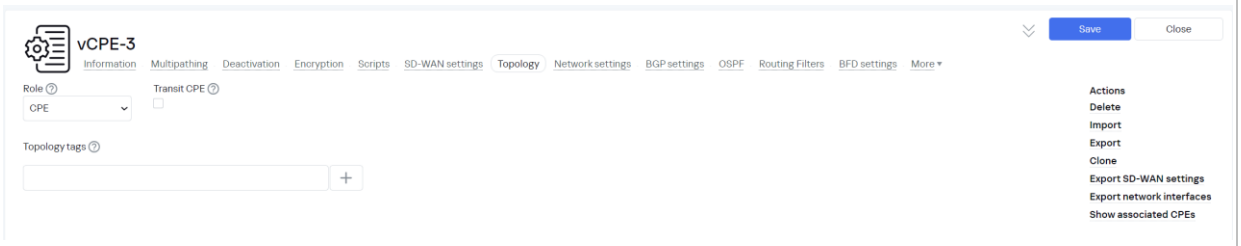
Задать IP адрес в ZTP URL для активации устройства. Указать адрес lan-интерфейса CPE.
В рамках данной лабораторной работы используются следующие IP адреса для lan сетевых интерфейсов CPE:

- lan vCPE-3: 10.20.3.1/24
- lan vCPE-4: 10.20.4.1/24
- lan vCPE-51: 10.20.5.1/24
- lan vCPE-52: 10.20.5.2/24



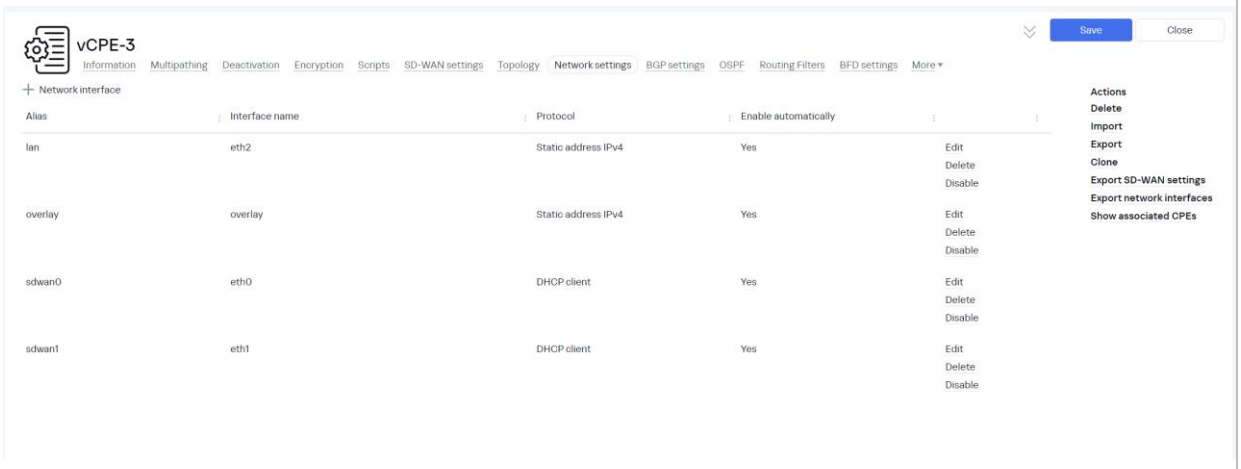
4.11.6. Перейти на вкладку Topology.

Задать роль: CPE.



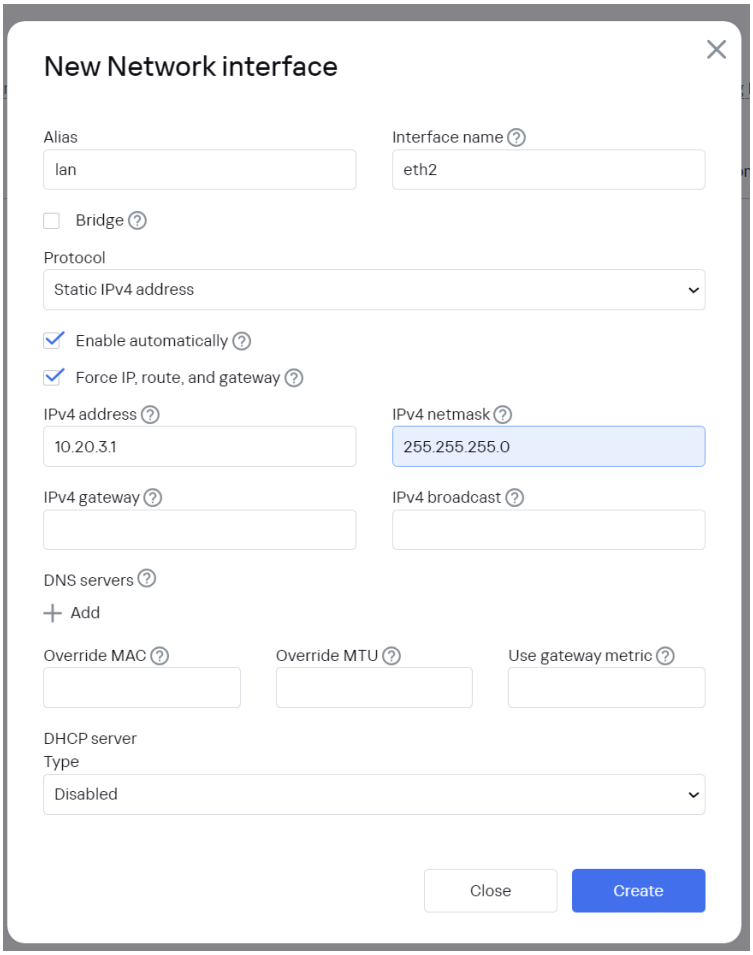
4.11.7. Перейти на вкладку Network Settings.

Создать сетевые интерфейсы: lan, overlay, sdwan0 и sdwan1.



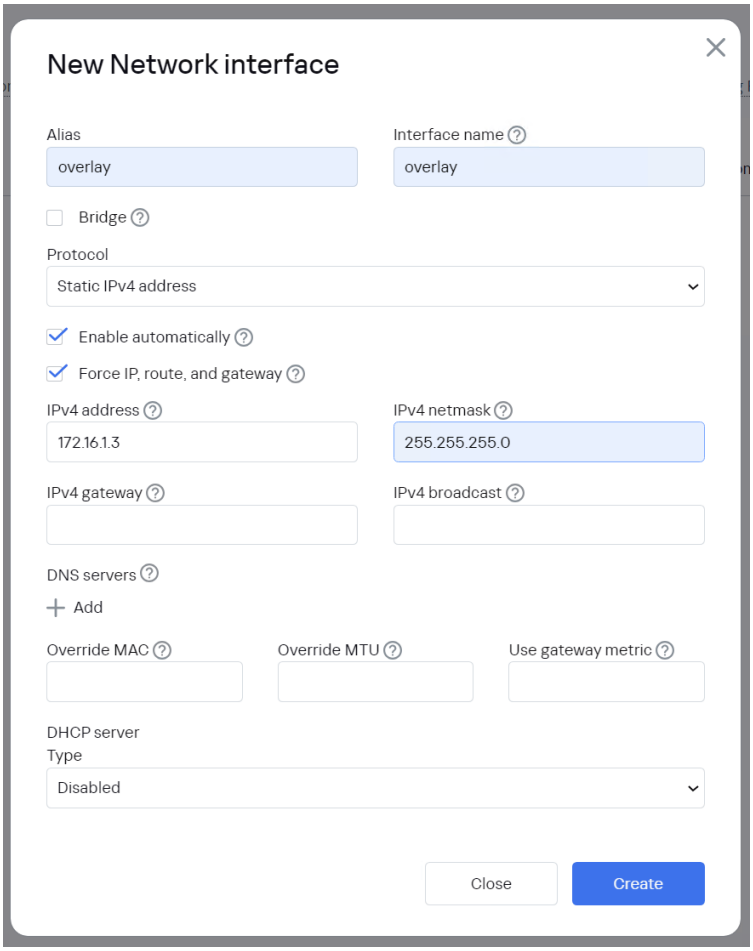
4.11.8. В рамках данной лабораторной работы IP адреса для lan сетевых интерфейсов:

- lan vCPE-3: 10.20.3.1/24
- lan vCPE-4: 10.20.4.1/24
- lan vCPE-51: 10.20.5.1/24
- lan vCPE-52: 10.20.5.2/24



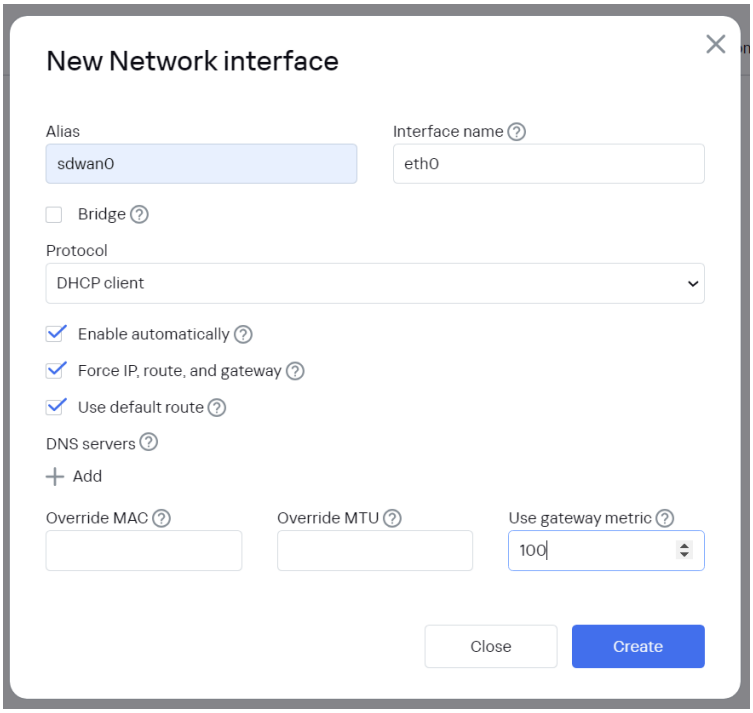
4.11.9. В рамках данной лабораторной работы IP адреса для overlay сетевых интерфейсов:

- overlay vCPE-3: 172.16.1.3
- overlay vCPE-4: 172.16.1.4
- overlay vCPE-51: 172.16.1.51
- overlay vCPE-52: 172.16.1.52



4.11.10. Сетевые интерфейсы sdwan0, sdwan1 получат настройки по DHCP.

Для сетевых интерфейсов sdwan0, sdwan1 задать значение Use gateway metric 100 и 101 соответственно.



4.11.11. Создание Prefix List для CPE.

Перейти на вкладку Routing filters > Prefix lists.

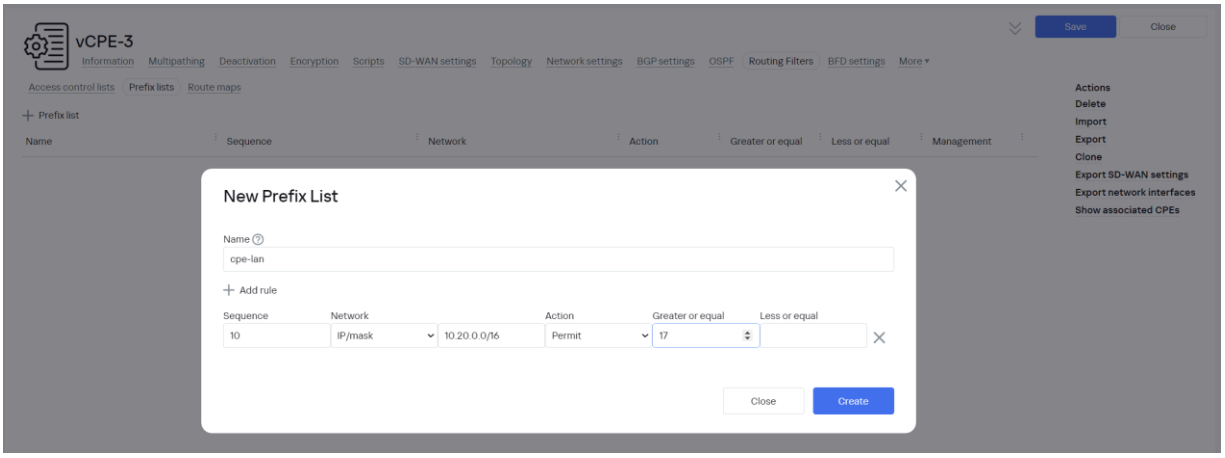
Нажать “+Prefix List”.

Name: cpe-lan.

Нажать “+Add Rule”.
Добавить сеть:

- Seq 10 10.20.0.0/16
- Greater of Equal 17

Нажать Create.



4.11.12. Создание Route Map для CPE.

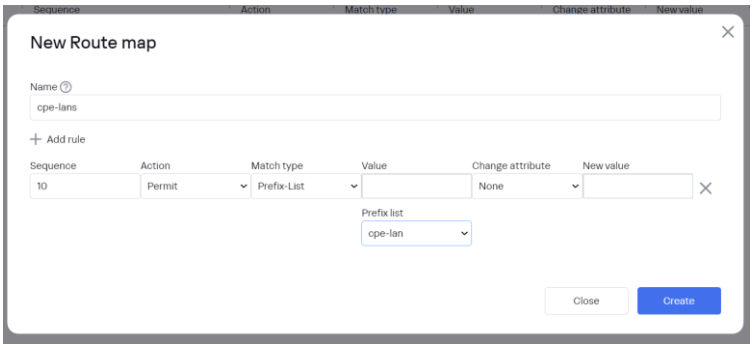
Перейти на вкладку Routing filters > Route maps.

Нажать “+Route Map”.
Задать Name: cpe-lans

Нажать Add Rule:

- Sequence: 10
- Action: Permit
- Match Type: Prefix-list
- Match Value: cpe-lan

Нажать Create.

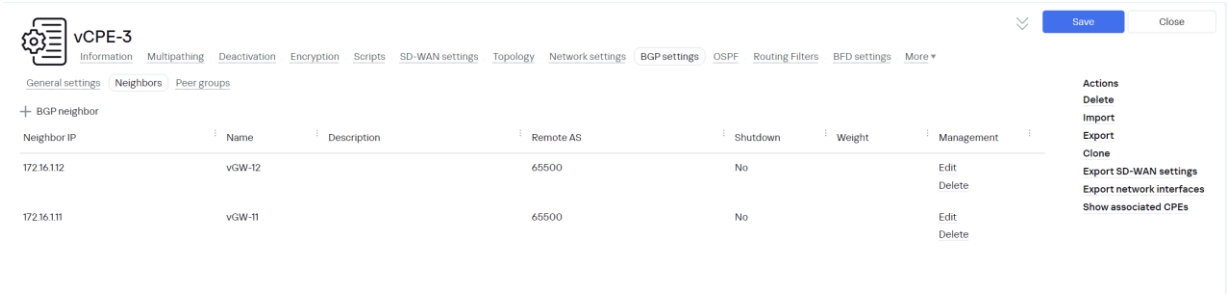


4.11.13. Перейти на вкладку BGP Settings > Neighbors.

Нажать “+ BGP Neighbor”.

В качестве соседей добавить vGW-11 и vGW-12 в AS65500.

Нажать Save.



4.11.14. Перейти на вкладку BGP Settings > General Settings.

Задать / проверить параметры BGP:

- BGP: Enabled
- AS: 65500
- Router ID: 172.16.1.3 (IP адрес сетевого интерфейса overlay).
- Maximum Paths: 2

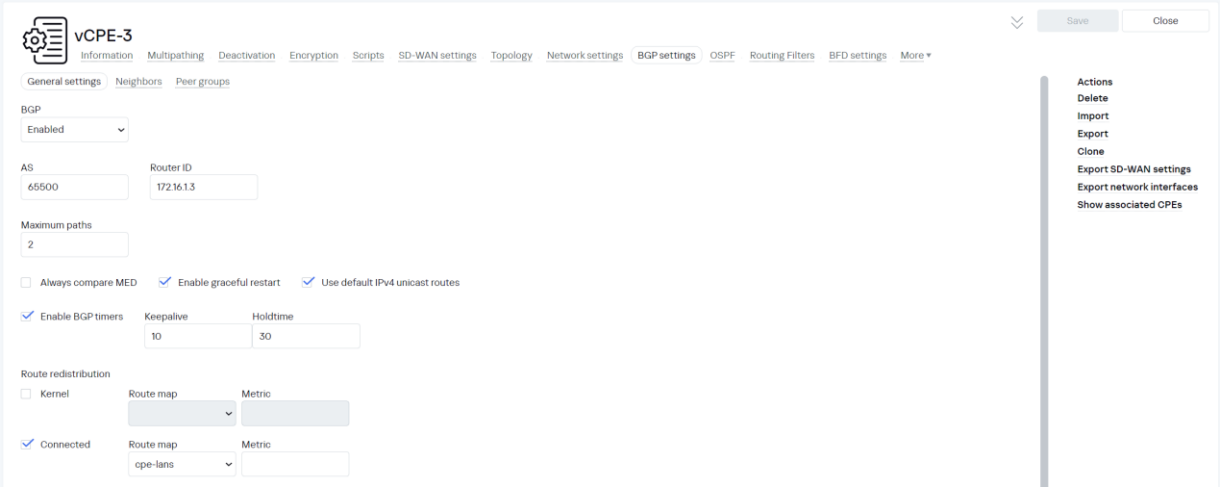
- Enable Graceful Restart
- Default IPv4 Unicast
- Enable BGP Timers:
  - Keepalive: 10
  - Hold: 30

Применить Route Map “cpe-lans” при анонсировании Connected маршрутов.

В рамках данной лабораторной работы BGP Router ID:

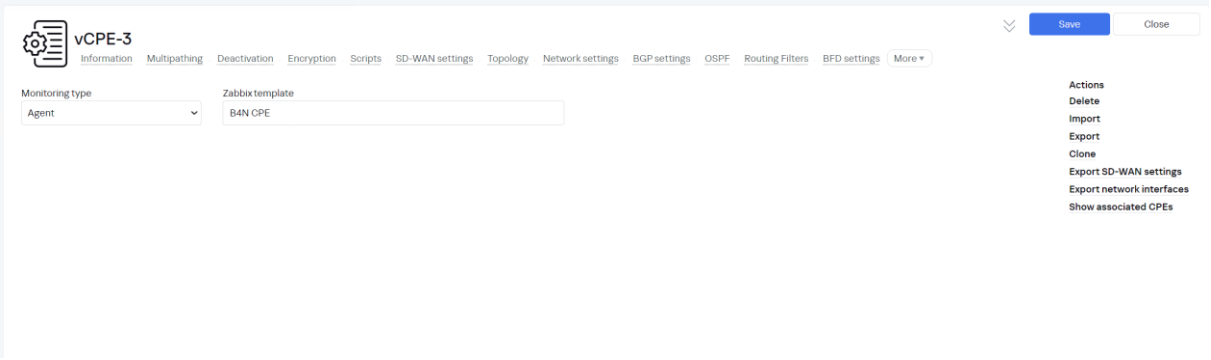
- vCPE-3: 172.16.1.3
- vCPE-4: 172.16.1.4
- vCPE-51: 172.16.1.51
- vCPE-52: 172.16.1.52

Нажать Save.



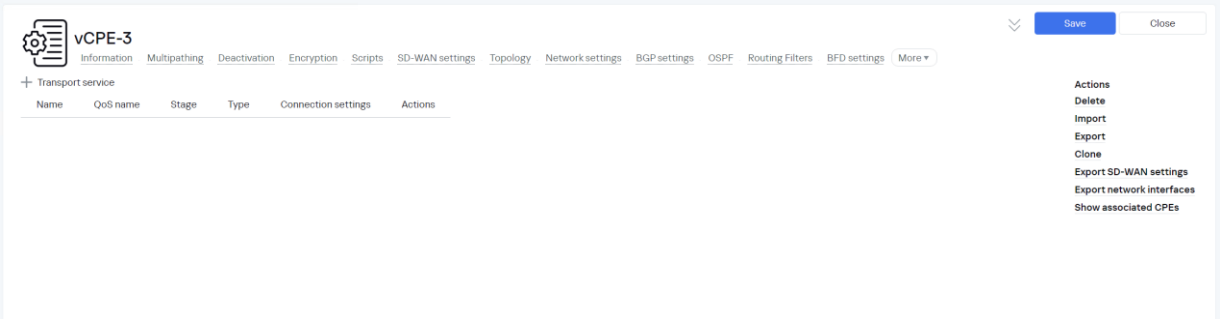
4.11.15. Перейти на вкладку Monitoring.

Задать Monitoring type: Agent.
Задать значение Zabbix template: “B4N CPE”.



4.11.16. Перейти на вкладку Transport Services.

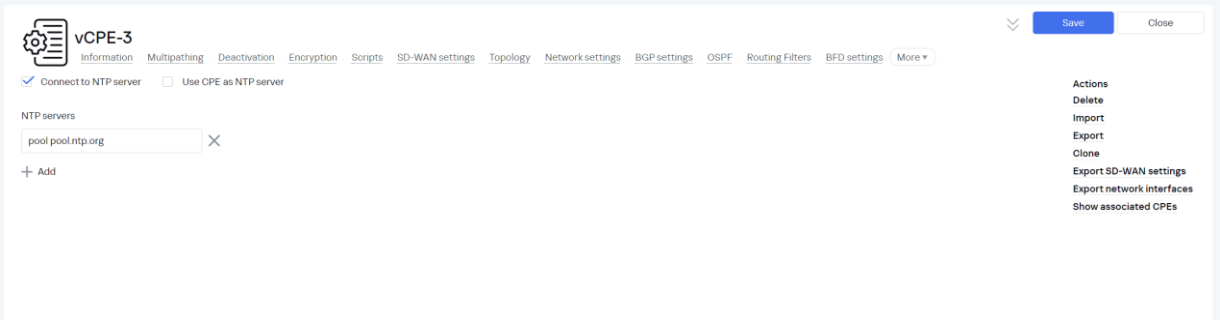
Оставить значение «по умолчанию».



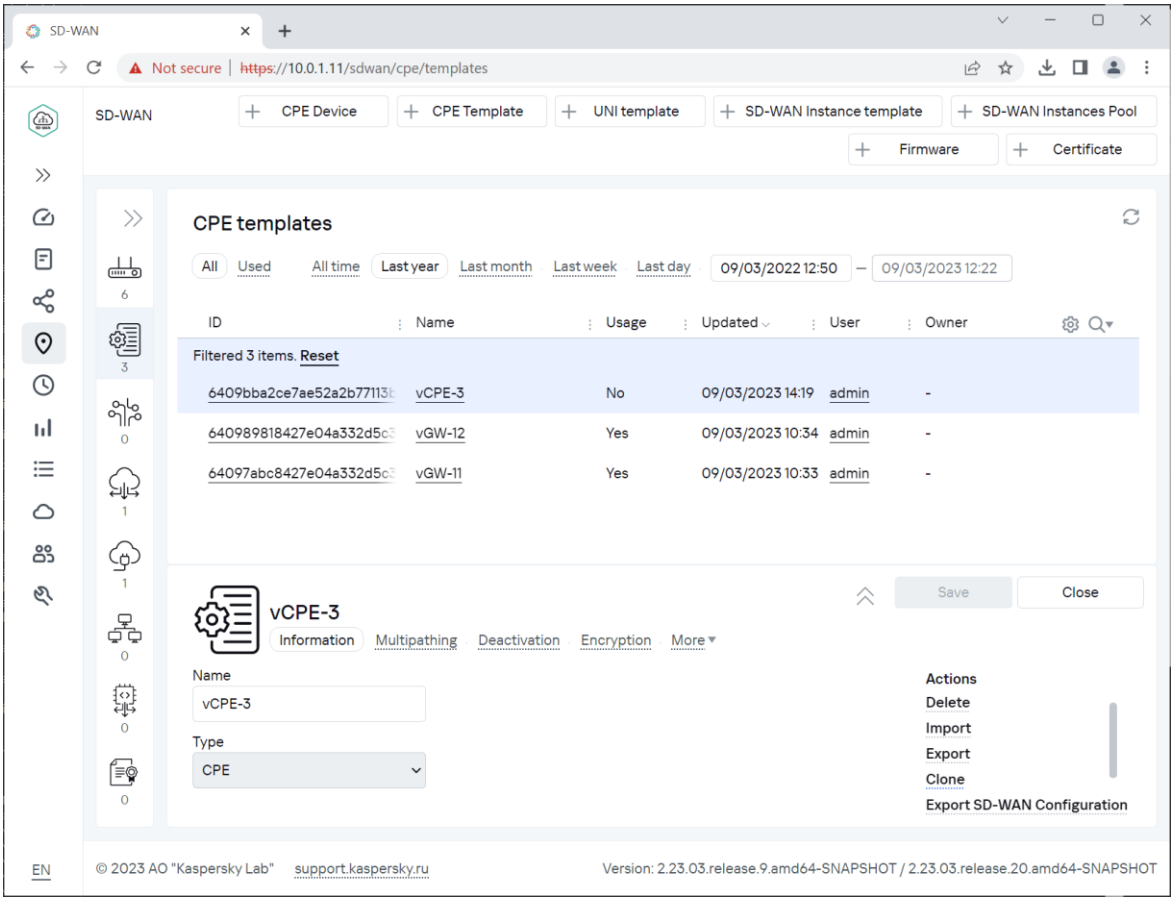
4.11.17. Перейти на вкладку NTP.

Настроить NTP серверы.

Нажать Save.



4.11.18. Выполнить создание шаблонов CPE устройств для vCPE-3, vCPE-4, vCPE-51 и vCPE-52 используя инструкции путем клонирования.

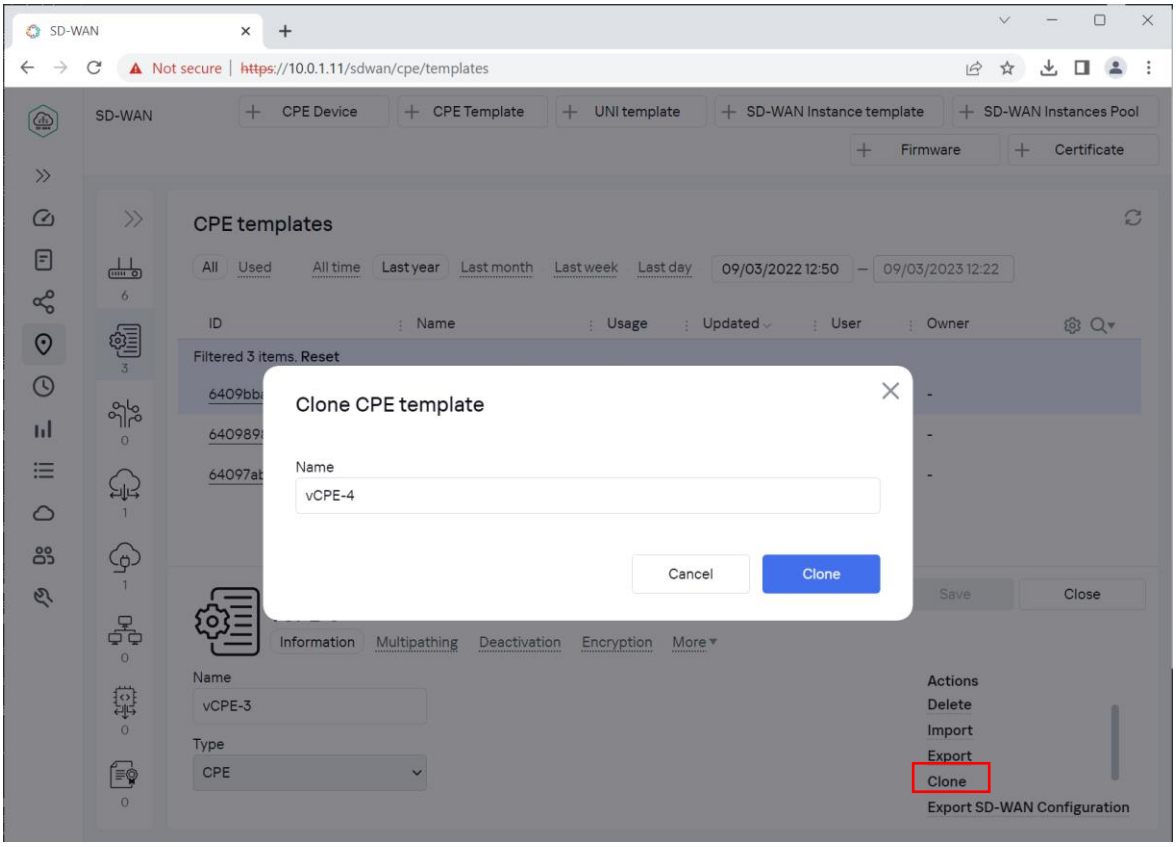


4.11.19. Клонировать шаблоны vCPE-4, vCPE-51 и vCPE-52из vCPE-3.

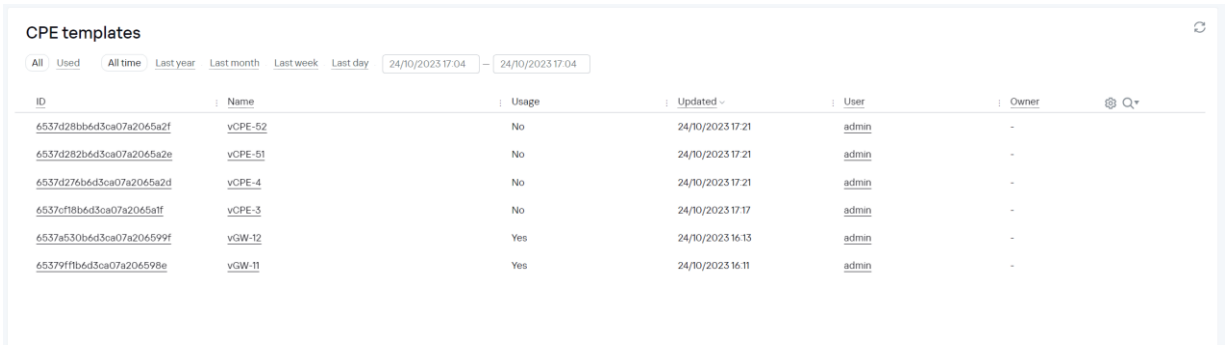
Нажать “Clone”.

Задать имя нового шаблона.

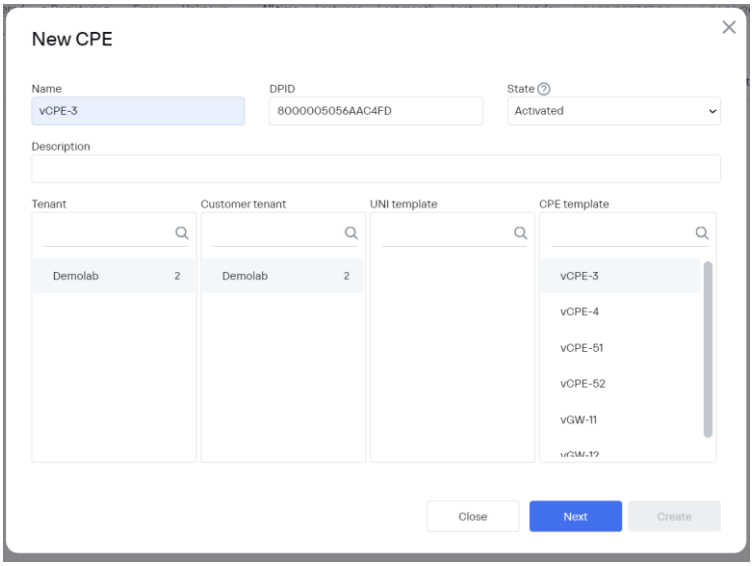
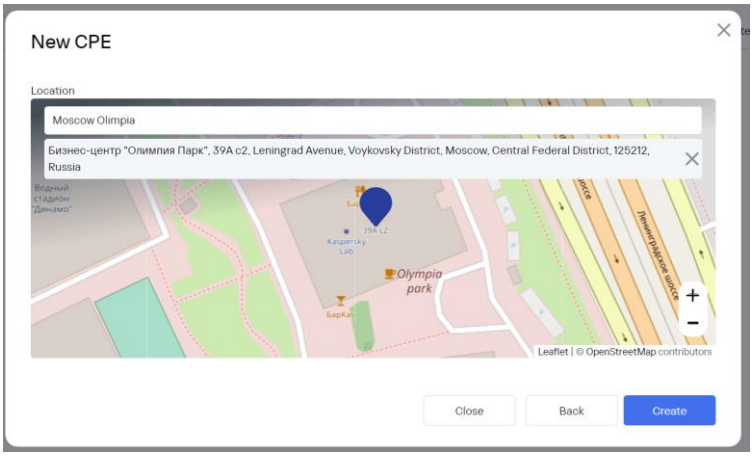
Повторить пункты 4.11.2-4.11.17 для склонированных шаблонов, изменить значения параметров на соответствующие каждому CPE устройству.



4.11.20. Созданные шаблоны для CPE устройств.



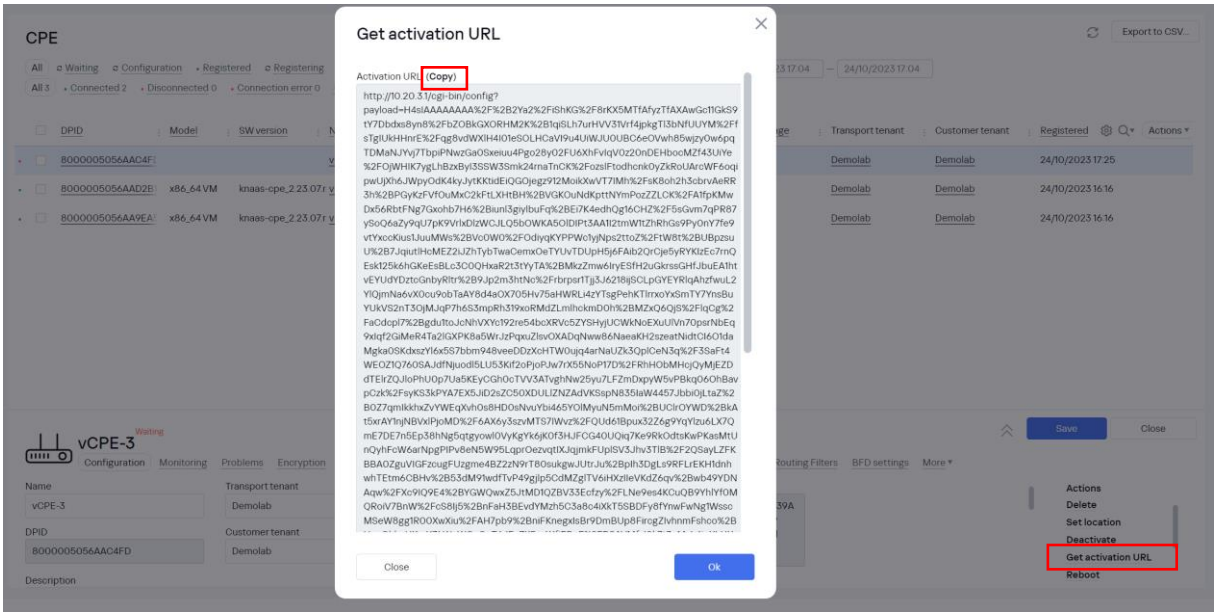
4.12. **Регистрация CPE устройств.**

4.12.1. Добавить CPE устройство. Перейти в меню SD-WAN > CPE, нажать +CPE Задать: • Name: vCPE-3. • DPID (посмотреть в cli консоли). • Set State: Activated. Выбрать: • Transport Tenant. • Customer Tenant. • CPE Template. Нажать кнопку Next.	
4.12.2. Нажать кнопку Create.	

4.12.3. Выполнить активацию с использованием ZTP URL.

Перейти в меню SD-WAN > CPE, выбрать CPE устройство и нажать Get Activation URL.

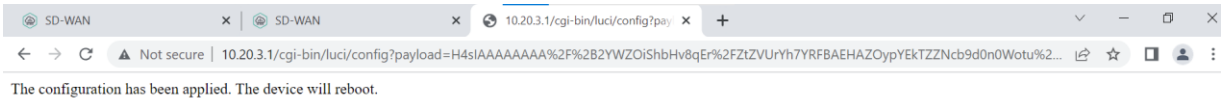
Нажать Copy.



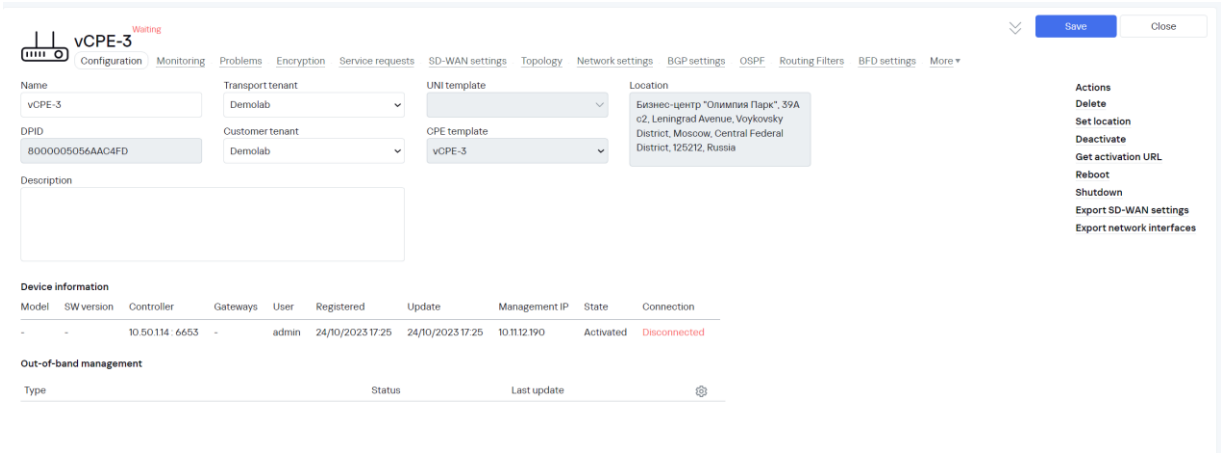
4.12.4. Конфигурация устройства предана на CPE устройство.

Затем CPE автоматически перезагрузится.

ZTP URL содержит сетевые настройки, сертификат CA, токен для 2FA.



4.12.5. CPE устройство перешло в статус Waiting.



4.12.6. Наблюдение за процессом регистрации CPE устройства.

Перейти в меню SD-WAN > CPE.

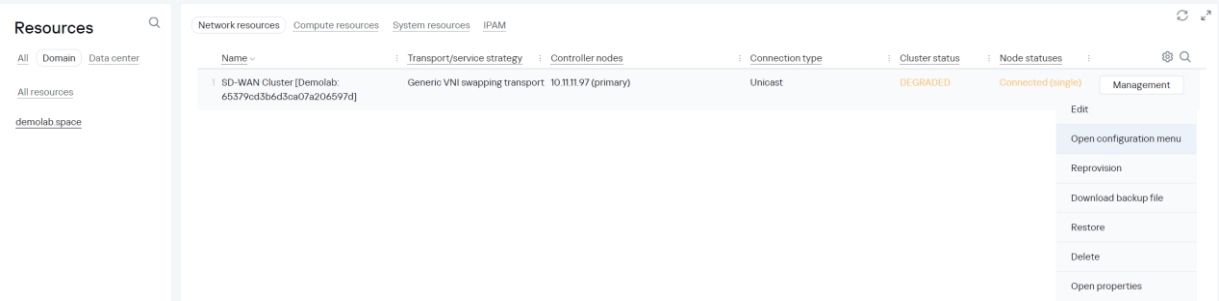
Выбрать CPE устройство, перейти на вкладку Service Request.

Нажать на Task ID у задачи CpeRegistration

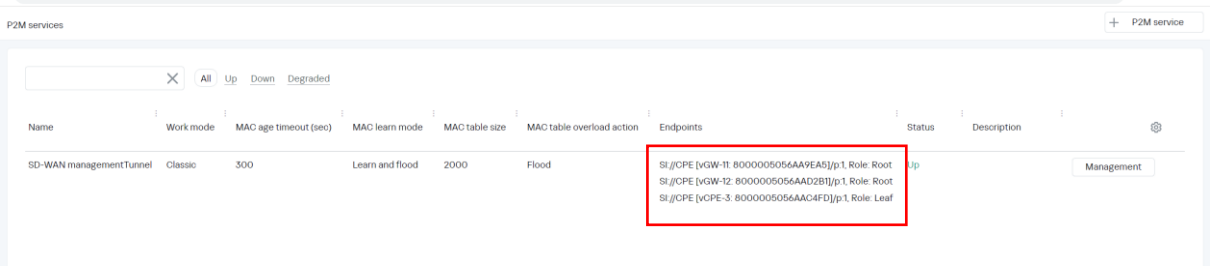
.

4.12.7. Перейти в меню Infrastructure > Domain > Data Center > Network Resources.

Выбрать SD-WAN контроллер > нажать Management > Open configuration menu.

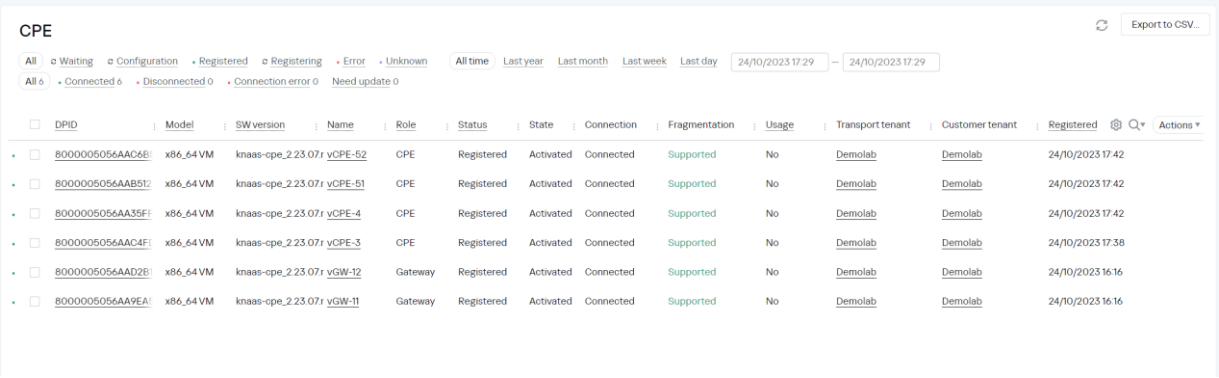


4.12.8. Перейти в настройки SD-WAN контроллера, открыть Management P2M транспортный сервис и проверить автоматическое добавление vCPE-3 с ролью Leaf.



4.12.9. Выполнить регистрацию CPE устройств vCPE-3, vCPE-4, vCPE-51 и vCPE-52 с использованием инструкций 4.12.1 -4.12.8.

Перейти в меню SD-WAN > CPE.

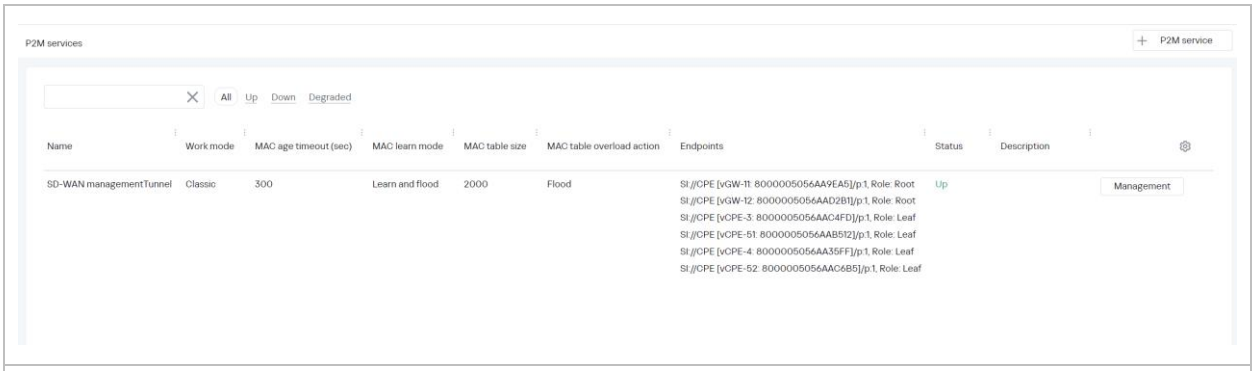


4.12.10. Проверка Management транспортного сервиса.

Перейти в меню SD-WAN > Infrastructure > SD-WAN контроллер > Management > Open configuration menu > P2M Services.

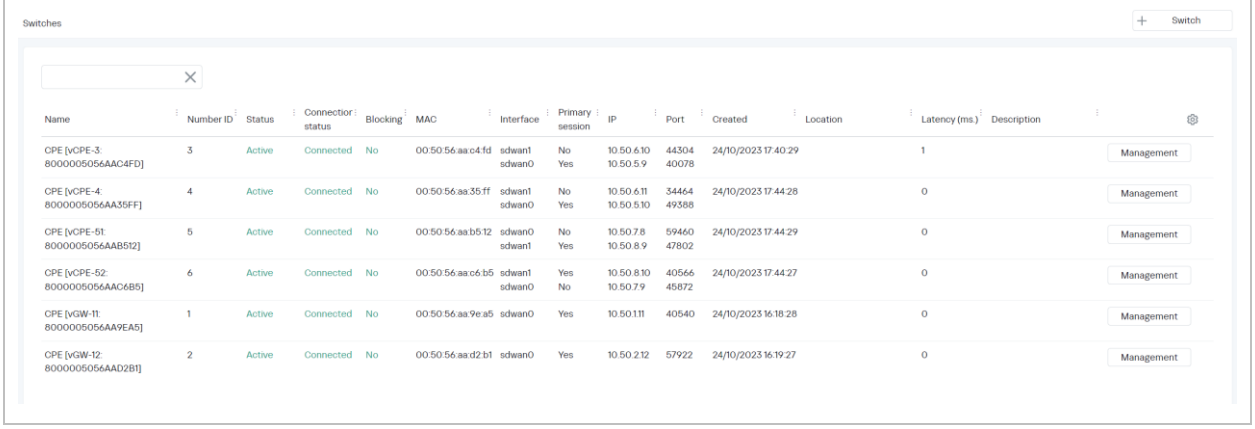
Сервис работает, состояние “UP”.

CPE устройства автоматически добавляются с ролью Leaf.



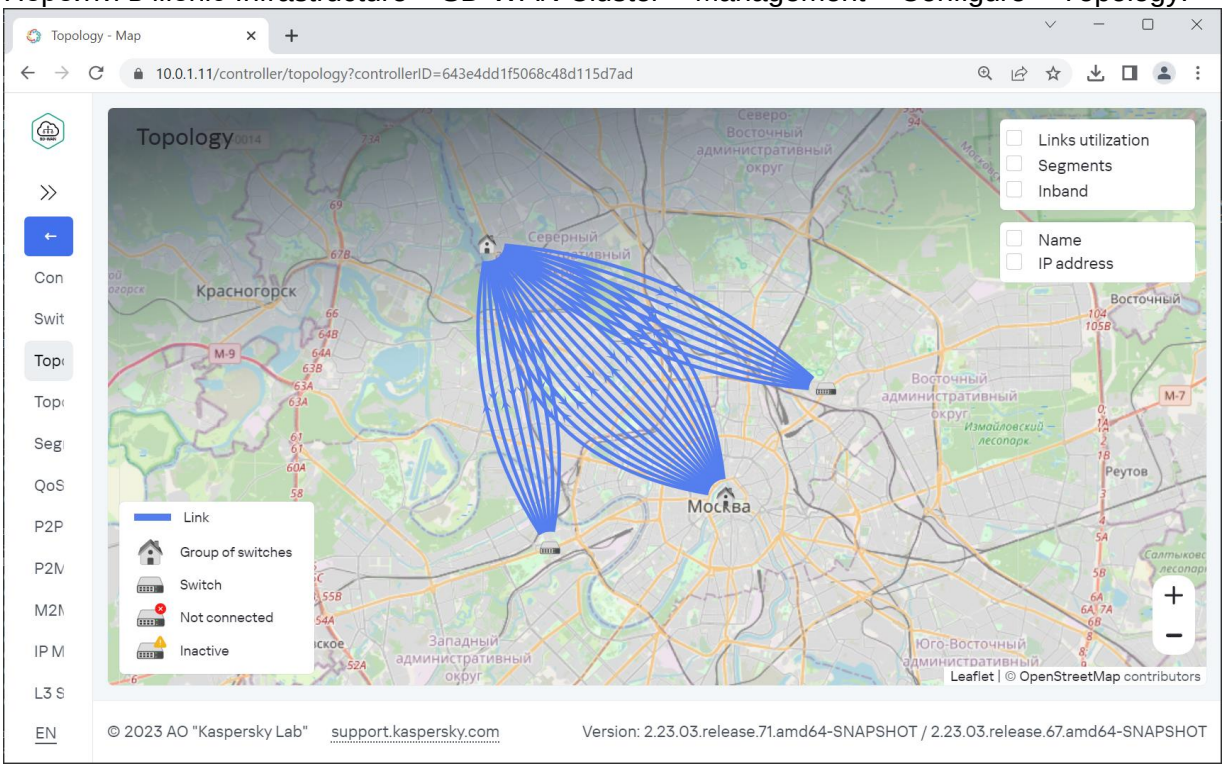
4.12.11. Проверка подключения CPE устройств к контроллеру.

Перейти в меню Infrastructure > SD-WAN Cluster > Management > Open configuration menu > Switches.



4.12.12. Топология SD-WAN сети.

Перейти в меню Infrastructure > SD-WAN Cluster > Management > Configure > Topology.

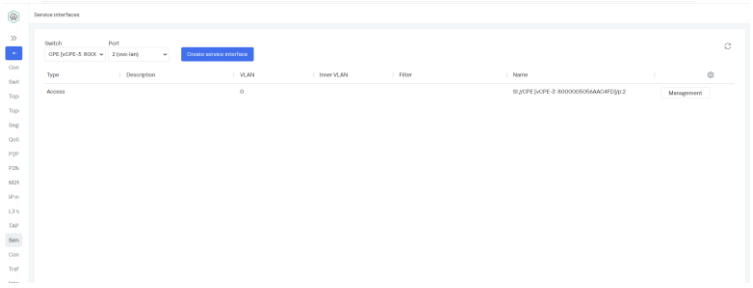
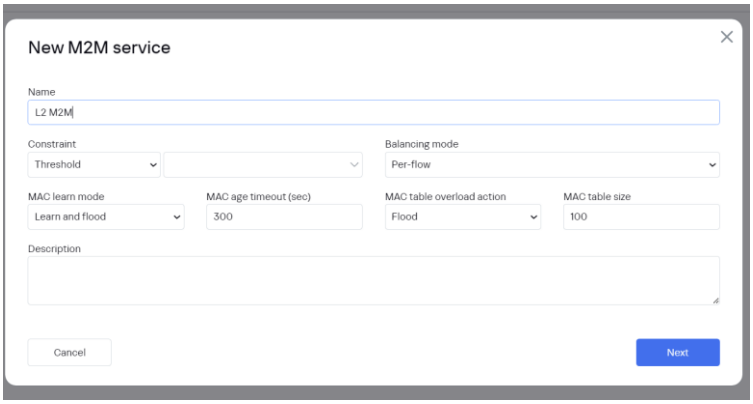


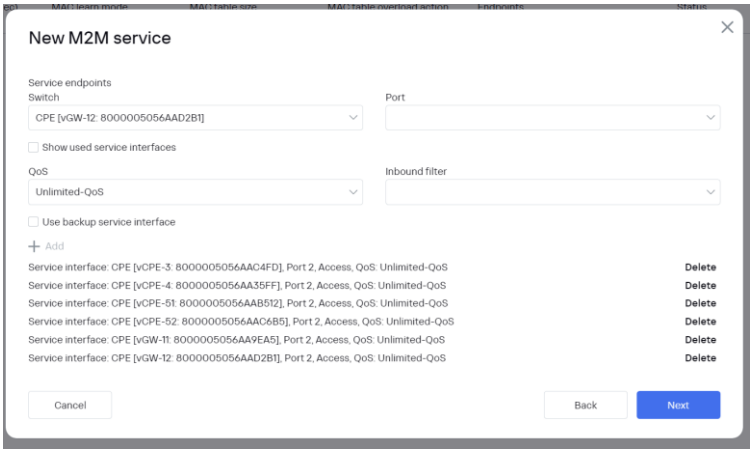
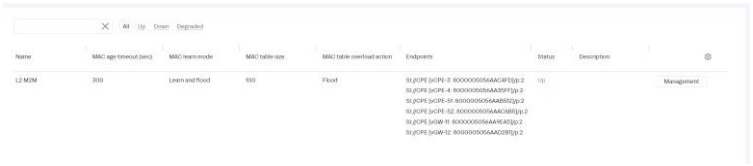
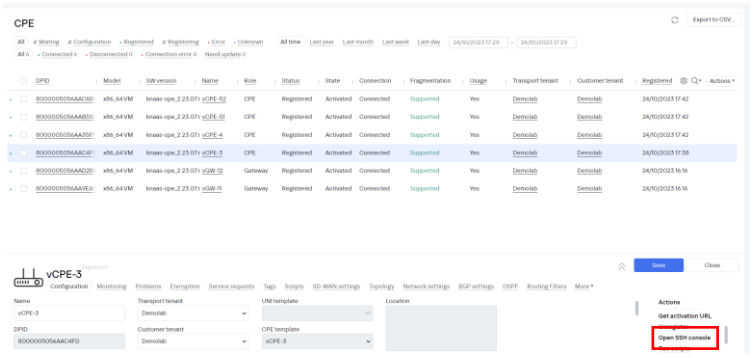
5. **Управление трафиком.**

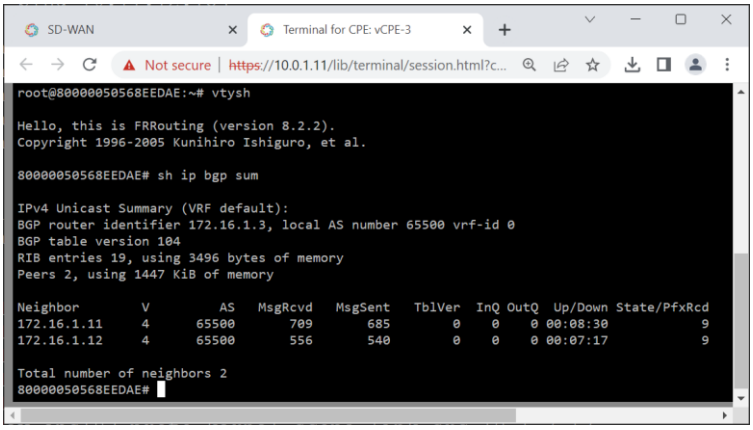
5.1. **Настройка транспортного сервиса L2 M2M.**

Топология Hub-and-Spoke является наиболее распространенной при построении сетей SD-WAN. В этом разделе описывается топология Hub-and-Spoke, в рамках которой удаленные площадки подключаются к SD-WAN шлюзам.

Чтобы построить топологию Hub-and-Spoke со связью между удаленными площадками через центральные SD-WAN шлюзы, необходимо создать транспортный сервис L2 типа M2M (Multipoint-to-Multipoint или E-LAN).

5.1.1. Создание сервисных интерфейсов. Перейти в меню SD-WAN > Infrastructure > SD-WAN контроллер > Management > Open configuration menu > Service Interfaces. Выбрать устройство, затем выбрать порт 2 (ovs-lan) и нажать «Create service interface». Нажать Create. Повторить для всех шлюзов и устройств CPE.	
5.1.2. Создание транспортного сервиса L2 типа M2M. Перейти в меню SD-WAN > Infrastructure > SD-WAN контроллер > Management > Open configuration menu > M2M Services и нажать “+M2M service”. Задать имя сервиса и нажать Next.	

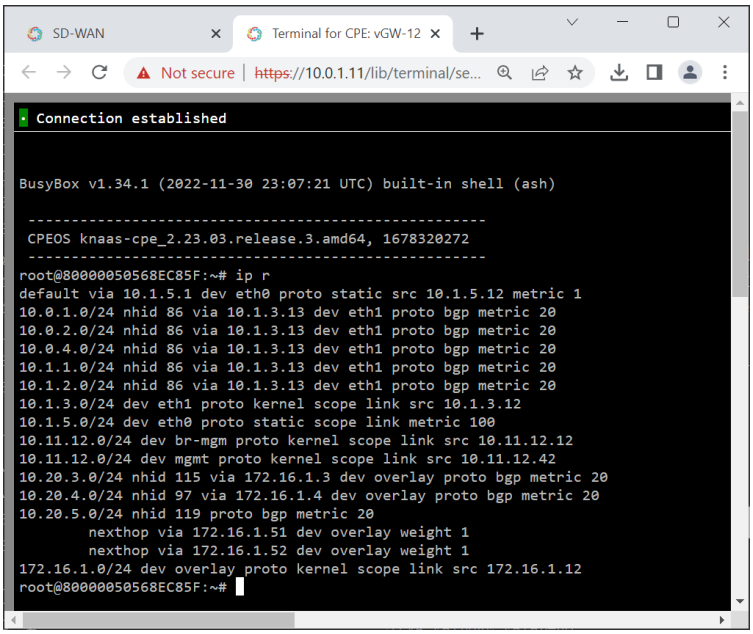
5.1.3. В разделе Service endpoints > в списке Switch поочередно выбрать все SD-WAN шлюзы, CPE устройства и добавить с использованием кнопки “+Add”. Значения параметров: • Port: Port 2 Access • QoS: Unlimited QoS Нажать Next.	
5.1.4. Нажать Create.	
5.1.5. Транспортный сервис M2M создан. Сервис работает, состояние “UP”.	
5.1.6. Проверка работы BGP на vCPE-3. Перейти в меню SD-WAN > CPE, выбрать CPE устройство и нажать Open SSH Console. Для BGP используется FRRouting. Подключиться к устройству CPE по ssh. Перейти в консоль vtysh: *# vtysh* Выполнить команды: *# show ip route* *# show ip bgp sum* *# show run*	



5.1.7. Проверка работы BGP на vGW-12.

Подключиться к SD-WAN шлюзу по ssh.

Выполнить команду:
 # ip r

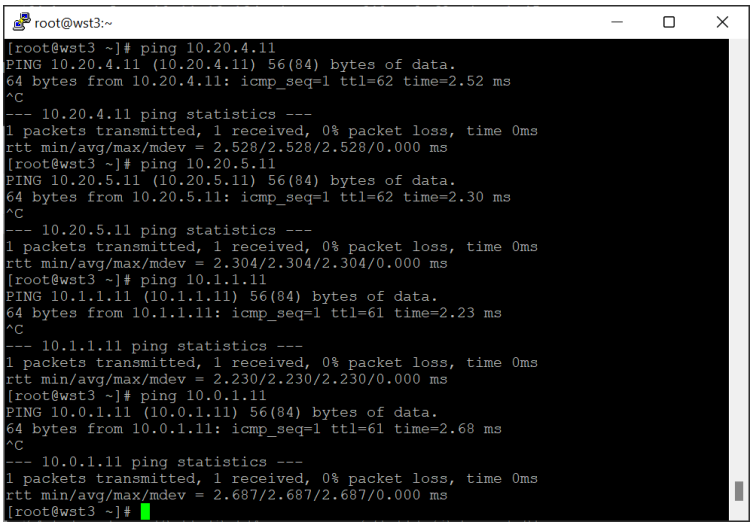


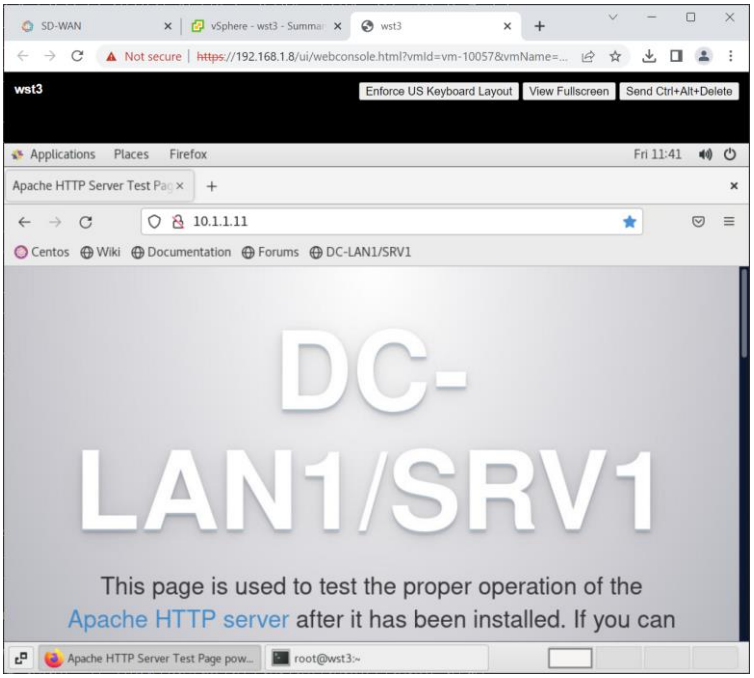
5.1.8. Проверка связи между wst3, wst4, wst5, srv1 и orc1.

Подключится к хосту wst3 через SSH.
Запустить команду ping поочередно до IP адресов хостов wst4, wst5, srv1 и orc1.

ICMP ping проходит успешно.

Повторить для хостов wst4 и wst5.



5.1.9. Проверить подключение к WWW серверу на srv1. Для этого открыть адрес 10.1.1.11 в браузере на рабочей станции wst3. Web-страница успешно отображается на wst3.	

6. Обновление компонентов системы управления Kaspersky SD-WAN.

6.1.1. Загрузить архивы с новыми версиями в папку с образами контейнеров, использованную при установке. По умолчанию папка находится внутри инсталлятора

При установке согласно данному руководству, то папка будет находится на хосте orc1 по пути: */home/sdwan/knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU/images/.*

Если файлы с плейбуками Ansible удалены, тогда необходимо загрузить архив *knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU.tar.gz* с плейбуками для установки компонентов системы управления Kaspersky SD-WAN в домашний каталог пользователя sdwan (изменить на другой в случае необходимости) на хост orc1, распаковать его *sdwan@orc1:~$ tar -xzvf knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU.tar.gz,* настроить параметры установки согласно пункту 3.2.9 и затем добавить новые образы в папку */home/sdwan/knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU/images/*

6.1.2. Обновить параметры плейбука для установки Kaspersky SD-WAN.

Открыть для редактирования конфигурационный файл.

Если установка проходила согласно данному руководству, то файл будет находится по пути */home/sdwan/aio.yml*.

sdwan@orc1:~$ vi /home/sdwan/aio.yml

Изменить значения файла и названия образов для контейнеров на обновленные

Пример обновления контроллера SD-WAN с версии *knaas-ctl:2.23.07.release.36.amd64_en-US_ru-RU на knaas-ctl:2.23.07.release.39.amd64_en-US_ru-RU*
Заменить значения переменных *tag* в файле *aio.yml* для контейнера контроллера*(ctl)*:
Исходные значения:

```
knaas-ctl:
  path: hub.brain4net.com/
  name: knaas-ctl
  tag: 2.23.07.release.36.amd64_en-US_ru-RU
```

Изменить на значения для новой версии:

```
knaas-ctl:
  path: hub.brain4net.com/
  name: knaas-ctl
  tag: 2.23.07.release.39.amd64_en-US_ru-RU
```

6.1.3. Запуск процесса обновления Kaspersky SD-WAN.

Запустить процесс установки системы управления Kaspersky SD-WAN, в ходе которого будут обновлены контейнеры системы управления Kaspersky SD-WAN. В случае, если версия контейнера будет совпадать с версией, настроенной в пункте 6.1.2 контейнер изменен не будет.

Должен быть сохранен файл с паролем от vault, созданный в ходе установки в п. 3.2.10!

Задать параметр согласия с EULA:

sdwan@orc1:~$ export KNAAS_EULA_AGREED="true"

Для запуска обновления компонентов Kaspersky SD-WAN необходимо перейти в каталог с плейбуками и выполнить команду:

sdwan@orc1:~$ cd /home/sdwan/knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU/
sdwan@orc1:~$ ansible-playbook -i inventory/generic -e "@/home/sdwan/aio.yml" -e "ansible_become_password= пароль sudo пользователя*" " --vault-password-file \$HOME/passwords/vault_password.txt knaas/knaas-install.yml*

После запуска дождаться окончания работы плейбука обновления компонентов Kaspersky SD-WAN.

6.1.4. Очистить историю команд.

sdwan@orc1:~$ history -c && history -w

Приложение A. Checklist.

Для успешного выполнения все тесты должны выполняться последовательно.

N	Название теста	Пункт настройки	Ожидаемый результат	Результат проверки (пройден/не пройден)
1	**Базовая настройка оркестратора.**			
1.1	Авторизация в web-интерфейсе оркестратора.	3.3.1	Авторизация проходит без ошибок, открывается раздел Dashboard.	
1.2	Смена пароля пользователя.	3.3.2	Пароль пользователя admin успешно изменен.	
1.3	Добавление домена.	4.1.1	Домен успешно добавлен.	
1.4	Добавление центра обработки данных.	4.1.2	Центр обработки данных успешно добавлен.	
1.5	Подключение к системе мониторинга Zabbix.	4.1.3	Подключение успешно настроено, успешно проходит тест соединения.	
1.6	Добавление Zabbix Proxy.	4.1.4	Zabbix Proxy успешно добавлен.	
1.7	Добавление пула IP адресов для сети управления.	4.1.5	Пул IP адресов успешно добавлен.	
1.8	Добавление дескриптора PNF контроллера в оркестратор.	4.1.7	Дескриптор контроллера успешно добавлен.	
1.9	Добавление PNF контроллера.	4.1.8-4.1.9	Контроллер успешно добавлен в оркестратор. В оркестраторе успешно проходит тест соединения с контроллером.	
1.10	Создание шаблона сервиса SD-WAN.	4.3	Шаблон сервиса SD-WAN создан и добавлен в оркестратор.	
1.11	Создание Tenant.	4.4.1	Tenant успешно создан.	
1.12	Развертывание сервиса SD-WAN.	4.4.2-4.4.6	Развертывание проведено успешно, в web-интерфейсе оркестратора есть записи о успешном создании сервиса.	

1.13	Импорт сертификата CA для CPE устройств.	4.6	CA сертификат успешно добавлен.	
2	**Работа с устройствами CPE и SD-WAN шлюзами.**			
2.1	Создание шаблонов SD-WAN шлюзов.	4.5	Шаблоны SD-WAN шлюзов успешно добавлены.	
2.2	Создание шаблонов устройств CPE.	4.11	Шаблоны устройств CPE успешно добавлены.	
2.3	Добавление SD-WAN шлюзов.	4.7, 4.8.2 - 4.8.3	SD-WAN шлюзы успешно добавлены в оркестратор.	
2.4	Настройка SD-WAN шлюзов при помощи ZTP URL.	4.8.4-4.8.11	SD-WAN шлюзы успешно настроены с помощью ZTP URL и находятся в статусе Registered.	
2.5	Настройка транспортного сервиса Management P2M.	4.9.1-4.9.9	Сервис Management P2M находится в статусе UP.	
2.6	Добавление устройств CPE.	4.10, 4.12.1-4.12.2	Устройства CPE успешно добавлены в оркестратор.	
2.7	Регистрация устройств CPE с использованием ZTP URL.	4.12.1-4.12.9	Устройства CPE успешно зарегистрированы с помощью ZTP URL и находятся в статусе Registered.	
2.8	Доступ к CLI консоли CPE из web-интерфейса оркестратора.	4.9.10-4.9.11	CLI консоль CPE успешно открывается из web-интерфейса оркестратора.	
2.9	Проверка работы подсистемы мониторинга.	4.9.12	Подсистема мониторинга работает, в web-интерфейсе оркестратора успешно отображается статистика для CPE.	

3	**Работа с транспортными сервисами.**			
3.1	Создание сервисных интерфейсов.	5.1.1	Сервисные интерфейсы для устройств CPE и SD-WAN шлюзов успешно созданы.	
3.2	Создание M2M транспортного сервиса.	5.1.2-5.1.5	M2M транспортный сервис успешно создан и находится в статусе UP.	
4	**Работа динамических протоколов маршрутизации на устройствах CPE и SD-WAN шлюзах.**			
4.1	Работа протокола BGP на устройствах CPE и SD-WAN шлюзах.	5.1.6-5.1.9	Установлены отношения BGP соседства между устройствами CPE и SD-WAN шлюзами. Устройства обмениваются маршрутной информацией. Обеспечена IP связность между хостами wst3, wst4, wst5 и srv1.	

kaspersky

Приложение Б. Настройки инфраструктурных компонентов демонстрационного стенда.

Маршрутизатор ISP.

```
!--------------
ISP
!--------------
!
vi /etc/sysconfig/network-scripts/ifcfg-ens224
!
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME= ens224
DEVICE=ens224
ONBOOT=yes
IPADDR=10.50.1.1
PREFIX=24
IPV6_PRIVACY=no
!
vi /etc/sysconfig/network-scripts/ifcfg-ens255
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens255
DEVICE=ens255
ONBOOT=yes
IPADDR=8.8.8.8
PREFIX=24
IPV6_PRIVACY=no
!
nano /etc/sysconfig/network
NOZEROCONF=yes
```

!
nano -w /etc/resolv.conf
nameserver 8.8.8.8
!
sysconfig restart network
!
Обновить пакеты до актуальных версий:
yum update -y
yum install -y epel-release
yum update -y
!
Проверить / установить NTP клиент:
yum install ntp ntpdate -y
timedatectl set-ntp true
ntpdate ntp.demolab.space
ntpdate -d ntp.demolab.space
timedatectl status
!
nano -w /etc/chrony.conf
chronyc tracking
chronyc sourcestats
!
nano /etc/sysctl.conf
net.ipv4.ip_forward=1
!
sysctl -w net.ipv4.ip_forward=1
!
Отключить SELINUX :
sed -i s/^SELINUX=.$/SELINUX=disabled/ /etc/selinux/config*
setenforce 0
!
Отключить Firewall:
systemctl disable firewalld
systemctl stop firewalld
systemctl disable NetworkManager
systemctl stop NetworkManager
systemctl enable network
systemctl start network
!
Установить iptables:
yum install iptables-services -y
systemctl enable iptables
systemctl start iptables
!
Очистить iptables :
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -F
iptables -t mangle -F
iptables -F

```
iptables -X
!
iptables -A INPUT -i ens192 -j ACCEPT
iptables -A INPUT -i ens224 -j ACCEPT
iptables -A INPUT -i ens256 -j ACCEPT
iptables -A INPUT -i ens225 -j ACCEPT
iptables -A INPUT -i ens257 -j ACCEPT
iptables -A INPUT -i ens162 -j ACCEPT
iptables -A INPUT -i ens194 -j ACCEPT
!
iptables -A FORWARD -i ens192 -j ACCEPT
iptables -A FORWARD -i ens224 -j ACCEPT
iptables -A FORWARD -i ens256 -j ACCEPT
iptables -A FORWARD -i ens225 -j ACCEPT
iptables -A FORWARD -i ens257 -j ACCEPT
iptables -A FORWARD -i ens162 -j ACCEPT
iptables -A FORWARD -i ens194 -j ACCEPT
!
```

Сохранить настройки iptables:

```
service iptables save
!
```

Проверить конфигурацию iptables:

```
iptables -L -n -v
!
yum install nano net-tools bind-utils tcpdump traceroute -y
!
DHCP
!
yum install dhcp
nano -w /etc/dhcp/dhcpd.conf
!
subnet 10.50.5.0 netmask 255.255.255.0 {
  range 10.50.5.3 10.50.5.253;
  option domain-name-servers 8.8.8.8;
  option domain-name "demolab.space";
  option routers 10.50.5.1;
  option broadcast-address 10.50.5.255;
  default-lease-time 600;
  max-lease-time 7200;
}

subnet 10.50.6.0 netmask 255.255.255.0 {
  range 10.50.6.3 10.50.6.253;
  option domain-name-servers 8.8.8.8;
  option domain-name "demolab.space";
  option routers 10.50.6.1;
  option broadcast-address 10.50.6.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

```
subnet 10.50.7.0 netmask 255.255.255.0 {
  range 10.50.7.3 10.50.7.253;
  option domain-name-servers 8.8.8.8;
  option domain-name "demolab.space";
  option routers 10.50.7.1;
  option broadcast-address 10.50.7.255;
  default-lease-time 600;
  max-lease-time 7200;
}

subnet 10.50.8.0 netmask 255.255.255.0 {
  range 10.50.8.3 10.50.8.253;
  option domain-name-servers 8.8.8.8;
  option domain-name "demolab.space";
  option routers 10.50.8.1;
  option broadcast-address 10.50.8.255;
  default-lease-time 600;
  max-lease-time 7200;
}
!
```

Проверить корректность конфигурационного файла можно командой:

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
!
```

Разрешаем автозапуск сервиса:

```
systemctl enable dhcpd
```

и запускаем его:

```
systemctl start dhcpd
!
```

DHCP должен работать только для определенных сетевых интерфейсов.

```
nano -w /etc/sysconfig/dhcpd
Добавить:
DHCPDARGS=ens225,ens257,ens162,ens194
!
```

Перезапускаем сервис:

```
systemctl restart dhcpd
!
cat /var/lib/dhcpd/dhcpd.leases
!
```

Маршрутизатор R13.

При изменении подсети mgmt в пункте 4.1.5 требуется поменять IP адреса шлюзов в маршрутах на актуальные.

```
------------
R13
------------
!
Очистить iptables:
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X
!
iptables -A FORWARD -j ACCEPT
iptables -A INPUT -j ACCEPT
!
service iptables save
iptables -L -n -v
!
# yum install -y https://github.com/FRRouting/frr/releases/download/frr-5.0.1/frr-5.0.1-
2018070501.el7.centos.x86_64.rpm
# nano -w /etc/frr/daemons
!
zebra=yes
bgpd=yes
1
# systemctl enable frr && systemctl start frr
# systemctl status frr
# vtysh
!
conf t
!
router bgp 65613
bgp router-id 10.1.3.13
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.1.3.11 remote-as 65500
neighbor 10.1.3.12 remote-as 65500
address-family ipv4 unicast
redistribute connected
exit-address-family
!
end
write
!
```

Маршрутизатор R14.

При изменении IP плана из пункта 2.3 использовать новый IP адрес хоста orc1 и публичный IP адрес (заменить 10.0.1.11 и 10.50.1.14).

R14

!
Очистить iptables:
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X
!
Создать правило в iptables, разрешающее передачу пакетов между внутренним (ens224) и внешним (ens192) интерфейсом:
iptables -A FORWARD -i ens224 -o ens192 -j ACCEPT
!
Разрешить передавать между интерфейсами пакеты, относящиеся к уже установленным соединениям.
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
!
Настройка SNAT
iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -o ens192 -j SNAT --to-source 10.50.1.14
iptables -t nat -A POSTROUTING -s 10.1.3.0/24 -o ens192 -j SNAT --to-source 10.50.1.14
iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -o ens192 -j SNAT --to-source 10.50.1.14
!
Настройка DNAT
iptables -A FORWARD -i ens192 -o ens224 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 443 -i ens192 -j DNAT --to-destination 10.0.1.11
iptables -t nat -A PREROUTING -p tcp --dport 6653 -i ens192 -j DNAT --to-destination 10.0.1.11
iptables -t nat -A PREROUTING -p tcp --dport 6654 -i ens192 -j DNAT --to-destination 10.0.1.11
iptables -t nat -A PREROUTING -p tcp --dport 6655 -i ens192 -j DNAT --to-destination 10.0.1.11
iptables -t nat -A PREROUTING -p tcp --dport 6656 -i ens192 -j DNAT --to-destination 10.0.1.11
!
service iptables save
iptables -L -n -v
iptables -t nat -L -n -v
!

Маршрутизатор R11.

R11

!
Очистить iptables:
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X
!
Создать правило в iptables, разрешающее передачу пакетов между внутренним (ens224) и внешним (ens192) интерфейсом:
iptables -A FORWARD -i ens224 -o ens192 -j ACCEPT
!
Разрешить передавать между интерфейсами пакеты, относящиеся к уже установленным соединениям.
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
!
Настройка SNAT:
iptables -t nat -A POSTROUTING -s 10.1.4.0/24 -o ens192 -j SNAT --to-source 10.50.1.11
!
Настройка DNAT:
iptables -A FORWARD -i ens192 -o ens224 -j ACCEPT
iptables -t nat -A PREROUTING -p udp --dport 4800 -i ens192 -j DNAT --to-destination 10.1.4.11
!
service iptables save
iptables -L -n -v
iptables -t nat -L -n -v
!

Маршрутизатор R12.

R12

!
Очистить iptables:
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X
!
Создать правило в iptables, разрешающее передачу пакетов между внутренним (ens224) и внешним (ens192) интерфейсом:
iptables -A FORWARD -i ens224 -o ens192 -j ACCEPT
!
Разрешить передавать между интерфейсами пакеты, относящиеся к уже установленным соединениям.
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
!
Настройка SNAT:
iptables -t nat -A POSTROUTING -s 10.1.5.0/24 -o ens192 -j SNAT --to-source 10.50.2.12
!
Настройка DNAT:
iptables -A FORWARD -i ens192 -o ens224 -j ACCEPT
iptables -t nat -A PREROUTING -p udp --dport 4800 -i ens192 -j DNAT --to-destination 10.1.5.12
!
service iptables save
iptables -L -n -v
iptables -t nat -L -n -v
!