



Kaspersky SD-WAN

Proof of Concept

Руководство по развертыванию демонстрационного стенда
Часть 1: установка, настройка и управление трафиком

06.05.2025

Версия документа:
2.4.0.0

RGB

0 168 142	29 29 27	51 194 255	51 92 255	112 51 255	255 51 92	239 237 238	239 255 252
-----------	----------	------------	-----------	------------	-----------	-------------	-------------

Изменения

Дата	Изменения
08.12.2022	Документ подготовлен по демо релизу Kaspersky SD-WAN 1.0.
10.03.2023	Документ обновлен по pre-релизу Kaspersky SD-WAN 2.0.
21.04.2023	Документ обновлен по релизу Kaspersky SD-WAN 2.0 от 12.04.2023, установка с использованием ОС CentOS.
16.05.2023	Документ обновлен по релизу SD-WAN 2.0, ОС для развёртывания решения изменена на Ubuntu, добавлена инструкция по установке с использованием Ansible Playbook. Добавлена секция для обновления компонентов SD-WAN
05.07.2023	Отредактирована схема решения (рисунок 2), внесены правки по оформлению п. 1, 1.1, таблицы 1-3, п. 3.3.4, 4.1.3, 4.5.16, 4.5.18, порядок настройки BGP – добавлен п 4.5.23, 4.6.1, 4.7.6, 4.8.5.
10.07.2023	Обновлены версии ПО. Обновлены скриншоты Configuration URL
27.07.2023	Добавлен чеклист для проверки PoC.
09.08.2023	Документ обновлен по релизу Kaspersky SD-WAN 2.0.2
15.08.2023	Документ обновлен по результатам обратной связи
31.10.2023	Обновлен процесс установки с использованием нового инсталлятора. Документ обновлен по релизу Kaspersky SD-WAN 2.1.1
16.04.2024	Документ обновлен по релизу Kaspersky SD-WAN. Добавлены секции настройки межсетевого экрана. Добавлена настройка DHCP на CPE. Добавлена настройка VRRP на vCPE-51/52
15.05.2024	Документ обновлен по релизу Kaspersky SD-WAN 2.2.1.
12.11.2024	Документ обновлен по релизу Kaspersky SD-WAN 2.3.1. Добавлены секции описания настройки NAT на vGW, настройки CFM, создание администратора тенанта. Обновлено описание требуемых ресурсов, выделяемые для CPE.
06.05.2025	Документ обновлен по релизу Kaspersky SD-WAN 2.4.0.

Содержание

1. Kaspersky SD-WAN	6
1.1. Архитектура решения Kaspersky SD-WAN	7
2. Описание схемы демонстрационного стенда Kaspersky SD-WAN	8
2.1. Схема демонстрационного стенда	9
2.2. План IP-адресации и требуемые ресурсы для компонентов SD-WAN	10
2.3. Сетевые порты, используемые компонентами решения	12
2.4. Схема внешних соединений контейнеров SD-WAN на хосте orc1	13
2.5. Версии программного обеспечения	14
2.6. Требования к аппаратным ресурсам решения Kaspersky SD-WAN	14
3. Установка и настройка компонентов системы управления Kaspersky SD-WAN	15
3.1. Установка операционной системы хоста orc1	15
3.2. Установка компонентов системы управления Kaspersky SD-WAN	27
3.3. Подключение к консоли управления Kaspersky SD-WAN	34
3.4. Подключение к консоли управления и настройка системы мониторинга Zabbix	36
4. Базовая настройка Kaspersky SD-WAN	39
4.1. Создание домена и центра обработки данных	39
4.2. Создание шаблона экземпляра SD-WAN	48
4.3. Создание шаблона сервиса SD-WAN	51
4.4. Создание Tenant и развертывание сервиса SD-WAN	56
4.5. Создание шаблона межсетевого экрана для SD-WAN шлюзов	65
4.6. Создание шаблонов SD-WAN шлюзов	69
4.7. Импорт сертификата CA для устройств CPE	90
4.8. Подготовка SD-WAN шлюзов	92
4.9. Регистрация SD-WAN шлюзов	95
4.10. Настройка транспортного сервиса P2M для управления CPE	103
4.11. Подготовка устройств CPE	107
4.12. Создание шаблона межсетевого экрана для устройств CPE	110
4.13. Создание шаблонов для устройств CPE	113
4.14. Регистрация устройств CPE	129
5. Управление трафиком	136
5.1. Настройка транспортного сервиса L2 M2M	136

6. Проверка работы протоколов BGP и VRRP на CPE.....	140
7. Обновление компонентов системы управления Kaspersky SD-WAN....	145
Приложение А. Настройки инфраструктурных компонентов демонстрационного стенда	146
Маршрутизатор ISP	146
Маршрутизатор R13.....	152
Маршрутизатор R14.....	154
Маршрутизатор R11.....	156
Маршрутизатор R12.....	157
Приложение Б. Программа и методика испытаний	159

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:

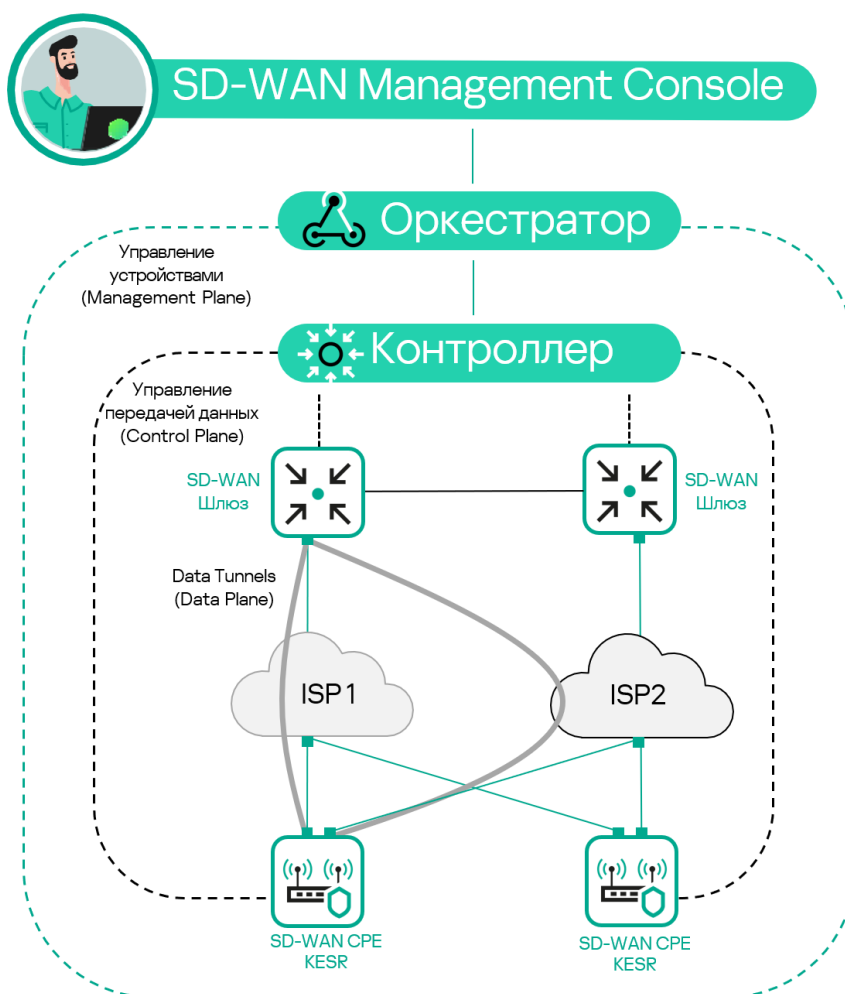
- Работа на основе проводных и беспроводных сетей различного типа.
- Использование несколько виртуальных каналов для обеспечения высокой доступности сети и балансировки трафика.
- Коррекция ошибок при передаче данных.
- Интеллектуальное управление трафиком.
- Легкая настройка устройств CPE с использованием Configuration URL.
- 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 устройств CPE.
- SD-WAN контроллер. Управляет наложенной сетью (англ. Overlay Network), обеспечивает построение топологии сети и создание транспортных сервисов внутри наложенных линков. 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 линками, выполняет мониторинг качества соединения и автоматическое переключение трафика на резервный линк в случае возникновения проблем на основном. Контроллер находится под управлением SD-WAN оркестратора.
- SD-WAN шлюзы. Объединяют устройства CPE в единую сеть. Наложённые линки 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 линков и образует SDN-фабрику в виде наложенной сети.

Архитектура решения Kaspersky SD-WAN представлена на рисунке 1.



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, контроллер 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 2
- 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 2 для Docker контейнеров SD-WAN оркестратора и SD-WAN контроллера.
- Хост ISP эмулирует подключение к сети Интернет / операторам связи ISP1 – ISP8.
- Для подключения устройств CPE, SD-WAN шлюзы должны быть доступны по определённым набору портов, перечисленных в таблице 2.
- Устройство vCPE-3 представляет собой пример подключения удаленной площадки с одним устройством CPE, 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.
- Устройства vCPE-51 и vCPE-52 представляют собой пример подключения удаленной площадки с двумя устройствами CPE с использованием протокола VRRP.

2.1. Схема демонстрационного стенда

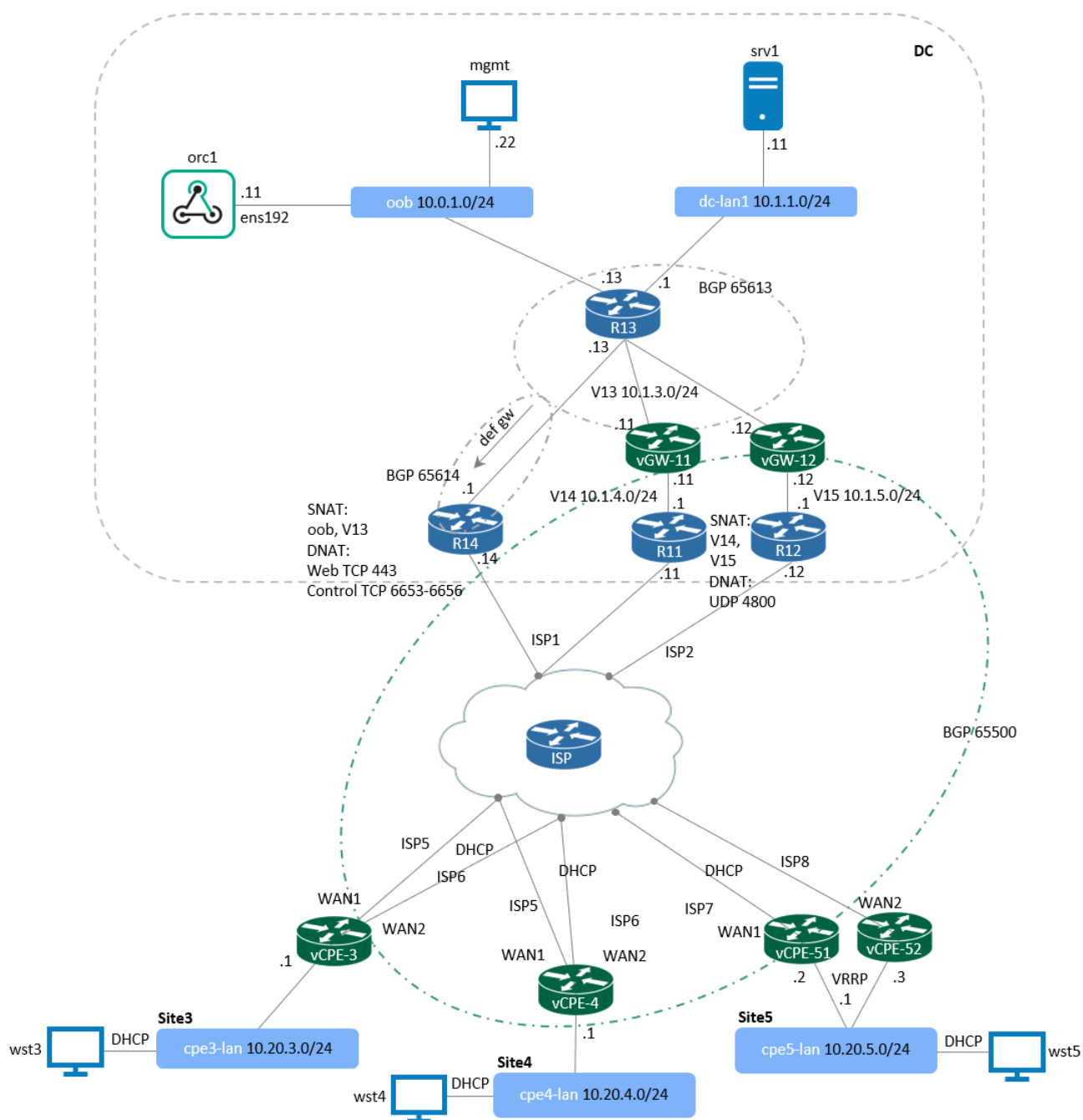


Рисунок 2 - Демонстрационный стенд Kaspersky SD-WAN

2.2. План IP-адресации и требуемые ресурсы для компонентов SD-WAN

Таблица ниже соответствует схеме из пункта 2.1. В случае использования других IP-адресов требуется изменить таблицу и все настройки SD-WAN в дальнейших шагах.

Таблица 1 – Параметры хостов, используемых в PoC

Имя	Операционная система	IP-адрес	Назначение	Требуемые ресурсы
orc1	Ubuntu 22.04.06 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-1, zabbix-www-1, zabbix-srv-1, zabbix-proxy-1, zabbix-db-1, syslog-1, mockpnf-1	24 x vCPU, 24 GB RAM
vGW-11	Образ vKESR-M2	wan 10.1.4.11 lan 10.1.3.11 overlay 172.16.1.11	SD-WAN шлюз	4 x vCPU, 8 GB RAM
vGW-12	Образ vKESR-M2	wan 10.1.5.12 lan 10.1.3.12 overlay 172.16.1.12	SD-WAN шлюз	4 x vCPU, 8 GB RAM
vCPE-3	Образ vKESR-M1	wan DHCP lan 10.20.3.1 overlay 172.16.1.3	CPE	2 x vCPU, 512 Mb RAM
vCPE-4	Образ vKESR-M1	wan DHCP lan 10.20.4.1 overlay 172.16.1.4	CPE	2 x vCPU, 512 Mb RAM
vCPE-51	Образ vKESR-M1	wan DHCP lan 10.20.5.2 / vIP 10.20.5.1 overlay 172.16.1.51	CPE	2 x vCPU, 512 Mb RAM
vCPE-52	Образ vKESR-M1	wan DHCP lan 10.20.5.3 / vIP 10.20.5.1 overlay 172.16.1.52	CPE	2 x vCPU, 512 Mb 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

Имя	Операционная система	IP-адрес	Назначение	Требуемые ресурсы
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
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	DHCP 10.20.3.0/24	Рабочая станция Site3	2 x vCPU, 4 GB RAM
wst4	CentOS 7	DHCP 10.20.4.0/24	Рабочая станция Site4	2 x vCPU, 4 GB RAM
wst5	CentOS 7	DHCP 10.20.5.0/24	Рабочая станция Site5	2 x vCPU, 4 GB RAM
mgmt	Windows Server 2022	10.0.1.22 10.1.1.22 10.1.3.22 10.50.1.22 10.20.3.22 10.20.4.22 10.20.5.22	Рабочая станция для управления демо стендом	6 x vCPU, 6 GB RAM

2.3. Сетевые порты, используемые компонентами решения

В таблице 2 представлены сетевые порты, используемые для взаимодействия SD-WAN шлюзов и устройств CPE с центральными компонентами решения, и доступа к веб-интерфейсу оркестратора для администрирования.

Таблица 2 - Сетевые порты, используемые для взаимодействия с решением SD-WAN.

Компонент	Порт	Назначение
SD-WAN оркестратор	TCP 443 / TLS	Доступ к веб-интерфейсу оркестратора и подключение CPE к оркестратору.
SD-WAN контроллер	TCP 6653-6656 / TLS	Подключение SD-WAN шлюзов и устройств CPE к контроллеру. CPE устройство подключается каждым WAN интерфейсом к отдельному порту контроллера: <ul style="list-style-type: none"> • sdwan0 - 6653 • sdwan1 – 6654 • sdwan2 - 6655 • sdwan3 - 6656
Zabbix	TCP 85 / TLS TCP10051 / TLS	Доступ к веб-интерфейсу Zabbix. Подключение агентов мониторинга Zabbix с CPE к системе мониторинга.
SD-WAN шлюзы	UDP 4800-4803	Дата трафик.

2.4. Схема внешних соединений контейнеров SD-WAN на хосте orc1

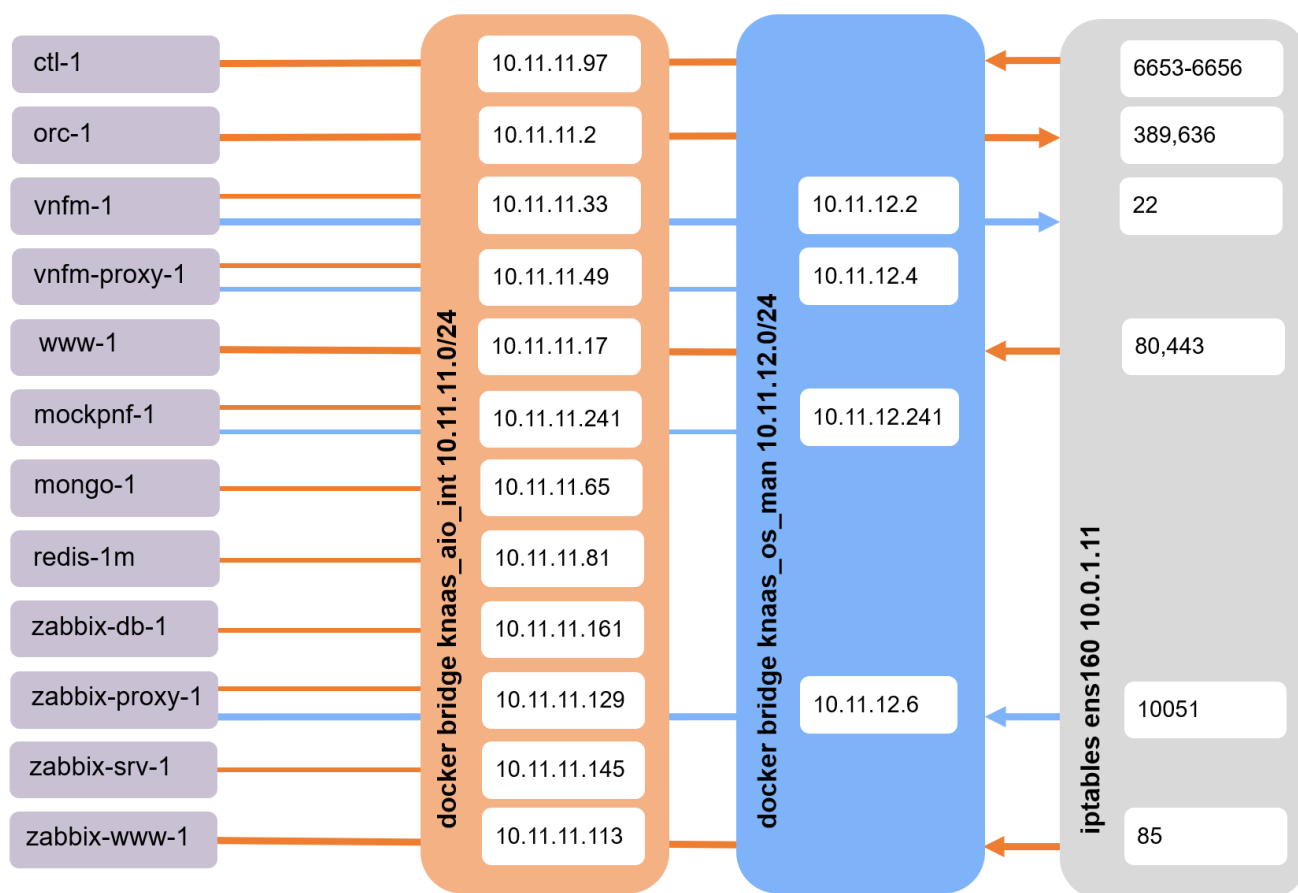


Рисунок 3 - Схема внешних соединений контейнеров SD-WAN.

Контейнеры SD-WAN разворачиваются на хосте `orc1`. В процессе установки создаются две сети `docker`: `knaas_aio_int` (10.11.11.0/24) и `knaas_os_man` (10.11.12.0/24).

Сеть `knaas_aio_int` является основной сетью и предназначена для взаимодействия между контейнерами, а также для связи с внешними хостами.

Сеть `knaas_os_man` предназначена для связи между центральными компонентами решения и CPE с целью управления и мониторинга.

Плейбуками установки решения SD-WAN будут настроены правила `iptables`: в цепочку `DOCKER_USER` добавляются правила, разрешающие следующие TCP соединения:

- Для контейнера `ctl-1` входящие по портам 6653-6656 (TLS подключения от CPE к контроллеру).
- Для контейнера `orc-1` исходящие по портам 389,636 (LDAP/LDAPS подключения к LDAP серверу).
- Для контейнера `vnfm-1` исходящие по порту 22 (SSH консоль до CPE из интерфейса оркестратора SD-WAN).
- Для контейнера `www-1` входящие по портам 80 и 443 (HTTPS/TLS подключение к web-интерфейсу оркестратора).
- Для контейнера `zabbix-proxy-1` входящие по порту 10051 (мониторинг CPE).
- Для контейнера `zabbix-www-1` входящие по порту 85 (HTTPS/TLS подключение к web-интерфейсу системы мониторинга Zabbix).

2.5. Версии программного обеспечения

Таблица 3 - Версии программного обеспечения Kaspersky SD-WAN, используемого в данном демонстрационном стенде

Компонент SD-WAN	Версия
www	knaas-www:2.25.03.release.57.cis.amd64_en-US_ru-RU
orc	knaas-orc:2.25.03.release.39.cis.amd64_en-US_ru-RU
mongo	mongo:5.0.7-r0amd64
ctl	knaas-ctl:2.25.03.release.17.cis.amd64_en-US_ru-RU
vnfm	knaas-vnfm:2.25.03.release.10.cis.amd64_en-US_ru-RU
vnfm-proxy	knaas-vnfm-proxy:2.25.03.release.6.cis.amd64_en-US_ru-RU
redis	redis:6.2.7-r0.amd64
zabbix-www	zabbix-web-nginx-mysql:6.0.32-r0.amd64
zabbix-proxy	zabbix-proxy:6.0.32-r0.amd64
zabbix-srv	zabbix-server:6.0.32-r0.amd64
zabbix-db	mariadb-ha:11.1.6.amd64
syslog	syslog-ng:3.30.1-r1.amd64
vCPE	knaas-cpe_2.25.03.release.28
mockpnf	mockpnf: 2.23.09.amd64
Хост orc1	Ubuntu 22.04.05 LTS Server
installer	knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU

2.6. Требования к аппаратным ресурсам решения Kaspersky SD-WAN

Таблица 4 - Требования к аппаратным ресурсам для управления до 50 устройств CPE

Хост	CPU	RAM, GB	Disk, GB, SSD
orc1	16 cores / 16 vCPU (HT disabled) / 32 vCPU (HT enabled)	32	50 используется в PoC / 256 рекомендуется

Более подробную информацию об аппаратных требованиях можно получить в Kaspersky SD-WAN Online Help: <https://support.kaspersky.com/help/SD-WAN/2.4/ru-RU/239105.htm>

3. Установка и настройка компонентов системы управления 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 22.04.05 LTS Server. Если виртуальная машина уже готова, то перейти к пункту 3.2.

Для установки используется дистрибутив Linux Ubuntu 22.04.05 LTS Server:
<https://releases.ubuntu.com/jammy/ubuntu-22.04.5-live-server-amd64.iso>

3.1. Установка операционной системы хоста **orc1**

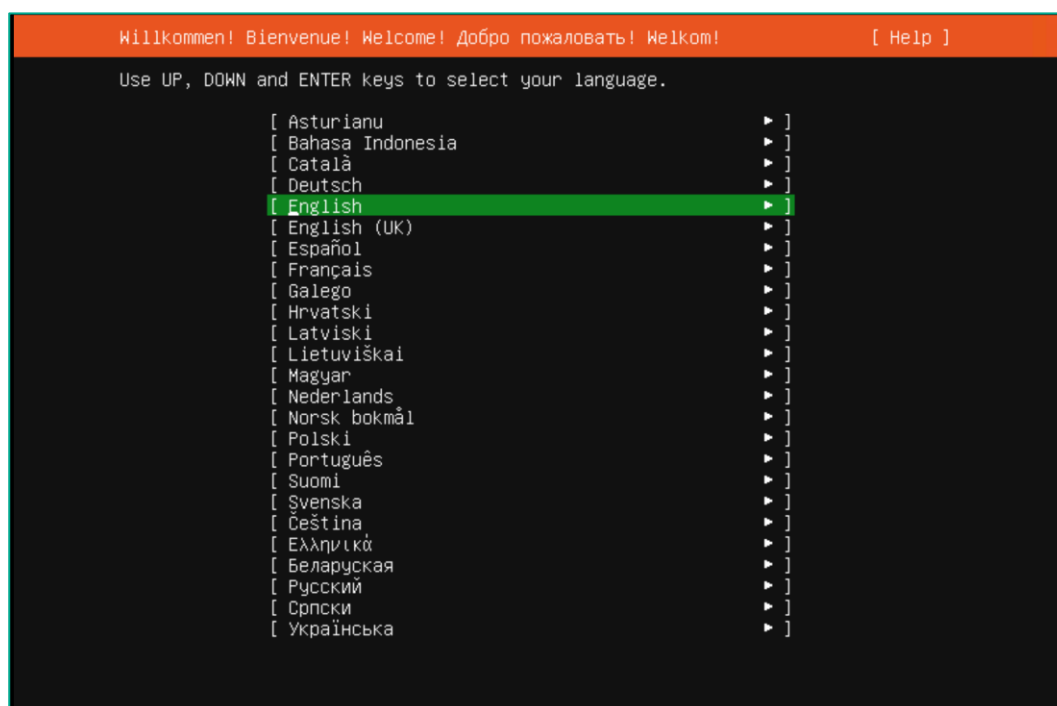
3.1.1. Создать виртуальную машину для хоста **orc1**.

Ресурсы CPU, RAM, Disk задать в соответствии с таблицей №4.

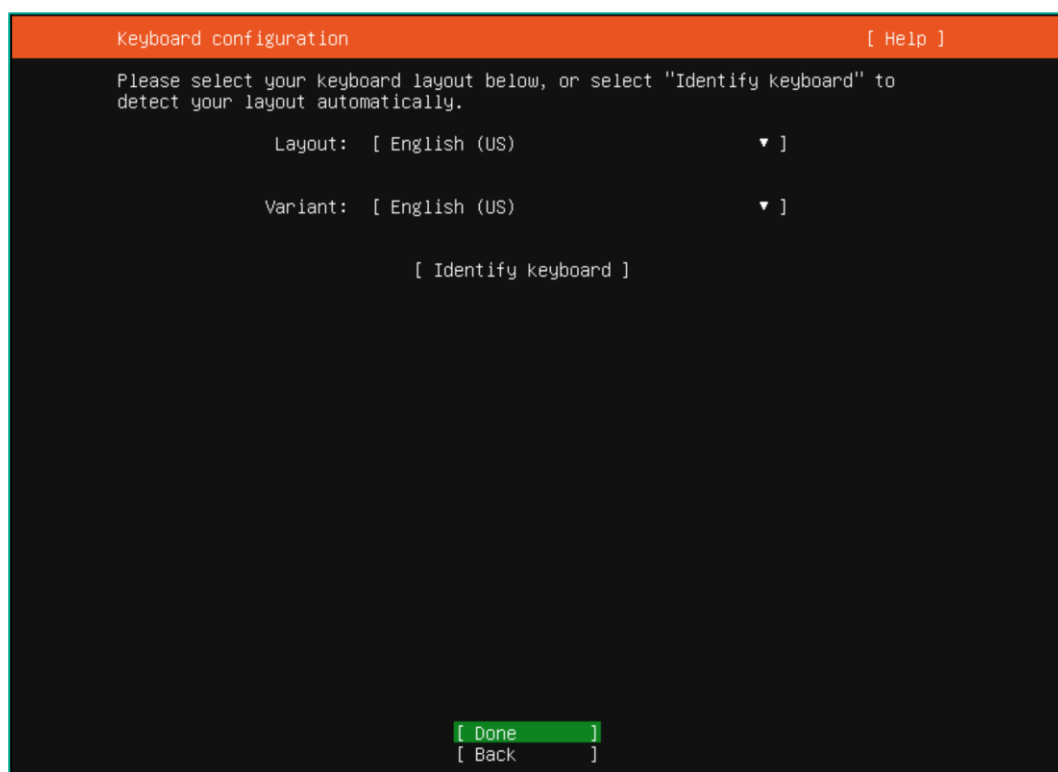
3.1.2. Запустить установку операционной системы на хост **orc1**.

Загрузка происходит с установочного образа Ubuntu 22.04.05 LTS Server.

Выбрать язык: **English** (оставить значение по умолчанию).

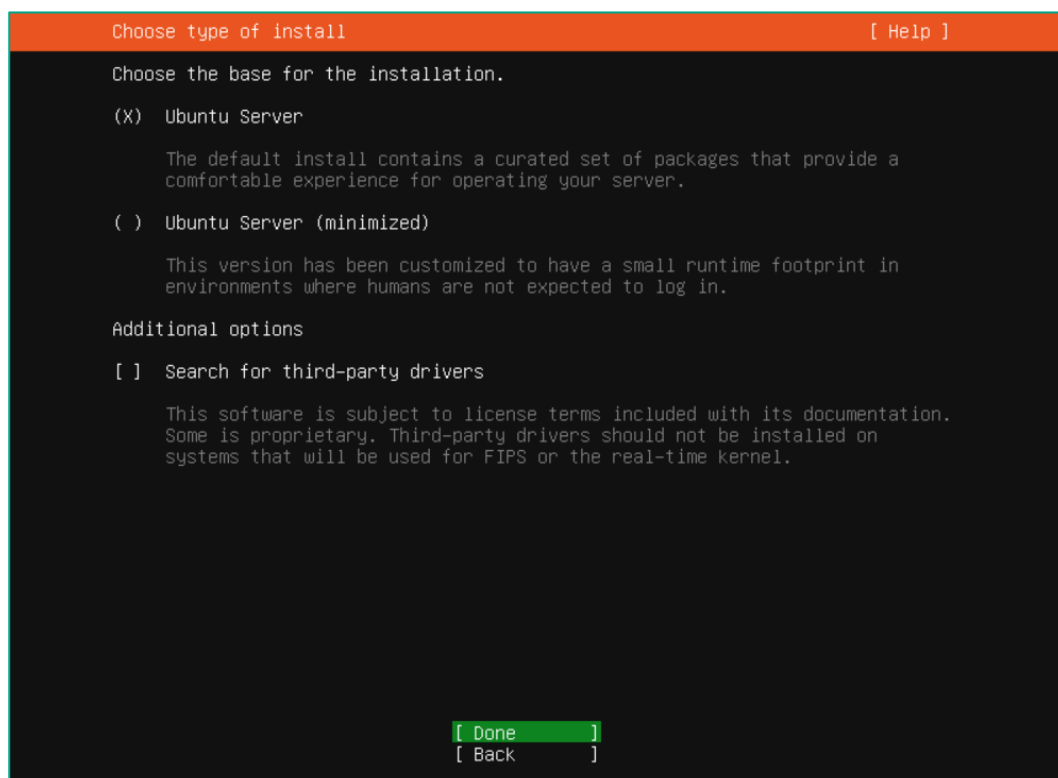


3.1.3. Выбрать раскладку клавиатуры: **US/US** (оставить значение по умолчанию).



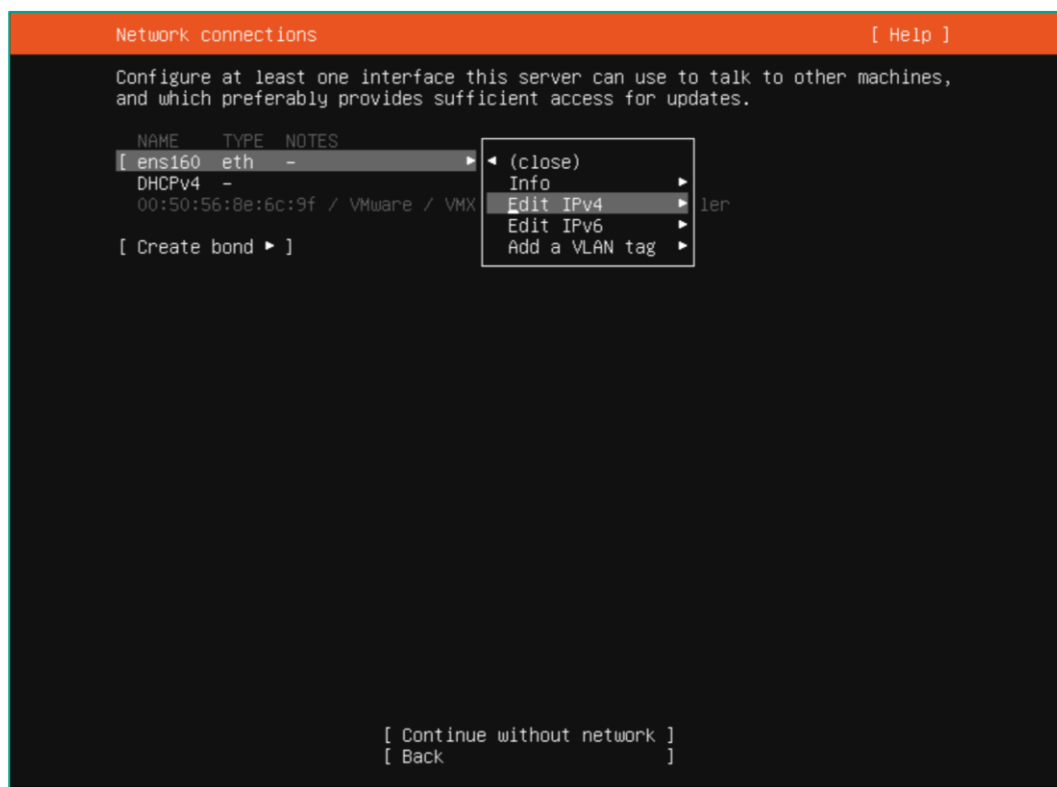
3.1.4. Выбрать версию для установки – **Ubuntu Server**.

Нажать **Done**.

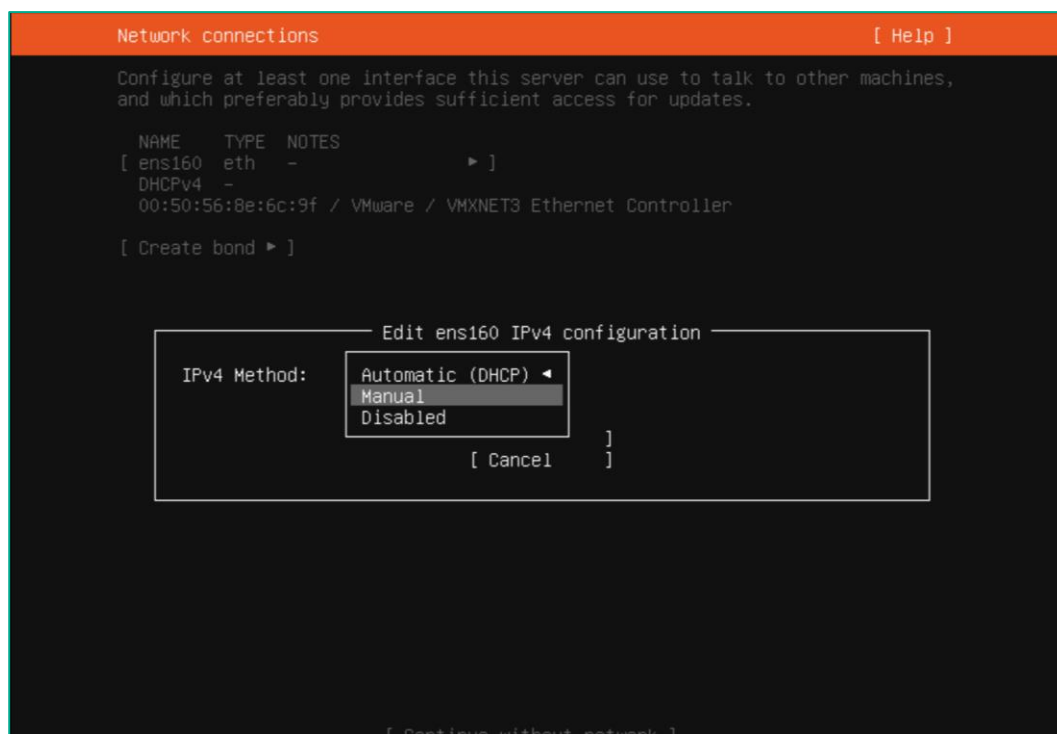


3.1.5. Настроить сетевой интерфейс хоста org1.

Выбрать редактирование настроек IPv4 сетевого интерфейса (в примере **ens160**).



Выбрать ручную настройку IPv4 (**Manual**).



Настроить параметры IPv4 сетевого интерфейса согласно таблице 1, нажать **Save**.

The screenshot shows a terminal window titled "Network connections" with a "[Help]" link in the top right. Below the title bar, there is a brief instruction: "Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient access for updates." Below this is a table with headers "NAME", "TYPE", and "NOTES". The main content is a configuration box titled "Edit ens160 IPv4 configuration". Inside this box, the "IPv4 Method" is set to "[Manual]". Below this are several input fields: "Subnet:" with the value "10.0.1.0/24", "Address:" with "10.0.1.11", "Gateway:" with "10.0.1.13", "Name servers:" with "8.8.8.8" and a subtext "IP addresses, comma separated", and "Search domains:" with an empty field and a subtext "Domains, comma separated". At the bottom of the configuration box are two buttons: "[Save]" (highlighted in green) and "[Cancel]". Below the configuration box, outside the box, are two more buttons: "[Continue without network]" and "[Back]".

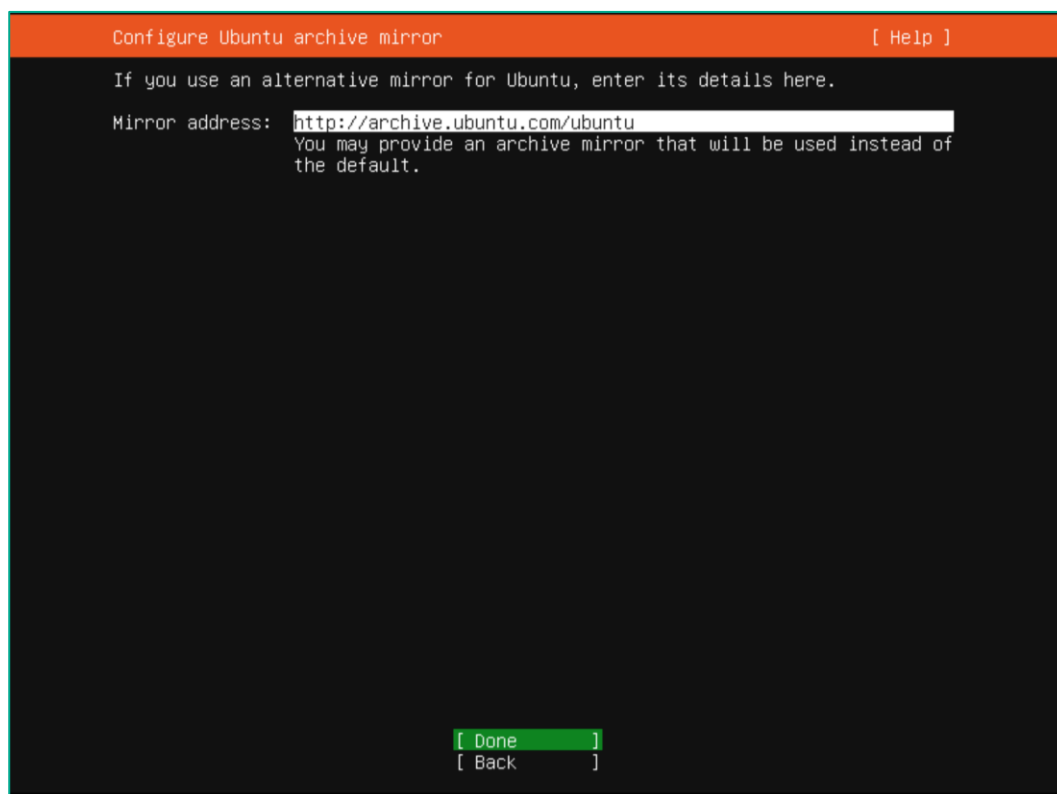
3.1.6. Пропустить (выполнить при необходимости) настройку прокси-сервера.

Выбрать **Done**.

The screenshot shows a terminal window titled "Configure proxy" with a "[Help]" link in the top right. Below the title bar, there is a brief instruction: "If this system requires a proxy to connect to the internet, enter its details here." Below this is a label "Proxy address:" followed by an empty input field. Below the input field, there is a subtext: "If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank." Below this is another subtext: "The proxy information should be given in the standard form of 'http://[[user] [:pass]@]host[:port]/'." At the bottom of the window are two buttons: "[Done]" (highlighted in green) and "[Back]".

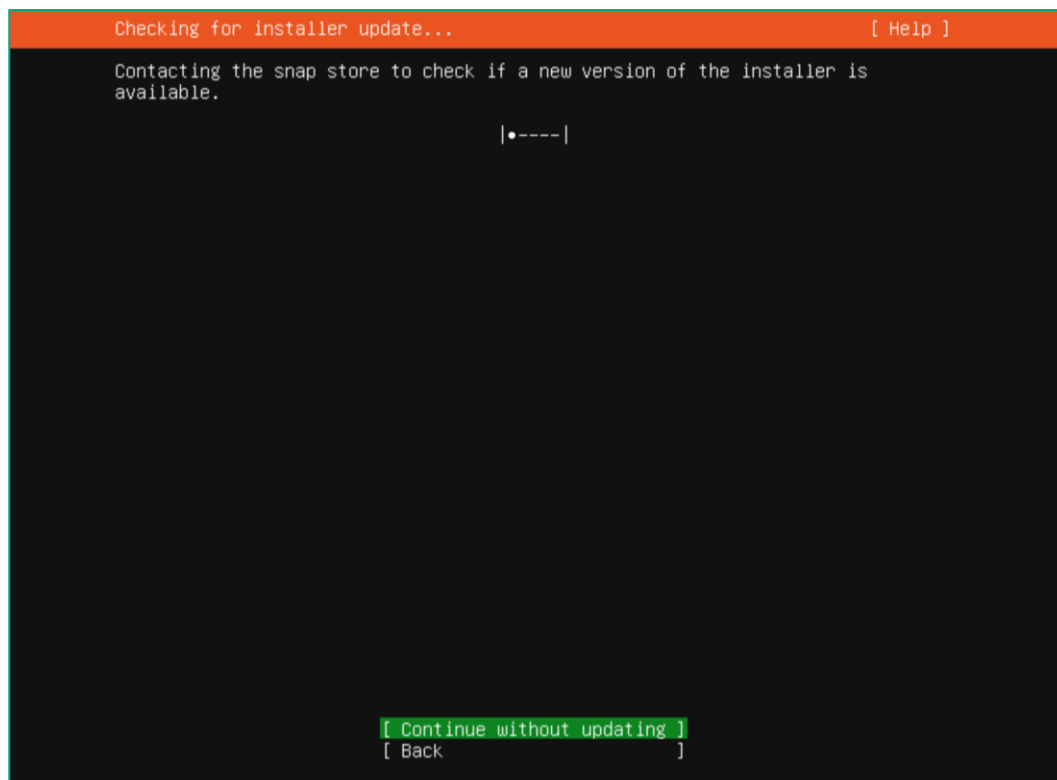
3.1.7. Настроить параметры зеркала архивов для Ubuntu.

Оставить значение по-умолчанию, нажать **Done**.



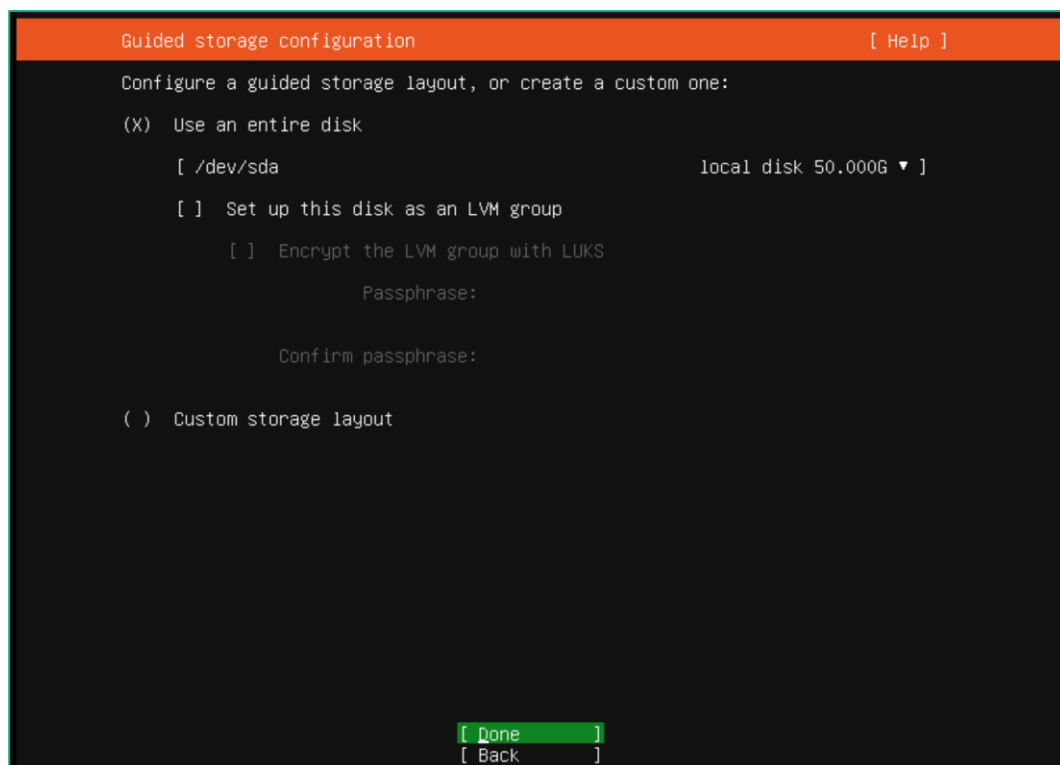
3.1.8. Пропустить обновление инсталлятора.

Выбрать **Continue without updating**.



3.1.9. Выбрать использование всего диска для установки, в данном примере без создания логических групп.

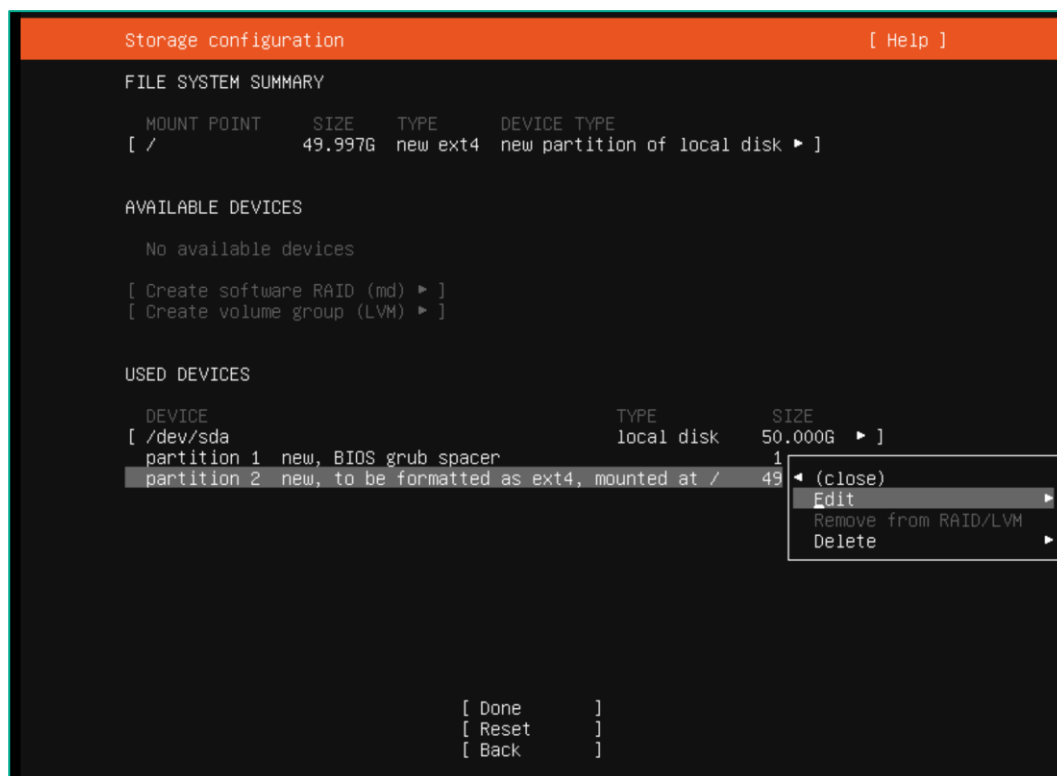
Нажать **Done**.



3.1.10. Настроить параметры дискового пространства.

Выбрать корневой раздел для редактирования.

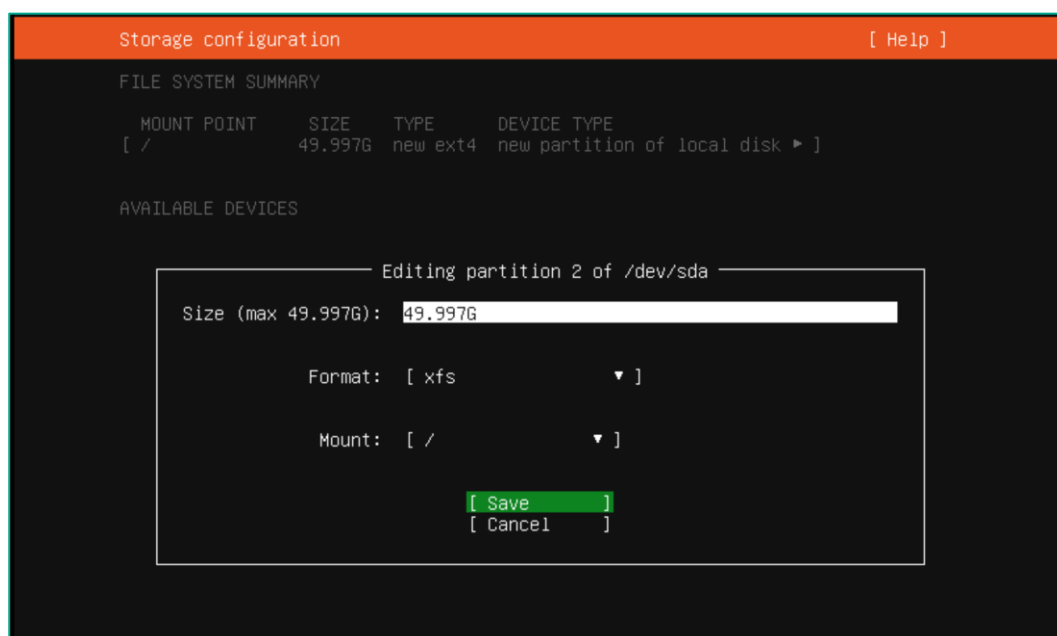
Выбрать **partition 2 – Edit**.



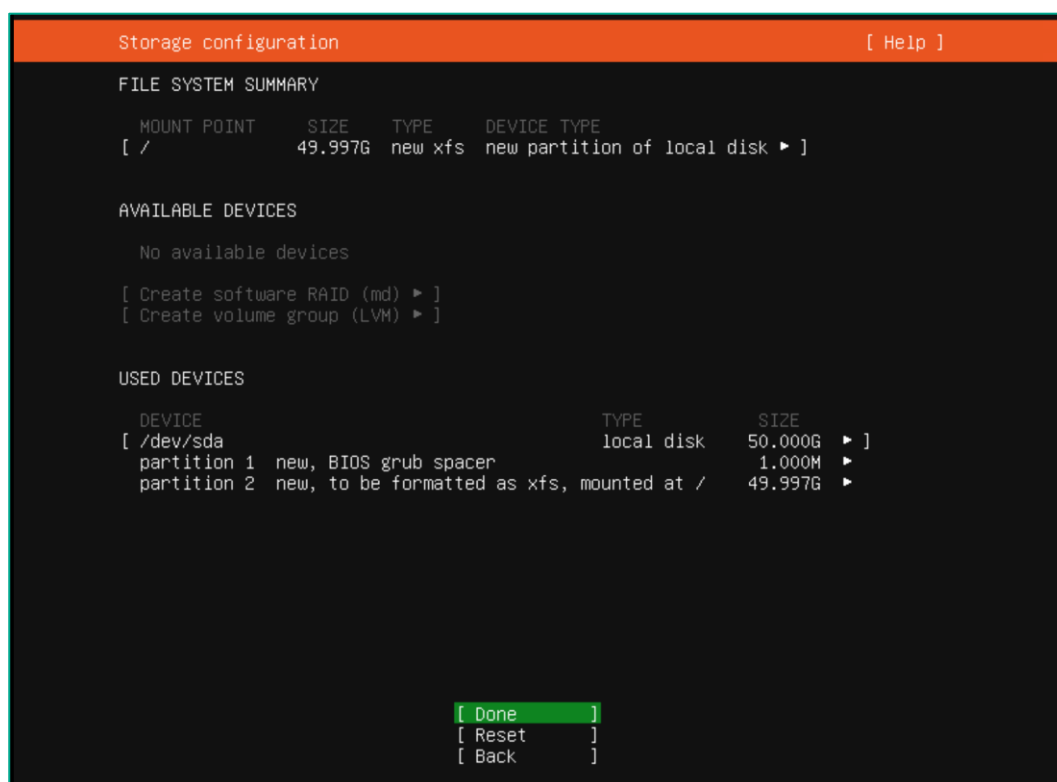
Указать формат файловой системы: **XFS**.

Нажать **Save**.

При разработке данного PoC документа используется диск 50GB, рекомендуемые значения для использования 50 x CPE – 256GB.

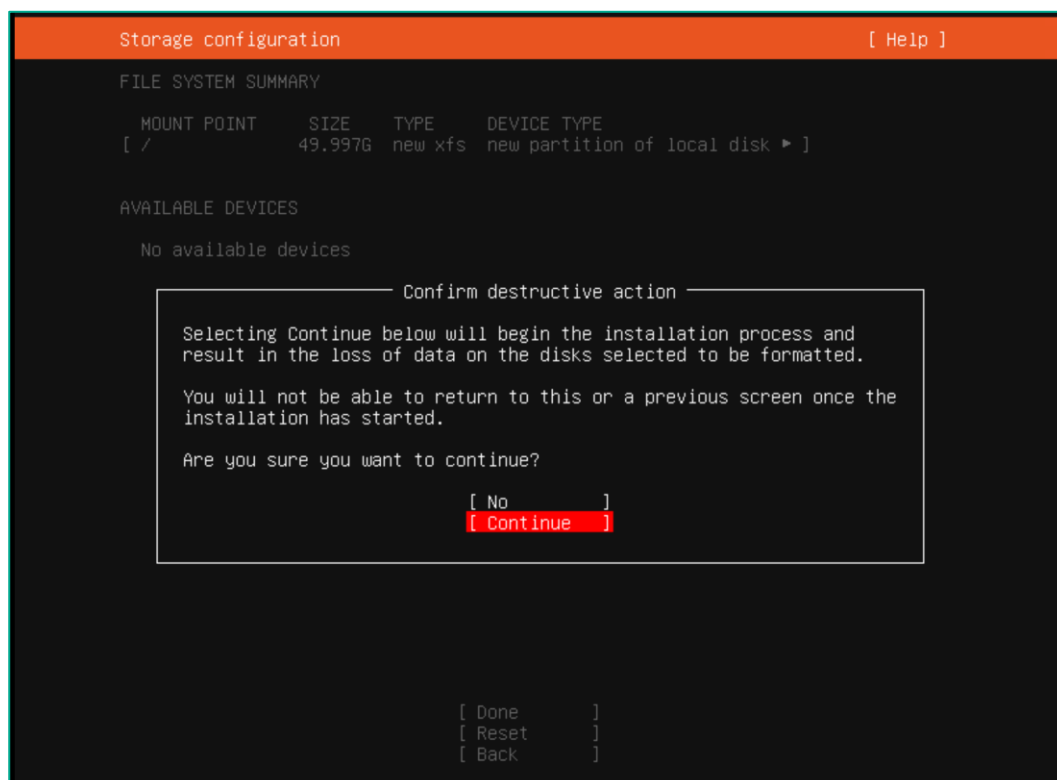


Сохранить изменения – нажать **Done**.



3.1.11. Подтвердить начало установки.

Выбрать **Continue**.



3.1.12. Создать пользователя с именем **sdwan**.

Данный пользователь используется при разворачивании системы управления Kaspersky SD-WAN.

Задать имя сервера (**orc1**).

Profile setup [Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Your name: Kaspersky SD-WAN

Your server's name: orc1
The name it uses when it talks to other computers.

Pick a username: sdwan

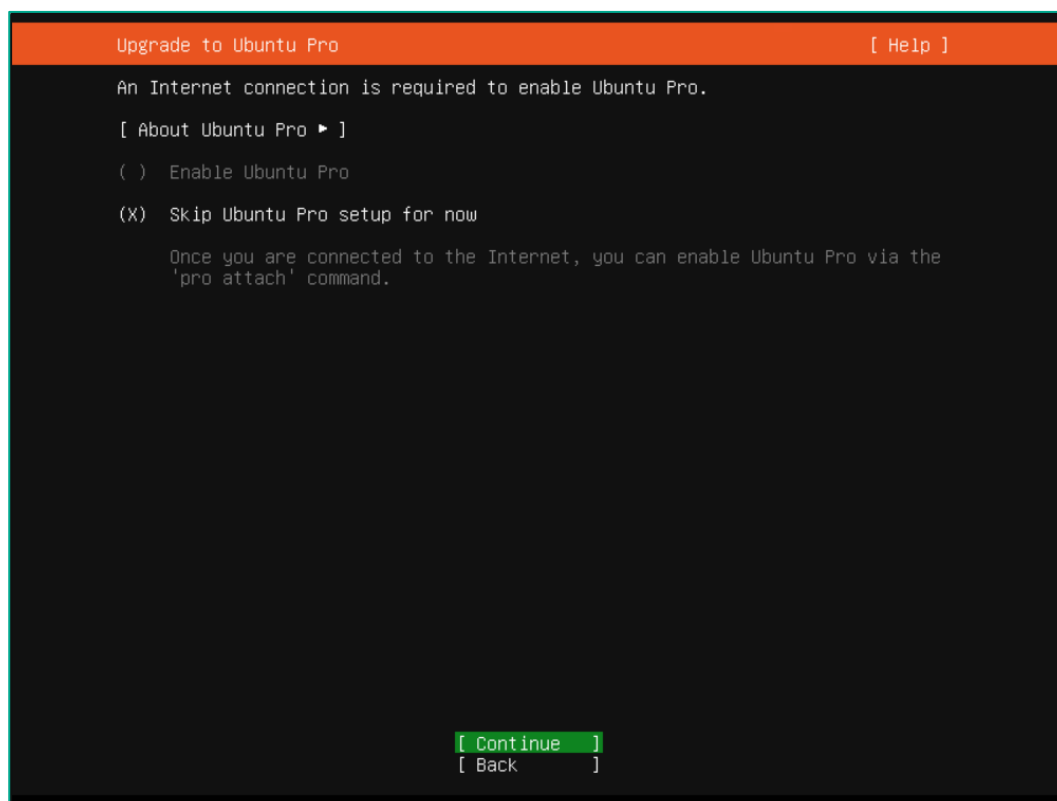
Choose a password: *****

Confirm your password: *****

[Done]

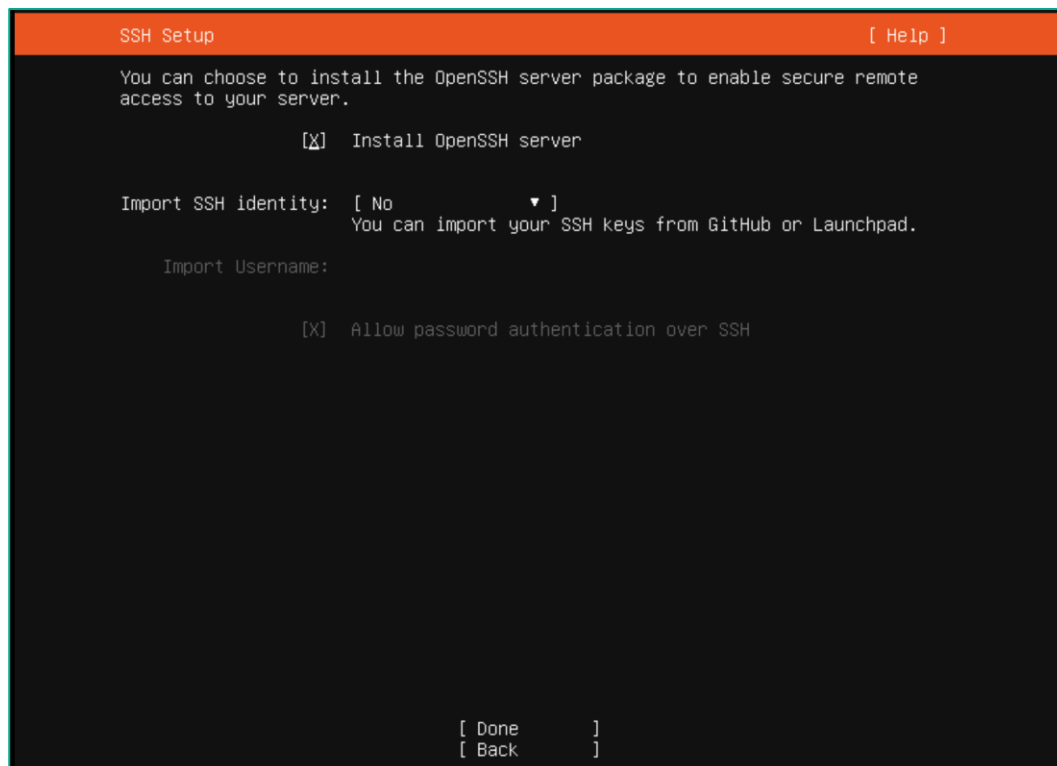
3.1.13. Пропустить включение Ubuntu Pro.

Выбрать **Continue**.



3.1.14. Добавить установку службы **OpenSSH**.

Отметить Install OpenSSH server, нажать **Done**.



3.1.15. Пропустить установку дополнительных пакетов/

Нажать **Done** (необходимые пакеты будут установлены позднее).

```

Featured Server Snaps [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE,
press ENTER to see more details of the package, publisher and versions
available.

[ ] microk8s      Kubernetes for workstations and appliances
[ ] nextcloud     Nextcloud Server - A safe home for all your data
[ ] wekan         The open-source kanban
[ ] kata-containers Build lightweight VMs that seamlessly plug into the c
[ ] docker        Docker container runtime
[ ] canonical-livepatch Canonical Livepatch Client
[ ] rocketchat-server Rocket.Chat server
[ ] mosquitto      Eclipse Mosquitto MQTT broker
[ ] etcd          Resilient key-value store by CoreOS
[ ] powershell    PowerShell for every system!
[ ] stress-ng      tool to load and stress a computer
[ ] sabnzbd        SABnzbd
[ ] wormhole       get things from one computer to another, safely
[ ] aws-cli        Universal Command Line Interface for Amazon Web Servi
[ ] google-cloud-sdk Google Cloud SDK
[ ] slcli          Python based SoftLayer API Tool.
[ ] doctl          The official DigitalOcean command line interface
[ ] conjure-up     Package runtime for conjure-up spells
[ ] postgresql10   PostgreSQL is a powerful, open source object-relatio
[ ] heroku         CLI client for Heroku
[ ] keepalived     High availability VRRP/BFD and load-balancing for Lin
[ ] prometheus     The Prometheus monitoring system and time series data
[ ] juju           Juju - a model-driven operator lifecycle manager for

[ Done ]
[ Back ]

```

3.1.16. Дождаться начала установки системы до появления подтверждающих сообщений.

```

Installing system [ Help ]

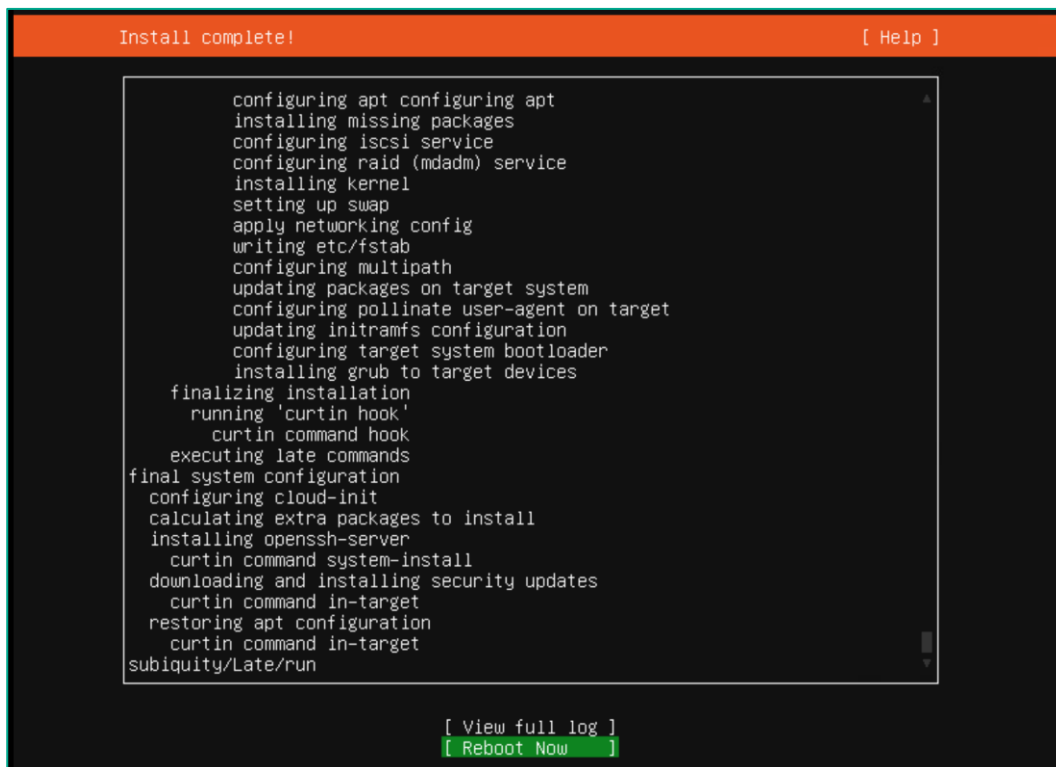
subiquity/Source/apply_autoinstall_config
subiquity/Late/apply_autoinstall_config
configuring apt
  curtin command in-target
installing system
  curtin command install
    preparing for installation
    configuring storage
      running 'curtin block-meta simple'
      curtin command block-meta
        removing previous storage devices
        configuring disk: disk-sda
        configuring partition: partition-3
        configuring partition: partition-4
        configuring format: format-0
        configuring mount: mount-0
    writing install sources to disk
      running 'curtin extract'
      curtin command extract
        acquiring and extracting image from cp:///tmp/tmp9m9tosor/mount
    configuring installed system
      running 'mount --bind /cdrom /target/cdrom'
      running 'curtin curthooks'
      curtin command curthooks
        configuring apt configuring apt
        installing missing packages
        configuring iscsi service
        configuring raid (mdadm) service
        installing kernel |

[ View full log ]

```

3.1.17. Перезагрузить хост orc1.

Выбрать **Reboot Now** для перезагрузки системы и завершения установки.



```
Install complete! [ Help ]

configuring apt configuring apt
installing missing packages
configuring iscsi service
configuring raid (mdadm) service
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
finalizing installation
  running 'curtin hook'
    curtin command hook
executing late commands
final system configuration
  configuring cloud-init
  calculating extra packages to install
  installing openssh-server
    curtin command system-install
  downloading and installing security updates
    curtin command in-target
  restoring apt configuration
    curtin command in-target
subiquity/Late/run

[ View full log ]
[ Reboot Now ]
```

3.2. Установка компонентов системы управления Kaspersky SD-WAN

3.2.1. Проверить работу NTP на хосте **orc1**.

Подключится к хосту **orc1**.

Проверить работу NTP:

```
timedatectl status
```

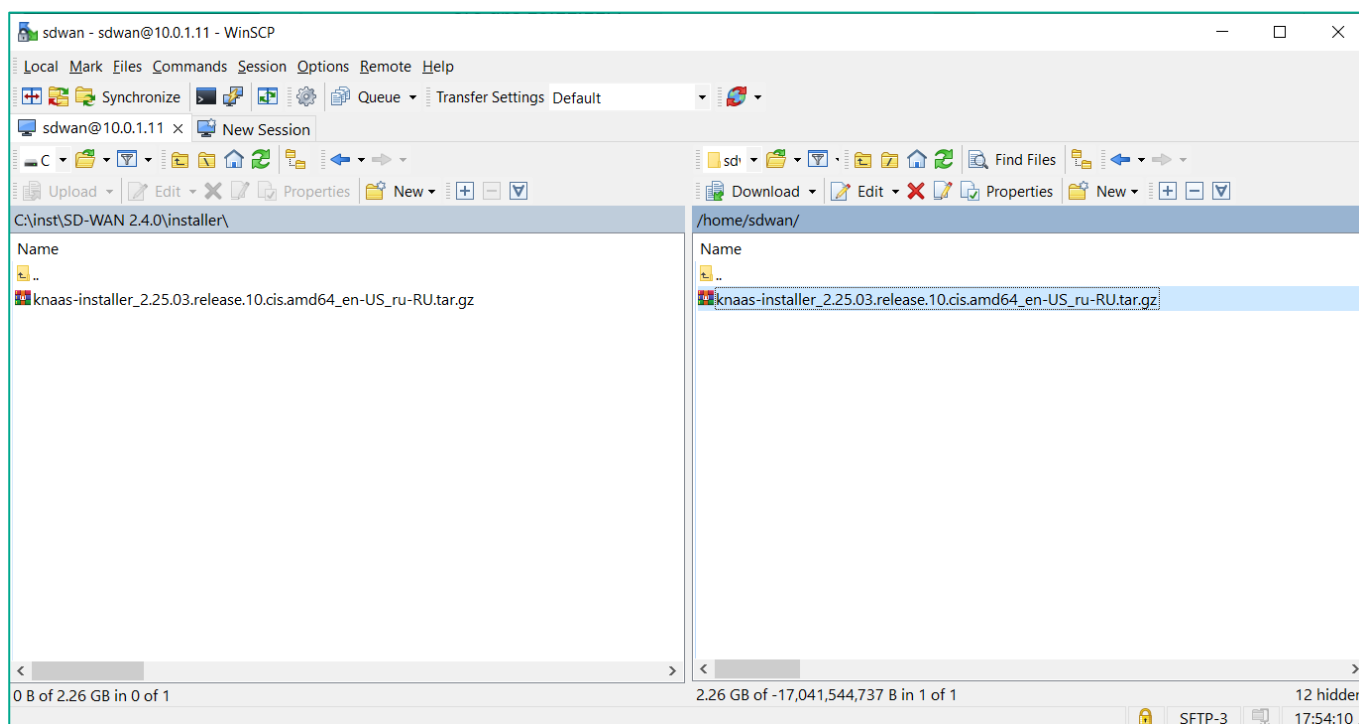
Время должно быть синхронизировано:

System clock synchronized: yes

3.2.2. Загрузить архив с инсталлятором на хост **orc1**.

Загрузить архив **knaas-installer.<release_name>.cis.amd64_en-US_ru-RU.tar.gz** с инсталлятором системы управления Kaspersky SD-WAN в домашний каталог пользователя **sdwan** на хост **orc1**.

Note: Для установки используется пользователь **sdwan**, созданный в пункте 3.1.12, в случае использования другого пользователя необходимо использовать соответствующий каталог.



3.2.3. Распаковать архив инсталлятора в каталог пользователя **sdwan**:

```
tar -xzf knaas-installer.<release_name>.cis.amd64_en-US_ru-RU.tar.gz
```

Перейти в папку с распакованным архивом:

```
cd knaas-installer.<release_name>.cis.amd64_en-US_ru-RU/
```

```
sdwan@orc1: ~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU
devices/baremetal/firmwares/KESR-M3/
devices/baremetal/firmwares/KESR-M3/knaas-cpe_2.25.03.release.91.efi.amd64-kesr-m3-k-4g-4s_en-US_ru-RU.tar.gz
devices/baremetal/firmwares/KESR-M4/
devices/baremetal/firmwares/KESR-M4/knaas-cpe_2.25.03.release.91.efi.amd64-kesr-m4-k-4g-2x_en-US_ru-RU.tar.gz
devices/baremetal/firmwares/KESR-M4/knaas-cpe_2.25.03.release.91.efi.amd64-kesr-m4-k-8g-4x_en-US_ru-RU.tar.gz
devices/baremetal/firmwares/KESR-M5/
devices/baremetal/firmwares/KESR-M5/knaas-cpe_2.25.03.release.91.efi.amd64-kesr-m5-k-4g-8x_en-US_ru-RU.tar.gz
devices/baremetal/firmwares/KESR-M5/knaas-cpe_2.25.03.release.91.efi.amd64-kesr-m5-k-8g-4x_en-US_ru-RU.tar.gz
devices/baremetal/firmwares/dpdk/
devices/baremetal/firmwares/dpdk/KESR-M5/
devices/baremetal/firmwares/dpdk/KESR-M5/knaas-cpe_2.25.03.release.91.efi.dpdk-kesr-m5-k-4g-8x_en-US_ru-RU.tar.gz
devices/
devices/firmwares/
devices/firmwares/vKESR-M1/
devices/firmwares/vKESR-M1/knaas-cpe_2.25.03.release.91.bios.amd64-vkesr-m1_en-US_ru-RU.tar.gz
devices/firmwares/vKESR-M2/
devices/firmwares/vKESR-M2/knaas-cpe_2.25.03.release.91.bios.amd64-vkesr-m2_en-US_ru-RU.tar.gz
devices/firmwares/vKESR-M3/
devices/firmwares/vKESR-M3/knaas-cpe_2.25.03.release.91.bios.amd64-vkesr-m3_en-US_ru-RU.tar.gz
devices/firmwares/vKESR-M4/
devices/firmwares/vKESR-M4/knaas-cpe_2.25.03.release.91.bios.amd64-vkesr-m4_en-US_ru-RU.tar.gz
devices/images/
devices/images/vKESR-M1/
devices/images/vKESR-M1/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m1.vKESR-M1-esxi.tar.gz
devices/images/vKESR-M1/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m1.vKESR-M1-kvm.tar.gz
devices/images/vKESR-M2/
devices/images/vKESR-M2/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m2.vKESR-M2-esxi.tar.gz
devices/images/vKESR-M2/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m2.vKESR-M2-kvm.tar.gz
devices/images/vKESR-M3/
devices/images/vKESR-M3/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m3.vKESR-M3-esxi.tar.gz
devices/images/vKESR-M3/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m3.vKESR-M3-kvm.tar.gz
devices/images/vKESR-M4/
devices/images/vKESR-M4/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m4.vKESR-M4-esxi.tar.gz
devices/images/vKESR-M4/knaas-cpe_2.25.03.release.91.combined.amd64-vkesr-m4.vKESR-M4-kvm.tar.gz
sdwan@orc1:~$ cd knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU/
sdwan@orc1:~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU$
```

3.2.4. Обновить списки и версии установленных пакетов.

Выполнить команду ниже:

```
sudo apt update && sudo apt upgrade --yes
```

3.2.5. Установить необходимые пакеты перед запуском плейбуков установки.

Установить PIP. Выполнить команду ниже:

```
sudo apt install python3-pip --yes
```

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

```
pip3 install -U --user -r requirements.txt
```

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

```
echo 'export PATH=$PATH:$HOME/.local/bin' >> ~/.bashrc
```

Выполнить **.bashrc**, для применения переменной **PATH**:

```
source ~/.bashrc
```

Проверить, что Ansible запускается корректно:

```
ansible --version
```


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

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

```
cp inventory/external/pnf/local.yml /home/sdwan/poc_aio.yml
```

Открыть для редактирования конфигурационный файл **poc_aio.yml**:

```
vi /home/sdwan/poc_aio.yml
```

Нажать **i** для перехода в режим редактирования, после внесения изменений нажать **esc** и ввести **:wq** для сохранения изменений и выхода из редактора.

Задать следующие основные параметры установки:

- Добавить в секцию **san_list: ip** внутренний и публичный IP-адреса хоста **orc1**: (**10.0.1.11** и **10.50.1.14**). Данные адреса будут добавлены в Subject Alternative Name (SAN) сертификата оркестратора SD-WAN. Оставить в секции адрес 10.11.12.1, он будет использоваться при подключении контроллера к оркестратору.
- Добавить в секцию **san_list: dns** доменное имя хоста **orc1** (sdwan.local как пример). Доменные имена будут добавлены в SAN сертификата оркестратора SD-WAN.
- Путь для сохранения сгенерированных паролей от баз данных и vault:
vault_passwords_dirname (/home/sdwan/passwords/).
- Путь для сохранения сертификатов: **ssl: path_local (/home/sdwan/ssl)**.

```
sdwan@orc1: ~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU
---
# Local All-In-One PNF Config Example
version: "2.25.03.0"

nodes:
  node_1:
    ip: 127.0.0.1
    knaas_aio_int:
      base: 10.11.11
      mode: bridge
    knaas_os_man:
      base: 10.11.12
      mode: bridge

external:
  vault_passwords_dirname: "/home/sdwan/passwords" # The directory where the keystore.yml and vault_password.txt f
  files are stored.
  ssl:
    san_list:
      ip:
        - "10.11.12.1"
        - "10.0.1.11"
        - "10.50.1.14"
      dns:
        - sdwan.local
    path_local: "/home/sdwan/ssl"

docker:
  local_path_to_images: "../images" # Directory where ansible will search docker images
  remote_path_to_images: "/tmp" # Directory where ansible will store files on remote VMs

syslog:
  docker_memory_limit: 1024 # in MegaBytes, depends on CPE count, <=250-1024,<=2K-4096M,<=5K-6144,<=10K-8192
  max_log_size: 32 # in GigaBytes, depends on customer requirements
  state: enabled
```

3.2.7. Подготовить хост к установке с использованием плейбука **bootstrap.yml**.

В процессе выполнения плейбука будут установлены необходимые пакеты.

Задать параметр согласия с EULA:

```
export KNAAS_EULA_AGREED="true"
```

Запустить плейбук подготовки хоста, при запуске плейбука будет запрошен пароль sudo:

```
ansible-playbook -i inventory/generic -e "@/home/sdwan/poc_aio.yml" -e "@inventory/external/images.yml"
-K knaas/utilities/node_prepare/bootstrap.yml
```

В процессе выполнения плейбука не должно быть невыполненных задач.

```
sdwan@orc1: ~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU

TASK [KNAAS | Restart Docker service] *****
skipping: [127.0.0.1]

TASK [KNAAS | PREPARE | Restore daemon.json from backup] *****
skipping: [127.0.0.1]

TASK [KNAAS | Restart Docker service if daemon.json restore] *****
skipping: [127.0.0.1]

PLAY [KNAAS | Docker prepare] *****

TASK [KNAAS | Docker prepare | Start and enable Docker] *****
ok: [127.0.0.1]

TASK [KNAAS | Docker prepare | Add current user to the docker group] *****
ok: [127.0.0.1]

TASK [KNAAS | Docker prepare | Reset ssh connection to apply user changes] *****
[WARNING]: Reset is not implemented for this connection

PLAY [KNAAS | Node prepare] *****

TASK [KNAAS | Node prepare | Update pip3] *****
changed: [127.0.0.1]

TASK [KNAAS | Node prepare | Install python packages] *****
changed: [127.0.0.1]

PLAY RECAP *****
127.0.0.1      : ok=11  changed=5  unreachable=0  failed=0  skipped=18  rescued=0  ignored=0
localhost     : ok=4   changed=1  unreachable=0  failed=0  skipped=0   rescued=0  ignored=0

sdwan@orc1:~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU$
```

3.2.8. Применить новые права для пользователя **sdwan**.

Пользователю **sdwan** требуется иметь доступ к группе docker для запуска контейнеров. В ходе выполнения плейбука **bootstrap**, пользователь был добавлен в группу, но для применения изменений требуется повторно вызвать оболочку пользователя:

```
su sdwan
```

3.2.9. Выполнить проверку перед установкой решения Kaspersky SD-WAN.

Для проверки требуется запустить плейбук **pre-flight**, при запуске плейбука будет запрошен пароль sudo. В результате проверки не должно быть невыполненных задач:

ansible-playbook -K knaas/utilities/pre-flight.yml

```
sdwan@orc1: ~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU
msg: Success

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Docker Permission Check] *****
ok: [Toolserver]

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Docker Permission Check Results] *****
ok: [Toolserver] =>
  msg: Docker is accessible by current user

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Java Installed Check] *****
changed: [Toolserver]

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Java Installed Check Results] *****
ok: [Toolserver] => changed=false
  msg: Success

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Java Installed Check Version] *****
ok: [Toolserver] => changed=false
  msg: Success

PLAY [KNAAS | Utilities | Pre Flight Toolserver Checks] *****

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Make Installed Check] *****
changed: [localhost]

TASK [KNAAS | Utilities | Pre Flight Toolserver Checks | Make Installed Check Results] *****
ok: [localhost] => changed=false
  msg: Success

PLAY RECAP *****
Toolserver      : ok=8    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
localhost       : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

sdwan@orc1:~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU$
```

3.2.10. Запустить плейбук установки компонентов системы управления Kaspersky SD-WAN.

Запустить плейбук **knaas-install** для 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.

Для запуска плейбука установки Kaspersky SD-WAN необходимо выполнить команду **ansible-playbook**, при запуске плейбука будет запрошен пароль sudo:

```
ansible-playbook -i inventory/generic -e "@/home/sdwan/poc_aio.yml" -e "@inventory/external/images.yml"
-K knaas/knaas-install.yml
```

После запуска дождаться окончания работы плейбука установки Kaspersky SD-WAN (Ansible playbook). В результате выполнения плейбука не должно быть невыполненных задач.

```
sdwan@orc1: ~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU$
```

PLAY RECAP							
127.0.0.1	: ok=17	changed=10	unreachable=0	failed=0	skipped=8	rescued=0	ignored=0
ctl1-1	: ok=33	changed=22	unreachable=0	failed=0	skipped=35	rescued=0	ignored=0
mongo-1	: ok=32	changed=15	unreachable=0	failed=0	skipped=33	rescued=0	ignored=2
orc-1	: ok=41	changed=27	unreachable=0	failed=0	skipped=32	rescued=0	ignored=0
redis-1m	: ok=18	changed=10	unreachable=0	failed=0	skipped=46	rescued=0	ignored=1
syslog-1	: ok=17	changed=11	unreachable=0	failed=0	skipped=38	rescued=0	ignored=0
vnfm-1	: ok=24	changed=18	unreachable=0	failed=0	skipped=34	rescued=0	ignored=0
vnfm-proxy-1	: ok=19	changed=12	unreachable=0	failed=0	skipped=36	rescued=0	ignored=0
www-1	: ok=20	changed=13	unreachable=0	failed=0	skipped=39	rescued=0	ignored=0
zabbix-db-1	: ok=24	changed=12	unreachable=0	failed=0	skipped=41	rescued=0	ignored=1
zabbix-proxy-1	: ok=24	changed=14	unreachable=0	failed=0	skipped=33	rescued=0	ignored=0
zabbix-srv-1	: ok=24	changed=15	unreachable=0	failed=0	skipped=32	rescued=0	ignored=0
zabbix-www-1	: ok=22	changed=13	unreachable=0	failed=0	skipped=33	rescued=0	ignored=0

В ходе установки будут сгенерированы пароли для баз данных и сертификатов. Они будут сохранены в **/home/sdwan/passwords/keystore.yml** (директория была задана в п. 3.2.6) и зашифрованы с помощью ansible-vault. Пароль vault, который используется для шифрования, также будет сгенерирован и сохранен в **/home/sdwan/passwords/vault_password.txt**

Note: Создайте копии файлов с паролями, SSL сертификатов, poc_aio.yml и файла с паролем vault для дальнейшего использования!

3.2.11. Очистить историю команд:

Выполнить:

```
history -c && history -w
```

3.2.12. При необходимости повторного запуска программы установки Kaspersky SD-WAN необходимо произвести удаление установленных компонентов.

Для удаления необходимо запустить плейбук **knaas-teardown.yml**:

```
ansible-playbook -i inventory/generic -e "@/home/sdwan/poc_aio.yml" -e "@inventory/external/images.yml"  
-K knaas/knaas-teardown.yml
```

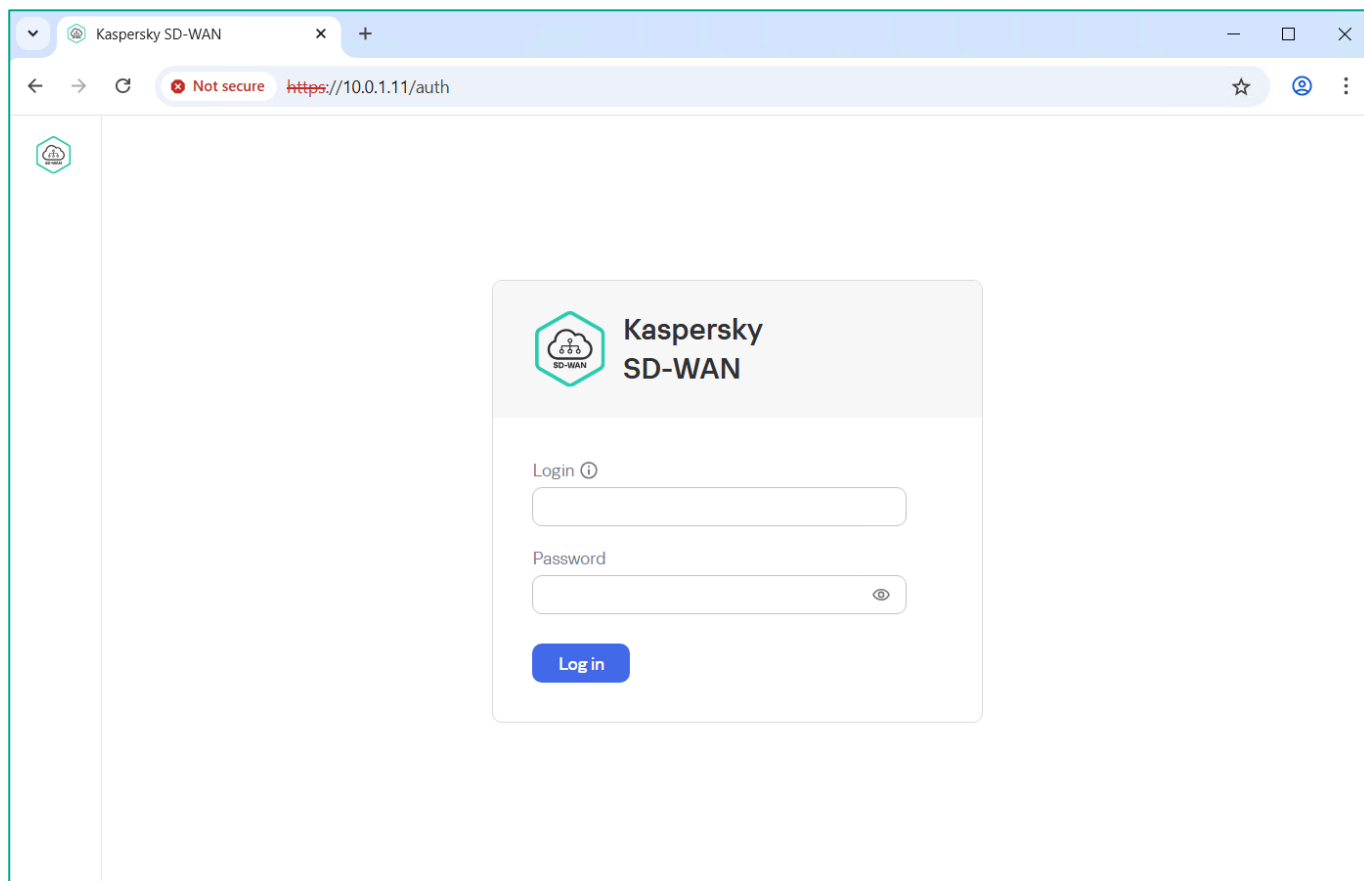
3.3. Подключение к консоли управления Kaspersky SD-WAN

3.3.1. Открыть портал администратора Kaspersky SD-WAN.

Данные для входа:

- Адрес веб-интерфейса оркестратора: <https://10.0.1.11>
- Логин и пароль по умолчанию: **admin** / **admin**.

Note: При изменении IP-адреса хоста orc1 из пункта 2.2 использовать новый IP-адрес.



3.3.2. Сменить пароль пользователя **admin**.

Перейти в меню **Users**. Выбрать пользователя **Administrator**.

Для смены пароля нажать **Change password**.

The screenshot shows the Kaspersky SD-WAN management interface. On the left, a sidebar contains navigation icons. The main panel has tabs for 'Users', 'Permissions', 'Groups', and 'LDAP connections'. The 'Users' tab is active, displaying a table with columns 'Name', 'Tenant', and 'Role'. Two users are listed: 'Administrator Administrator' (Role: Administrator) and 'User User' (Role: Tenant). The 'Administrator Administrator' user is selected. A modal window titled 'User Online' is open, showing the user's profile. The 'Change password' button is highlighted in the top bar of the modal. Below it, the user's details are displayed: Login (admin), Role (Administrator), Two-factor authentication (Disabled), Request confirmation is required (Off), First name (Administrator), Last name (Administrator), and Email (admin@example.com). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Ввести новый пароль и нажать **Save**.

This screenshot shows the same interface as the previous one, but with the 'Password' modal window open. The modal has a title bar 'Password' and a close button. It contains two input fields: 'New password' and 'Password confirmation', both with masked characters (dots) and toggle icons for visibility. At the bottom of the modal are 'Save' and 'Cancel' buttons. The background shows the 'User' profile for 'Administrator' with the 'Change password' button highlighted.

3.4. Подключение к консоли управления и настройка системы мониторинга Zabbix

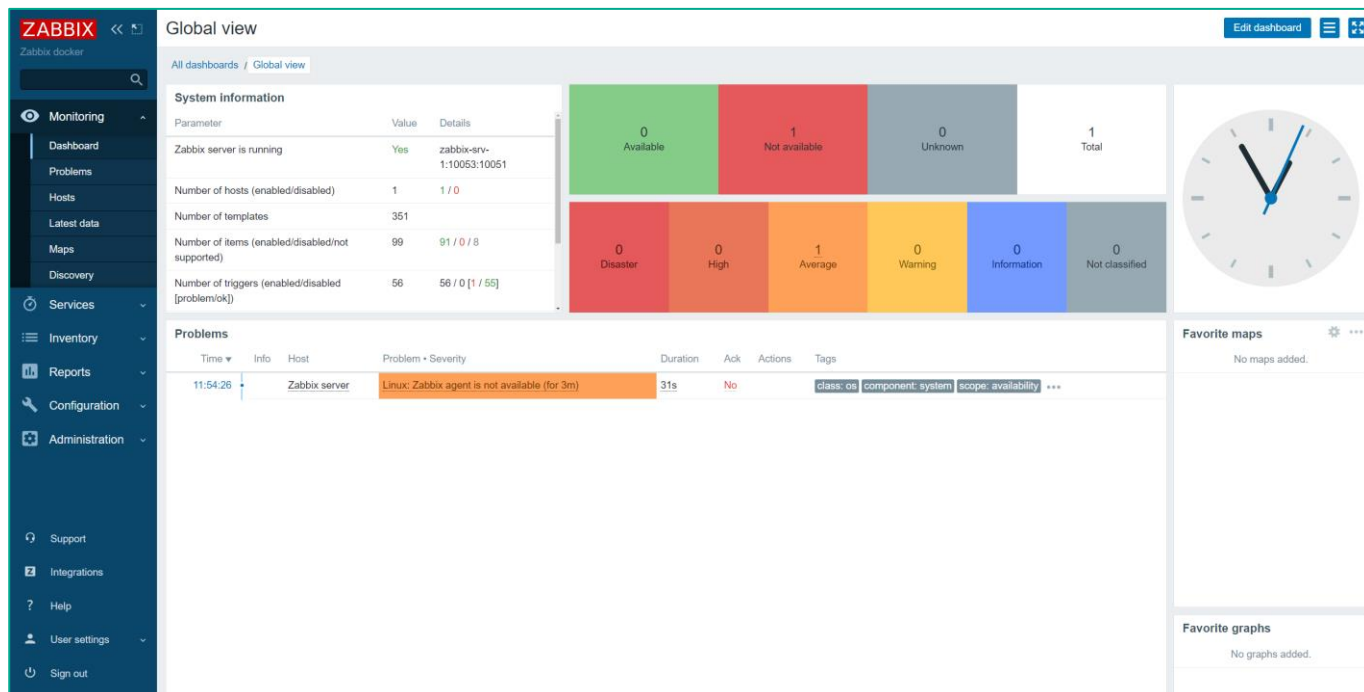
3.4.1. Открыть консоль управления Zabbix.

Для подключения к веб-консоли управления Zabbix необходимо перейти по ссылке:

<https://10.0.1.11:85>

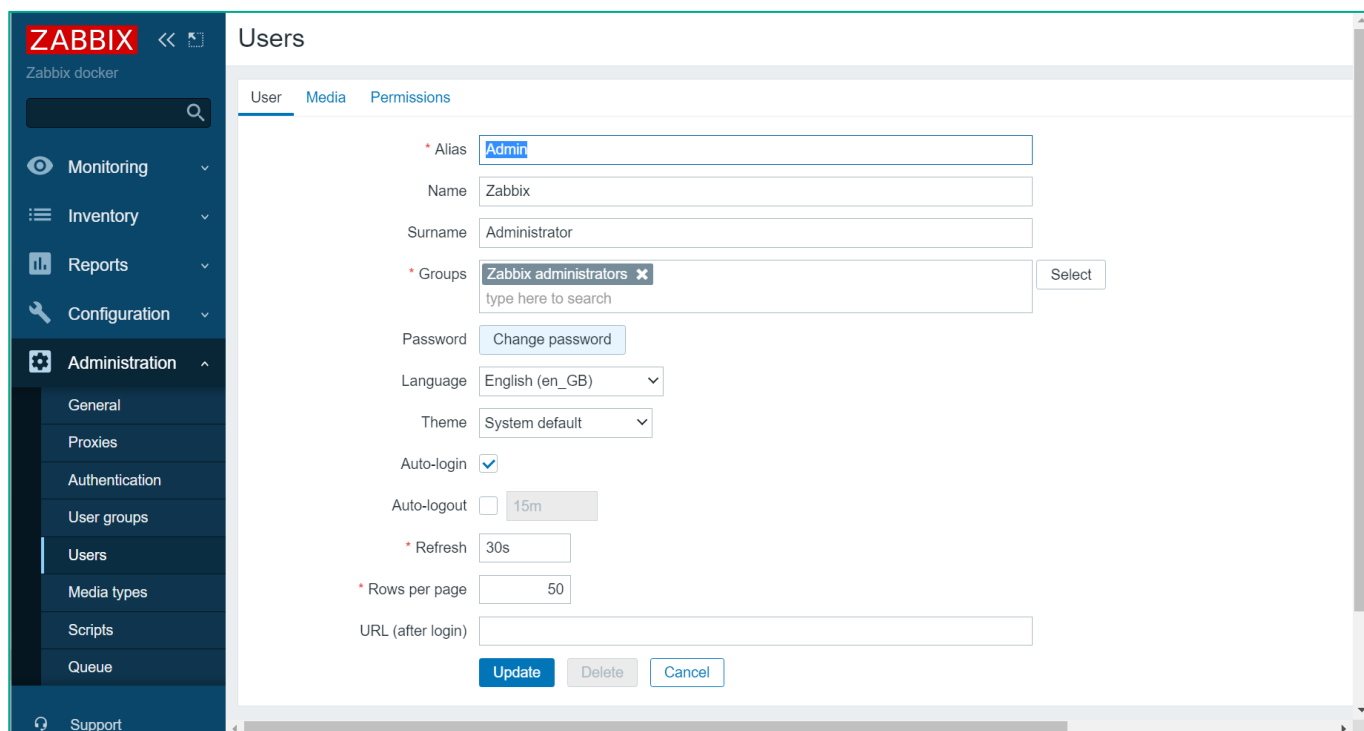
Данные для входа по умолчанию: **Admin / zabbix**.

Note: При изменении IP-адреса хоста orc1 из пункта 2.2 использовать новый IP-адрес.



3.4.2. Сменить пароль пользователя **Admin**.

Перейти в меню **Administration** → **Users** → **Admin** → **Change password**.



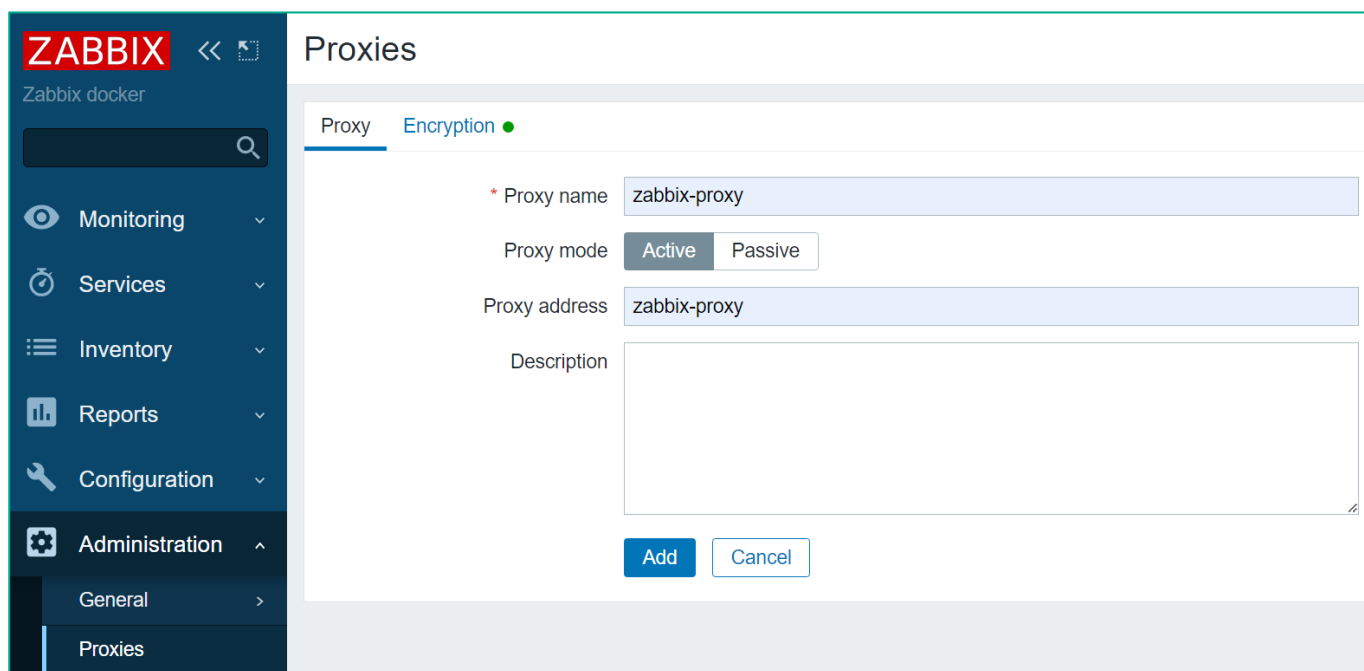
The screenshot shows the Zabbix web interface. On the left is a dark blue sidebar with the ZABBIX logo and a search bar. Below the search bar are menu items: Monitoring, Inventory, Reports, Configuration, Administration (expanded), General, Proxies, Authentication, User groups, Users (selected), Media types, Scripts, Queue, and Support. The main content area is titled 'Users' and has three tabs: User, Media, and Permissions. The 'User' tab is active. It displays configuration fields for the 'Admin' user. Fields include: Alias (Admin), Name (Zabbix), Surname (Administrator), Groups (Zabbix administrators), Password (Change password button), Language (English (en_GB)), Theme (System default), Auto-login (checked), Auto-logout (15m), Refresh (30s), Rows per page (50), and URL (after login). At the bottom are buttons for Update, Delete, and Cancel.

После ввода нового пароля нажать **Update** для применения настроек.

3.4.3. Добавить Zabbix Proxy.

Перейти в меню **Administration** → **Proxies**, нажать **Create Proxy**.

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



ZABBIX << Zabbix docker

Proxies

Proxy Encryption ●

* Proxy name zabbix-proxy

Proxy mode Active Passive

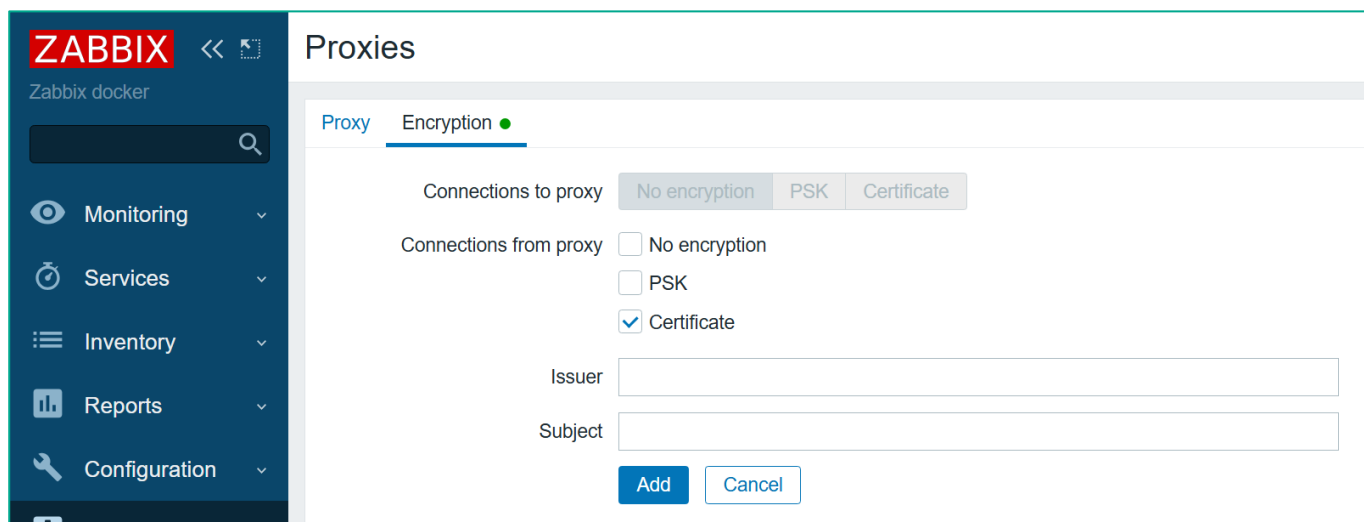
Proxy address zabbix-proxy

Description

Add Cancel

При подключении прокси к серверу Zabbix будет использоваться шифрование с использованием сертификатов, созданных в процессе установки системы.

На вкладке **Encryption** отметить **Certificate**, затем нажать **Add**.



ZABBIX << Zabbix docker

Proxies

Proxy Encryption ●

Connections to proxy No encryption PSK Certificate

Connections from proxy ☐ No encryption ☐ PSK ☒ Certificate

Issuer

Subject

Add Cancel

4. Базовая настройка Kaspersky SD-WAN

4.1. Создание домена и центра обработки данных

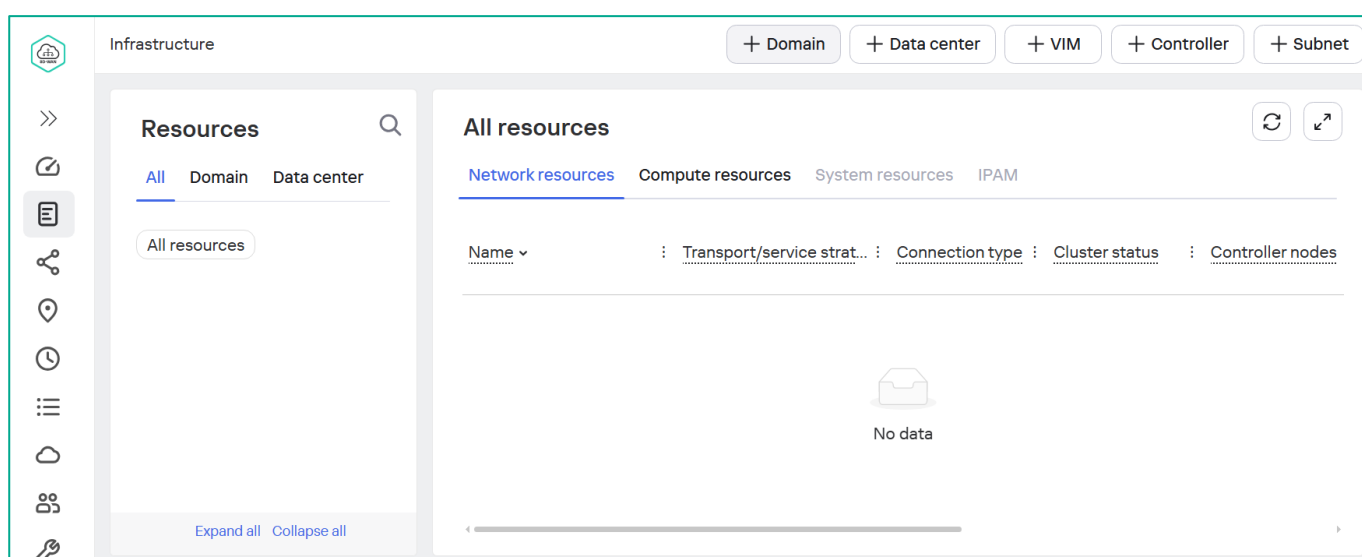
Оркестратор управляет сетевыми и вычислительными ресурсами, которые могут принадлежать разным доменам (Domain) и центрам обработки данных (Data Center).

Домен - логическая группа ресурсов под единым административным управлением.

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

4.1.1. Создать домен.

В разделе **Infrastructure** нажать кнопку **+ Domain**.



При создании домена необходимо ввести его имя и, опционально, комментарий.

Нажать **Create** для создания домена.

New domain

Name

demolab.space

Description

Create

Cancel

4.1.2. Создать Data Center.

В разделе **Infrastructure** использовать кнопку **+ Data Center**.

Задать:

- **Name:** Название data center.
- **Domain:** Выбрать домен, созданный в п.4.1.1.
- **VNF URL:** <https://vnfm-proxy:86>

Нажать **Test Connection** (тест соединения должен быть успешным), затем **Add**.

New data center [X]

Name
DC

Description

Domain
demolab.space [v]

VNFM URL
https://vnfm-proxy:86

Test connection

Successful

Location

Moscow Olimpia Park

Бизнес-центр "Олимпия Парк", 39А с2, Leningrad Avenue, Voykovsky District, Moscow, Central Federal District, 125212, Russia [X]

39 с253 39а 54 с23 39 с223 Баркас

Add **Cancel**

4.1.3. Настроить подключение к серверу мониторинга Zabbix.

Перейти в меню **System** и открыть вкладку **Monitoring**.

Задать параметры:

- **Type: Zabbix.**
- **URL:** https://zbx-www:8443/api_jsonrpc.php (URL для подключения к Zabbix API).
- **Login / Password:** использовать **Login** и **Password**, заданные в п.3.4.2 (имя пользователя для подключения к Zabbix API с правами read/write в группах, где будут создаваться CPE для мониторинга).
- **VNF/PNF Group: VNFGROUP** (группа Zabbix, куда будут добавляться VNF/PNF).
- **CPE Group: CPEGROUP** (группа Zabbix, куда будут добавляться CPE).

Нажать кнопку **Generate**, чтобы сгенерировать токен для подключения к серверу Zabbix.

Нажать **Test connection** для проверки доступности сервера Zabbix с заданными параметрами подключения.

Нажать **Apply** для применения настроек.

The screenshot shows the 'Monitoring' tab in the Kaspersky SD-WAN configuration interface. The left sidebar contains various icons for navigation. The main panel displays the following configuration fields:

- Type:** Zabbix (dropdown menu)
- URL:** https://zbx-www:8443/api_jsonrpc.pl
- Login:** Admin
- Password:** (password field with visibility toggle)
- Grouping by Zabbix:** By specified groups (dropdown menu)
- VNF/PNF group:** VNFGROUP
- CPE group:** CPEGROUP
- Trigger synchronization (sec):** 600 (spin box)
- Token:** (password field with visibility toggle)

Below the fields are two buttons: 'Clear' and 'Generate'. At the bottom of the form are two buttons: 'Test connection' and 'Apply'. A green status message 'Successful' is displayed at the bottom left of the form area.

4.1.4. Настроить системные ресурсы.

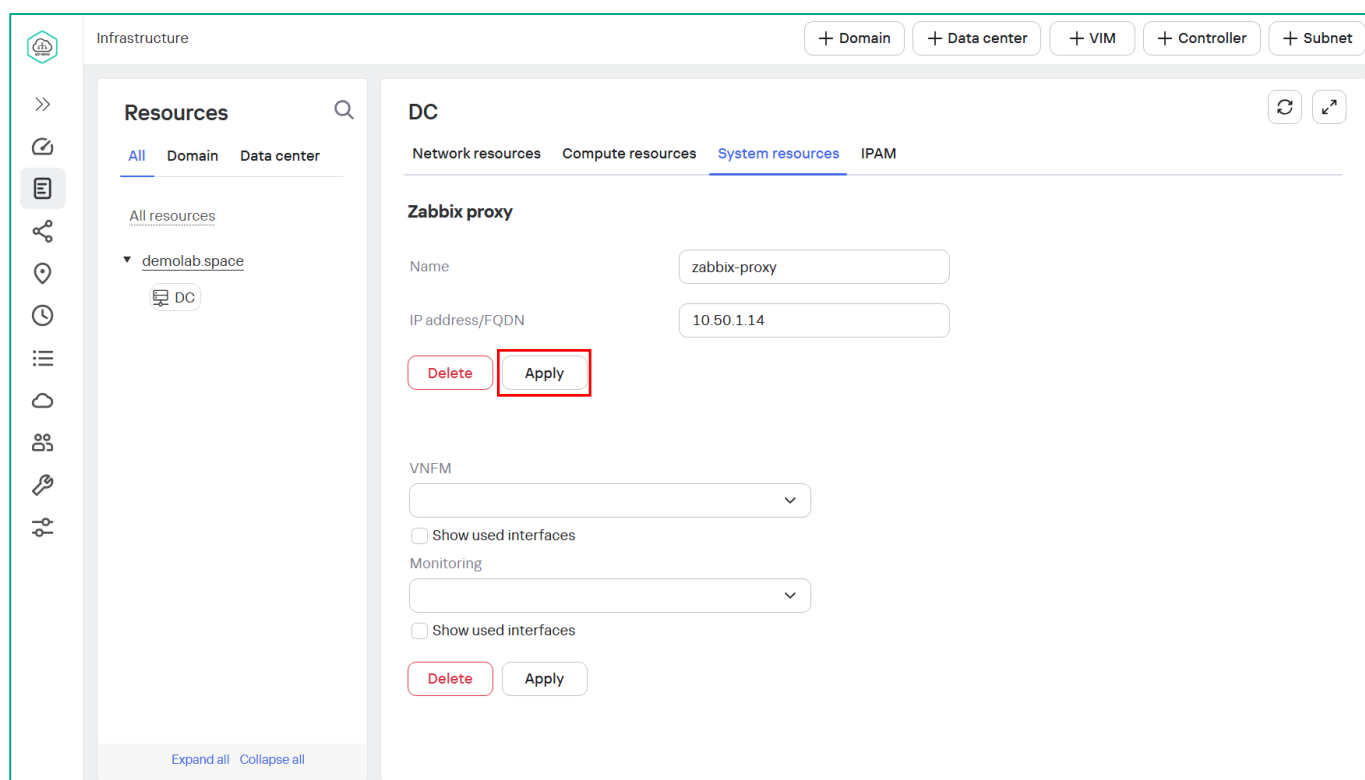
В основном меню слева выбрать раздел **Infrastructure**, далее в дереве ресурсов выбрать **DC**, созданный ранее и перейти на вкладку **System resources**.

Указать информацию для подключения к серверу Zabbix Proxy:

- Имя Zabbix Proxy (должно совпадать с именем, указанным в настройках Zabbix Server): **zabbix-proxy**.
- IP-адрес: **10.50.1.14** (публичный IP-адрес хоста orc1).

Note: При изменении публичного IP-адреса хоста orc1 из пункта 2.2 изменить на актуальный.

Нажать **Apply**.



4.1.5. Добавить пул IP-адресов для сети управления.

Для каждого Data center выделяются один или несколько диапазонов адресов.

Перейти на вкладку **Infrastructure** → **Domain** → **DC** → **IPAM** и нажать кнопку **+ Subnet**.

Задать параметры сети управления:

- **Name:** mgmt.
- **CIDR:** 10.11.13.0/24.
- **IP Range:** 10.11.13.13 – 10.11.13.253. Для добавления нового диапазона нажать **+ Add**.

Нажать **Create**.

New subnet ×

Domain

demolab.space ▼

Data center

DC ▼

Name

mgmt

Type

Management ▼

IP version

IPv4 ▼

CIDR

10.11.13.0/24

Gateway

IP range

10.11.13.13

10.11.13.253 ×

+ Add

Create

Cancel

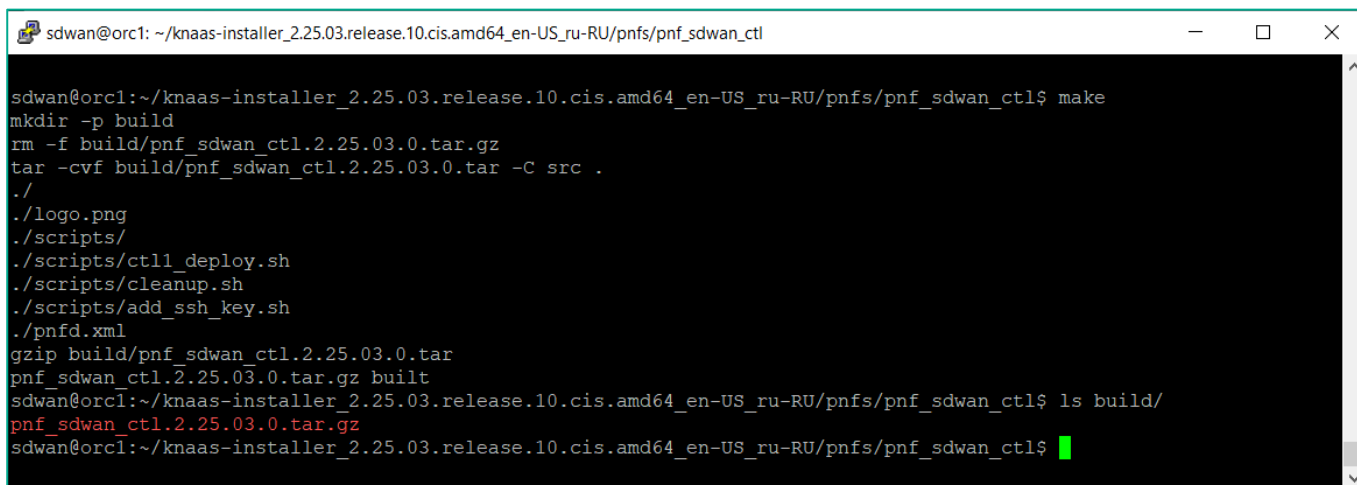
4.1.6. Создать дескриптор PNF для SD-WAN контроллера.

Пример дескриптора PNF находится в архиве с плейбуками установки по пути: `/home/sdwan/knaas-installer.<release_name>.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl/src`

Для создания архива с дескриптором выполнить `make` из папки

`/home/sdwan/knaas-installer.<release_name>.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl/`

Архив с PNF будет создан по пути: `/home/sdwan/knaas-installer.<release_name>.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl/build/pnf_sdwan_ctl.2.25.03.0.tar.gz`



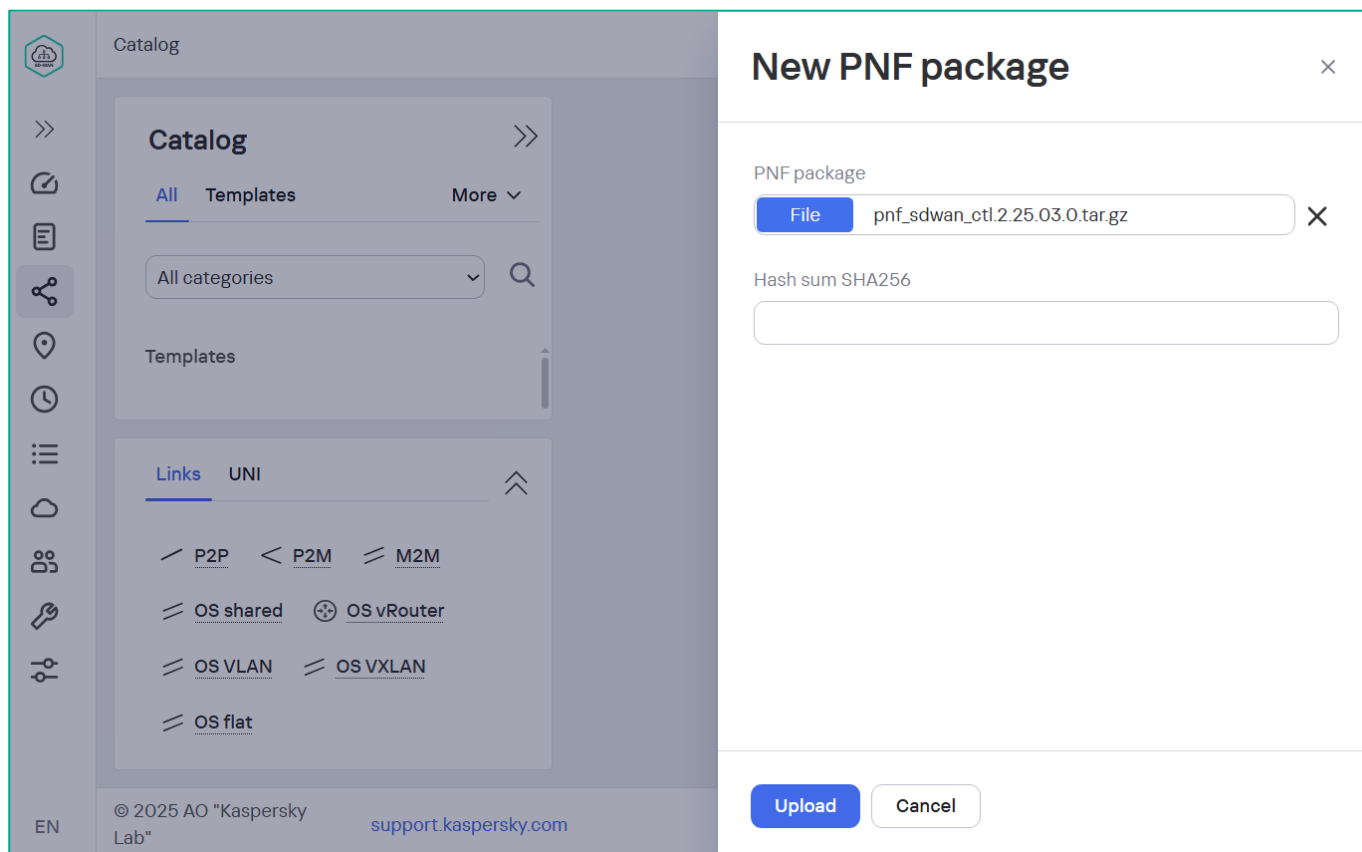
```
sdwan@orc1: ~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl
sdwan@orc1:~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl$ make
mkdir -p build
rm -f build/pnf_sdwan_ctl.2.25.03.0.tar.gz
tar -cvf build/pnf_sdwan_ctl.2.25.03.0.tar -C src .
./
./logo.png
./scripts/
./scripts/ctl1_deploy.sh
./scripts/cleanup.sh
./scripts/add_ssh_key.sh
./pnfd.xml
gzip build/pnf_sdwan_ctl.2.25.03.0.tar
pnf_sdwan_ctl.2.25.03.0.tar.gz built
sdwan@orc1:~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl$ ls build/
pnf_sdwan_ctl.2.25.03.0.tar.gz
sdwan@orc1:~/knaas-installer_2.25.03.release.10.cis.amd64_en-US_ru-RU/pnfs/pnf_sdwan_ctl$
```

После создания дескриптора скачать архив с хоста **orc1**.

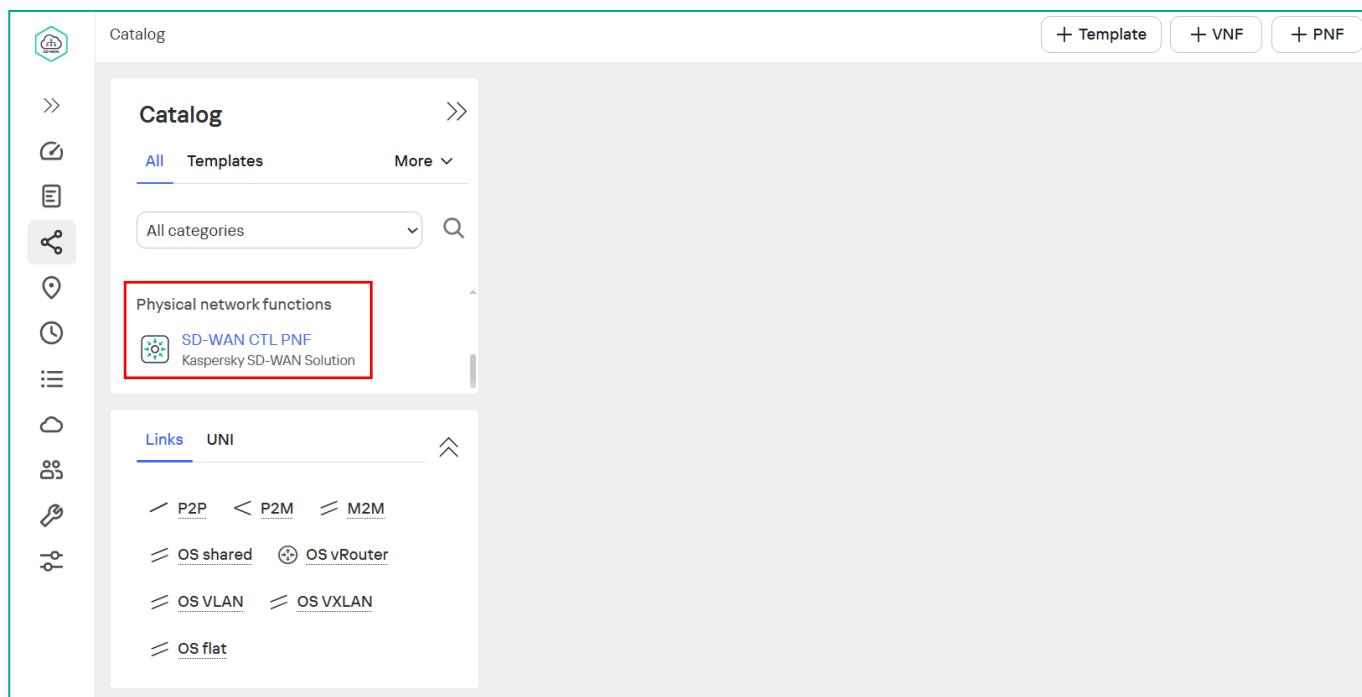
4.1.7. Импортировать PNF CTL в Catalog.

В меню слева выбрать **Catalog**, нажать кнопку **+ PNF** для добавления нового дескриптора PNF.

Указать путь и выбрать готовый для загрузки архив **pnf_sdwan_ctl.2.25.03.0.tar.gz**, затем нажать **Upload**.



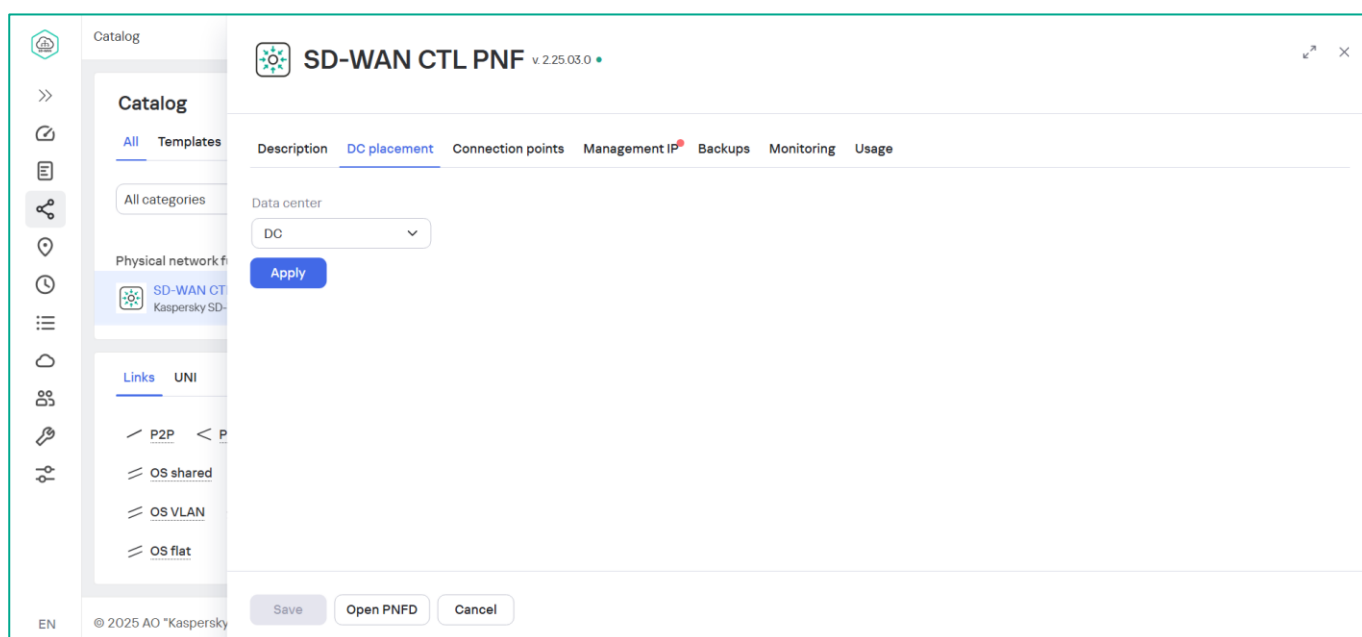
Дождаться загрузки дескриптора PNF в каталог.



4.1.8. Задать Data center для PNF контроллера.

Открыть **PNF** контроллера SD-WAN: нажать на **Physical Network Function** → **SD-WAN-CTL-PNF**.

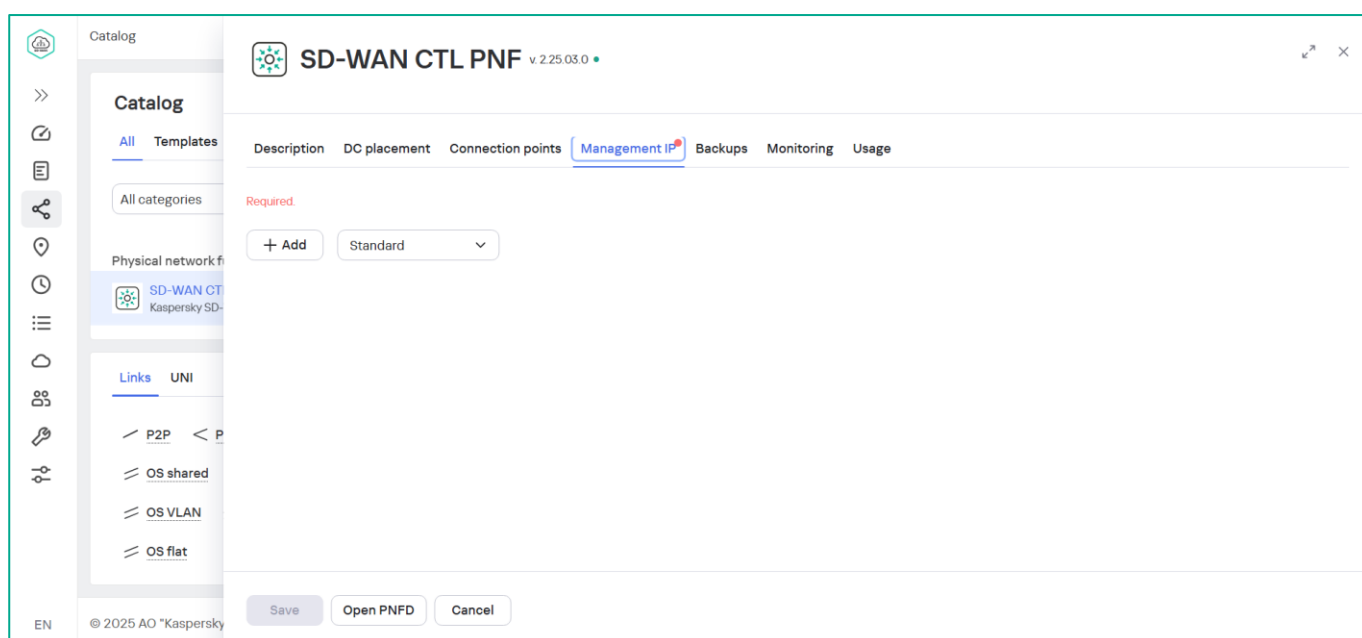
Перейти на вкладку **DC Placement**, выбрать **DC**, нажать **Apply**.



4.1.9. Задать адрес для подключения к PNF контроллера.

Перейти на вкладку **Management IP**.

Нажать **+ Add** для выбора Flavour **Standard**.



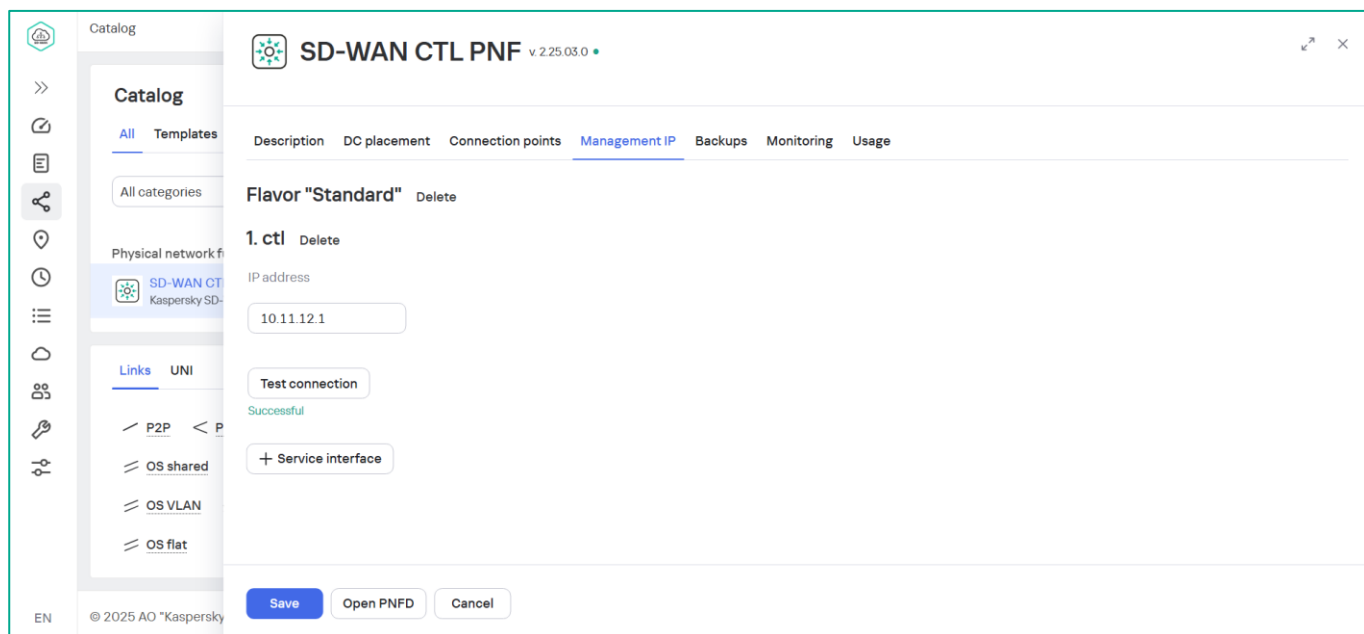
Затем нажать **+ Add** для добавления IP-адреса SD-WAN контроллера.

Ввести начальный IP-адрес из сети **knaas_os_man: 10.11.12.1**.

Note: При изменении этой сети изменить адрес на новый IP-адрес контроллера.

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

Нажать **Save**.

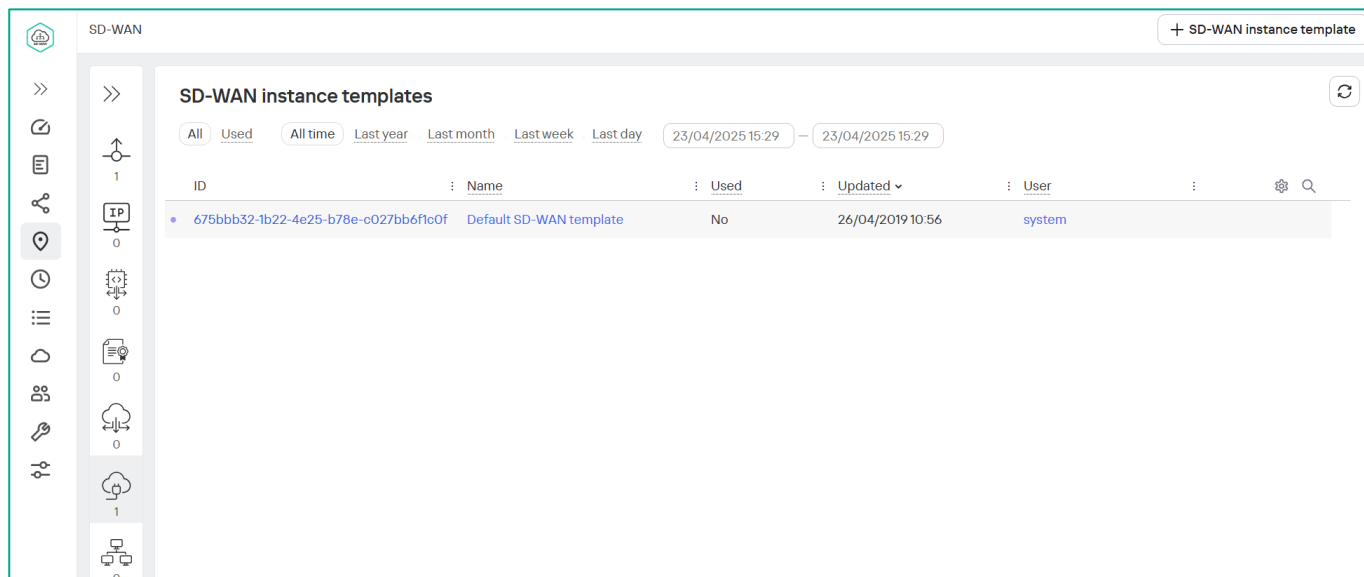


4.2. Создание шаблона экземпляра SD-WAN

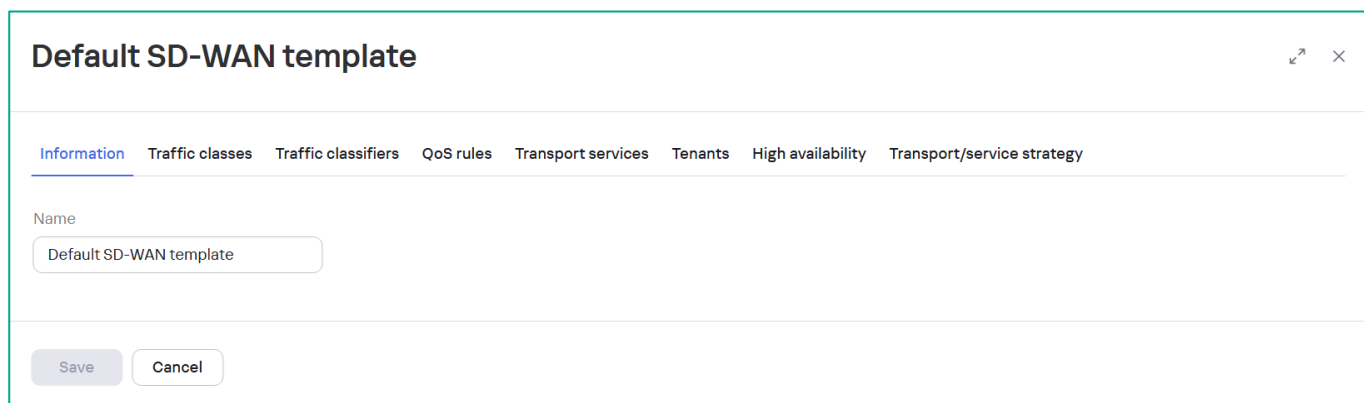
Шаблон экземпляра SD-WAN (англ. SD-WAN Instance template) содержит параметры наложенной сети. Применяется к контроллеру SD-WAN после развертывания сервиса SD-WAN.

4.2.1. Открыть шаблон SD-WAN Instance.

Перейти в раздел **SD-WAN → SD-WAN Instance templates** и нажать на шаблон **Default SD-WAN template** для его редактирования.



В поле **Name** изменить название шаблона или оставить значение по умолчанию.



4.2.2. Настроить транспортные сервисы в шаблоне экземпляра SD-WAN.

Перейти на вкладку **Transport Services**.

Удалить сервис **SD-WAN P2M Data** (нажать **Delete** для сервиса).

Создание транспортного сервиса для передачи данных будет описано в п. 5.1.

Оставить только **SD-WAN managementTunnel**.

Default SD-WAN template

Information Traffic classes Traffic classifiers QoS rules **Transport services** Tenants High availability Transport/service strategy

X2M services L3 services

+ Transport service

Name	Type	Management transport service	Mode	MAC age (sec)	MAC learn mode	MAC table size	MAC table overload	Actions
SD-WAN managementTunnel	P2M	Yes	Classic	300	Learn and flood	2000	Flood	Edit Delete

Save Cancel

4.2.3. Проверить настройки транспортного сервиса для управления CPE.

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

Настройки по умолчанию соответствуют информации на снимке экрана.

Default SD-WAN template

Information Traffic classes Traffic classifiers QoS rules **Transport services**

X2M services L3 services

+ Transport service

Name	Type	Management transport service	Mode
SD-WAN managementTunnel	P2M	Yes	Classic

Save Cancel

Transport service

Name: SD-WAN managementTunnel

Type: P2M ☒ Management transport service

MAC learn mode: Learn and flood

MAC age (sec): 300

MAC table size: 2000

MAC table overload: Flood

Mode: Classic

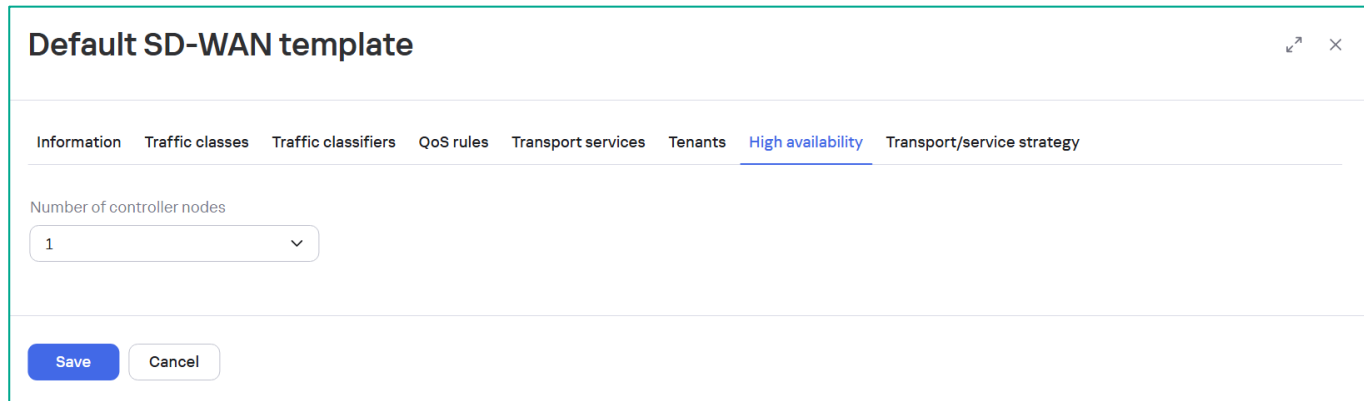
Save Cancel

4.2.4. Настроить количество контроллеров, используемых сервисом SD-WAN.

Перейти на вкладку **High Availability**.

Оставить значение по умолчанию:

- **Number of controller nodes: 1** (соответствует количеству контроллеров в PoC).



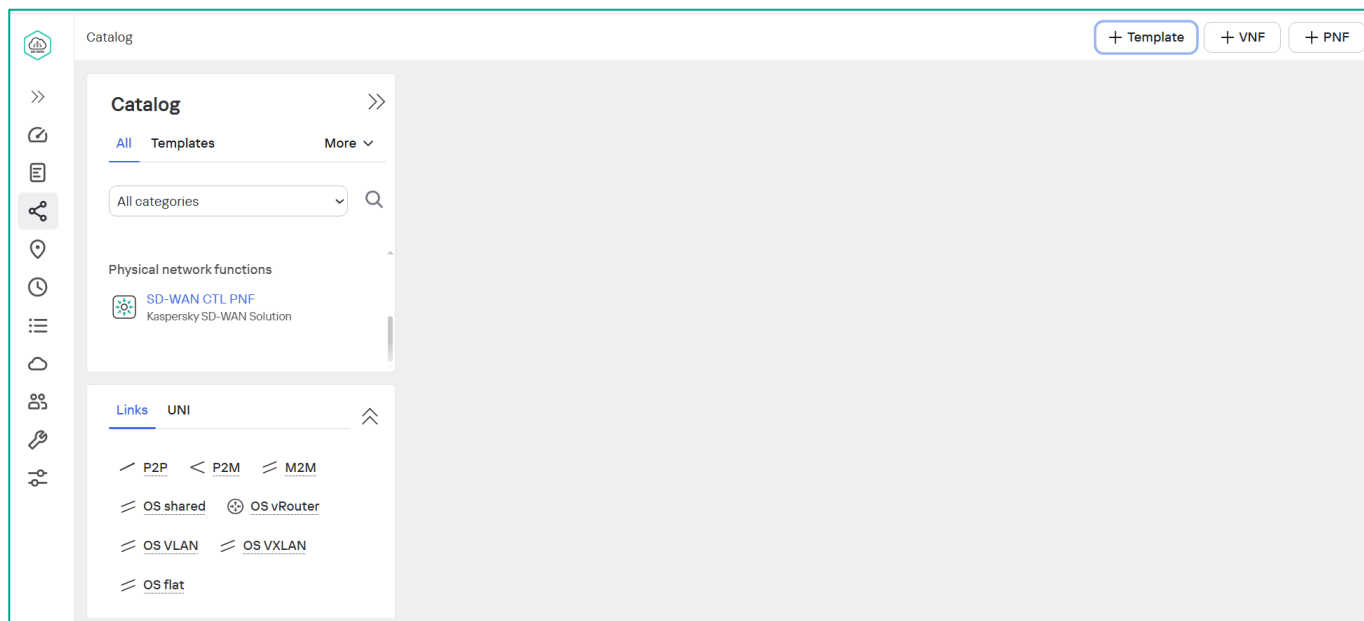
The screenshot shows a web interface titled "Default SD-WAN template". At the top, there is a navigation bar with several tabs: "Information", "Traffic classes", "Traffic classifiers", "QoS rules", "Transport services", "Tenants", "High availability" (which is currently selected and underlined), and "Transport/service strategy". Below the navigation bar, the main content area is labeled "Number of controller nodes". It contains a dropdown menu with the value "1" selected. At the bottom of the form, there are two buttons: "Save" (in blue) and "Cancel" (in light gray).

Нажать **Save** для сохранения изменений.

4.3. Создание шаблона сервиса SD-WAN

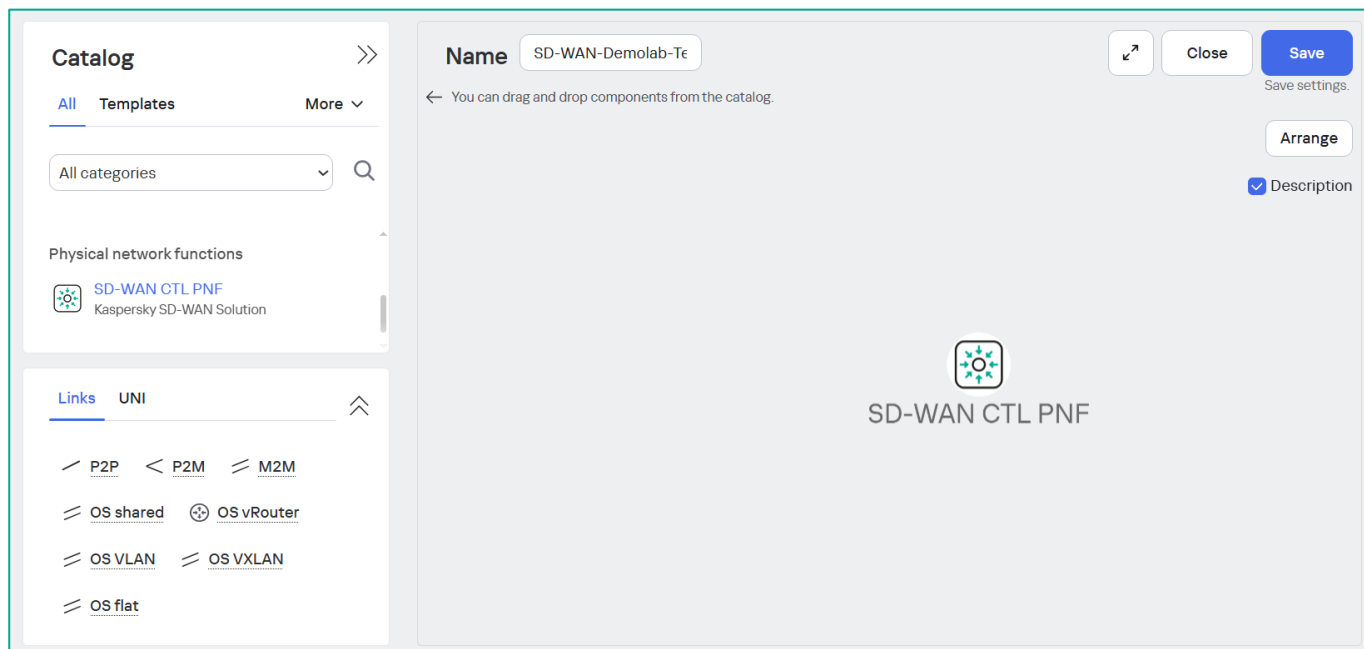
4.3.1. Создать шаблон сервиса SD-WAN.

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

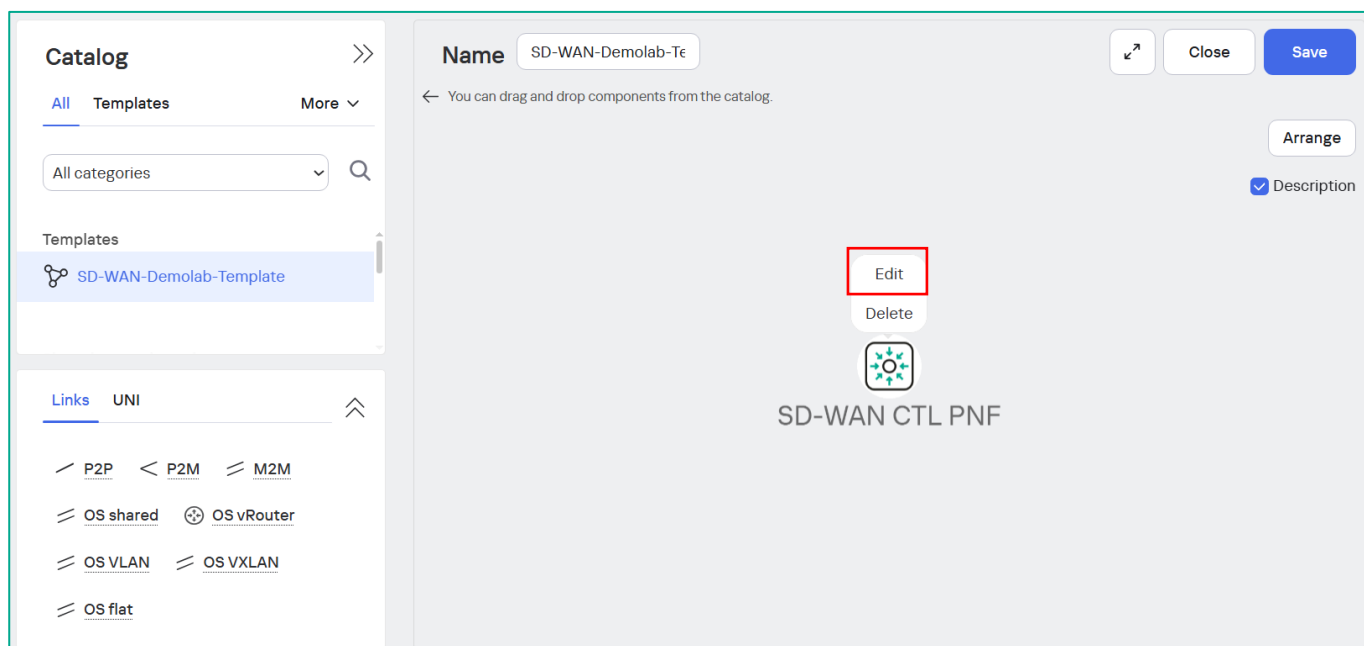


Перетащить с помощью мыши в окно конструктора SD-WAN контроллер в виде PNF (**SD-WAN-CTL-PNF**).

Задать имя шаблона (в примере **SD-WAN-Demolab-Template**) и нажать **Save**.

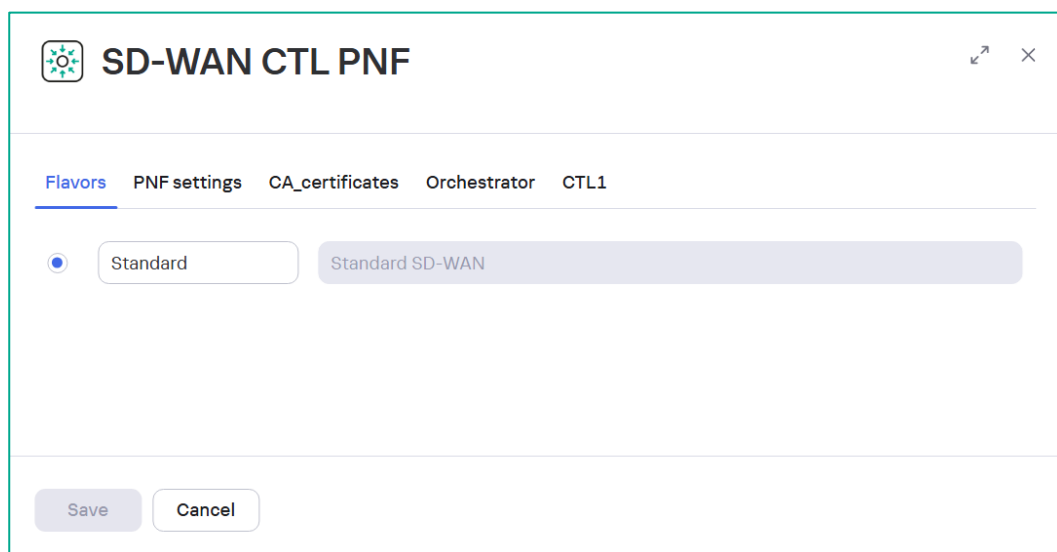


4.3.2. Открыть контроллер в шаблоне сервиса SD-WAN для редактирования параметров.
Нажать на объект **SD-WAN-CTL-PNF** и выбрать **Edit**.



Перейти на вкладку **PNF Settings**.

Изменить имя SD-WAN контроллера при необходимости.

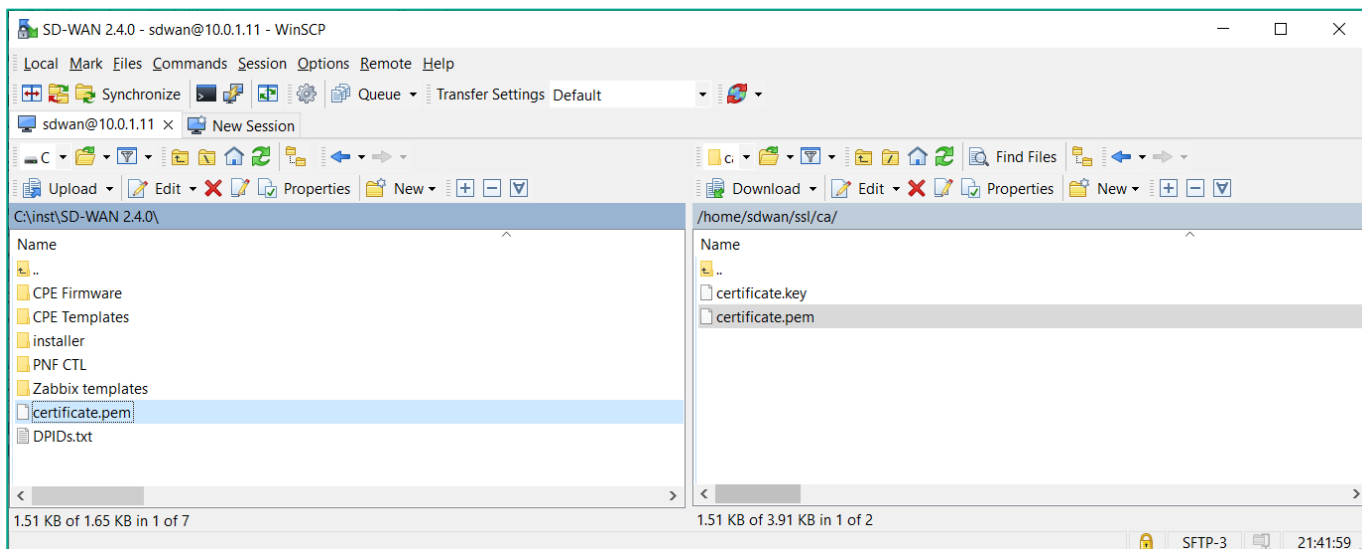


4.3.3. Добавить корневой сертификат оркестратора в PNF контроллера.

При подключении контроллера к оркестратору происходит проверка сертификатов, в связи с этим необходимо добавить корневой сертификат, которым был подписан сертификат оркестратора на контроллер.

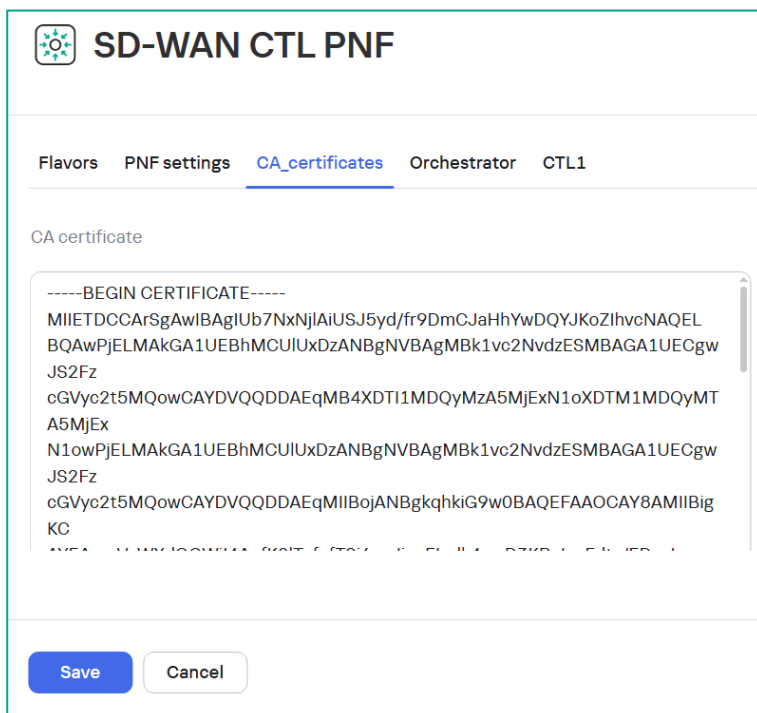
В процессе установки системы управления SD-WAN корневой сертификат CA был сохранен в файл: **/home/sdwan/ssl/ca/certificate.pem**

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



Перейти на вкладку **CA_certificates**.

Добавить полностью содержимое файла корневого сертификата (**certificate.pem**) в **CA certificate** в текстовом виде (поле возможно растянуть для удобства отображения).

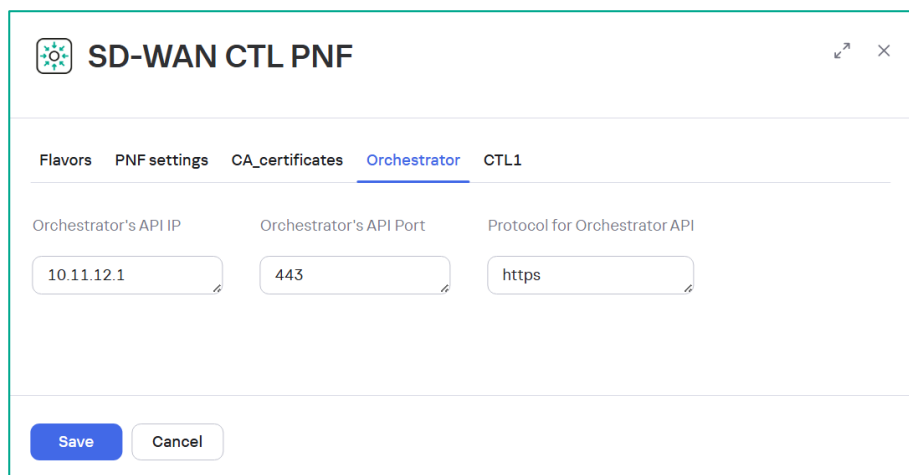


4.3.4. Задать параметры для подключения контроллера к оркестратору SD-WAN.

Перейти на вкладку **Orchestrator**.

Задать IP-адрес оркестратора: ввести начальный IP-адрес из сети **knaas_os_man** (заданной в пункте 3.2.6): **10.11.12.1**.

Note: При изменении сети **knaas_os_man** изменить IP-адрес на актуальный.



The screenshot shows the 'SD-WAN CTL PNF' configuration window with the 'Orchestrator' tab selected. The 'Orchestrator's API IP' field contains '10.11.12.1', the 'Orchestrator's API Port' field contains '443', and the 'Protocol for Orchestrator API' field contains 'https'. At the bottom, there are 'Save' and 'Cancel' buttons.

4.3.5. Задать параметры, для подключения оркестратора и устройств CPE к контроллеру.

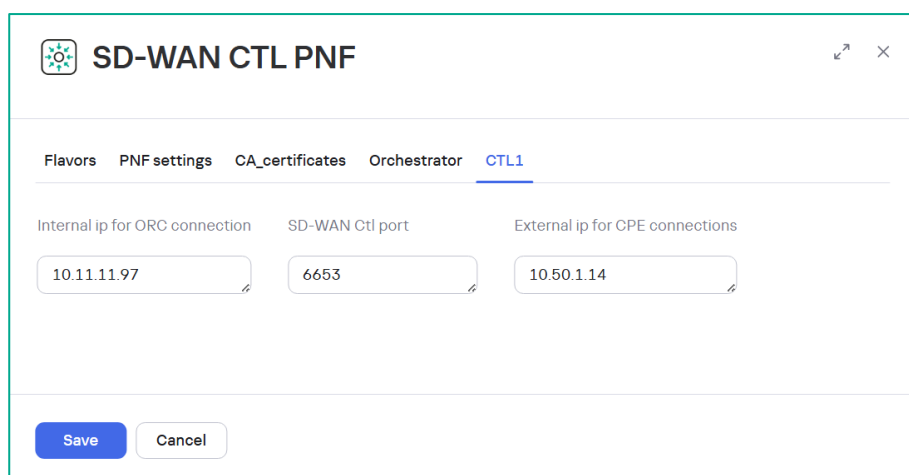
Перейти на вкладку **CTL1**.

В качестве внутреннего IP-адреса, который используется для подключения оркестратора к контроллеру, задать IP-адрес контейнера контроллера: **10.11.11.97**

В качестве внешнего IP-адреса задать публичный IP-адрес контроллера: **10.50.1.14**, этот адрес будет передан CPE для подключения к контроллеру. На R14 настроен DNAT портов 6653-6656 в IP-адрес хоста org.

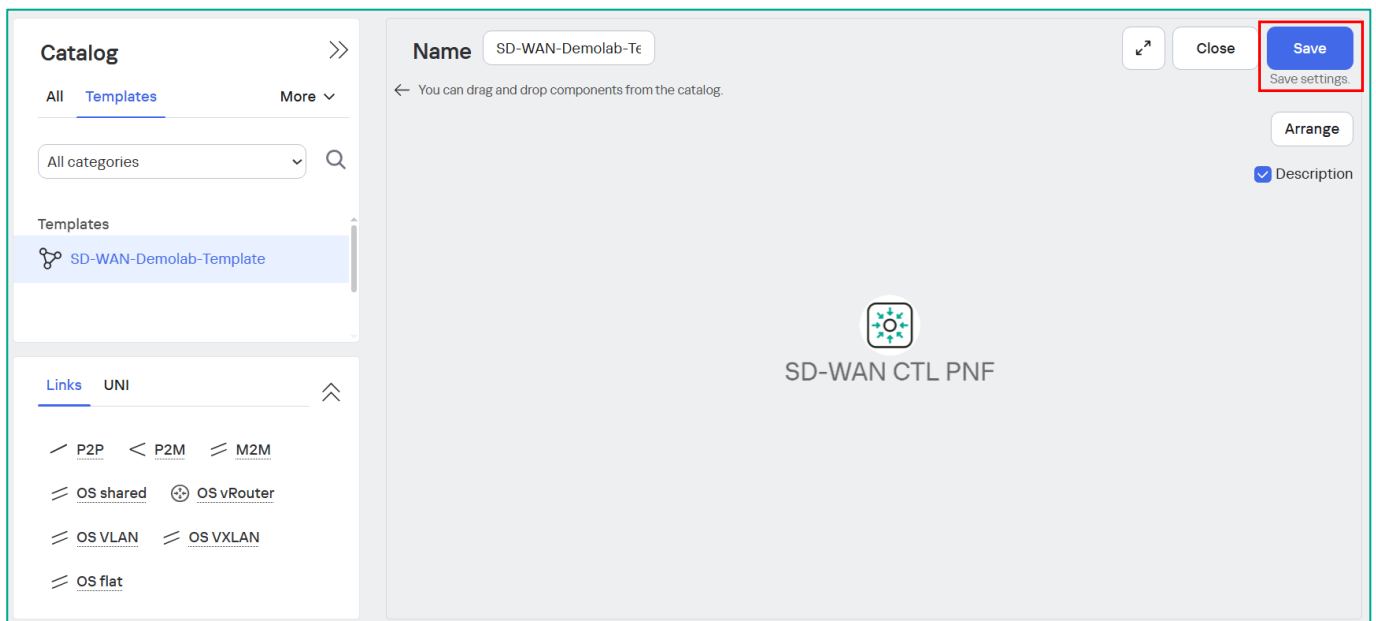
Note: При изменении публичного IP-адреса хоста org1 из пункта 2.2 изменить на актуальный.

Нажать **Save** в настройках контроллера.



The screenshot shows the 'SD-WAN CTL PNF' configuration window with the 'CTL1' tab selected. The 'Internal ip for ORC connection' field contains '10.11.11.97', the 'SD-WAN Ctl port' field contains '6653', and the 'External ip for CPE connections' field contains '10.50.1.14'. At the bottom, there are 'Save' and 'Cancel' buttons.

Затем нажать **Save** в настройках шаблона.



4.4. Создание Tenant и развертывание сервиса SD-WAN

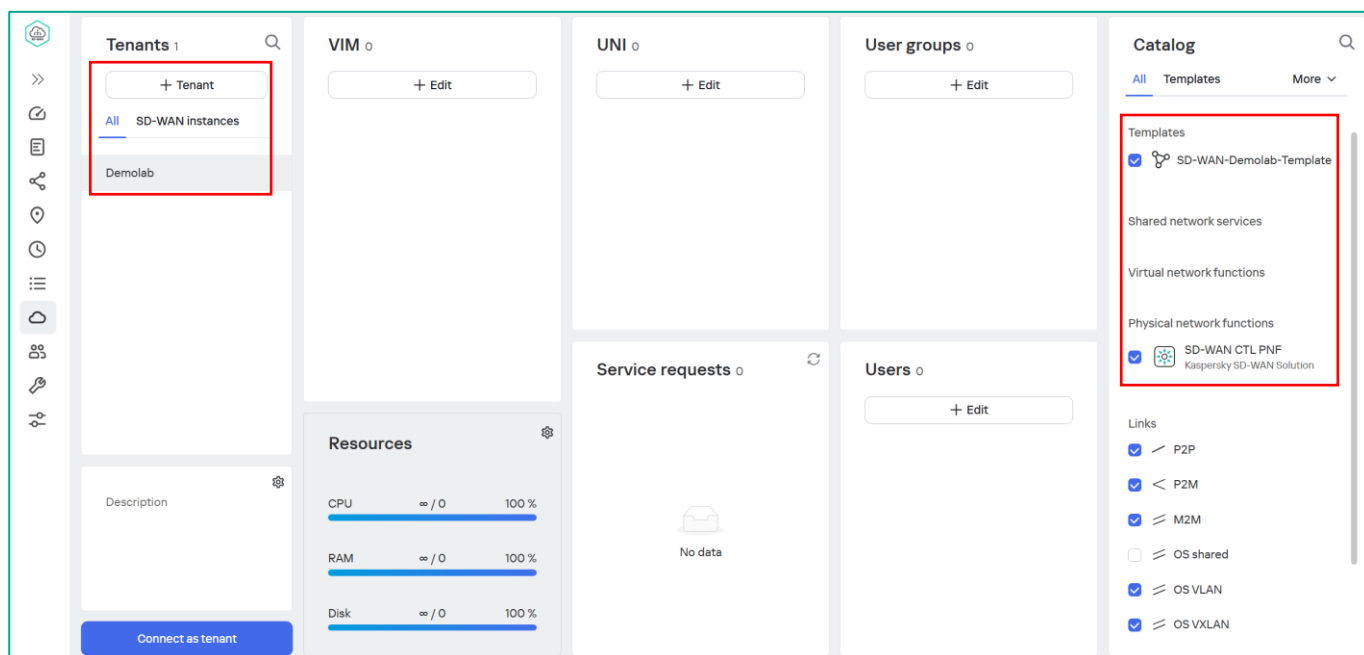
4.4.1. Создать новый тенант.

Перейти в меню **Tenants**.

Нажать кнопку **+ Tenant**, ввести имя нового тенанта (в примере используется **Demolab**) и нажать **+** для создания нового тенанта.

Note: Не используйте "." и специальные символы в имени тенанта.

В области **Catalog** отметить: **Templates** и **Physical Network Functions**. Данные объекты будут доступны для использования в тенанте.



4.4.2. Добавить администратора тенанта (Опционально).

Создать нового пользователя с ролью тенант.

Перейти в меню **Users**. Нажать **+ Add** для добавления нового пользователя.

The screenshot displays the Kaspersky SD-WAN management interface. On the left is a sidebar with various icons, including a highlighted 'Users' icon. The main panel has a top navigation bar with tabs: 'Users' (selected), 'Permissions', 'Groups', 'LDAP connections', and 'Two-factor authentication'. Below the tabs is a '+ Add' button. A table lists the current users:

Name	Tenant	Role	Source	Group	State	Two-factor authentication
Administrator Administrator		Administrator	Local	Default	Online	Disabled
User User		Tenant	Local	Default	Offline	Disabled

Задать:

- **Login** (имя пользователя).
- **Password** (пароль) и подтвердить его.
- **Role: Tenant** (назначить роль арендатор пользователю).
- **Permissions: Full access** (предоставить полные права пользователю).
- **First name / Last name** (Задать Имя / Фамилию пользователя).

Нажать **Create** для создания пользователя.

New user

×

Source

Local

▼

Login

demolab-admin

Password

.....

👁

Password confirmation

.....

👁

Role

Tenant

▼

Permissions

Full access

▼

Two-factor authentication

☐ Off

Request confirmation is required

☐ Off

First name

Tenant

Last name

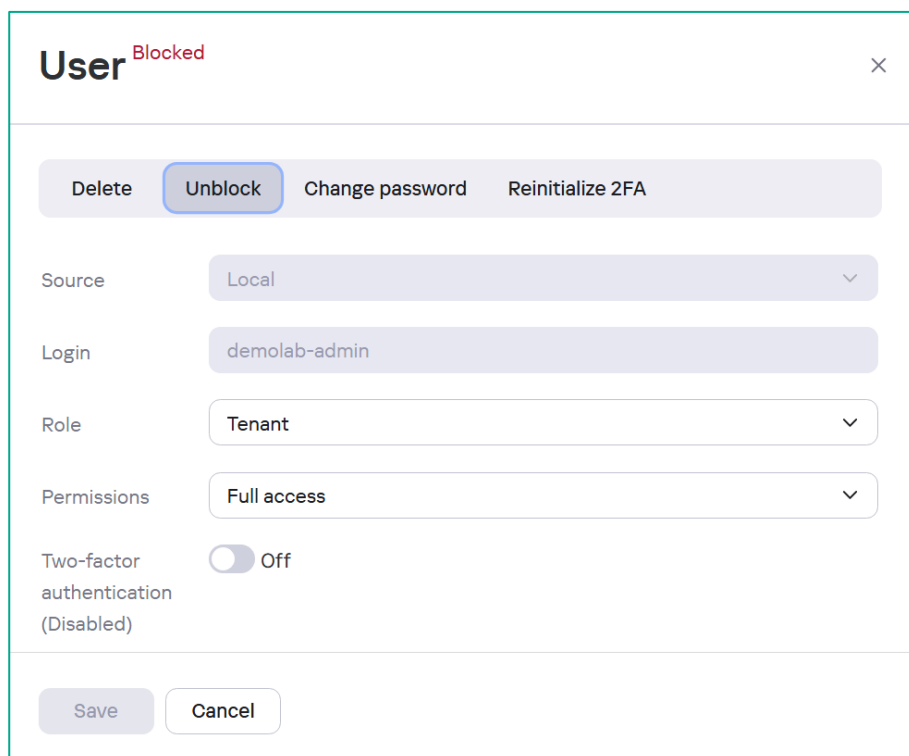
Tenant

Create

Cancel

4.4.3. Активировать нового пользователя.

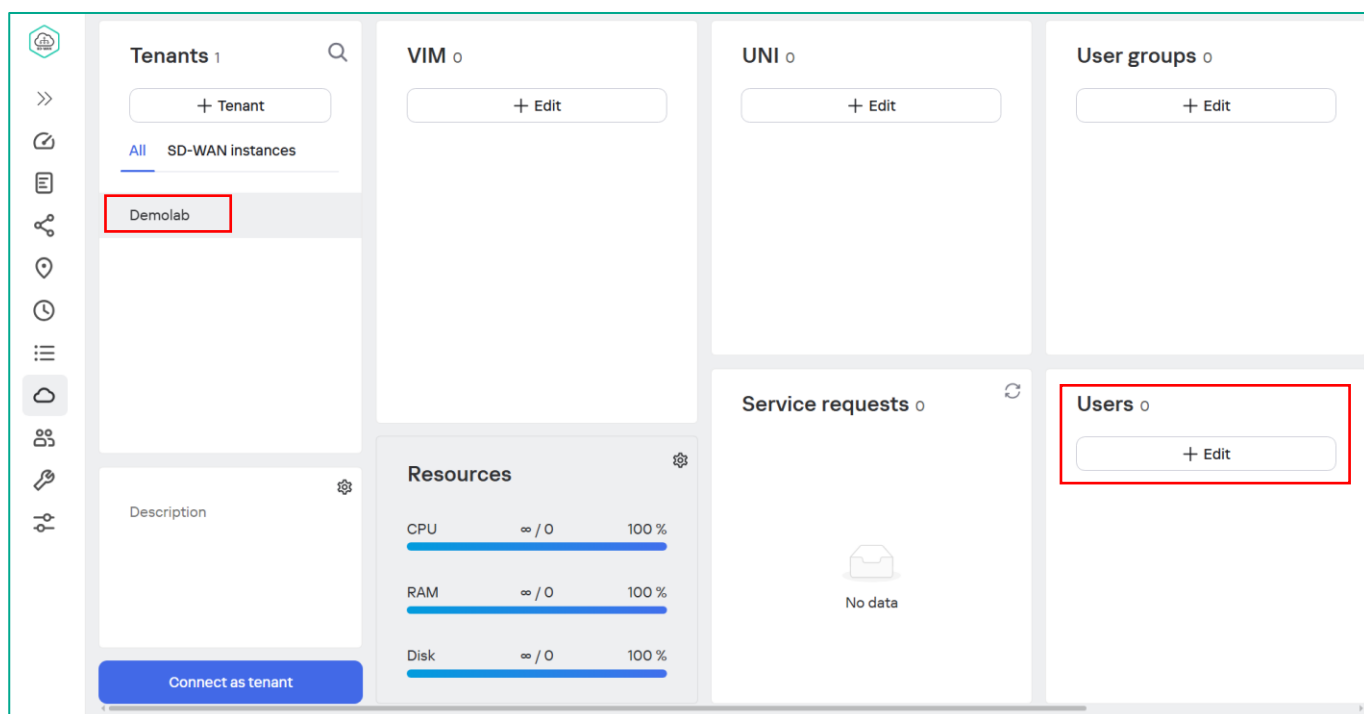
Выбрать необходимую учетную запись, затем нажать **Unblock**.



The image shows a 'User' management modal window with a red 'Blocked' status indicator. The window contains several sections: a top bar with action buttons (Delete, Unblock, Change password, Reinitialize 2FA), a 'Source' dropdown set to 'Local', a 'Login' field with 'demolab-admin', a 'Role' dropdown set to 'Tenant', a 'Permissions' dropdown set to 'Full access', and a 'Two-factor authentication' toggle set to 'Off' (Disabled). At the bottom are 'Save' and 'Cancel' buttons.

4.4.4. Добавить пользователя в созданный ранее тенант.

Перейти в меню **Tenants**. Выбрать созданный ранее тенант и в разделе **Users** нажать **+ Edit**.



The image is a screenshot of the Kaspersky SD-WAN management interface. It features a sidebar with navigation icons and a main content area. The main area is divided into several panels: 'Tenants' (with a search bar and a list containing 'Demolab'), 'VIM' (with a '+ Edit' button), 'UNI' (with a '+ Edit' button), 'User groups' (with a '+ Edit' button), 'Resources' (showing CPU, RAM, and Disk usage at 100%), 'Service requests' (showing 'No data'), and 'Users' (with a '+ Edit' button). The 'Demolab' tenant and the 'Users' section are highlighted with red rectangles.

Выбрать созданного пользователя (переместить в **Assign users**) и нажать **Save**.

Tenant's users

Users

User User

Assign users

< Tenant Tenant

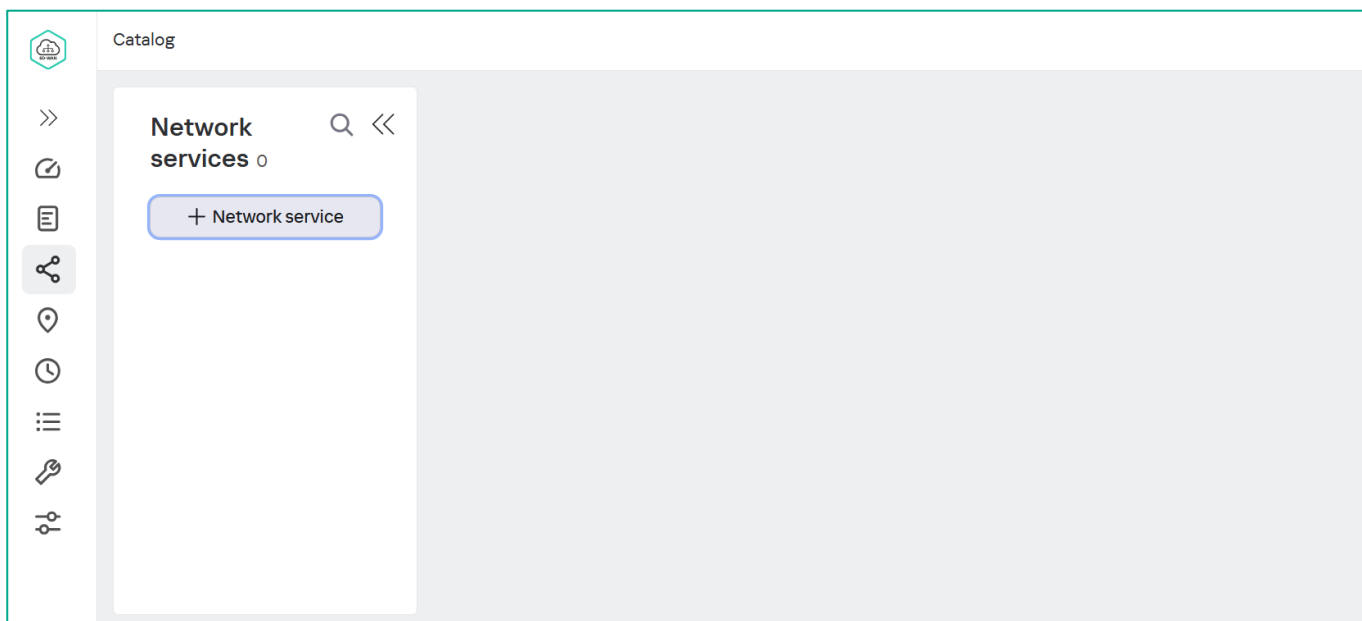
Save

Cancel

4.4.5. Развернуть сетевой сервис SD-WAN из шаблона SD-WAN.

Подключиться к portalу самообслуживания тенанта: нажать кнопку **Connect as Tenant** из меню **Tenants** или подключиться к SD-WAN оркестратору администратором созданного тенанта.

В меню **Catalog** нажать кнопку **+ Network service**.

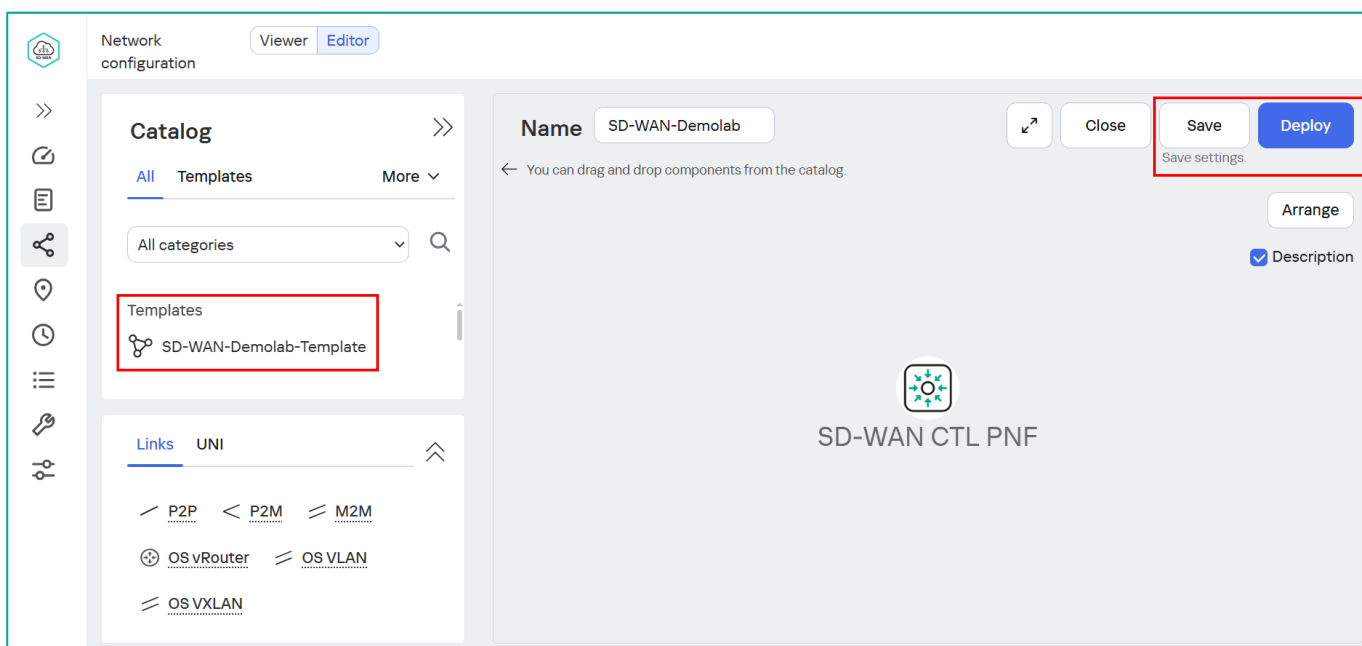


В секции **Templates** выбрать созданный ранее шаблон SD-WAN и перетащить в окно конструктора сервисов.

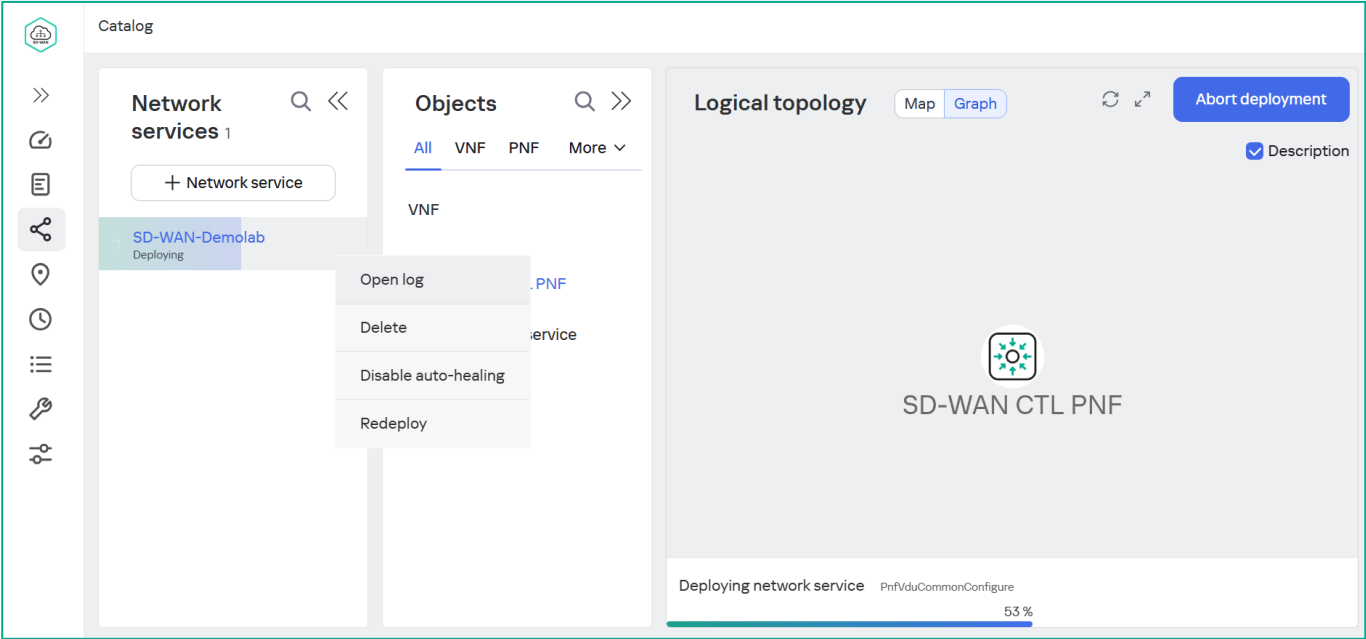
Задать имя сервиса SD-WAN (в примере используется **SD-WAN-Demolab**).

Нажать **Save**.

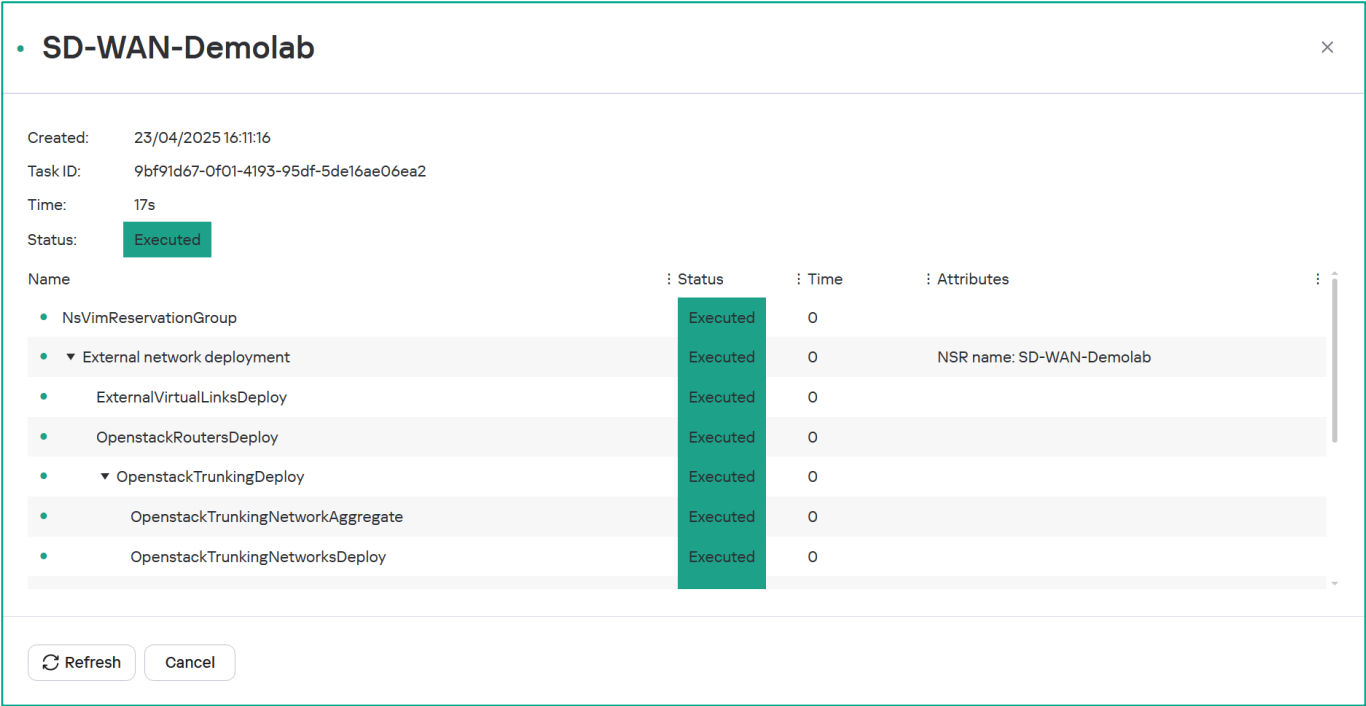
Нажать кнопку **Deploy**.



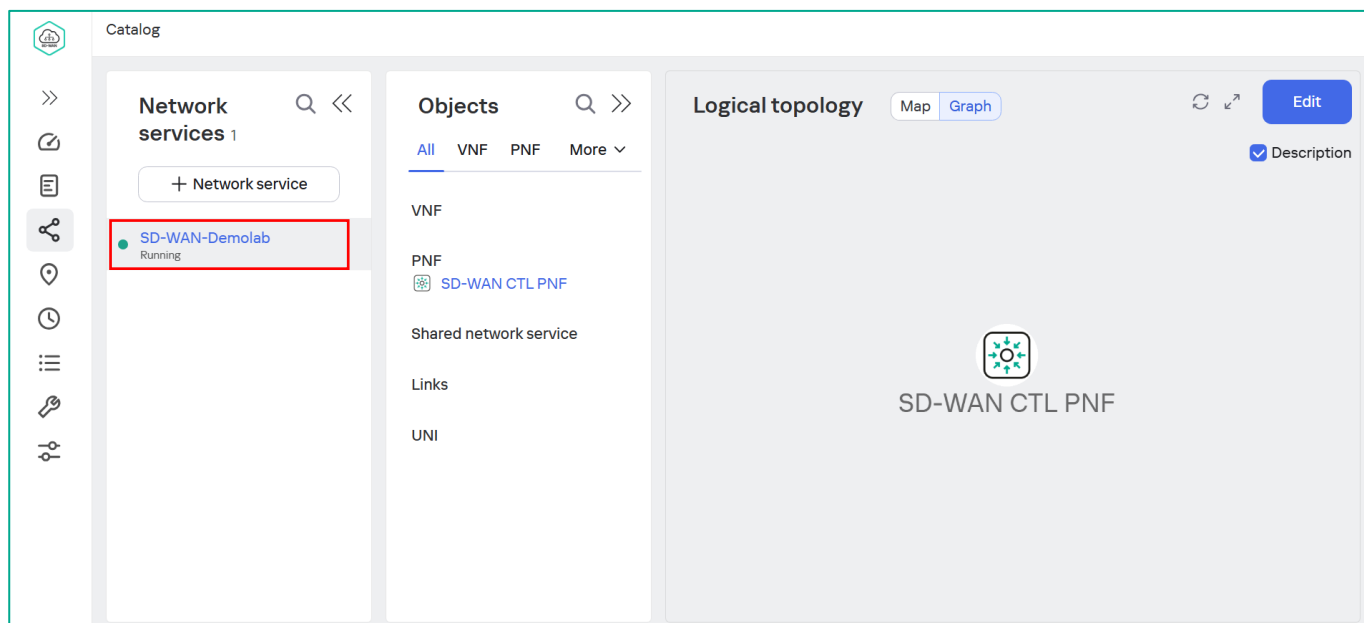
Для наблюдения за процессом развертывания сервиса нажать кнопку настройки сервиса (шестеренка) и выбрать **Open log**.



В интерфейсе отобразится процесс развертывания сервиса с детальным статусом по отдельным задачам.



Дождаться окончания развертывания сервиса SD-WAN. В области **Network services** сервис SD-WAN должен быть отмечен зеленым индикатором со статусом **Running**.



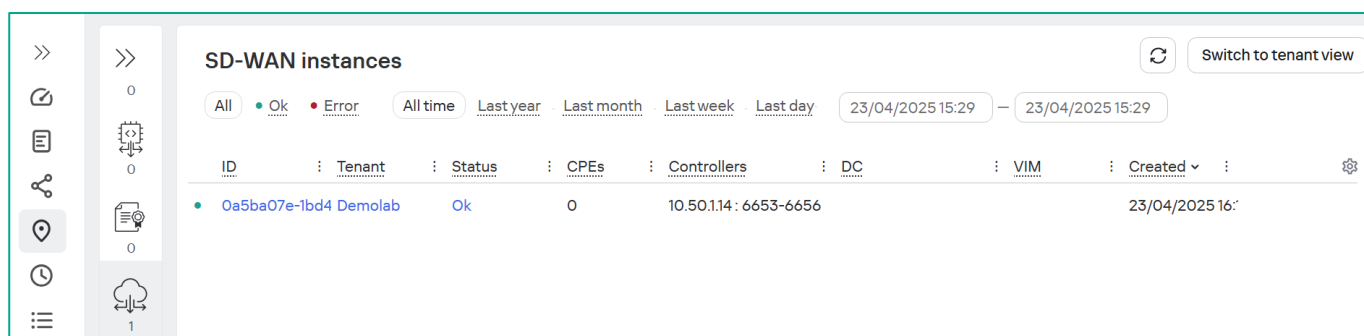
4.4.6. Проверить развертывание экземпляра сети SD-WAN.

После запуска сервиса на стороне Tenant необходимо убедиться в успешном завершении конфигурации сервиса.

Подключиться к порталу администратора SD-WAN: повторить п. 3.3.1 или перейти на предыдущую вкладку браузера.

Перейти в меню **SD-WAN → SD-WAN Instances**.

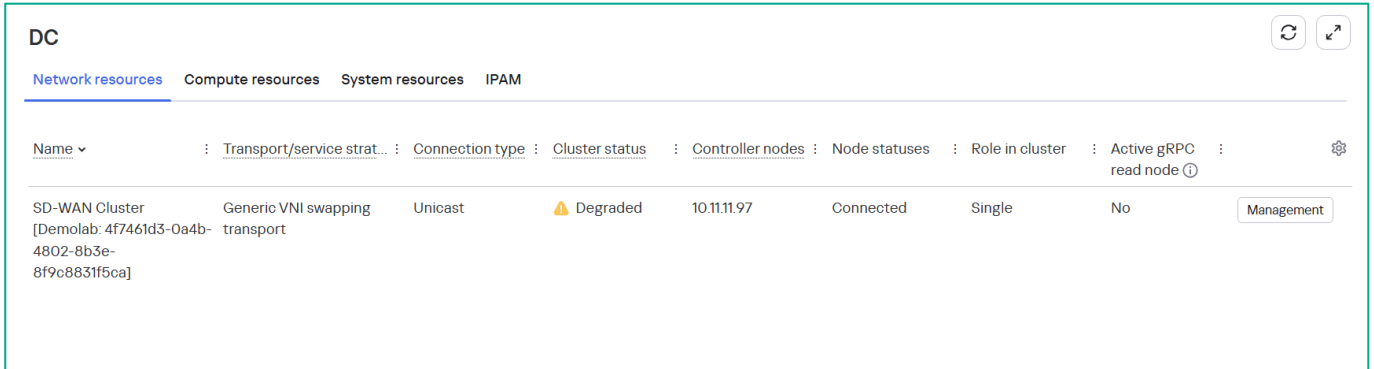
Перед **ID** экземпляра SD-WAN должен отображаться индикатор зеленого цвета.



4.4.7. Проверить статус созданного кластера контроллеров.

Перейти в меню **Infrastructure → Domain → DC → Network resources**.

Проверить статус SD-WAN контроллера. **Cluster status - Degraded** указывает на то, развернут один (single) контроллер, без отказоустойчивости.



DC								
Network resources Compute resources System resources IPAM								
Name	Transport/service strat...	Connection type	Cluster status	Controller nodes	Node statuses	Role in cluster	Active gRPC read node	
SD-WAN Cluster [Demolab: 4f7461d3-0a4b-4802-8b3e-8f9c8831f5ca]	Generic VNI swapping transport	Unicast	Degraded	10.11.11.97	Connected	Single	No	Management

4.4.8. Остановить временный контейнер mockpnf-1.

При развёртывании сервиса SD-WAN и настройке контроллера оркестратор подключается к контроллеру через контейнер **mockpnf-1**. После развертывание сервиса требуется остановить временный контейнер.

Выполнить на хосте otc1 команду:

```
docker stop mockpnf-1
```

4.5. Создание шаблона межсетевого экрана для SD-WAN шлюзов

Шаблон межсетевого экрана CPE содержит параметры, которые применяются на устройствах CPE после их регистрации в оркестраторе.

4.5.1. Создать дополнительную зону межсетевого экрана для шлюзов.

Подключиться к порталу самообслуживания тенанта, созданному в 4.4.1 (в PoC используется тенант **Demolab**), для этого нажать кнопку **Connect as Tenant** из меню **Tenants** или подключиться к SD-WAN оркестратору администратором созданного тенанта.

Note: При создании зон и шаблонов межсетевого экрана администратором из портала администратора они не будут доступны пользователям с правами tenant.

Для работы доступа к SSH консоли CPE из веб-интерфейса оркестратора необходимо обеспечить сетевую связность между контейнером vnfm-1 оркестратора и IP-адресами CPE из сети управления (mgmt). Интерфейсы CPE в сети управления автоматически добавляются в отдельный транспортный P2M сервис, из которого нет связности с другими сетями, в том числе и с подсетью оркестратора. Для обеспечения связности от оркестратора до адресов управления CPE требуется настроить masquerading для зоны, в которой будут находиться интерфейсы управления шлюзов, таким образом IP-адрес оркестратора будет транслирован в IP-адреса интерфейсов управления (mgmt) шлюзов.

Также возможно настроить Source NAT в шаблоне межсетевого экрана из IP-адреса оркестратора в IP-адреса интерфейсов mgmt шлюзов, выделенные IP-адреса можно посмотреть в **Infrastructure → DC → IPAM → Usage**.

Перейти в меню **SD-WAN → Firewall zones**.

Нажать кнопку **+ Firewall Zone**.

SD-WAN

+ Firewall zone

Firewall zones

All time Last year Last month Last week Last day 29/04/2025 11:15 — 29/04/2025 11:15

Name	Usage	Author	Created
lan	Yes	admin (Demolab)	23/04/2025 15:57:47
wan	Yes	admin (Demolab)	23/04/2025 15:57:47
mgmt	No	admin (Demolab)	23/04/2025 15:57:47

В поле **Name** задать название зоны: **mgmt_gw**.

Отметить **Masquerading**.

При пересылке пакетов из других зон в зону mgmt_gw будет происходить Source Network Address Translation (SNAT) в адрес интерфейса из зоны mgmt_gw.

New firewall zone

Name

mgmt_gw

Input

ACCEPT

Output

ACCEPT

Forwarding

REJECT

☒ Masquerading

☒ MSS clamp to PMTU

☐ Drop logging

Masquerading source subnets

+ Add

Masquerading destination subnets

+ Add

Networks

+ Add

Create

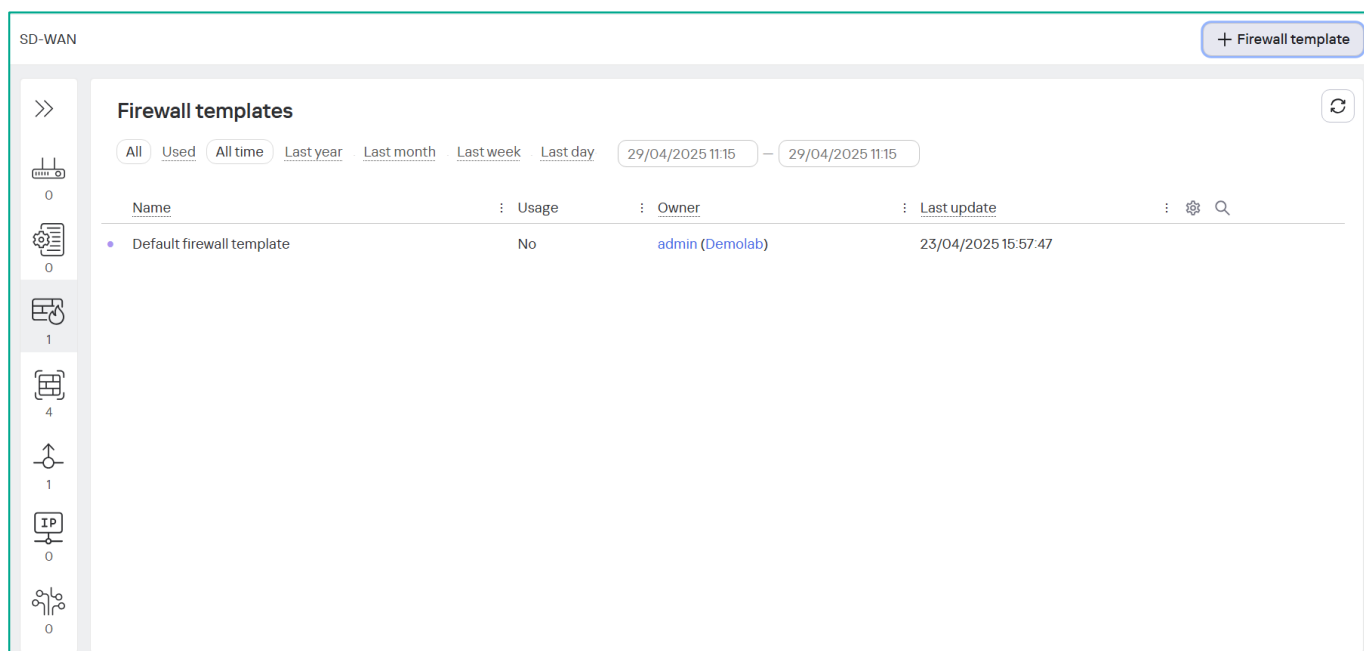
Cancel

Нажать **Create**.

4.5.2. Создать шаблон межсетевого экрана для SD-WAN шлюзов.

Перейти в меню **SD-WAN → Firewall templates**.

Нажать кнопку **+ Firewall Template**.



В поле **Name** задать название шаблона: **gateway_firewall_template**.

Нажать **Create**.

The screenshot shows a 'New firewall template' dialog box. It has a title bar with a close button (X). The main area contains a 'Name' label and a text input field. The input field contains the text 'gateway_firewall_template'. At the bottom of the dialog, there are two buttons: 'Create' (highlighted in blue) and 'Cancel'.

4.5.3. Настроить правила форвардинга между зонами для шаблона межсетевого экрана SD-WAN шлюзов.

Открыть созданный шаблон.

В шаблоне перейти на вкладку **Zone forwarding**.

Создать два правила forwarding: из зоны **lan** в зону **mgmt_gw** и из зоны **mgmt_gw** в **lan**.

Для этого нажать **+ Forwarding**, выбрать необходимые зоны, затем нажать **Create**.

The screenshot shows the 'gateway_firewall_template' configuration window. The 'Zone forwarding' tab is selected, showing a table with two forwarding rules. The first rule is from 'lan (Demolab)' to 'mgmt_gw (Demolab)'. The second rule is from 'mgmt_gw (Demolab)' to 'lan (Demolab)'. Each rule has a 'Delete' button next to it. The interface includes tabs for 'General settings', 'Rules', 'NAT', 'Zone forwarding', 'IP address sets', and 'DPI marking'. There are also buttons for 'Set as designated', 'Delete', 'Import', 'Export', 'Clone', and 'Show associated CPEs'. At the bottom, there are 'Save' and 'Cancel' buttons.

From	To	Actions
lan (Demolab)	mgmt_gw (Demolab)	Delete
mgmt_gw (Demolab)	lan (Demolab)	Delete

Нажать **Save** для сохранения шаблона.

4.6. Создание шаблонов SD-WAN шлюзов

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

4.6.1. Создать шаблон для шлюза vGW-11.

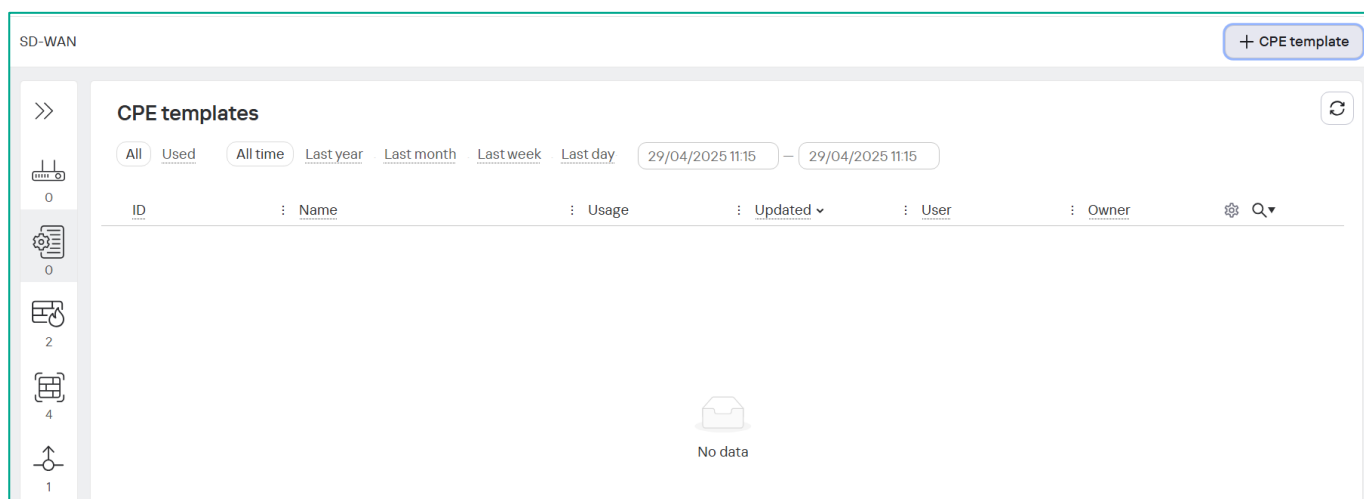
Для SD-WAN шлюзов используются отдельные шаблоны CPE.

Подключиться к portalу самообслуживания тенанта, созданному в 4.4.1 (в PoC используется тенант **Demolab**), для этого нажать кнопку **Connect as Tenant** из меню **Tenants** или подключиться к SD-WAN оркестратору администратором созданного тенанта.

Note: При создании шаблонов из портала администратора они не будут доступны пользователям с правами tenant.

Перейти в меню **SD-WAN → CPE templates**.

Нажать кнопку **+ CPE Template**.



В поле **Name** задать имя шлюза: **vGW-11**.

Установить значение **Type: CPE**

Нажать **Create**.

New CPE template

Name

vGW-11

Type

CPE

Create

Cancel

Для шлюза vGW-12 будет создан отдельный шаблон.

4.6.2. Задать параметры multipathing в шаблоне vGW-11.

Открыть созданный шаблон.

Перейти в меню **Multipathing**.

- Оставить параметры по умолчанию: **8/2/10**.
- Выключить параметр **Multi-weight balancing** (не будет производится балансировка трафика с учетом веса путей).

Более подробно про настройку multipathing можно узнать в SD-WAN Online Help:

<https://support.kaspersky.com/help/SD-WAN/2.4/ru-RU/243185.htm>

The screenshot shows the 'vGW-11' configuration window with the 'Multipathing' tab selected. The left sidebar lists 'Information', 'Multipathing', 'Deactivation', 'Encryption', 'Scripts', 'SD-WAN', and 'Topology'. The main area contains three dropdown menus: 'Maximum number of paths' set to 8, 'Auto-SPF maximum' set to 2, and 'Cost variance multiplier' set to 10.0. Below these is an unchecked checkbox for 'Multi-weight balancing'. At the bottom are 'Save' and 'Cancel' buttons.

4.6.3. Задать параметры шифрования в шаблоне vGW-11.

Перейти в меню **Encryption**.

Включить шифрование: **Enabled**.

The screenshot shows the 'vGW-11' configuration window with the 'Encryption' tab selected. The left sidebar lists 'Information', 'Multipathing', 'Deactivation', 'Encryption', 'Scripts', 'SD-WAN', and 'Topology'. The main area contains a 'Default encryption policy' dropdown menu set to 'Enabled'. At the bottom are 'Save' and 'Cancel' buttons.

4.6.4. Задать параметры SD-WAN в шаблоне vGW-11.

Перейти на вкладку **SD-WAN → General settings**.

Задать адрес для подключения к оркестратору (в PoC требуется задать адрес хоста orc1 после NAT, также возможно использовать доменное имя для подключения).

- **Orchestrator IP address /FQDN: 10.50.1.14.**
- **Orchestrator port: 443.**
- **OpenFlow transport: ssl.**
- **Control SD-WAN interface: sdwan0.**
- Изменить IP-адрес **192.168.7.1** в **Configuration URL** на **10.1.3.11**.

vGW-11

Information

Multipathing

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

PBR

BFD

Static routes

Multicast

VRRP

CFM

Monitoring

Transport services

Log files

General settings Interfaces

Connection to orchestrator

Orchestrator IP address/FQDN

10.50.1.14

Orchestrator port

443

☐ Backup orchestrator IP address and port

Orchestrator protocol

https

Update interval (sec)

30

Interactive update interval (sec)

3

Interactive mode timeout (sec)

180

Connection to controller

OpenFlow transport

SSL

Control SD-WAN interface

sdwan0

☐ Preemption

Auto-reboot

No

Reboot timeout (sec)

86400

Configuration URL

http://10.1.3.11/cgi-bin/config?payload={config}

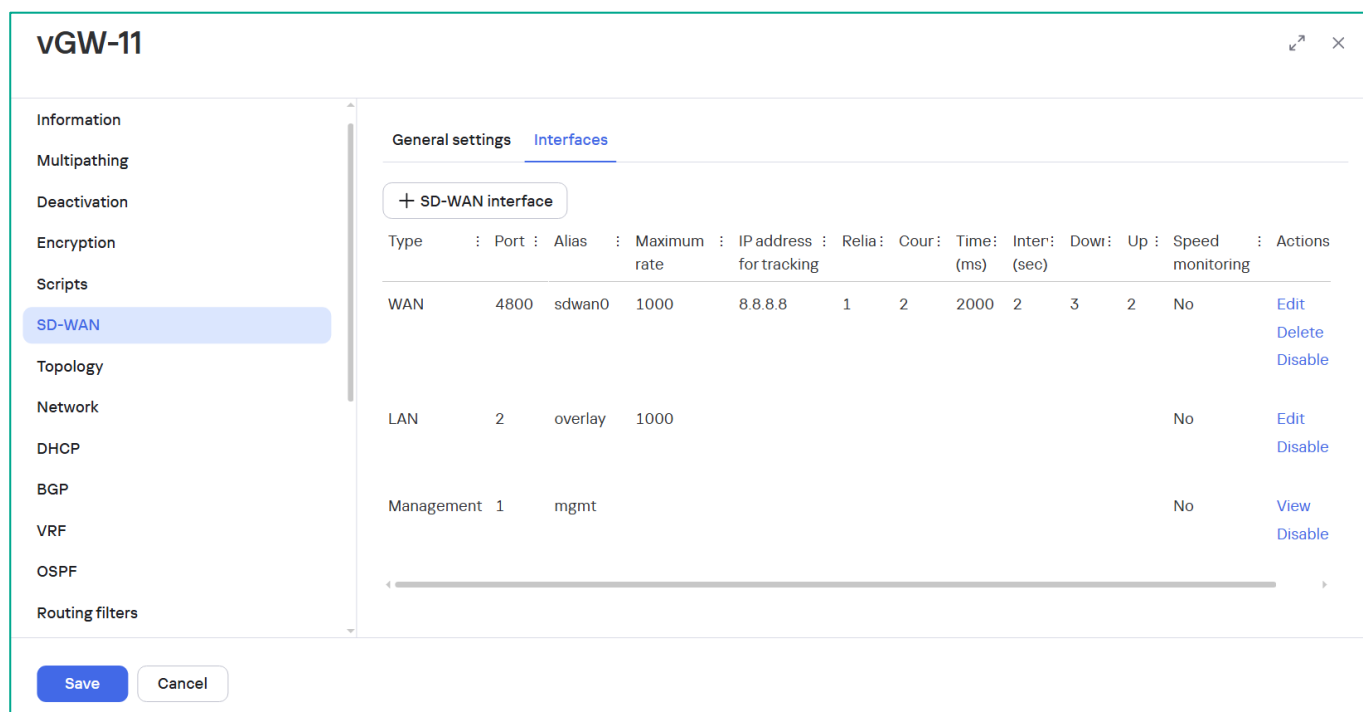
Save

Cancel

4.6.5. Настроить SD-WAN интерфейсы в шаблоне vGW-11.

Перейти на вкладку **SD-WAN → Interfaces**.

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



Задать параметры сетевого интерфейса **sdwan0**.

Открыть для редактирования интерфейс **sdwan0** – нажать **Edit** для **sdwan0**.

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

Нажать **Save**.

В случае недоступности tracking IP, устройства CPE считают сетевой интерфейс не работоспособным и не будут строить через него линки. В таком случае метрика маршрута с данного интерфейса будет равна 21.

SD-WAN interface ×

General settings QoS NAT and disjoint WAN underlay Controllers

Type
WAN

OpenFlow port: 4800

Interface (alias): sdwan0

Maximum rate: 1000

IP address for tracking: 8.8.8.8 ×

IP address for fragmentation check: 1.1.1.1

+ Add

Reliability: 1

Interval (sec): 2

Count: 2

Timeout (ms): 2000

Down: 3

Up: 2

Speed monitoring: No

Save Cancel

4.6.6. Настроить роль CPE в шаблоне vGW-11.

Перейти на вкладку **Topology**.

Задать роль: **Gateway**.

vGW-11 ↗ ×

Information

Multipathing

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

Role: Gateway

Save Cancel

4.6.7. Настроить сетевые интерфейсы в шаблоне vGW-11.

Перейти на вкладку **Network**.

Далее требуется создать следующие сетевые интерфейсы:

- **sdwan0: eth0.**
- **lan: eth1.**
- **overlay: overlay.**
- **nfvmgmt: mgmt.**

Для создания нового интерфейса нажать **+ Network interface**. Параметры интерфейсов описываются дальше.

vGW-11

Information

Multipathing

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

PBR

BFD

Static routes

+ Network interface

Alias	Zone	Interface name	Protocol	IP address/mask	MTU	Enable automatically	Actions
lan	lan	eth1	Static IPv4 address	IP address: 10.1.3.11 Mask: 255.255.255.0		Yes	Edit Delete Disable
nfvmgmt	mgmt_gw	mgmt	None			Yes	Edit Delete Disable
overlay	lan	overlay	Static IPv4 address	IP address: 172.16.1.11 Mask: 255.255.255.0		Yes	Edit Delete Disable
sdwan0	wan	eth0	Static IPv4 address	IP address: 10.1.4.11 Mask: 255.255.255.0		Yes	Edit Delete Disable

Save

Cancel

Добавить сетевой интерфейс **lan** со следующими параметрами:

- **Alias:** lan.
- **Zone:** lan.
- **Interface name:** eth1.
- **Protocol:** Static IPv4 address.
- **IPv4 address:** 10.1.3.11/24.

Нажать **Create** для создания интерфейса.

The screenshot shows the 'New network interface' dialog box. The 'Alias' field is 'lan', the 'Zone' is 'lan (Demolab)', and the 'Interface name' is 'eth1'. The 'Protocol' is set to 'Static IPv4 address'. Under 'Settings', 'Enable automatically' is checked. The 'IPv4 address' is '10.1.3.11' and the 'IPv4 netmask' is '255.255.255.0'. The 'Create' button is highlighted in blue.

Добавить сетевой интерфейс **overlay** со следующими параметрами:

- **Alias:** overlay.
- **Zone:** lan.
- **Interface name:** overlay.
- **Protocol:** Static IPv4 address.
- **IPv4 address:** 172.16.1.11/24.
- Отметить **Generate MAC address automatically**. При этой настройке MAC адрес интерфейса сгенерируется автоматически из пула и будет сохраняться после перезагрузки устройства, что позволит не изучать заново MAC адреса смежным устройствам и ускорит время сходимости протоколов маршрутизации.

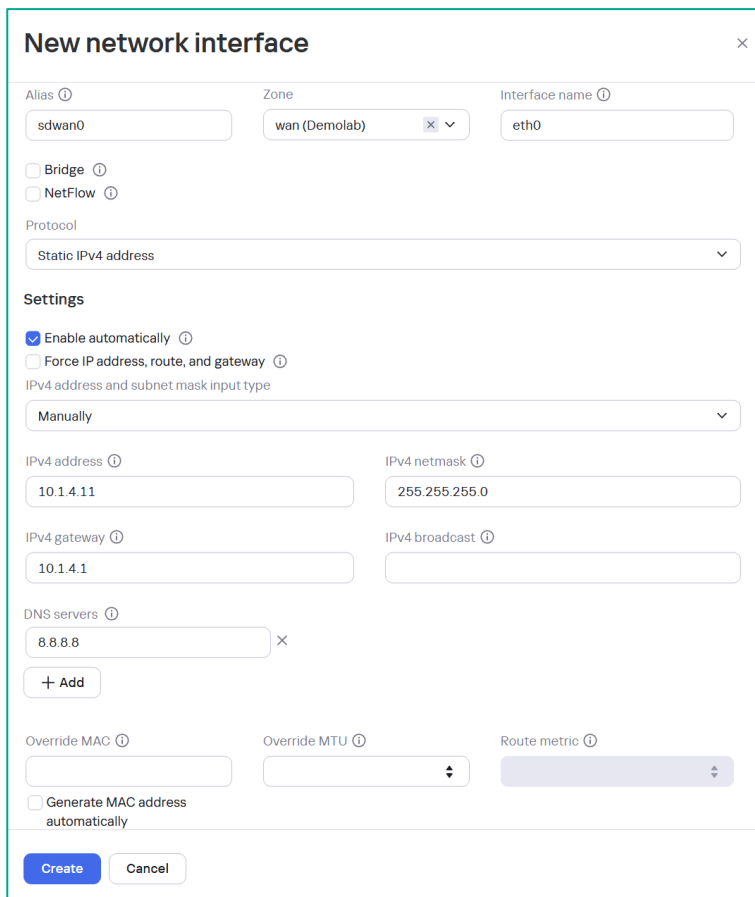
Нажать **Create** для создания интерфейса.

The screenshot shows the 'New network interface' dialog box for the 'overlay' interface. The 'Alias' is 'overlay', the 'Zone' is 'lan (Demolab)', and the 'Interface name' is 'overlay'. The 'Protocol' is 'Static IPv4 address'. Under 'Settings', 'Enable automatically' is checked, and 'Generate MAC address automatically' is also checked. The 'IPv4 address' is '172.16.1.11' and the 'IPv4 netmask' is '255.255.255.0'. The 'Create' button is highlighted in blue.

Добавить сетевой интерфейс **sdwan0**:

- **Alias:** sdwan0.
- **Zone:** wan.
- **Interface name:** eth0.
- **Protocol:** Static IPv4 address.
- **IPv4 address:** 10.1.4.11/24.
- **IPv4 gateway:** 10.1.4.1.
- **DNS servers:** 8.8.8.8.

Нажать **Create** для создания интерфейса.



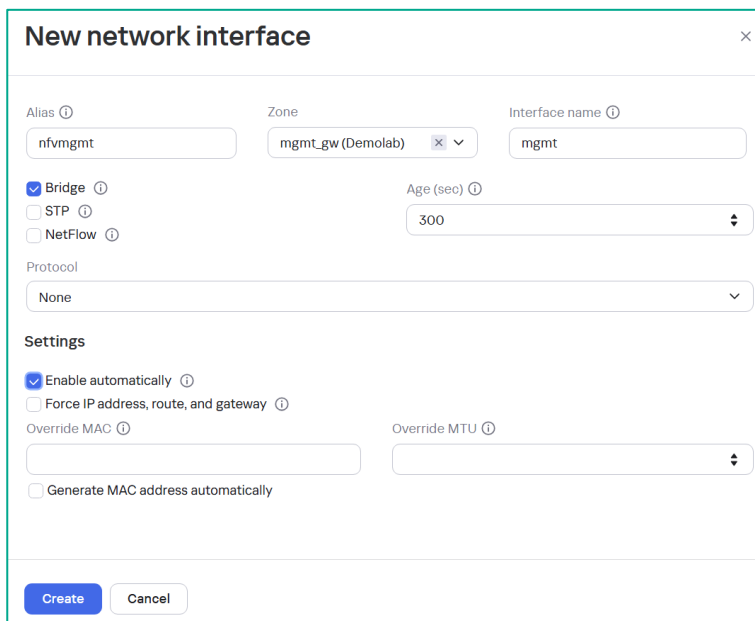
The screenshot shows the 'New network interface' configuration window. The 'Alias' is 'sdwan0', the 'Zone' is 'wan (Demolab)', and the 'Interface name' is 'eth0'. The 'Bridge' checkbox is unchecked, and 'NetFlow' is also unchecked. The 'Protocol' is set to 'Static IPv4 address'. Under 'Settings', 'Enable automatically' is checked, and 'Force IP address, route, and gateway' is unchecked. The 'IPv4 address and subnet mask input type' is set to 'Manually'. The 'IPv4 address' is '10.1.4.11', the 'IPv4 netmask' is '255.255.255.0', the 'IPv4 gateway' is '10.1.4.1', and the 'IPv4 broadcast' is empty. The 'DNS servers' list contains '8.8.8.8'. The 'Override MAC' and 'Override MTU' fields are empty, and 'Route metric' is set to 1. The 'Generate MAC address automatically' checkbox is unchecked. The 'Create' button is highlighted in blue.

Добавить сетевой интерфейс **nfvmgmt**:

- **Alias:** nfvmgmt.
- **Zone:** mgmt_gw.
- **Interface name:** mgmt.
- Отметить **Bridge**.
- **Age:** 300.
- **Protocol:** None.
- Отметить **Enable automatically**.

Данный интерфейс создан для обеспечения связности сети mgmt на CPE и хоста orcl (требуется для работы SSH консоли из веб-интерфейса оркестратора).

Нажать **Create** для создания интерфейса.



The screenshot shows the 'New network interface' configuration window. The 'Alias' is 'nfvmgmt', the 'Zone' is 'mgmt_gw (Demolab)', and the 'Interface name' is 'mgmt'. The 'Bridge' checkbox is checked, and 'STP' and 'NetFlow' are unchecked. The 'Age (sec)' is set to 300. The 'Protocol' is set to 'None'. Under 'Settings', 'Enable automatically' is checked, and 'Force IP address, route, and gateway' is unchecked. The 'Override MAC' and 'Override MTU' fields are empty. The 'Generate MAC address automatically' checkbox is unchecked. The 'Create' button is highlighted in blue.

4.6.8. Настроить параметры CFM в шаблоне vGW-11.

Функция Connectivity Fault Management позволяет обнаруживать недоступные линки между устройствами CPE. Когда функция CFM включена, устройство CPE отправляет контрольные пакеты Continuity Check Message (CCM) через линки до других CPE с указанным интервалом времени и ожидает получения ответных контрольных пакетов через встречные линки. При отсутствии ответных контрольных пакетов устройство CPE считает линк нерабочим и начинает передавать трафик по случайно выбранному доступному линку.

Перейти на вкладку **CFM**.

Задать:

- **CFM: Enabled** (включить CFM для линков) .
- **Interval: 300 ms** (интервал отправки контрольных пакетов CFM) .

The screenshot shows the 'vGW-11' configuration window with the 'CFM' tab selected in the left sidebar. The sidebar also lists 'Routing filters', 'PBR', 'BFD', 'Static routes', 'Multicast', 'VRRP', and 'Monitoring'. In the main area, there are two dropdown menus: 'CFM' set to 'Enabled' and 'Interval' set to '300 ms'. At the bottom, there are 'Save' and 'Cancel' buttons.

4.6.9. Настроить параметры мониторинга в шаблоне vGW-11.

Перейти на вкладку **Monitoring**.

Задать:

- **Monitoring type: Agent**.
- **Zabbix template: Linux by Zabbix agent active**.

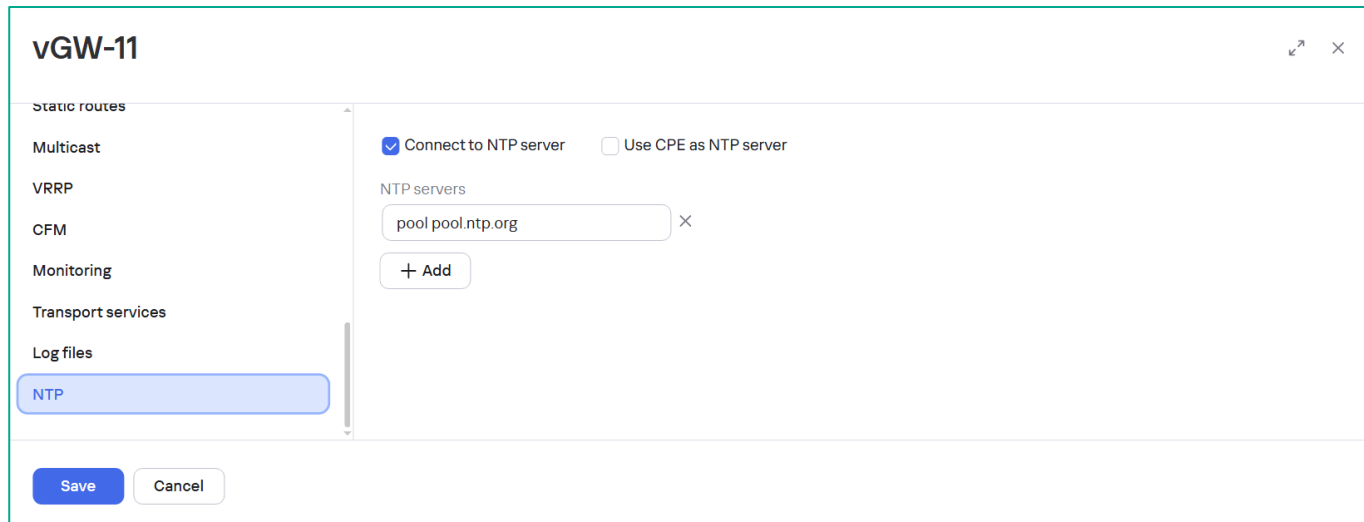
The screenshot shows the 'vGW-11' configuration window with the 'Monitoring' tab selected in the left sidebar. The sidebar also lists 'Static routes', 'Multicast', 'VRRP', 'CFM', and 'Transport services'. In the main area, there are two dropdown menus: 'Monitoring type' set to 'Agent' and 'Zabbix template' set to 'Linux by Zabbix agent active'. At the bottom, there are 'Save' and 'Cancel' buttons.

4.6.10. Настроить параметры NTP в шаблоне vGW-11.

Перейти на вкладку **NTP**.

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

Задать адреса NTP серверов или использовать настройки по умолчанию.



The screenshot shows the 'vGW-11' configuration window. On the left is a sidebar with a list of configuration categories: Static routes, Multicast, VRRP, CFM, Monitoring, Transport services, Log files, and NTP. The 'NTP' category is selected and highlighted in blue. The main area of the window displays the NTP configuration. At the top, there are two checkboxes: 'Connect to NTP server' (checked) and 'Use CPE as NTP server' (unchecked). Below these is a section labeled 'NTP servers' containing a text input field with the value 'pool pool.ntp.org' and a small 'x' icon to its right. Below the input field is a button labeled '+ Add'. At the bottom of the window are two buttons: 'Save' and 'Cancel'.

4.6.11. Создать Prefix List в шаблоне vGW-11

Перейти на вкладку **Routing filters** → **Prefix lists**.

Нажать **+ Prefix List**

Задать **Name: dc-net-list**

Нажать **+ 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 10.11.13.0/24.**

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

New prefix list

Name ⓘ
dc-net-list

+ Rule

Sequence	Network	Action	Greater or equal	Less or equal	
10	IP addre... ▾	10.0.1.0/24	Permit ▾		×
20	IP addre... ▾	10.1.1.0/24	Permit ▾		×
30	IP addre... ▾	10.1.3.0/24	Permit ▾		×
40	IP addre... ▾	10.11.13.0/24	Permit ▾		×

Create Cancel

Нажать **Create**.

4.6.12. Создать Route Map в шаблоне vGW-11.

Перейти на вкладку **Routing filters** → **Route maps**.

Нажать **+ Route Map**.

Задать **Name: dc-route-map**

Нажать **+ Rule** и задать параметры правила:

- **Sequence: 10.**
- **Action: Permit.**
- **Match Type: Prefix-list.**
- **Prefix list: dc-net-list.**

Нажать **Create**.

The screenshot shows the 'vGW-11' configuration page on the left and a 'New route map' dialog box on the right. The dialog box has a close button (X) in the top right corner. Inside the dialog, the 'Name' field is set to 'dc-route-map'. Below this is a '+ Rule' button. A table with one row is displayed, showing the rule configuration:

Sequence	Action	Match type	Value	Change attribute	New value
10	Permit	Prefix-L...	805dc020-24df-11	None	

Below the table, the 'Prefix list' is set to 'dc-net-list'. At the bottom of the dialog, there are 'Create' and 'Cancel' buttons. The background shows the 'vGW-11' configuration page with the 'Routing filters' tab selected.

4.6.13. Настроить BGP в шаблоне vGW-11.

Перейти в меню вкладку **BGP**.

Задать номер автономной системы: **Autonomous System** → **65500**.

Нажать **+ BGP** для добавления нового экземпляра BGP.

The screenshot shows the configuration window for vGW-11. On the left is a sidebar with a list of configuration tabs: Deactivation, Encryption, Scripts, SD-WAN, Topology, Network, DHCP, BGP (selected), VRF, and OSPF. The main area is titled 'vGW-11' and contains the following settings:

- Autonomous System:** A dropdown menu with the value '65500'.
- Default BGP Instance with VRF:** A dropdown menu with a downward arrow.
- + BGP:** A button to add a new BGP instance.
- Table:** A table with columns: State, VRF, Router ID, BGP neighbor, Peer groups, Route Distinguisher, Export routes, Import routes, and A. The table is currently empty, showing 'No data'.

At the bottom of the window are two buttons: 'Save' and 'Cancel'.

Перейти на вкладку **General settings**.

Задать параметры BGP:

- **BGP: Enabled.**
- **Router ID: 172.16.1.11** (IP-адрес сетевого интерфейса overlay).
- **Maximum Paths: 2.**
- **Graceful Restart.**
- **Default IPv4 Unicast.**
- **BGP Timers:**
 - **Keepalive: 10.**
 - **Holdtime: 30.**

Включить редистрибуцию **Connected** маршрутов. Применить **Route map: dc-route-map** к **Connected** маршрутам.

BGP instance

[General settings](#) [Neighbors](#) [Peer groups](#) [Route leaking](#)

BGP

Enabled

VRF

main/254

AS

65500

Router ID

172.16.1.11

☐ Router ID from IP pool

Maximum paths

2

☐ Always compare MED

☒ Graceful restart (helper mode)

☒ Use default IPv4 unicast routes

☒ BGP timers

Keepalive (sec)

10

Holdtime (sec)

30

Route redistribution

☐ Kernel

Route map

Metric

☒ Connected

Route map

dc-route-map

Metric

Save

Cancel

4.6.14. Настроить группу соседей BGP, которая будет использоваться vGW-11 для установления BGP-соседства с устройствами CPE.

Перейти на вкладку **BGP → Peer groups**.

Нажать **+ Peer group**.

Задать параметры:

- **Name:** CPE.
- **BGP Range:** 172.16.1.0/24 (сеть overlay) .
- **Remote AS:** 65500.

The screenshot shows the 'New peer group' dialog box with the 'General settings' tab selected. The 'Name' field contains 'CPE'. The 'Shutdown peer group' checkbox is unchecked. The 'BGP range' field contains '172.16.1.0/24'. The 'Remote AS' field contains '65500'.

Перейти на вкладку **Advanced Settings**.

Отметить **Route Reflector Client**.

The screenshot shows the 'New peer group' dialog box with the 'Advanced settings' tab selected. The 'Route reflector client' checkbox is checked. Other checkboxes include 'Soft-reconfiguration inbound', 'Allow AS in', 'Next-hop self', 'Attribute unchanged AS path', 'Attribute unchanged next-hop', and 'Attribute unchanged MED', all of which are unchecked. The 'Local AS', 'Weight', and 'Maximum prefix' fields are empty. The 'Send community' and 'Default originate' checkboxes are also unchecked. At the bottom, there are 'Create' and 'Cancel' buttons.

Нажать **Create**.

4.6.15. Создать BGP соседства от vGW-11 до R13 и vGW-12.

Перейти на вкладку **Neighbors** и нажать **+ BGP Neighbor**.

Создать 2 BGP соседа.

Задать параметры:

- **Name: R13.**
- **Neighbor IP: 10.1.3.13.**
- **Remote AS: 65613.**
- **Name: vGW-12.**
- **Neighbor IP: 10.1.3.12.**
- **Remote AS: 65500.**

BGP instance

General settings **Neighbors** Peer groups Route leaking

+ BGP neighbor

Neighbor IP	Name	Description	Remote AS	Shutdown	Weight	Actions
10.1.3.12	vGW-12		65500	No		Edit Delete
10.1.3.13	R13		65613	No		Edit Delete

Save

Cancel

Нажать **Save** для сохранения экземпляра BGP.

Задать **Default BGP Instance with VRF: main/254** (VRF по умолчанию для экземпляров BGP, используется для обратной совместимости со старыми версиями устройств CPE).

Нажать **Save** для сохранения шаблона.

vGW-11

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

Autonomous System: 65500

Default BGP Instance with VRF: main/254

+ BGP

	Router ID	BGP neighbor	Peer groups	Route Distinguisher	Export routes	Import routes	Actions
4	172.16.1.11	2	1	65500:254	Off	Off	Edit Delete

Save Cancel

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

Открыть шаблон **vGW-11**, перейти в меню **Information**, нажать **Export** и скачать файл с шаблоном.

vGW-11

Information

Multipathing

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

Delete Import **Export** Clone Export SD-WAN settings Export network interfaces

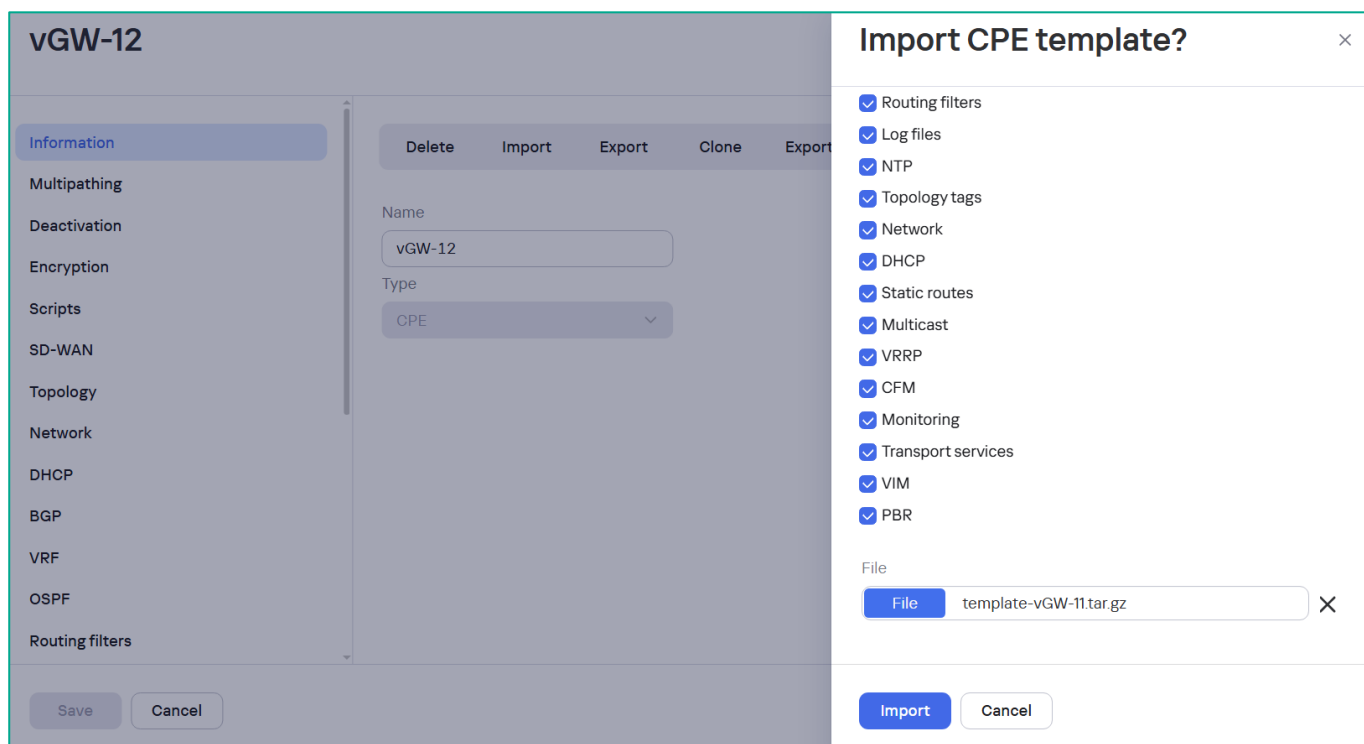
Name: vGW-11

Type: CPE

Save Cancel

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

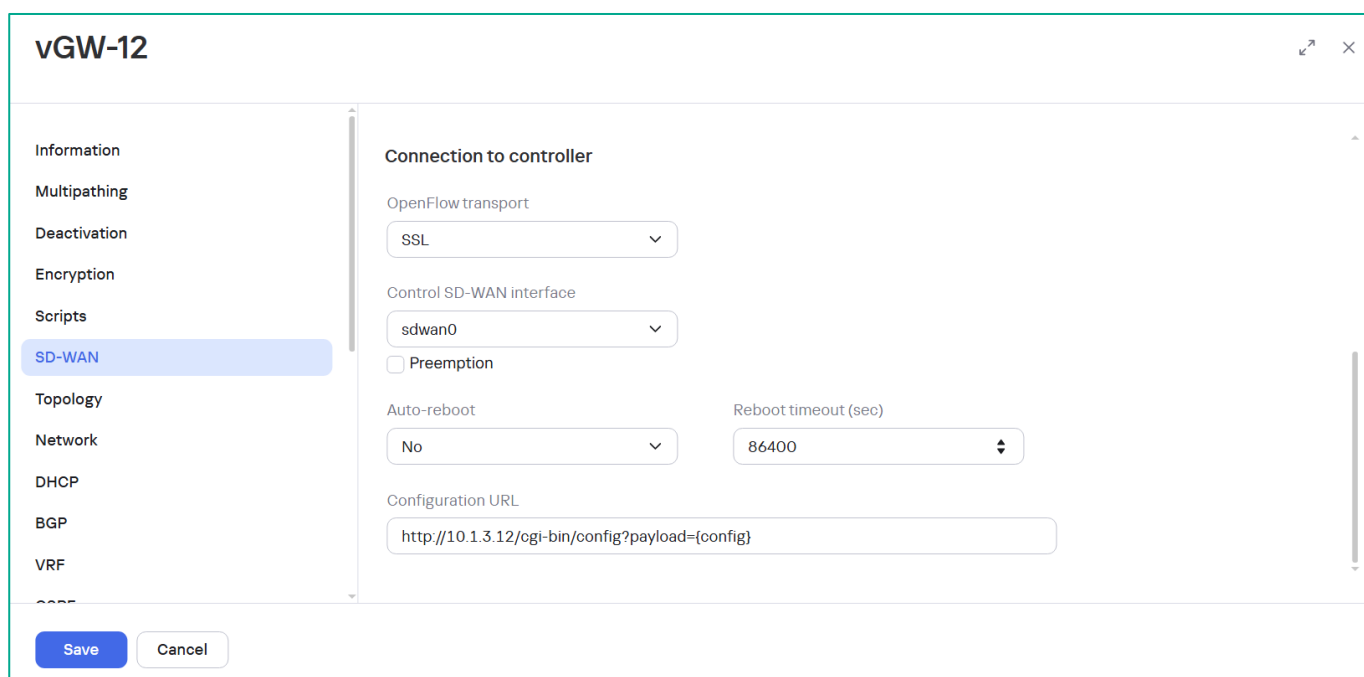
Создать новый шаблон для vGW-12, затем повторить шаги 4.6.1 – 4.6.15 или выполнить импорт шаблона vGW-11. Для этого создать шаблон vGW-12, затем внутри шаблона нажать **Import** и выбрать файл: **template-vGW-11.tar.gz**, затем нажать **Import**.



Также возможно скопировать (**Clone**) шаблон vGW-11 в шаблон vGW-12.

4.6.18. Адаптировать шаблон для шлюза vGW-12.

На вкладке **SD-WAN** → **General settings** изменить IP-адрес **10.1.3.11** в **Configuration URL** на **10.1.3.12**



На вкладке **Network** изменить параметры сетевых интерфейсов:

- **sdwan0 IPv4 address: 10.1.5.12/24.**
- **sdwan0 IPv4 gateway: 10.1.5.1.**
- **lan IPv4 address: 10.1.3.12/24.**
- **overlay IPv4 address: 172.16.1.12/24.**

vGW-12

Information

Multipathing

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

PBR

BFD

+ Network interface

Alias	Zone	Interface name	Protocol	IP address/mask	MTU	Enable automaticall	Actions
lan	lan	eth1	Static IPv4 address	IP address: 10.1.3.12 Mask: 255.255.255.0		Yes	<a>Edit <a>Delete <a>Disable
nfvmgmt	mgmt_gw	mgmt	None			Yes	<a>Edit <a>Delete <a>Disable
overlay	lan	overlay	Static IPv4 address	IP address: 172.16.1.12 Mask: 255.255.255.0		Yes	<a>Edit <a>Delete <a>Disable
sdwan0	wan	eth0	Static IPv4 address	IP address: 10.1.5.12 Mask: 255.255.255.0 GW: 10.1.5.1		Yes	<a>Edit <a>Delete <a>Disable

Save

Cancel

Открыть экземпляр BGP для редактирования: перейти в меню **BGP** и нажать **Edit** для экземпляра BGP.

vGW-12

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

Autonomous System: 65500

Default BGP Instance with VRF: main/254

+ BGP

State	VRF	Router ID	BGP neighbor	Peer groups	Route Distinguisher	Export routes	Import routes	Actions
Enabled	main/254	172.16.1.11	2	1	65500:254	Off	Off	Edit Delete

Save Cancel

В экземпляре **BGP** изменить **Router ID: 172.16.1.12**.

BGP instance

General settings Neighbors Peer groups Route leaking

BGP: Enabled

VRF: main/254

AS: 65500

Router ID: 172.16.1.12

☐ Router ID from IP pool

Maximum paths: 2

☐ Always compare MED ☐ Graceful restart (helper mode) ☒ Use default IPv4 unicast routes

Save Cancel

На вкладке **Neighbors** изменить параметры BGP соседей:

Заменить **vGW-12** на **vGW-11** (IP-адрес **10.1.3.11**).

BGP instance

General settings **Neighbors** Peer groups Route leaking

+ BGP neighbor

Neighbor IP	Name	Description	Remote AS	Shutdown	Weight	Actions
10.1.3.11	vGW-11		65500	No		Edit Delete
10.1.3.13	R13		65613	No		Edit Delete

Save

Cancel

Нажать **Save** для сохранения изменений в экземпляре BGP, затем нажать **Save** для сохранения изменений в шаблоне.

4.7. Импорт сертификата СА для устройств CPE

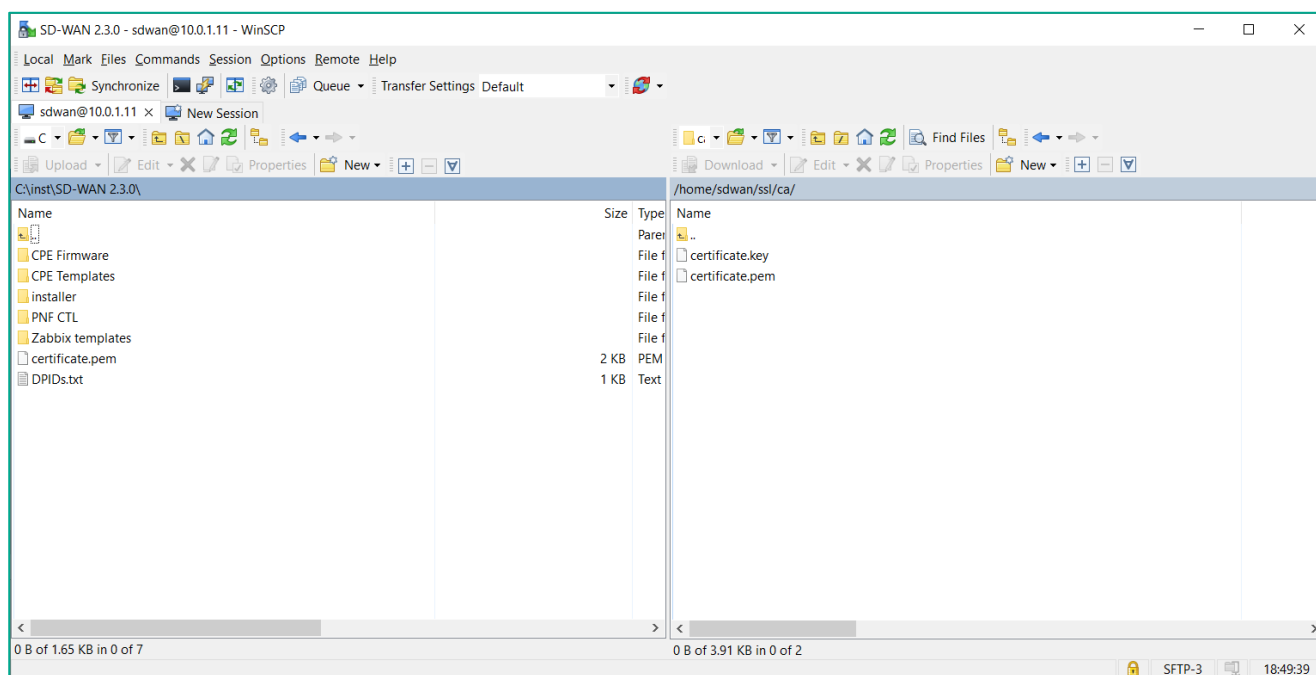
Для предотвращения MITM-атак (англ. Man in the middle) при обращении к оркестратору устройство CPE проверяет, можно ли доверять сертификату оркестратора. По умолчанию на устройствах CPE установлены корневые сертификаты публичных центров сертификации. Если для оркестратора используется сертификат, подписанный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

Более подробно можно узнать в SD-WAN Online Help: Загрузка сертификата в веб-интерфейс оркестратора: <https://support.kaspersky.com/help/SD-WAN/2.4/ru-RU/270629.htm>

4.7.1. Скачать корневой сертификат СА.

В процессе установки системы управления SD-WAN корневой сертификат СА был сохранен в файл: **/home/sdwan/ssl/ca/certificate.pem**

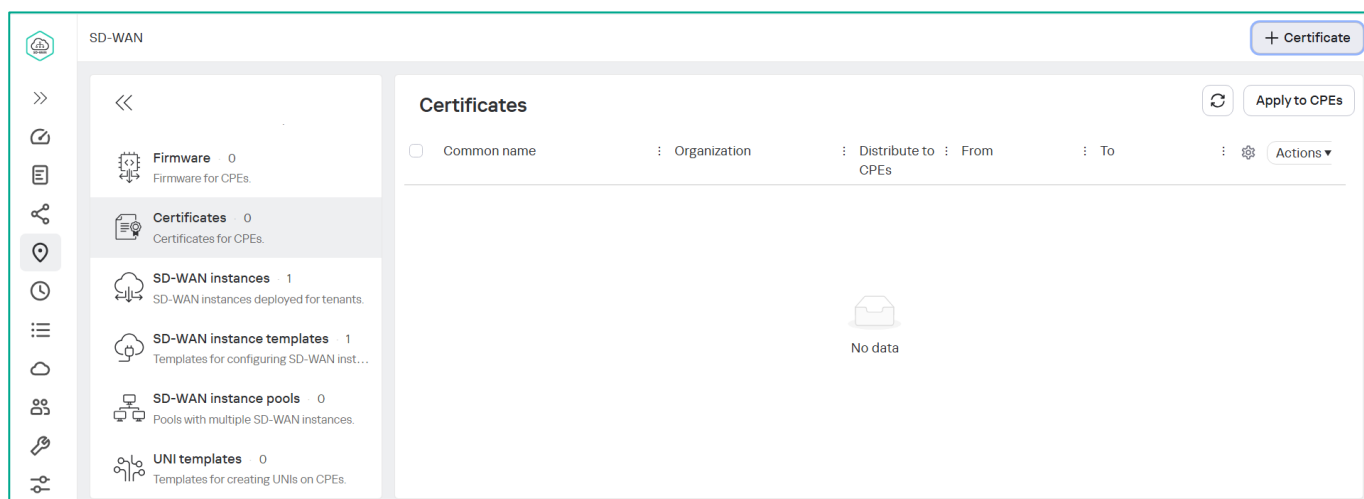
Скачать сертификат с хоста orc1, например, с использованием WinSCP.



4.7.2. Загрузить корневой сертификат в оркестратор.

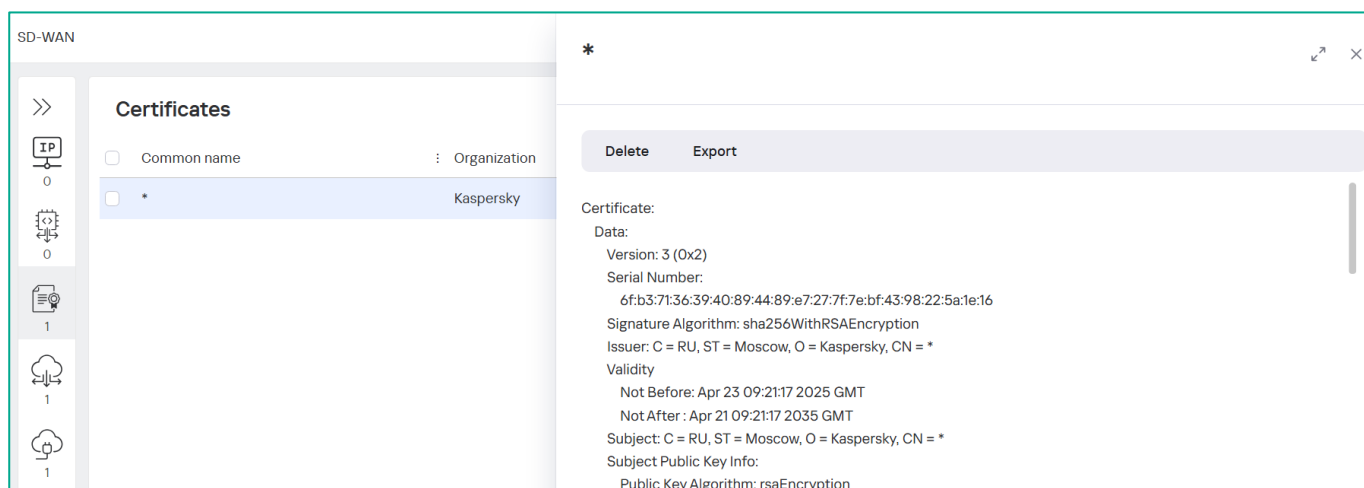
Под администратором перейти в меню **SD-WAN → Certificates**.

Нажать **+Certificate**, выбрать **.pem** файл сертификата CA для загрузки.



4.7.3. Проверить загруженный сертификат.

Нажать на загруженный сертификат для его отображения.



4.8. Подготовка SD-WAN шлюзов

4.8.1. Развернуть VM vGW-11 и vGW-12 из образа CPE vKESR-M2 (knaas-cpe.<release_name>.combined.amd64-vkesr-m2.vKESR-M2-esxi.tar.gz).

Deploy OVF Template

- Select an OVF template**
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

☒ Local file

UPLOAD FILES 4 files

CANCEL NEXT

Ресурсы виртуальной машины для vKESR-M2:

- 4 x CPU.
- 8 Gb RAM.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details**
- Select storage
- Select networks
- Customize template
- Ready to complete

Review details

Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Product	vCPE
Vendor	Kaspersky Lab
Description	vKESR-M2 vCPU - 4 vRAM - 8192M knaas-cpe_2.24.09.release.23.combined.amd64-vkesr-m2
Download size	Unknown
Size on disk	Unknown (thin provisioned) 1.0 GB (thick provisioned)
Extra configuration	guestinfo.urlactivated = false nvram = ovf:/file/file2

CANCEL BACK NEXT

Назначить сети в соответствии со схемой PoC на рисунке 2:

- **WAN1: DC-EDGE1.**
- **LAN1: DC-PERIM.**
- (Опционально) Удалить адаптер WAN2.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
LAN1	DC-PERIM
WAN1	DC-EDGE1
WAN2	Browse ...

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Повторить предыдущие шаги и развернуть виртуальную машину vGW-12 из образа vKESR-M2

4.8.2. Настроить сетевой интерфейс **lan**.

Открыть консоль к виртуальной машине vGW-11.

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

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

Открыть в редакторе **vi** конфигурационный файл сетевой службы для редактирования:

vi /etc/config/network

Требуется настроить сетевой интерфейс **lan** для применения Configuration URL с рабочей станции mgmt.

Изменить IP-адрес интерфейса **lan** на адрес lan vGW-11 в соответствии с таблицей 1 в п.2.2.

Изменить **ifname** в **lan** на **eth1**.

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

config interface 'lan'
    option type 'bridge'
    option proto 'static'
    option ipaddr '10.1.3.11'
    option netmask '255.255.255.0'
    option ifname 'eth1'
    option auto '1'
    option force_link '1'

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

Перезагрузить сетевую службу:

```
/etc/init.d/network restart
```

Проверить примененные настройки:

```
ip -br a
```

```
root@8000005056891685:/# ip -br a
lo                UNKNOWN      127.0.0.1/8  ::1/128
eth0              UP           10.1.3.176/24  fe80::250:56ff:fe89:1685/64
eth1              UP
ip6tnl0@NONE      DOWN
gre0@NONE         DOWN
gretap0@NONE      DOWN
erspan0@NONE      DOWN
ip6gre0@NONE      DOWN
bond0             DOWN
br-lan            UP           10.1.3.11/24  fe80::250:56ff:fe89:adaa/64
overlay@ovs-lan   UP           fe80::1494:d9ff:fe07:f0fb/64
ovs-lan@overlay   UP           fe80::78a2:65ff:fe39:5fcf/64
mgmt@ovs-mgmt     UP           fe80::bc5c:75ff:feca:e72f/64
ovs-mgmt@mgmt     UP           fe80::98f8:51ff:fe4d:5ba/64
```

Повторить шаги выше и настроить **lan** интерфейс vGW-12.

После регистрации (выполнения configuration URL в пункте 4.9) SD-WAN шлюзы получают и применяют сетевые настройки в соответствии настройками в главе 4.6.

Note: Также возможно передать Configuration URL при разворачивании шлюзов из OVF. Для этого требуется предварительно создать CPE, используя ранее созданные шаблоны шлюзов, с произвольным DPID и получить Configuration URL (описано в п. 4.9). При настройке CPE требуется использовать адрес по умолчанию для Configuration URL – 192.168.7.1. После загрузки, CPE появится в оркестраторе со статусом Unknown. Далее необходимо будет открыть CPE, в меню Configuration нажать Register, затем настроить параметры CPE, как описано в п. 4.9.

4.9. Регистрация SD-WAN шлюзов

4.9.1. Создать vGW-11 в оркестраторе.

Перейти в меню **SD-WAN → CPE**.

Нажать **+ CPE**. Задать:

- Имя SD-WAN шлюза: **vGW-11**.
- **DPID**: Уникальный идентификатор DPID устройства, отображается в командной строке CPE устройства.
- **Transport tenant**: **Demolab** (используется тенант, созданный в п.4.4.1) .
- **Customer tenant**: **Demolab** (используется тенант, созданный в п.4.4.1) .
- **CPE template**: **vGW-11** (шаблон шлюза, созданный в п.4.6) .
- **Firewall template**: **gateway_firewall_template** (шаблон межсетевого экрана, созданный в п.4.5) .

Устройство CPE подключается к контроллеру экземпляра SD-WAN, который был развернут для транспортного тенанта. Из клиентского тенанта возможно управлять устройством CPE на своем портале самообслуживания. Для одного транспортного тенанта возможно существование многих клиентских.

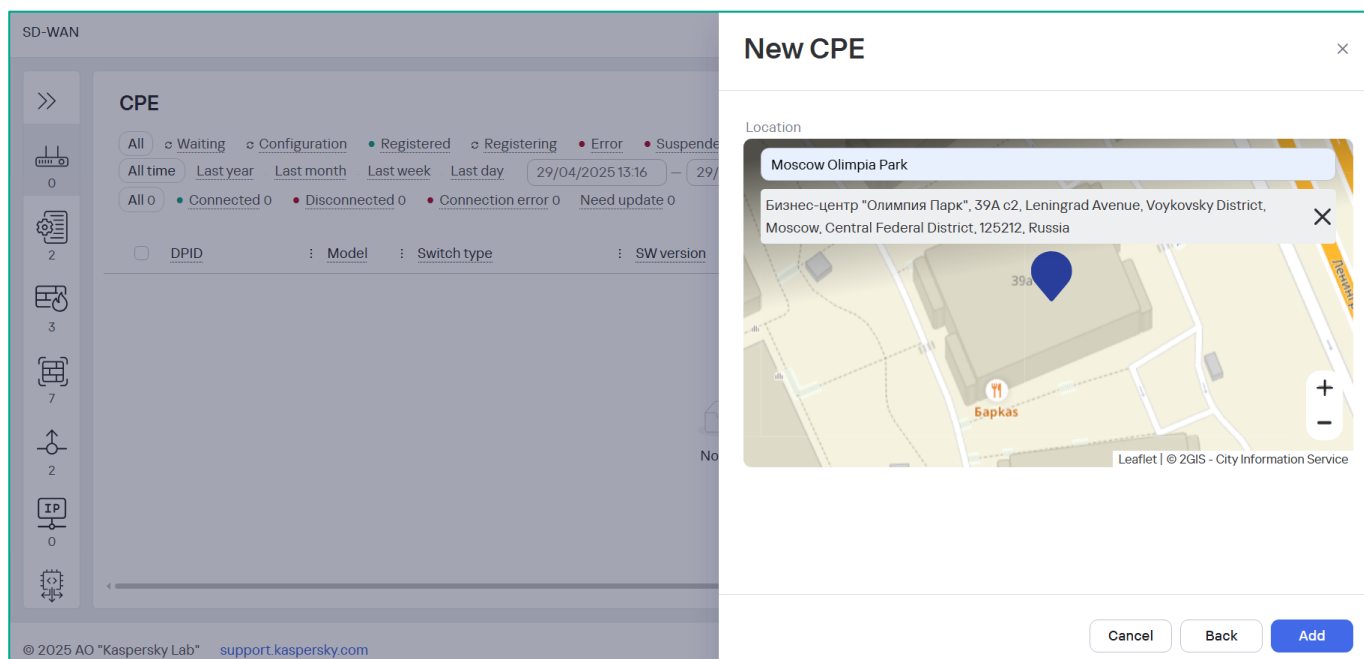
Нажать **Next**.

The screenshot displays the Kaspersky SD-WAN management interface. On the left, the 'SD-WAN' menu is visible with 'CPE' selected. The main area shows a list of CPE devices with filters like 'All', 'Waiting', 'Configuration', 'Registered', etc. Overlaid on this is the 'New CPE' configuration window. This window contains the following fields and values:

- Name**: vGW-11
- DPID**: 8000005056AA9EA5
- State**: Enabled
- Description**: (empty field)
- Transport tenant**: Demolab
- Customer tenant**: Demolab
- UNI template**: (empty dropdown)
- CPE template**: vGW-11
- NetFlow template**: Default NetFlow template
- Firewall template**: gateway_firewall_template (Demolab) (Demolab)

At the bottom of the 'New CPE' window are three buttons: 'Cancel', 'Back', and 'Next'.

Задать расположение устройства (опционально).

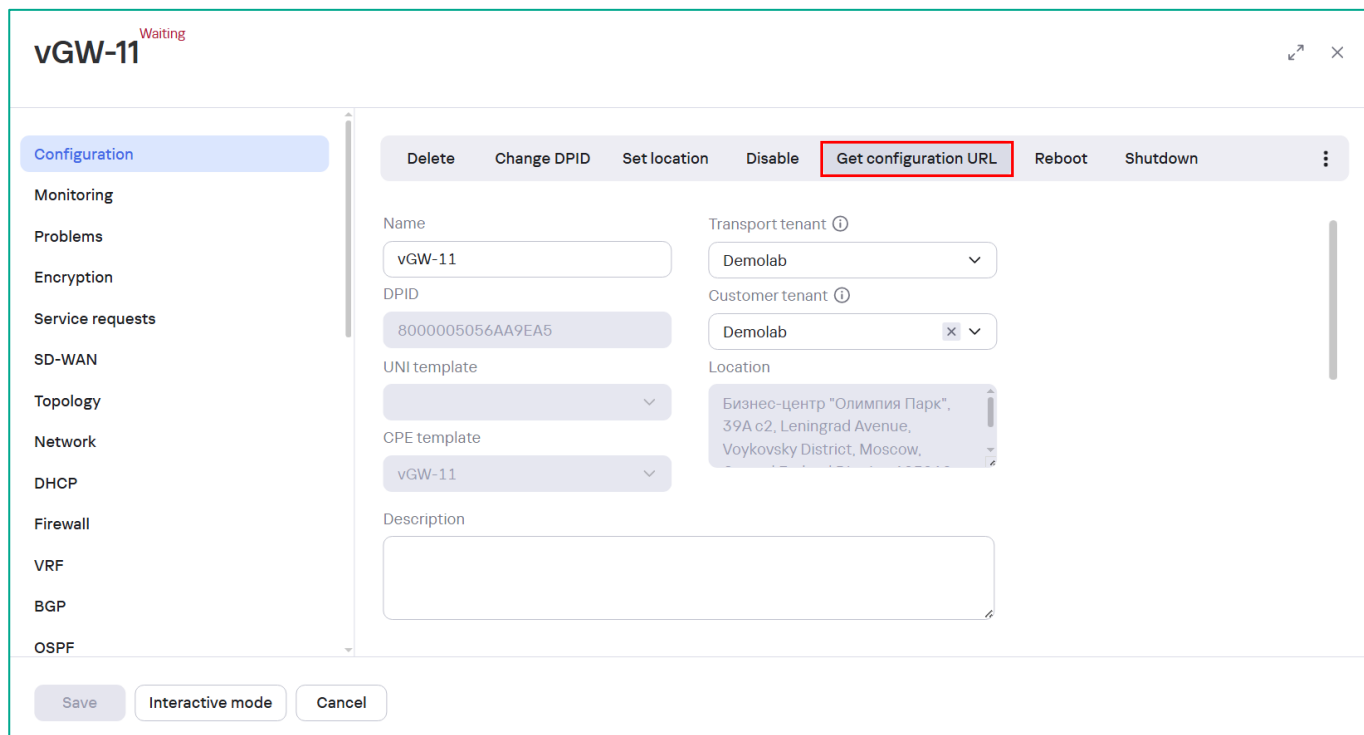


Нажать **Add**.

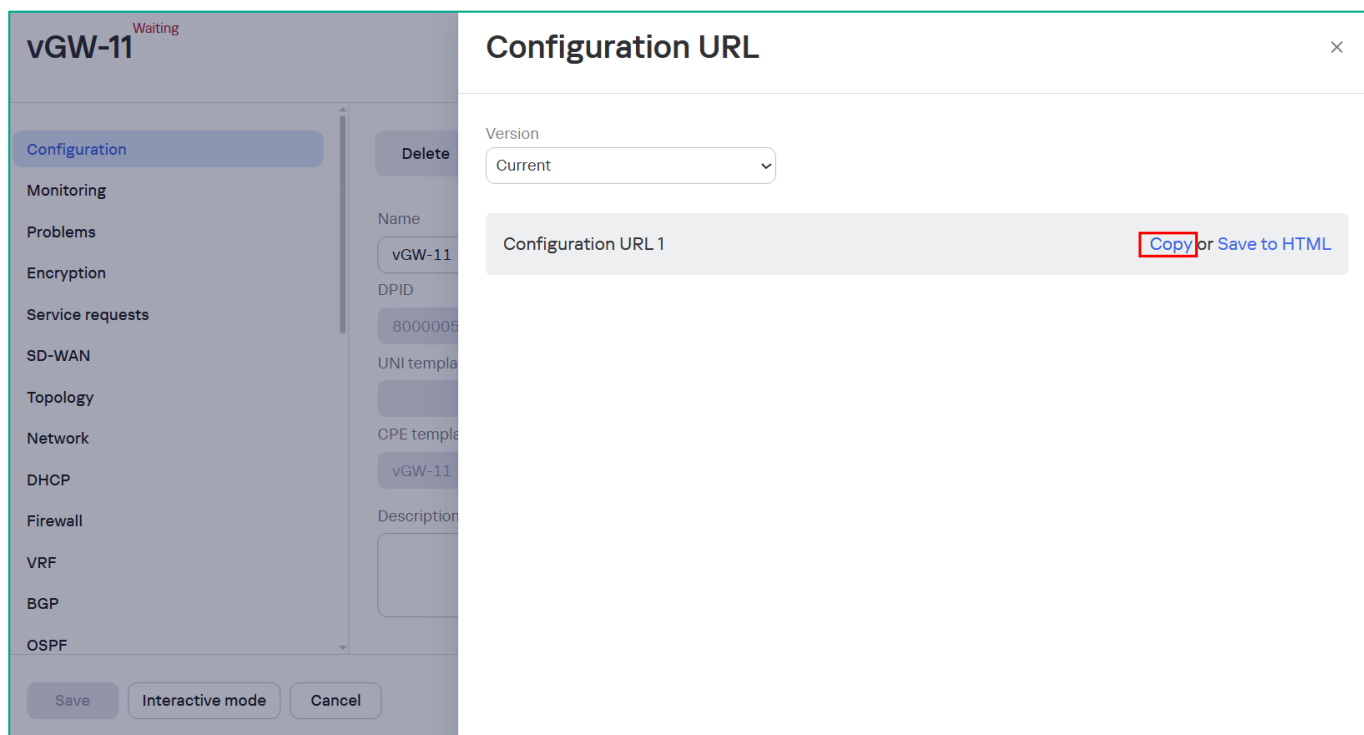
4.9.2. Настроить SD-WAN шлюз vGW-11 при помощи Configuration URL.

Сгенерировать Configuration URL для активации устройства.

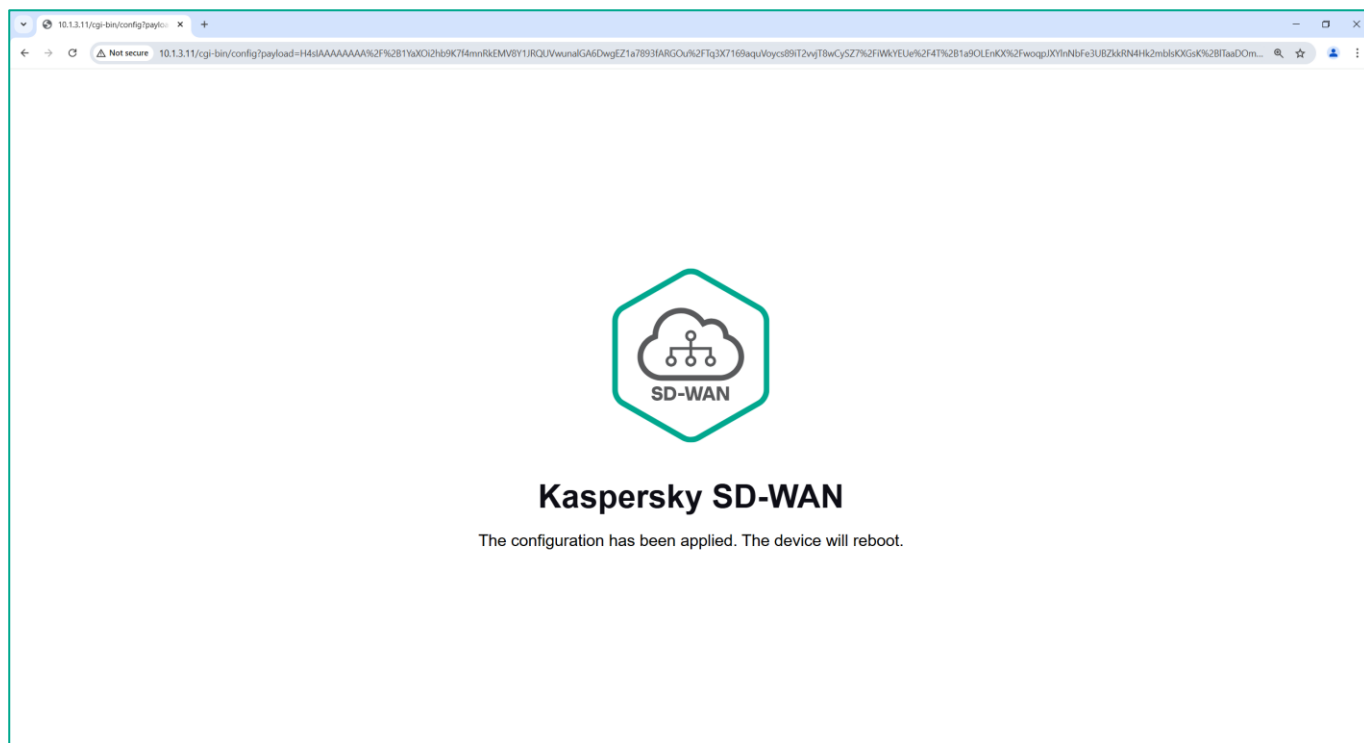
Перейти в меню **SD-WAN** → **CPE**, выбрать SD-WAN шлюз и нажать **Get Configuration URL**.



Скопировать ссылку (нажать **Copy**).



Открыть скопированную ссылку в адресной строке браузера (должна быть связность с интерфейсом lan шлюзов) для применения настроек к vGW-11. Устройство CPE применит настройки и начнётся процесс регистрации.



После перезагрузки CPE перейдет в статус **Registering**.

vGW-11

Registering

Configuration

Monitoring

Problems

Encryption

Service requests

SD-WAN

Topology

Network

DHCP

Firewall

VRF

BGP

OSPF

Delete

Show password

Get configuration URL

Reboot

Shutdown

Export SD-WAN settings

Export network interfaces

Name

vGW-11

Transport tenant ⓘ

Demolab

UNI template

DPID

8000005056AA9EA5

Customer tenant ⓘ

Demolab

CPE template

vGW-11

Location

Бизнес-центр "Олимпия Парк",
39А с2, Leningrad Avenue,
Voykovsky District, Moscow,

Description

NetFlow template

Default NetFlow template

Firewall template

gateway_firewall_template (De...

Save

Interactive mode

Cancel

Появится вкладка **Service Requests**, на которой отображаются сервисные запросы для данного CPE. Будет создан запрос для регистрации CPE.

vGW-11

Registered

Configuration

Monitoring

Problems

Encryption

Service requests

Reload service requests

Cancel all service requests

Delete all service requests

Name	Created	Task ID	Time	Status	Actions
CpeRegistration	29/04/2025 13:26:55	9711850a-1e48-4298-a00f-4b0c74fdd4e4	1m 31s	Executed	Delete

Для получения деталей регистрации нажать на **Task ID** задачи.

CpeRegistration

Created: 29/04/2025 13:26:55

Task ID: 9711850a-1e48-4298-a00f-4b0c74fdd4e4

Time: 1m 31s

Status: Executed

Name	Status	Time	Attributes
CommutatorAttachCommand	Executed	1m 20s	cluster: SD-WAN Cluster [Demolab: 4f7461d3-0a4b-
CommutatorRenameCommand	Executed	0	name: vGW-11: 8000005056AA9EA5
CommutatorUpdatePortsStateSet	Executed	0	
CommutatorUpdatePortStateCommand	Executed	0	number: 4800
CommutatorSetLinksEncryptionCommand	Executed	0	encrypted: true
CommutatorSetCfmCommand	Executed	0	cfmEnabled: true
CommutatorUpdatePublicPortSettingsSet	Executed	0	
CommutatorUpdatePublicPortSettingsCommand	Executed	0	number: 4800
CommutatorSetGeoAddressCommand	Executed	0	

Refresh

Cancel

Устройство CPE перешло в статус **Registered** и **Connected**.

CPE

Export to CSV...

All

Waiting

Configuration

Registered

Registering

Error

Suspended

Unknown

All time

Last year

Last month

Last week

Last day

29/04/2025 13:16

29/04/2025 13:16

All 1

Connected 0

Disconnected 0

Connection error 0

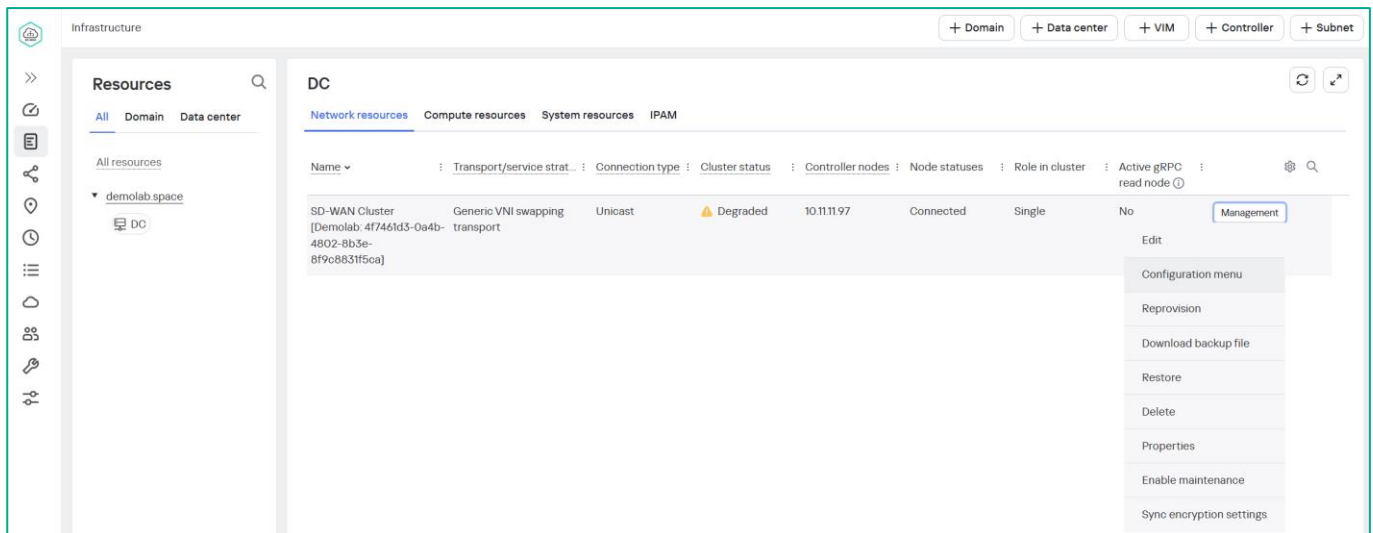
Need update 0

DPID	Model	Switch type	SW version	Name	Role	Status	State	Connection
<input type="checkbox"/> 8000005056AA9EA5	vKESR-M2	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vGW-11	Gateway	Registered	Enabled	Connected

Настройка SD-WAN шлюза vGW-11 завершена.

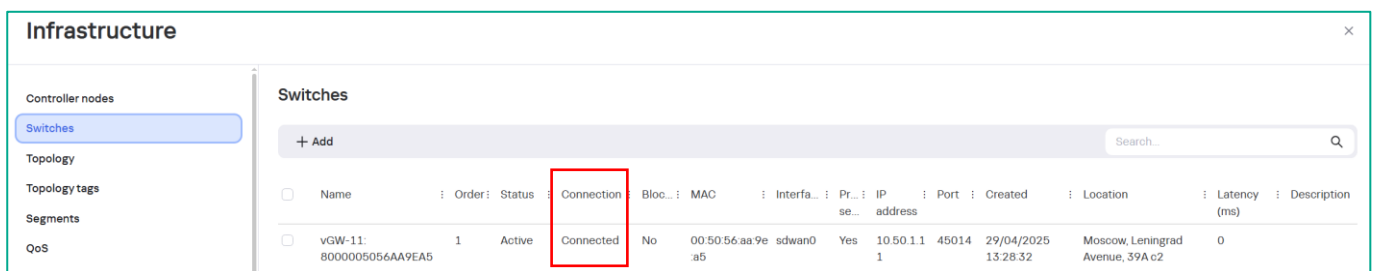
4.9.3. Проверить подключение vGW-11 к контроллеру.

На портале администратора перейти в меню **Infrastructure** → **Domain** → **DC** → **Network Resources** → **SD-WAN Cluster** → **Management** → **Configuration menu**.



Перейти в меню **Switches**.

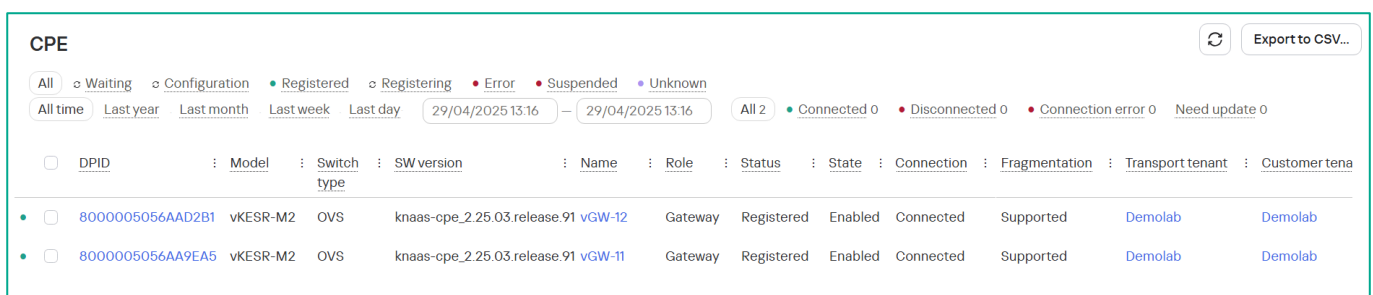
Проверить статус подключения шлюза vGW-11.



4.9.4. Зарегистрировать шлюз vGW-12.

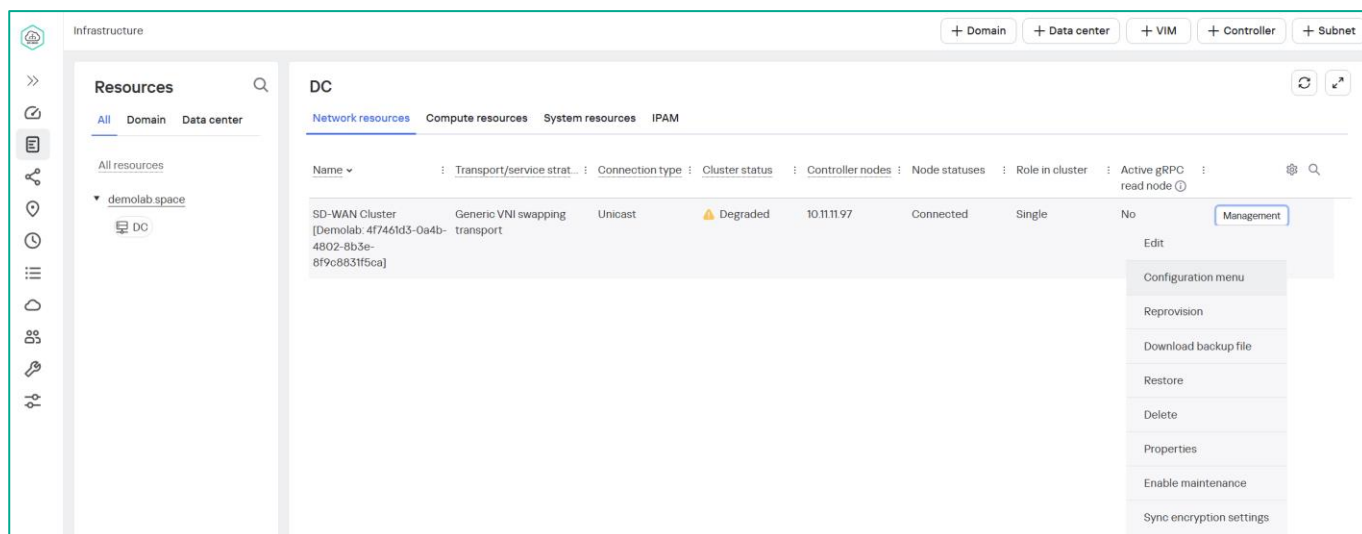
Выполнить шаги 4.9.1 – 4.9.3 для vGW-12.

Регистрация SD-WAN шлюзов завершена.

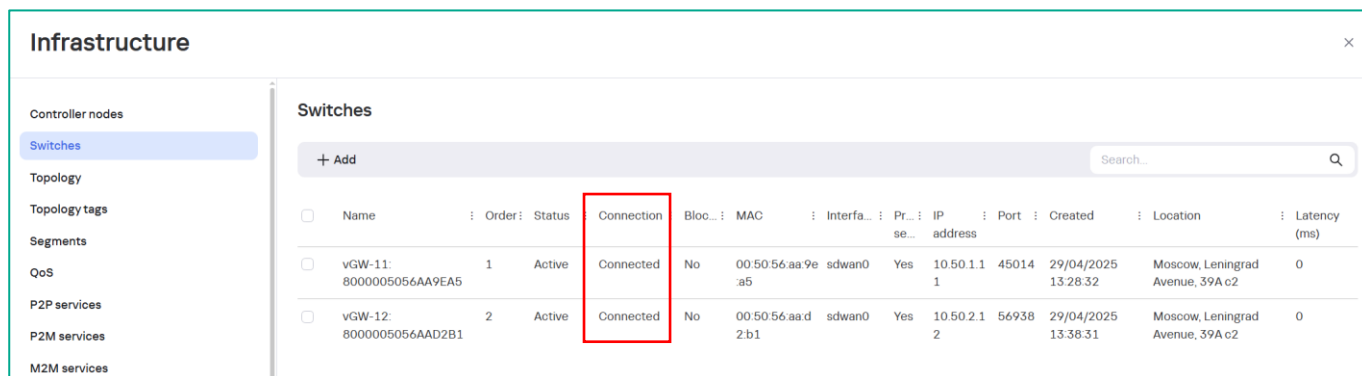


4.9.5. Проверить построение GENEVE туннелей между шлюзами.

Под администратором перейти в меню **Infrastructure** → **Domain** → **DC** → **Network Resources** → **SD-WAN Cluster** → **Management** → **Configuration menu**.

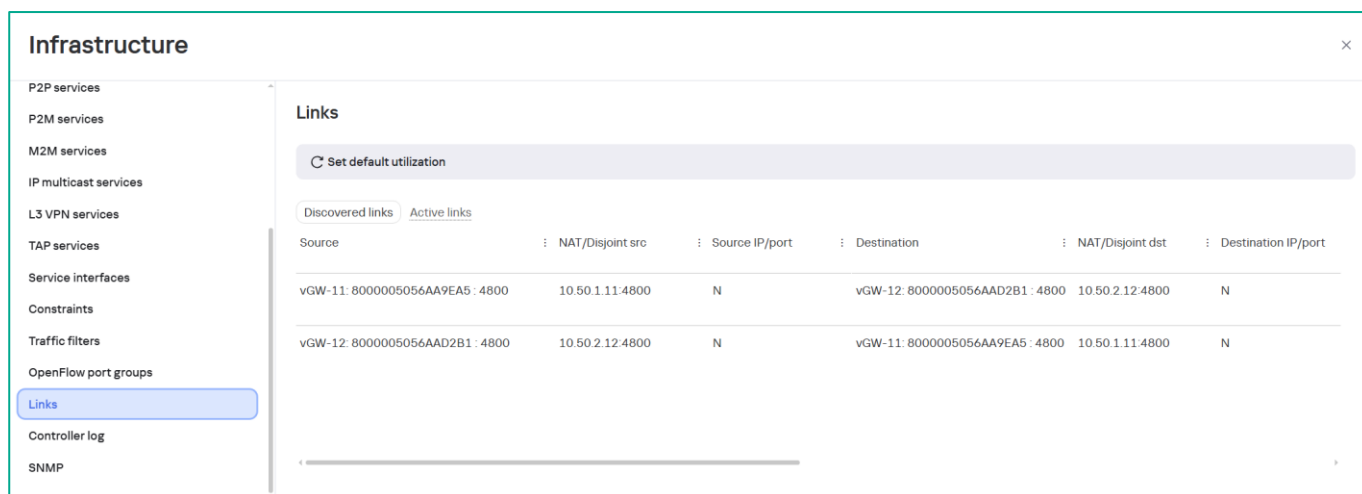


Перейти в раздел **Switches** и проверить статус подключения OVS (Open vSwitch) SD-WAN шлюзов к контроллеру.



Перейти в раздел **Links** и проверить построенные GENEVE туннели между SD-WAN шлюзами.

Отобразятся построенные туннели.



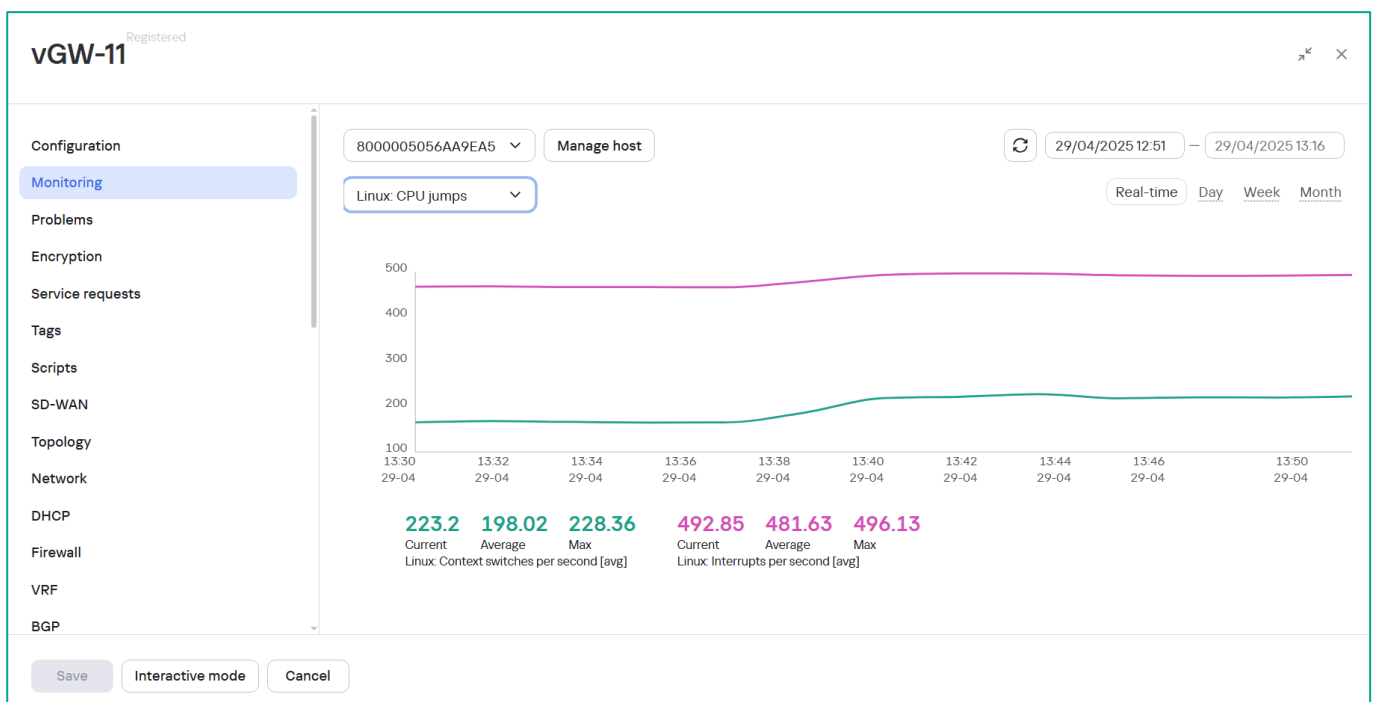
4.9.6. Отобразить пароль CPE для подключения через SSH.

После регистрации устройств CPE оркестратор сменит пароль на устройствах. Для просмотра нового пароля требуется перейти в меню **SD-WAN → CPE**, выбрать CPE и затем нажать **Show password**. Пользователь по умолчанию: **root**.

4.9.7. Проверить работу подсистемы мониторинга.

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

Отобразятся данные мониторинга CPE, возможно потребуется подождать некоторое время для обнаружения интерфейсов системой мониторинга и накопления данных для отображения.

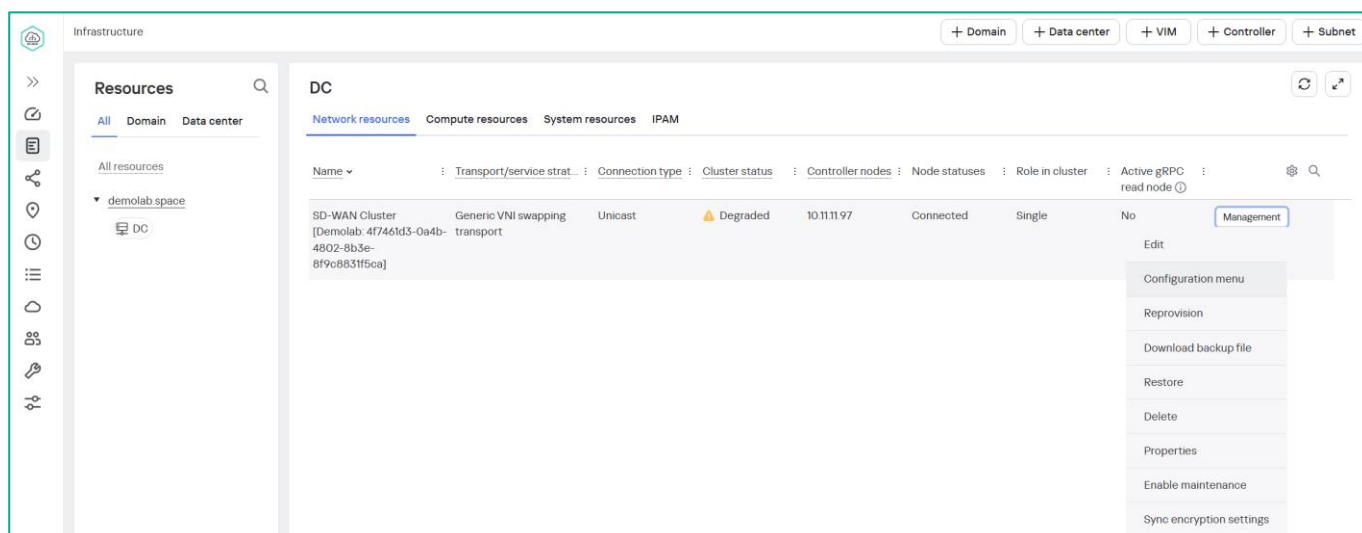


4.10. Настройка транспортного сервиса P2M для управления CPE

Устройства CPE автоматически добавляются к системному транспортному сервису P2M, который используется для управления устройствами, в частности, для работы web-консоли SSH.

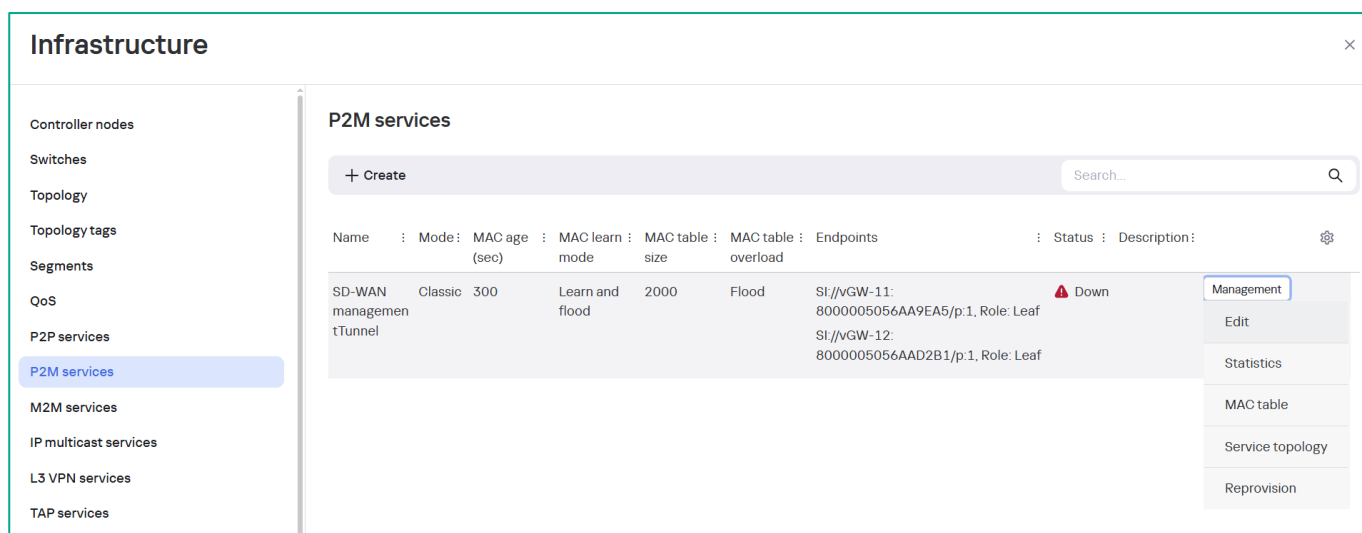
4.10.1. Открыть P2M сервис для редактирования.

Под администратором перейти в меню **Infrastructure** → **Domain** → **DC** → **Network Resources** → **SD-WAN Cluster** → **Management** → **Configuration menu**.

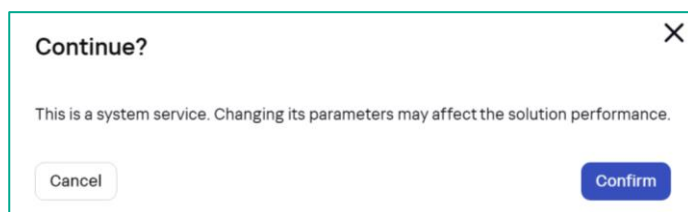


Слева в меню перейти в **P2M Services**.

Выбрать **SD-WAN managementTunnel**, затем нажать **Management** → **Edit**.



Подтвердить открытие системного сервиса для редактирования – нажать **Confirm**.



4.10.2. Задать параметры транспортного сервиса P2M для управления.

В окне редактирования сервиса нажать **Next**.

P2M service

Name: SD-WAN managementTunnel

Constraint: Threshold

Balancing mode: Per-flow

Mode: Classic

MAC learn mode: Learn and flood

MAC age (sec): 300

MAC table overload: Flood

MAC table size: 2000

Description:

Buttons: Cancel, Back, Next

Point-to-Multipoint (E-tree в классификации MEF, далее также P2M-сервис) – транспортный сервис, в рамках которого трафик передается между несколькими сервисными интерфейсами в соответствии с топологией дерева. Каждому добавленному в P2M-сервис сервисному интерфейсу требуется назначить одну из следующих ролей:

- Root – сервисный интерфейс может передавать трафик на сервисный интерфейс с любой ролью.
- Leaf – сервисный интерфейс может передавать трафик только на сервисные интерфейсы с ролью Root. По умолчанию интерфейсы добавляются в P2M сервис с ролью Leaf.

В PoC связность между сетью управления CPE и оркестратором проходит через шлюзы, поэтому сервисным интерфейсам управления шлюзов требуется назначить роль Root. Также без интерфейсов с ролью Root транспортный сервис P2M будет находиться в состоянии Down.

Изменить роли сервисных интерфейсов управления (Service interface) SD-WAN шлюзов на **Root**.

Нажать **Next**.

P2M service

Service endpoints

+ Add

Switch	Service interface	QoS rule	Inbound filter	Role	Backup switch	Backup service interface
vGW-11: 8000005056AA9E...	Port 1, Access	Unlimited-QoS	—	Root	—	—
vGW-12: 8000005056AAD...	Port 1, Access	Unlimited-QoS	—	Root	—	—

Cancel
Back
Next

Нажать **Save** для сохранения изменений в сервисе.

P2M service

Port groups

+ Add

Cancel
Back
Save

Настройка транспортного сервиса **SD-WAN managementTunnel** завершена.

Сервис перешёл в состояние **Up**.

Infrastructure

Controller nodes
Switches
Topology
Topology tags
Segments
QoS
P2P services
P2M services
M2M services
IP multicast services

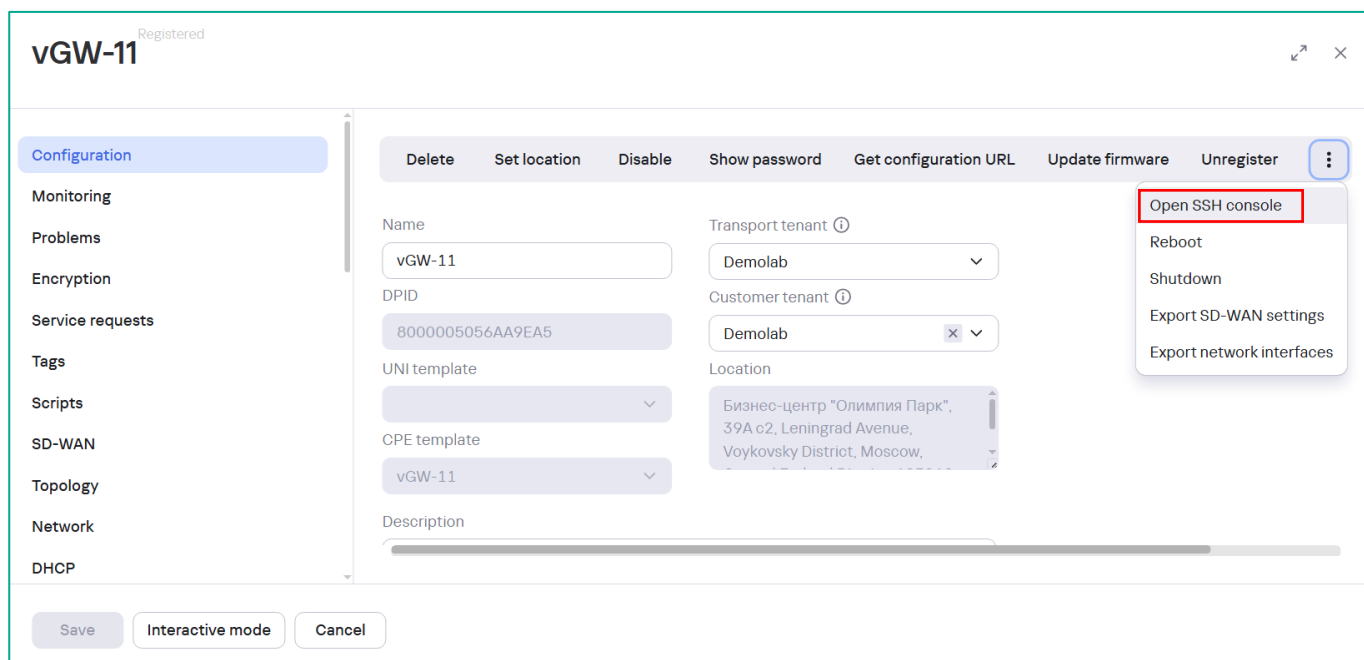
P2M services

+ Create

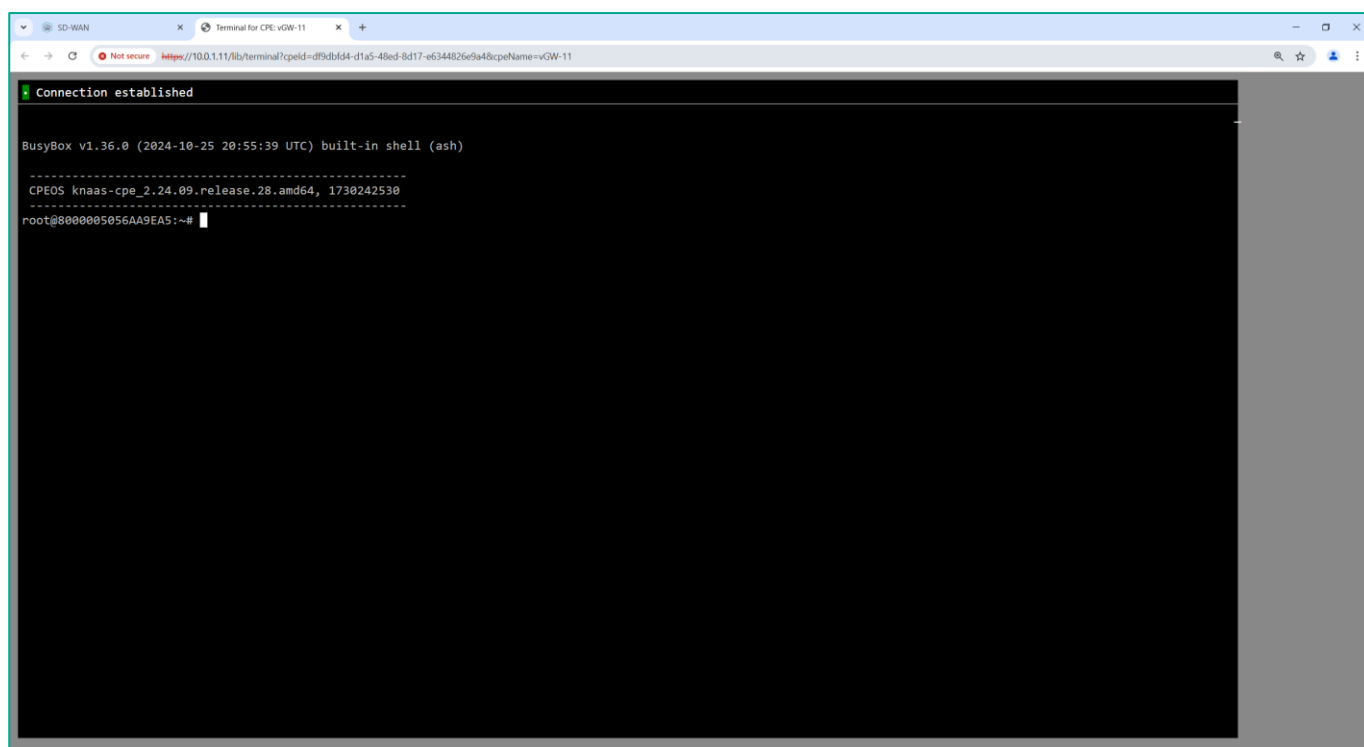
Search...

Name	Mode	MAC age (sec)	MAC learn mode	MAC table size	MAC table overload	Endpoints	Status	Description
SD-WAN management Tunnel	Classic	300	Learn and flood	2000	Flood	SI://vGW-11: 8000005056AA9EA5/p:1, Role: Root SI://vGW-12: 8000005056AAD2B1/p:1, Role: Root	Up	Management

4.10.3. Проверить работу доступа к SSH консоли SD-WAN шлюза из веб-интерфейса оркестратора. В меню **CPE** выбрать SD-WAN шлюз, нажать **Open SSH Console**.



Откроется SSH консоль CPE в браузере.



4.11. Подготовка устройств CPE

4.11.1. Развернуть VM vCPE-3 из образа CPE vKESR-M1 (knaas-cpe.<release_name>.combined.amd64-vkesr-m1.vKESR-M1-esxi.tar.gz).

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

☒ Local file

4 files

Ресурсы виртуальной машины для vKESR-M2:

- 2 x CPU.
- 512 Mb RAM.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

Review details

Verify the template details.

The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Product	vCPE
Vendor	Kaspersky Lab
Description	vKESR-M1 vCPU - 2 vRAM - 512M knaas-cpe_2.24.09.release.23.combined.amd64-vkesr-m1
Download size	Unknown
Size on disk	Unknown (thin provisioned) 1.0 GB (thick provisioned)
Extra configuration	guestinfo.urlactivated = false nvram = ovf:/file/file2

Назначить сети в соответствии со схемой PoC на рисунке 2.

На скриншоте представлен пример для vCPE-3.

- **WAN1: ISP5.**
- **WAN2: ISP6.**
- **LAN1: cpe3-lan.**

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
LAN1	SD-WAN Network
WAN1	ISP5
WAN2	ISP6

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Повторить предыдущие шаги и развернуть виртуальные машины vCPE-4, vCPE-51, vCPE-52 из образа CPE vKESR-M1.

4.11.2. Настроить сетевой интерфейс **lan**.

Открыть консоль к виртуальным машинам CPE.

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

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

Открыть в редакторе **vi** конфигурационный файл сетевой службы для редактирования:

vi /etc/config/network

Требуется настроить сетевой интерфейс **lan** для применения Configuration URL с рабочей станции mgmt.

Изменить IP-адрес интерфейса **lan** на адрес lan CPE в соответствии с таблицей 1 в п.2.2.

На скриншоте пример настройки vCPE-3.

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

config interface 'lan'
    option type 'bridge'
    option proto 'static'
    option ipaddr '10.20.3.1'
    option netmask '255.255.255.0'
    option ifname 'eth2'
    option auto '1'
    option force_link '1'
```

Перезагрузить сетевую службу:

```
/etc/init.d/network restart
```

Проверить примененные настройки:

```
ip -br a
```

```
root@8000005056AAC4FD:~# ip -br a
lo                UNKNOWN      127.0.0.1/8 ::1/128
eth0              UP            10.50.5.9/24 fe80::250:56ff:feaa:c4fd/64
eth1              UP            10.50.6.15/24 fe80::250:56ff:feaa:abf2/64
eth2              UP
ip6tnl0@NONE      DOWN
gre0@NONE          DOWN
gretap0@NONE       DOWN
erspan0@NONE       DOWN
ip6gre0@NONE       DOWN
bond0             DOWN
br-lan            UP            10.20.3.1/24
overlay@ovs-lan    UP
ovs-lan@overlay    UP
mgmt@ovs-mgmt      UP
ovs-mgmt@mgmt      UP
```

После регистрации (выполнения configuration URL в пункте 4.14) CPE получит и применит сетевые настройки в соответствии настройками в главе 4.13.

Note: Также возможно передать Configuration URL при развертывании CPE из OVF. Для этого требуется предварительно создать CPE, используя ранее созданные шаблоны шлюзов, с произвольным DPID и получить Configuration URL (описано в п. 4.9). При настройке CPE требуется использовать адрес по умолчанию для Configuration URL – 192.168.7.1. После загрузки, CPE появится в оркестраторе со статусом Unknown. Далее необходимо будет открыть CPE, в меню Configuration нажать Register, затем настроить параметры CPE, как описано в п. 4.9.

4.12. Создание шаблона межсетевого экрана для устройств CPE

Рабочие станции, подключенные к CPE, должны иметь возможность доступа в публичные сети. Для этого требуется создать дополнительную зону WAN с включенной опцией masquerading и создать шаблон с настроенными правилами forwarding между зоной lan и зоной wan

4.12.1. Создать дополнительную зону межсетевого экрана для устройств CPE.

Подключиться к portalу самообслуживания tenants, созданному в 4.4.1 (в PoC используется tenant **Demolab**), для этого нажать кнопку **Connect as Tenant** из меню **Tenants** или подключиться к SD-WAN оркестратору администратором созданного tenants.

Note: При создании шаблонов из портала администратора они не будут доступны пользователям с правами tenant.

Перейти в меню **SD-WAN > Firewall zones**.

Name	Usage	Author	Created
lan	Yes	admin (Demolab)	23/04/2025 15:57:47
wan	Yes	admin (Demolab)	23/04/2025 15:57:47
mgmt	No	admin (Demolab)	23/04/2025 15:57:47
mgmt_gw	Yes	admin (Demolab)	29/04/2025 11:17:34

Нажать кнопку **+ Firewall Zone**.

В поле **Name** задать название зоны: **wan_cpe**.

Отметить **Masquerading**.

Нажать **Create**.

New firewall zone

Name: wan_cpe

Input: ACCEPT, Output: ACCEPT, Forwarding: REJECT

☒ Masquerading, ☒ MSS clamp to PMTU, ☐ Drop logging

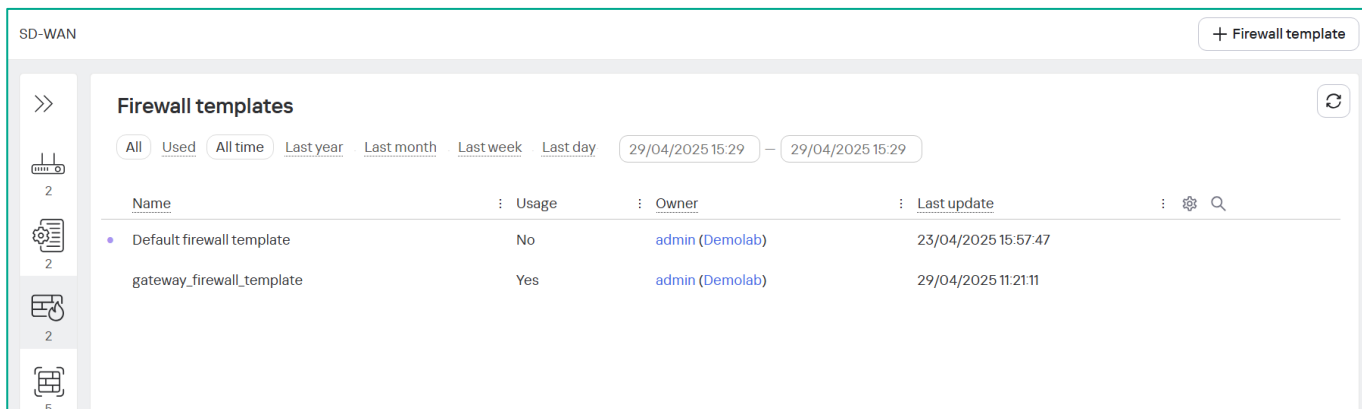
Masquerading source subnets: + Add, Masquerading destination subnets: + Add

Networks: + Add

Create, Cancel

4.12.2. Создать шаблон межсетевого экрана для CPE.

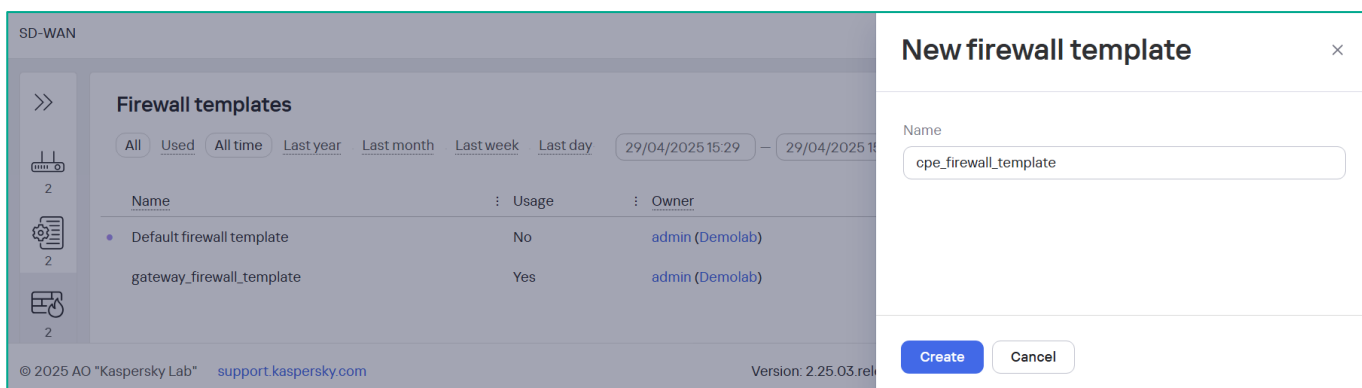
Перейти в меню **SD-WAN > Firewall templates**.



Нажать кнопку **+ Firewall Template**.

В поле **Name** задать название шаблона: **cpe_firewall_template**.

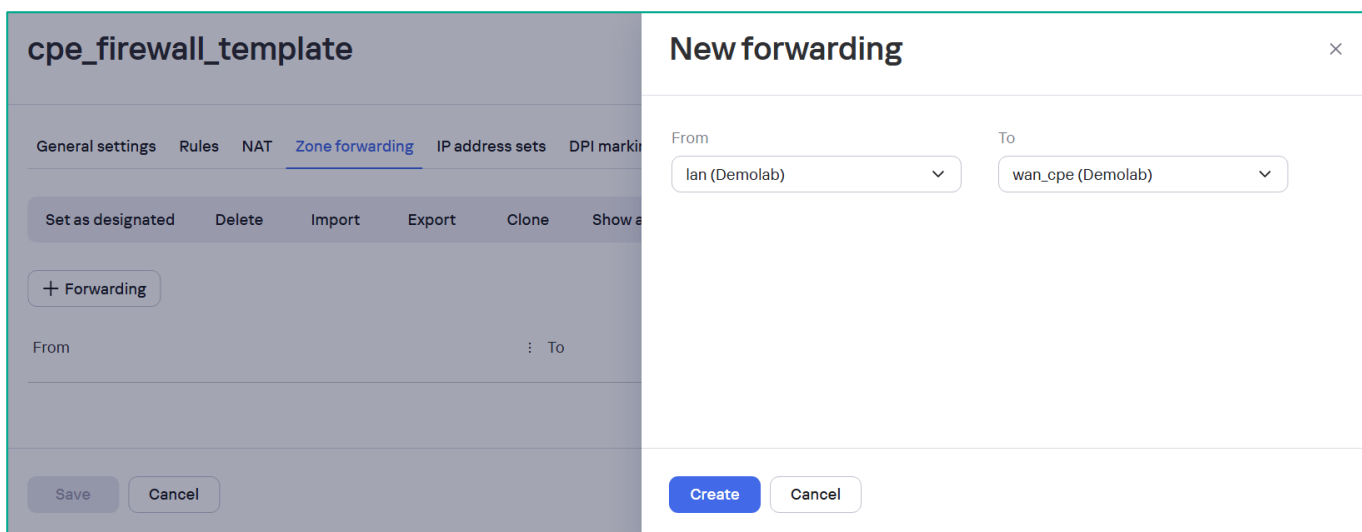
Нажать **Create**.



В шаблоне перейти на вкладку **Zone forwarding**.

Создать новое правила forwarding: из зоны **lan** в зону **wan_cpe**.

Для этого нажать **+ Forwarding** и выбрать необходимые зоны.



Нажать **Save** для сохранения шаблона.

cpe_firewall_template

General settingsRulesNATZone forwardingIP address setsDPI marking

Set as designatedDeleteImportExportCloneShow associated CPEs

+ Forwarding

From	To	Actions
lan (Demolab)	wan_cpe (Demolab)	Delete

Save

Cancel

4.13. Создание шаблонов для устройств CPE

4.13.1. Создать шаблон для vCPE-3.

Подключиться к portalу самообслуживания тенанта, созданному в 4.4.1 (в PoC используется тенант **Demolab**), для этого нажать кнопку **Connect as Tenant** из меню **Tenants** или подключиться к SD-WAN оркестратору администратором созданного тенанта.

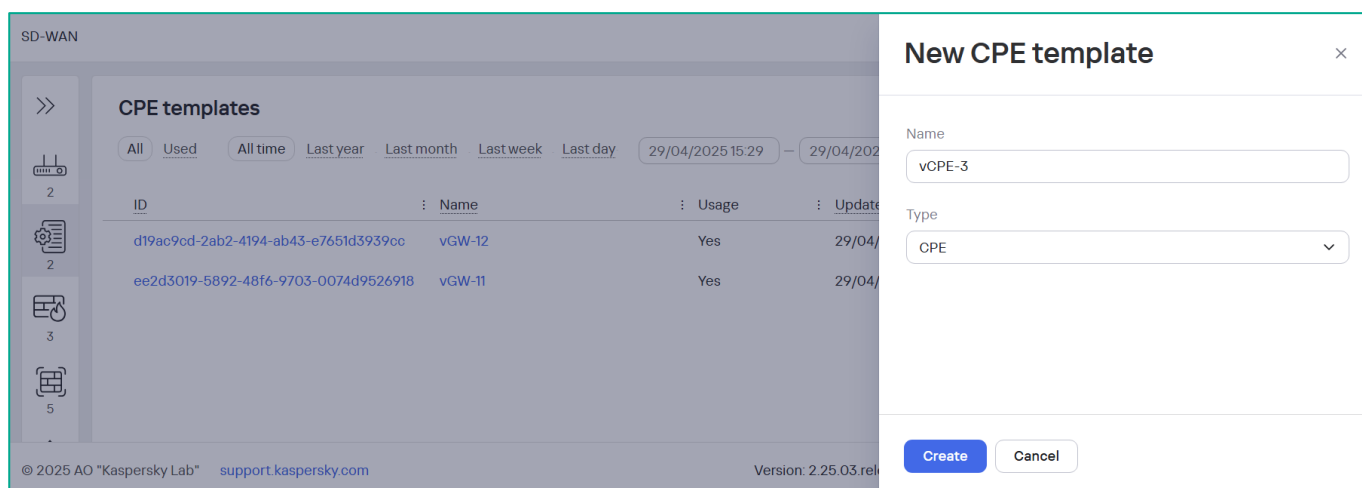
Note: При создании шаблонов из портала администратора они не будут доступны пользователям с правами tenant.

Перейти в меню **SD-WAN > CPE Templates**.

Нажать **+ CPE Template**.

Задать имя шаблона: **vCPE-3**.

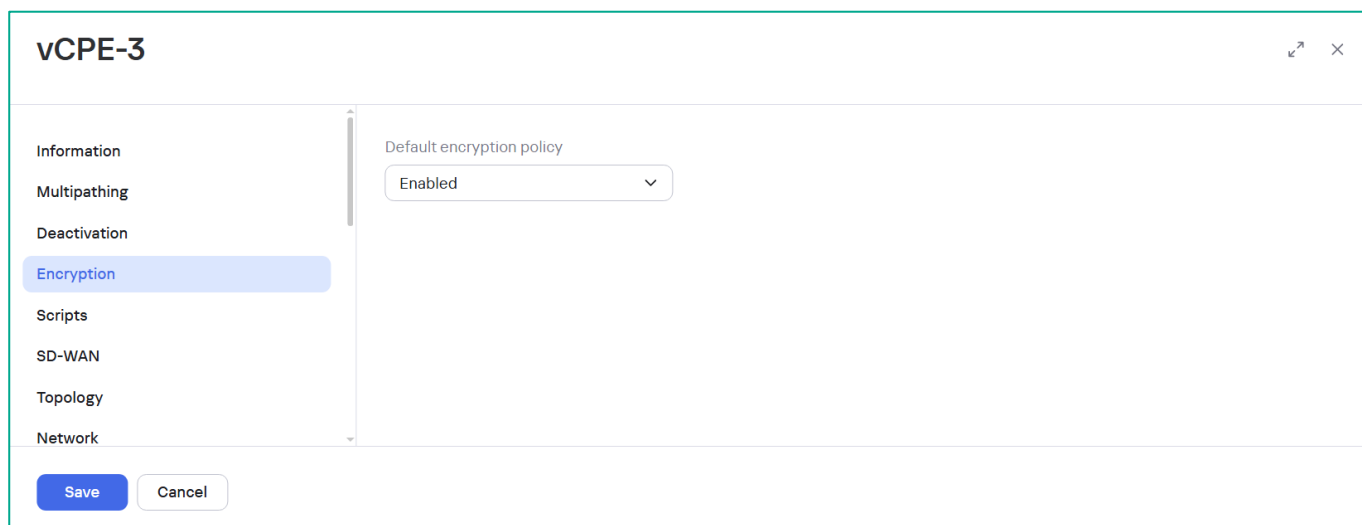
Нажать **Create**.



4.13.2. Задать политику шифрования по умолчанию в шаблоне vCPE-3.

Перейти в меню **Encryption**.

Включить шифрование: **Enabled**.



4.13.3. Задать параметры SD-WAN в шаблоне vCPE-3.

Перейти на вкладку **SD-WAN → General settings**.

Задать адрес для подключения к оркестратору (в PoC требуется задать публичный IP-адрес хоста ocs1, также возможно использовать доменное имя для подключения).

- **Orchestrator IP/FQDN: 10.50.1.14.**
- **Orchestrator Port: 443.**
- **Openflow Transport: ssl.**
- **Control SD-WAN interface: sdwan0.**
- Изменить IP-адрес **192.168.7.1** в **Configuration URL** на **10.20.3.1** (IP-адрес интерфейса lan).

The screenshot shows the vCPE-3 configuration window with the 'SD-WAN' tab selected in the left sidebar. The main area is divided into two sections: 'Connection to orchestrator' and 'Connection to controller'.

Connection to orchestrator:

- Orchestrator IP address/FQDN: 10.50.1.14
- Orchestrator port: 443
- ☐ Backup orchestrator IP address and port
- Orchestrator protocol: https
- Update interval (sec): 30
- Interactive update interval (sec): 3
- Interactive mode timeout (sec): 180

Connection to controller:

- OpenFlow transport: SSL
- Control SD-WAN interface: sdwan0
- ☐ Preemption
- Auto-reboot: No
- Reboot timeout (sec): 86400
- Configuration URL: http://10.20.3.1/cgi-bin/config?payload={config}

At the bottom of the window are 'Save' and 'Cancel' buttons.

4.13.4. Настроить роль CPE в шаблоне vCPE-3.

Перейти в меню **Topology**.

Задать роль: **CPE**.

The screenshot shows the 'vCPE-3' configuration window. On the left is a sidebar menu with the following items: Information, Multipathing, Deactivation, Encryption, Scripts, SD-WAN, **Topology** (highlighted with a blue bar), Network, DHCP, and BGP. The main area of the window is titled 'vCPE-3' and contains the following settings:

- Role**: A dropdown menu with 'CPE' selected.
- Transit CPE**: An unchecked checkbox.
- Topology tags**: An empty dropdown menu.

At the bottom of the window are two buttons: 'Save' and 'Cancel'.

4.13.5. Настроить сетевые интерфейсы в шаблоне vCPE-3.

Перейти в меню **Network**.

Далее будут созданы следующие сетевые интерфейсы:

- **sdwan0: eth0.**
- **sdwan1: eth1.**
- **lan: eth1.**
- **overlay: overlay.**

Для создания нового интерфейса нажать **+ Network interface**. Параметры интерфейсов описываются дальше.

vCPE-3

Information

Multipathing

Deactivation

Encryption

Scripts

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

PBR

BFD

+ Network interface

Alias	Zone	Interface name	Protocol	IP address/mask	MTU	Enable automatically	Actions
lan	lan	eth2	Static IPv4 address	IP address: 10.20.3.1 Mask: 255.255.255.0		Yes	Edit Delete Disable
overlay	lan	overlay	Static IPv4 address	IP address: 172.16.1.3 Mask: 255.255.255.0		Yes	Edit Delete Disable
sdwan0	wan_cpe	eth0	DHCP client			Yes	Edit Delete Disable
sdwan1	wan_cpe	eth1	DHCP client			Yes	Edit Delete Disable

Save

Cancel

Добавить сетевой интерфейс **lan** со следующими параметрами:

- **Alias:** lan.
- **Zone:** lan.
- **Interface name:** eth1.
- **Protocol:** Static IPv4 address.
- **IPv4 address:** 10.20.3.1/24.

Нажать **Create** для создания интерфейса.

The screenshot shows the 'New network interface' dialog box. The 'Alias' field is 'lan', the 'Zone' is 'lan (Demolab)', and the 'Interface name' is 'lan'. The 'Bridge' and 'NetFlow' checkboxes are unchecked. The 'Protocol' is set to 'Static IPv4 address'. Under 'Settings', 'Enable automatically' is checked, and 'Force IP address, route, and gateway' is unchecked. The 'IPv4 address and subnet mask input type' is set to 'Manually'. The 'IPv4 address' is '10.20.3.1' and the 'IPv4 netmask' is '255.255.255.0'. At the bottom, there are 'Create' and 'Cancel' buttons.

Добавить сетевой интерфейс **overlay** со следующими параметрами:

- **Alias:** overlay.
- **Zone:** lan.
- **Interface name:** overlay.
- **Protocol:** Static IPv4 address.
- **IPv4 address:** 172.16.1.3/24.
- Отметить **Generate MAC address automatically**. При этой настройке MAC адрес интерфейса сгенерируется автоматически из пула и будет сохраняться после перезагрузки устройства, что позволит не изучать заново MAC адреса смежным устройствам и ускорит время сходимости протоколов маршрутизации.

Нажать **Create** для создания интерфейса.

The screenshot shows the 'New network interface' dialog box. The 'Alias' field is 'overlay', the 'Zone' is 'lan (Demolab)', and the 'Interface name' is 'overlay'. The 'Bridge' and 'NetFlow' checkboxes are unchecked. The 'Protocol' is set to 'Static IPv4 address'. Under 'Settings', 'Enable automatically' is checked, and 'Force IP address, route, and gateway' is unchecked. The 'IPv4 address and subnet mask input type' is set to 'Manually'. The 'IPv4 address' is '172.16.1.3' and the 'IPv4 netmask' is '255.255.255.0'. There are empty fields for 'IPv4 gateway' and 'IPv4 broadcast'. Under 'DNS servers', there is an '+ Add' button. At the bottom, there are 'Create' and 'Cancel' buttons. The 'Generate MAC address automatically' checkbox is checked.

Добавить сетевые интерфейсы
sdwan0 и **sdwan1**:

- **Alias:** sdwan0 / sdwan1.
- **Zone:** wan_cpe.
- **Interface name:** eth0 / eth1.
- **Protocol:** DHCP client.

Нажать **Create** для создания интерфейсов.

4.13.6. Включить DHCP сервер на интерфейсе lan.

Необходимо добавить DHCP Server на интерфейсе, чтобы рабочие станции могли получать IP-адреса по DHCP.

Перейти в меню **DHCP**.

Нажать **+ DHCP Server** для добавления нового сервера.

Задать параметры DHCP сервера:

- **Network interface alias:** lan.
- **Type:** Server.
- **Start IP** (начальный адрес диапазона): **51**.
- **Limit** (размер диапазона): **50**.
- **Lease time:** **12 hours**.
- **DNS servers:** **8.8.8.8**.

Нажать **Create** для создания сервера DHCP.

The screenshot displays the 'vcPE-3' configuration window with the 'Network' section selected. The 'DHCP' sub-section is highlighted in the left sidebar. A '+ DHCP server' button is visible in the top right of the network configuration area. The 'New DHCP server' dialog box is open, showing the following configuration:

- Network interface alias:** lan
- Network interface IP/mask:** 10.20.3.0/24
- Type:** ☒ Server (Other options: Disabled, Relay)
- Start IP:** 51
- Limit:** 50
- DHCP range:** 10.20.3.51 - 10.20.3.100
- Lease time:** 12 hours
- DHCP options:**
 - IPv4 gateway (3):
 - DNS servers (6): 8.8.8.8
 - NTP servers (42):
 - Custom option: + Option

At the bottom of the dialog are 'Create' and 'Cancel' buttons. The main configuration window also has 'Save' and 'Cancel' buttons at the bottom left.

4.13.7. Настроить параметры CFM в шаблоне vCPE-3.

Функция Connectivity Fault Management позволяет обнаруживать недоступные линки между устройствами CPE. Когда функция CFM включена, устройство CPE отправляет контрольные пакеты Continuity Check Message (CCM) через линки до других CPE с указанным интервалом времени и ожидает получения ответных контрольных пакетов через встречные линки. При отсутствии ответных контрольных пакетов устройство CPE считает линк нерабочим и начинает передавать трафик по случайно выбранному доступному линку.

Перейти на вкладку **CFM**.

Задать:

- **CFM: Enabled** (включить CFM для линков) .
- **Interval: 300 ms** (интервал отправки контрольных пакетов CFM) .

The screenshot shows the 'vCPE-3' configuration window with the 'CFM' tab selected in the left sidebar. The main area contains two dropdown menus: 'CFM' set to 'Enabled' and 'Interval' set to '300 ms.'. At the bottom are 'Save' and 'Cancel' buttons.

4.13.8. Настроить параметры мониторинга в шаблоне vCPE-3.

Перейти на вкладку **Monitoring**.

Задать:

- **Monitoring type: Agent**.
- **Zabbix template: Linux by Zabbix agent active**.

The screenshot shows the 'vCPE-3' configuration window with the 'Monitoring' tab selected in the left sidebar. The main area contains two dropdown menus: 'Monitoring type' set to 'Agent' and 'Zabbix template' set to 'Linux by Zabbix agent active'. At the bottom are 'Save' and 'Cancel' buttons.

4.13.9. Настроить параметры NTP в шаблоне vCPE-3.

Перейти на вкладку **NTP**.

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

Задать адреса NTP серверов или использовать настройки по умолчанию.

The screenshot shows the vCPE-3 configuration window with the 'NTP' tab selected in the left sidebar. The main area contains two radio buttons: 'Connect to NTP server' (checked) and 'Use CPE as NTP server'. Below them is a section for 'NTP servers' with a text input field containing 'pool pool.ntp.org' and an 'Add' button. At the bottom are 'Save' and 'Cancel' buttons.

4.13.10. Создать Prefix List в шаблоне vCPE-3

Перейти на вкладку **Routing filters → Prefix lists**.

Нажать **+ Prefix List**

Задать **Name: cpe-lan**

Нажать **+ Rule**.

Добавить префикс:

- **Seq: 10 10.20.0.0/16.**
- **Greater of Equal: 17.**

The screenshot shows the 'New prefix list' dialog box. The 'Name' field is set to 'cpe-lan'. Below it is a '+ Rule' button. A table lists the rules with columns: Sequence, Network, Action, Greater or equal, and Less or equal. The first rule has Sequence 10, Network IP address..., Action Permit, and Greater or equal 17. At the bottom are 'Create' and 'Cancel' buttons.

Sequence	Network	Action	Greater or equal	Less or equal
10	IP address...	Permit	17	

Нажать **Create**.

4.13.11. Создать Route Map в шаблоне vCPE-3.

Перейти на вкладку **Routing filters** → **Route maps**.

Нажать **+ Route Map**.

Задать **Name: cpe-route-map**

Нажать **+ Rule** и задать параметры правила:

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

Нажать **Create**.

vCPE-3

New route map

Name ①
cpe-route-map

+ Rule

Sequence	Action	Match type	Value	Change attribute	New value
10	Permit	Prefix-L...	66710700-24fb-11	None	

Prefix list
cpe-lan

Save Cancel Create Cancel

4.13.12. Настроить BGP в шаблоне vCPE-3.

Перейти в меню вкладки **BGP**.

Задать номер автономной системы: **Autonomous System** → **65500**.

Нажать **+ BGP** для добавления нового экземпляра BGP.

vCPE-3

Autonomous System 65500

Default BGP Instance with VRF ①

+ BGP

State	VRF	Router ID	BGP neighbor	Peer groups	Route Distinguisher	Export routes	Import routes	A
No data								

Save Cancel

Перейти на вкладку **General settings**.

Задать параметры BGP:

- **BGP: Enabled.**
- **Router ID: 172.16.1.3** (IP-адрес сетевого интерфейса overlay).
- **Maximum Paths: 2.**
- **Graceful Restart.**
- **Default IPv4 Unicast.**
- **BGP Timers:**
 - **Keepalive: 10.**
 - **Holdtime: 30.**

Включить редистрибуцию **Connected** маршрутов. Применить **Route map: cpe-route-map** к **Connected** маршрутам.

New BGP instance

[General settings](#) [Neighbors](#) [Peer groups](#) [Route leaking](#)

BGP

Enabled

VRF

main/254

AS

65500

Router ID

172.16.1.3

☐ Router ID from IP pool

Maximum paths

2

☐ Always compare MED

☒ Graceful restart (helper mode)

☒ Use default IPv4 unicast routes

☒ BGP timers

Keepalive (sec)

10

Holdtime (sec)

30

Route redistribution

☐ Kernel

Route map

Metric

☒ Connected

Route map

cpe-route-map x

Metric

Save

Cancel

4.13.13. Создать BGP соседства от vCPE-3 до vGW-11 и vGW-12.

Перейти на вкладку **Neighbors** и нажать **+BGP Neighbor**.

Создать 2 BGP соседа. Задать параметры:

- **Name: vGW-11.**
- **Neighbor IP: 172.16.1.11.**
- **Remote AS: 65500.**
- **Name: vGW-12.**
- **Neighbor IP: 172.16.1.12.**
- **Remote AS: 65500.**

New BGP instance

General settings

Neighbors

Peer groups

Route leaking

+ BGP neighbor

Neighbor IP	Name	Description	Remote AS	Shutdown	Weight	Actions
172.16.1.12	vGW-12		65500	No		<a>Edit <a>Delete
172.16.1.11	vGW-11		65500	No		<a>Edit <a>Delete

Save

Cancel

Нажать **Save** для сохранения экземпляра BGP.

Задать **Default BGP Instance with VRF: main/254** (VRF по умолчанию для экземпляров BGP, используется для обратной совместимости со старыми версиями устройств CPE).

Нажать **Save** для сохранения шаблона.

vCPE-3

SD-WAN

Topology

Network

DHCP

BGP

VRF

OSPF

Routing filters

PBR

BFD

Static routes

Autonomous System

65500

Default BGP Instance with VRF

main/254

+ BGP

State	VRF	Router ID	BGP neighbor	Peer groups	Route Distinguisher	Export routes	Import routes	Actions
Enabled	main/254	172.16.1.3	2	0	65500/254	Off	Off	<a>Edit <a>Delete

Save

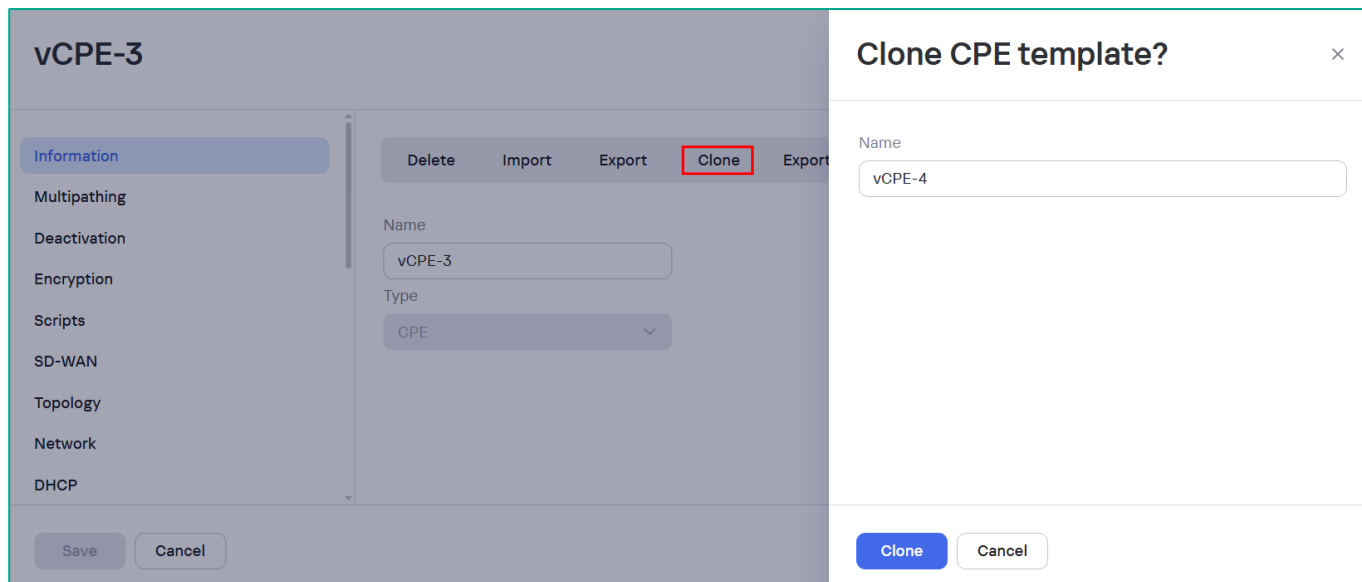
Cancel

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

Открыть шаблон **vCPE-3** и перейти в меню **Information**.

Нажать **Clone** из шаблона CPE, затем задать имя нового шаблона.

Нажать **Clone** для создания нового шаблона из текущего.



Повторить пункты 4.13.2 - 4.13.13 для клонированных шаблонов, изменить значения параметров на соответствующие каждому устройству CPE в соответствии с таблицей 1.

Требуется изменить адреса:

- **Configuration URL.**
- Интерфейса **lan**.
- Интерфейса **overlay**.
- **BGP Router ID.**

Также требуется добавить DHCP сервер аналогично п. 4.13.6.

4.13.15. Настроить VRRP на vCPE-51 и vCPE-52.

Kaspersky SD-WAN поддерживает установку нескольких устройств CPE на площадках для обеспечения высокой доступности. Одним из вариантов организации высокой доступности является использование протокола VRRP (Virtual Router Redundancy Protocol).

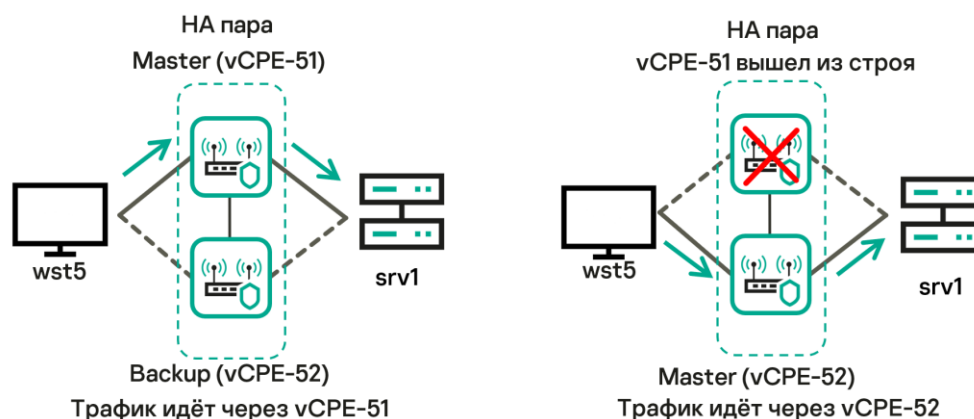


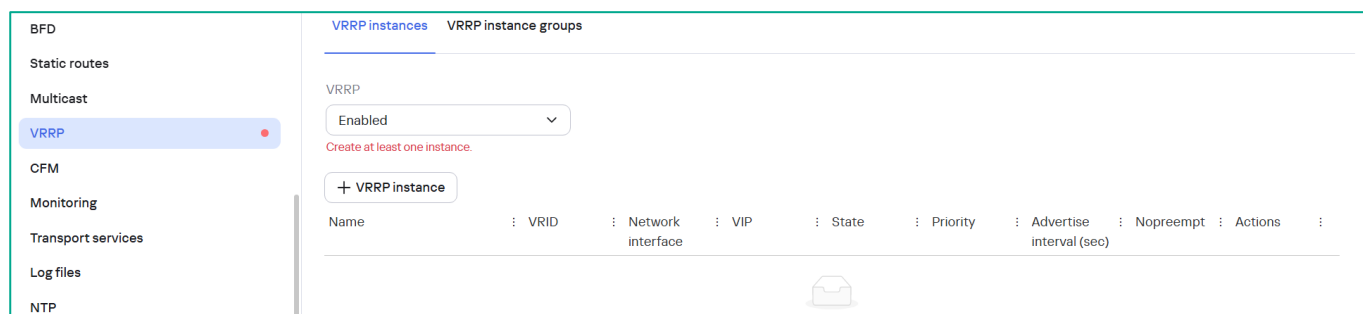
Рисунок 4 - Резервирование CPE с помощью протокола VRRP

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help: <https://support.kaspersky.com/help/SD-WAN/2.4/ru-RU/246585.htm>

В шаблонах для vCPE-51 и vCPE-52 требуется настроить VRRP.

Для настройки открыть соответствующий шаблон CPE и перейти в меню **VRRP**.

Включить **VRRP** → **Enabled**.



Добавить экземпляр VRRP.

Нажать **+ VRRP instance**.

Задать параметры экземпляра VRRP, затем нажать **Create**.

Для vCPE-51:

- **Name: vCPE-5.**
- **VRID: 5.**
- **Network interface: lan.**
- **VIP: 10.20.5.1/24.**
- **State: Master.**
- **Priority: 101.**

Для vCPE-52:

- **Name: vCPE-5.**
- **VRID: 5.**
- **Network interface: lan.**
- **VIP: 10.20.5.1/24.**
- **State: Backup.**
- **Priority: 100.**

New VRRP instance

Name

VRID ⓘ

Network interface ⓘ

VIP ⓘ

State

vCPE-5

5

lan ▾

10.20.5.1/24

Master ▾

Priority

Advertise interval (sec) ⓘ

☐ Nopreempt ⓘ

101

5

☐ Unicast

Unicast source IP

Unicast peer IP

☐ Authentication

Password

👁 📄

Create

Cancel

Нажать **Save** для сохранения шаблонов vCPE-51 и vCPE-52.

4.13.16. Изменить диапазон выдачи адресов для DHCP сервера и добавить DHCP опцию 3 на vCPE-51 и vCPE-52.

Устройства vCPE-51 и vCPE-52 включены в одну подсеть, где являются DHCP серверами для рабочих станций. В связи с этим, для избежание конфликтов адресов требуется настроить разные пулы IP-адресов в настройках DHCP сервера. Также требуется отдавать VIP рабочим станциям в качестве шлюза по умолчанию.

Открыть шаблон CPE, перейти в меню DHCP, открыть сервер на интерфейсе **lan** для редактирования.

Добавить **IPv4 gateway** (DHCP опция 3), чтобы отдавать адрес VIP в качестве шлюза по умолчанию:
10.20.5.1

На **vCPE-52** изменить диапазон выдачи адресов DHCP, чтобы он не пересекался с vCPE-51.

Задать:

- **Start IP** (начальный адрес диапазона): **151**.
- **Limit** (размер диапазона): **50**.

The screenshot displays the configuration interface for a Kaspersky SD-WAN device. The left sidebar shows the 'vCPE-51' configuration page with a list of network settings. The main area on the left shows a table with the following data:

Network interface alias	Type	Start IP
lan	Server	10.20.5.51

The right panel, titled 'DHCP server', shows the configuration for the selected server. The 'IPv4 gateway (3)' field is highlighted with a red box, indicating the VIP address to be assigned to clients.

DHCP server configuration details:

- Start IP: 151
- Limit: 50
- DHCP range: 10.20.5.151 - 10.20.5.200
- Lease time: 12 hours
- DHCP options:
 - IPv4 gateway (3): 10.20.5.1
 - DNS servers (6): 8.8.8.8
 - NTP servers (42):

4.14. Регистрация устройств CPE

4.14.1. Добавить устройство vCPE-3.

Подключиться к portalу самообслуживания тенанта, созданному в 4.4.1 (в PoC используется тенант **Demolab**), для этого нажать кнопку **Connect as Tenant** из меню **Tenants** или подключиться к SD-WAN оркестратору администратором созданного тенанта.

Перейти в меню **SD-WAN → CPE**, нажать **+ CPE**.

Задать:

- **Name:** vCPE-3.
- **DPID** (посмотреть в CLI CPE).
- **State:** Enabled.
- **CPE Template:** vCPE-3.
- **Firewall template:** cpe_firewall_template.

Нажать кнопку **Next**.

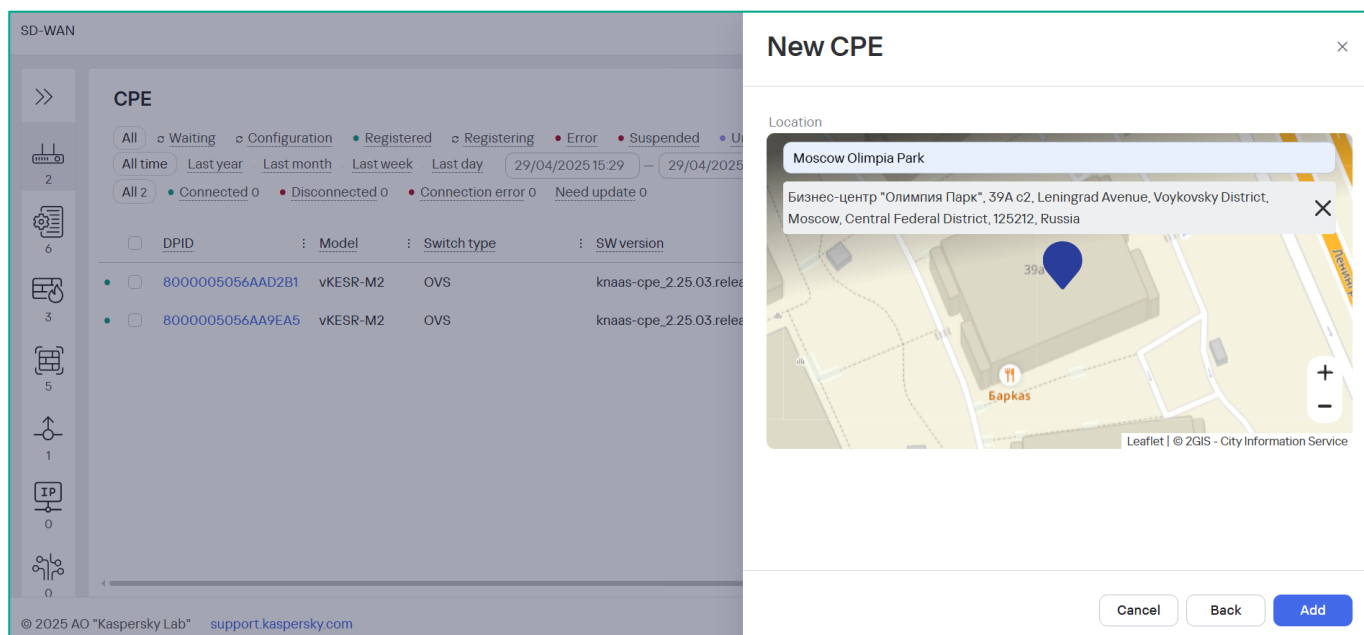
The screenshot displays the Kaspersky SD-WAN management interface. On the left, a sidebar shows navigation icons. The main panel is titled 'CPE' and contains a list of devices with columns for DPID, Model, Switch type, and SW version. Two devices are listed: 8000005056AAD2B1 and 8000005056AA9EA5, both vKESR-M2 models using OVS switch type.

Overlaid on the right is the 'New CPE' form. It includes the following fields and options:

- Name:** vCPE-3
- DPID:** 8000005056AAC4FD
- State:** Enabled (dropdown menu)
- Description:** (empty text field)
- UNI template:** (empty dropdown menu)
- CPE template:** vCPE-3 (dropdown menu)
- NetFlow template:** Default NetFlow template (Demolab) (dropdown menu)
- Firewall template:** cpe_firewall_template (Demolab) (Demolab) (dropdown menu)

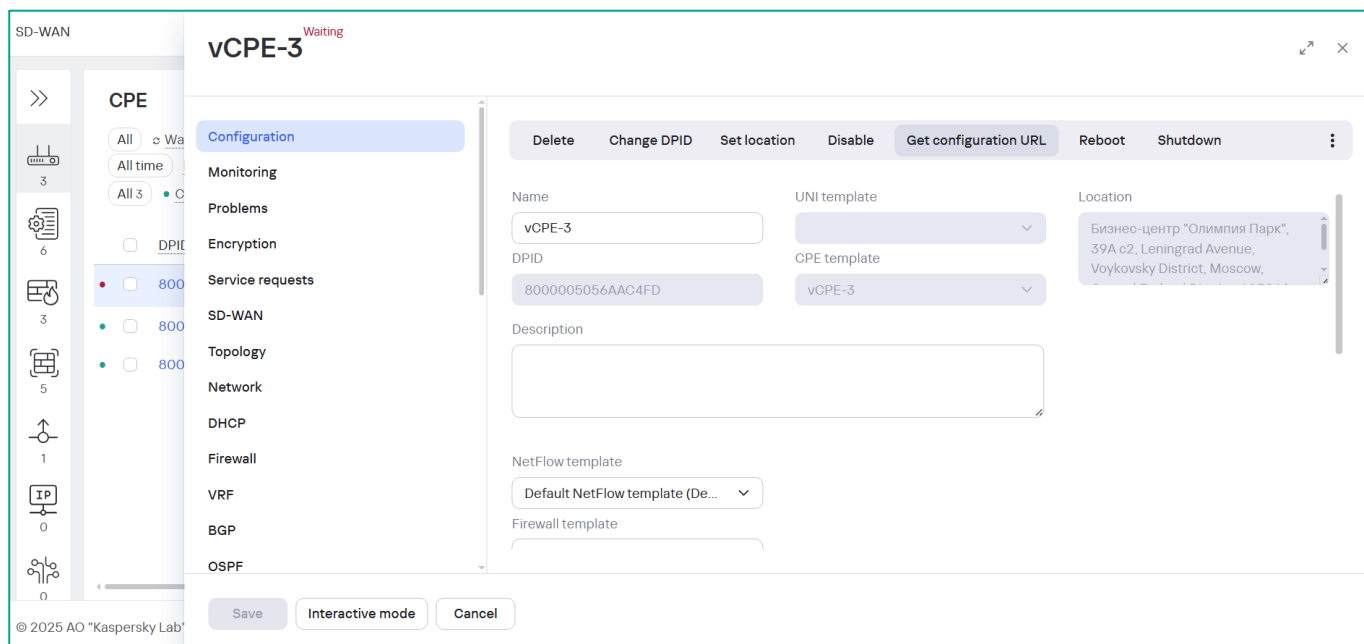
At the bottom right of the form are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button is highlighted in blue.

Опционально задать местоположение CPE, затем нажать кнопку **Add**.

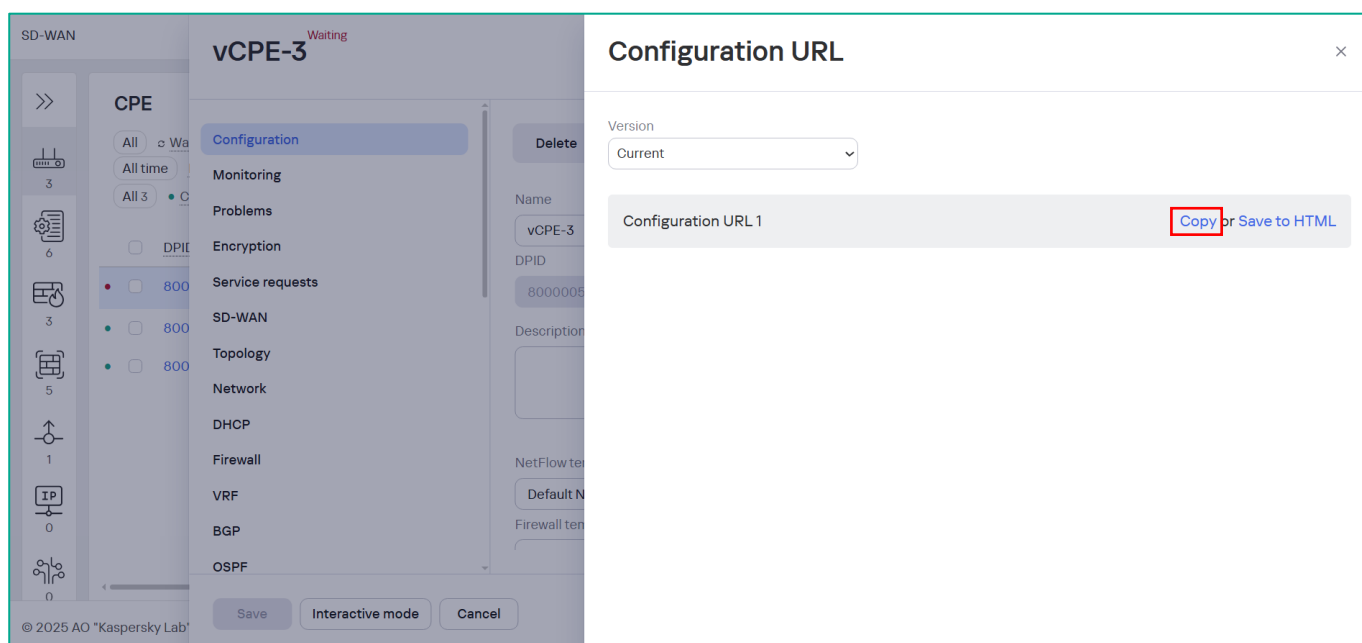


4.14.2. Выполнить настройку vCPE-3 с использованием Configuration URL.

Перейти в меню **SD-WAN** → **CPE**, выбрать устройство CPE и нажать **Get configuration URL**.



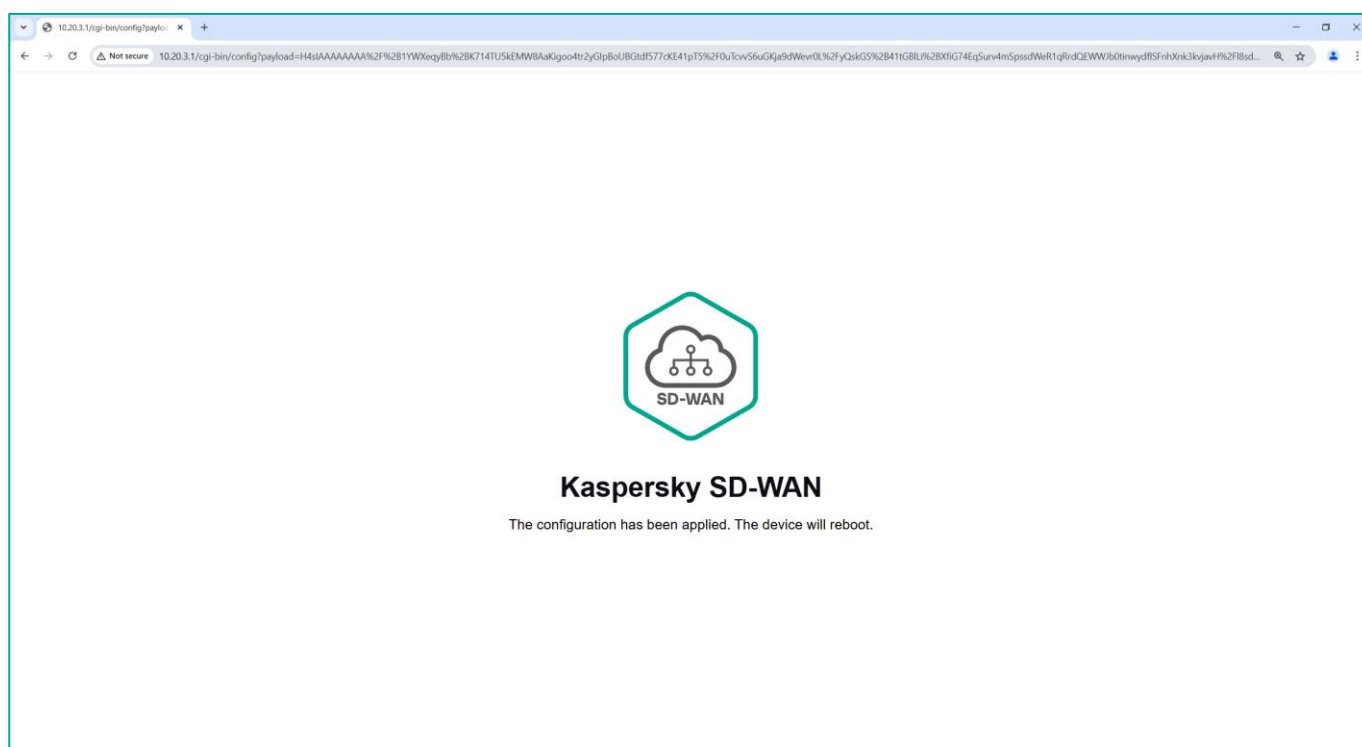
Нажать **Copy**.



Открыть скопированную ссылку в браузере (должна быть связность с интерфейсом lan CPE).

Конфигурация будет передана на устройство CPE, после CPE автоматически перезагрузится.

Configuration URL содержит сетевые настройки, сертификат CA.



После перезагрузки vCPE-3 перейдёт в статус **Registering**.

Registering

vCPE-3

Configuration

Monitoring

Problems

Encryption

Service requests

SD-WAN

Topology

Network

DHCP

Firewall

VRF

BGP

OSPF

DeleteShow passwordGet configuration URLRebootShutdownExport SD-WAN settingsExport network interfaces

NamevCPE-3UNI templateLocationБизнес-центр "Олимпия Парк", 39А с2, Leningrad Avenue, Vaykovsky District, Moscow.

DPID8000005056AAC4FD

CPE templatevCPE-3

Description

NetFlow templateDefault NetFlow template (De...Firewall templatecpe_firewall_template (Demolab)

Device information

Model	SW version	Controller	User	Registered	Update	Management IP	State	Connection
-------	------------	------------	------	------------	--------	---------------	-------	------------

SaveInteractive modeCancel

Появится вкладка **Service Requests**, на которой отображаются сервисные запросы для данного CPE. Будет создан запрос для регистрации CPE.

Registered

vCPE-3

Configuration

Monitoring

Problems

Encryption

Service requests

Tags

Scripts

Reload service requestsCancel all service requests

Name	Created	Task ID	Time	Status	Actions
CpeRegistration	29/04/2025 16:39:08	343e395a-9ee5-42b5-86b7-4b07de42170e	2m 17s	Executed	
CpeApplyConfiguration	29/04/2025 16:41:26	d8c09dfb-21b4-4675-a49f-d237e558ff12	0	Executed	

SaveInteractive modeCancel

Для получения деталей регистрации нажать на Task ID задачи.

Registered

vCPE-3

Configuration

Monitoring

Problems

Encryption

Service requests

Tags

Scripts

SD-WAN

Topology

Network

DHCP

Firewall

VRF

BGP

Save

Interactive mode

CpeRegistration

Created: 29/04/2025 16:39:08

Task ID: 343e395a-9ee5-42b5-86b7-4b07de42170e

Time: 2m 17s

Status: Executed

Name	Status	Time	Attributes
CommutatorAttachCommand	Executed	2m 6s	cluster: SD-WAN Cluster [Demolab: 4f7461d3-0a4b-
CommutatorRenameCommand	Executed	0	name: vCPE-3: 8000005056AAC4FD
CommutatorUpdatePortsStateSet	Executed	0	
CommutatorUpdatePortStateCommand	Executed	0	number: 4800
CommutatorUpdatePortStateCommand	Executed	0	number: 4801
CommutatorSetLinksEncryptionCommand	Executed	0	encrypted: true
CommutatorSetCfmCommand	Executed	0	cfmEnabled: true
CommutatorUpdatePublicPortSettingsSet	Executed	0	
CommutatorUpdatePublicPortSettingsCommand	Executed	0	number: 4800

Refresh

Cancel

vCPE-3 перешло в статус **Registered** и **Connected**.

SD-WAN

+ CPE

>>

3

6

3

5

1

CPE

All

Waiting

Configuration

Registered

Registering

Error

Suspended

Unknown

All time

Last year

Last month

Last week

Last day

29/04/2025 15:29

29/04/2025 15:29

All 3

Connected 0

Disconnected 0

Connection error 0

Need update 0

DPID	Model	Switch type	SW version	Name	Role	Status	State	Connection
8000005056AAC4FD	vKESR-M1	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vCPE-3	CPE	Registered	Enabled	Connected
8000005056AAD2B1	vKESR-M2	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vGW-12	Gateway	Registered	Enabled	Connected
8000005056AA9EA5	vKESR-M2	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vGW-11	Gateway	Registered	Enabled	Connected

Export to CSV...

Настройка vCPE-3 завершена.

4.14.3. Выполнить регистрацию устройств CPE vCPE-3, vCPE-4, vCPE-51 и vCPE-52.

Повторить инструкции 4.14.1 - 4.14.2 для остальных CPE.

Перейти в меню **SD-WAN → CPE**. Все CPE находятся в статусе **Registered** и **Connected**.

CPE

Refresh

Export to CSV...

All

Waiting

Configuration

Registered

Registering

Error

Suspended

Unknown

All time

Last year

Last month

Last week

Last day

29/04/2025 15:29

29/04/2025 15:29

All 6

Connected 0

Disconnected 0

Connection error 0

Need update 0

<input type="checkbox"/>	DPID	Model	Switch type	SW version	Name	Role	Status	State	Connection
<input checked="" type="checkbox"/>	8000005056AAC6B5	vKESR-M1	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vCPE-52	CPE	Registered	Enabled	Connected
<input checked="" type="checkbox"/>	8000005056AAB512	vKESR-M1	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vCPE-51	CPE	Registered	Enabled	Connected
<input checked="" type="checkbox"/>	8000005056AA35FF	vKESR-M1	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vCPE-4	CPE	Registered	Enabled	Connected
<input checked="" type="checkbox"/>	8000005056AAC4FD	vKESR-M1	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vCPE-3	CPE	Registered	Enabled	Connected
<input checked="" type="checkbox"/>	8000005056AAD2B1	vKESR-M2	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vGW-12	Gateway	Registered	Enabled	Connected
<input checked="" type="checkbox"/>	8000005056AA9EA5	vKESR-M2	OVS	knaas-cpe_2.25.03.release.91.bios.amd64	vGW-11	Gateway	Registered	Enabled	Connected

4.14.4. Проверить настройку P2M транспортного сервиса управления.

Перейти в меню **Infrastructure → SD-WAN Cluster → Configuration menu → P2M Services**.

Сервис работает, состояние **UP**.

Устройства CPE автоматически добавляются с ролью **Leaf**.

Infrastructure

Switches

Topology

Segments

P2P services

P2M services

M2M services

IP multicast services

L3 VPN services

TAP services

Service interfaces

Constraints

Traffic filters

OpenFlow port groups

Links

P2M services

+ Create

Search...

Name	Mode	MAC age (sec)	MAC learn mode	MAC table size	MAC table overload	Endpoints	Status	Description
SD-WAN management Tunnel	Classic	300	Learn and flood	2000	Flood	St://VGW-11: 8000005056AA9EA5/p.1, Role: Root St://VGW-12: 8000005056AAD2B1/p.1, Role: Root St://vCPE-3: 8000005056AAC4FD/p.1, Role: Leaf St://vCPE-51: 8000005056AAB512/p.1, Role: Leaf St://vCPE-4: 8000005056AA35FF/p.1, Role: Leaf St://vCPE-52: 8000005056AAC6B5/p.1, Role: Leaf	Up	Management

4.14.5. Проверить подключение устройств CPE к контроллеру.

Перейти в меню **Infrastructure** → **SD-WAN Cluster** → **Configuration menu** → **Switches**.

Все CPE находятся в статусе **Connected**.

Infrastructure																																																																																																																																																																							
Switches																																																																																																																																																																							
<div> <div>Switches</div> <div>Topology</div> <div>Segments</div> <div>P2P services</div> <div>P2M services</div> <div>M2M services</div> <div>IP multicast services</div> <div>L3 VPN services</div> <div>TAP services</div> <div>Service interfaces</div> <div>Constraints</div> <div>Traffic filters</div> <div>OpenFlow port groups</div> <div>Links</div> </div>																																																																																																																																																																							
Switches																																																																																																																																																																							
<div> <div>+ Add</div> <div>Search...</div> </div>																																																																																																																																																																							
<table> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Order</th> <th>Status</th> <th>Connection</th> <th>Bloc...</th> <th>MAC</th> <th>Interfa...</th> <th>Pr...</th> <th>IP</th> <th>Port</th> <th>Created</th> <th>Location</th> <th></th> </tr> <tr> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>se...</th> <th>address</th> <th></th> <th></th> <th></th> <th></th> </tr> <tr> <td><input type="checkbox"/></td> <td>vCPE-3: 8000005056AAC4FD</td> <td>3</td> <td>Active</td> <td>Connected</td> <td>No</td> <td>00:50:56:aa:c4:fd</td> <td>sdwan0</td> <td>Yes</td> <td>10.50.5.9</td> <td>34946</td> <td>29/04/2025</td> <td>Moscow, Leningrad Avenue, 39A c2</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>vCPE-4: 8000005056AA35FF</td> <td>5</td> <td>Active</td> <td>Connected</td> <td>No</td> <td>00:50:56:aa:35:ff</td> <td>sdwan1</td> <td>No</td> <td>10.50.6.1</td> <td>52378</td> <td>29/04/2025</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>sdwan0</td> <td>Yes</td> <td>10.50.6.1</td> <td>56942</td> <td>16:50:31</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>vCPE-51: 8000005056AAB512</td> <td>4</td> <td>Active</td> <td>Connected</td> <td>No</td> <td>00:50:56:aa:b5:12</td> <td>sdwan0</td> <td>Yes</td> <td>10.50.7.8</td> <td>39176</td> <td>29/04/2025</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>sdwan1</td> <td>No</td> <td>10.50.8.1</td> <td>45890</td> <td>16:48:32</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>vCPE-52: 8000005056AAC6B5</td> <td>6</td> <td>Active</td> <td>Connected</td> <td>No</td> <td>00:50:56:aa:c6:b5</td> <td>sdwan0</td> <td>Yes</td> <td>10.50.7.9</td> <td>40524</td> <td>29/04/2025</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>sdwan1</td> <td>No</td> <td>10.50.8.1</td> <td>33584</td> <td>16:51:47</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>vGW-11: 8000005056AA9EA5</td> <td>1</td> <td>Active</td> <td>Connected</td> <td>No</td> <td>00:50:56:aa:9e:a5</td> <td>sdwan0</td> <td>Yes</td> <td>10.50.1.1</td> <td>45014</td> <td>29/04/2025</td> <td>Moscow, Leningrad Avenue, 39A c2</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>vGW-12: 8000005056AAD2B1</td> <td>2</td> <td>Active</td> <td>Connected</td> <td>No</td> <td>00:50:56:aa:d2:b1</td> <td>sdwan0</td> <td>Yes</td> <td>10.50.2.1</td> <td>56938</td> <td>29/04/2025</td> <td>Moscow, Leningrad Avenue, 39A c2</td> <td></td> </tr> </table>														<input type="checkbox"/>	Name	Order	Status	Connection	Bloc...	MAC	Interfa...	Pr...	IP	Port	Created	Location										se...	address					<input type="checkbox"/>	vCPE-3: 8000005056AAC4FD	3	Active	Connected	No	00:50:56:aa:c4:fd	sdwan0	Yes	10.50.5.9	34946	29/04/2025	Moscow, Leningrad Avenue, 39A c2		<input type="checkbox"/>	vCPE-4: 8000005056AA35FF	5	Active	Connected	No	00:50:56:aa:35:ff	sdwan1	No	10.50.6.1	52378	29/04/2025										sdwan0	Yes	10.50.6.1	56942	16:50:31			<input type="checkbox"/>	vCPE-51: 8000005056AAB512	4	Active	Connected	No	00:50:56:aa:b5:12	sdwan0	Yes	10.50.7.8	39176	29/04/2025										sdwan1	No	10.50.8.1	45890	16:48:32			<input type="checkbox"/>	vCPE-52: 8000005056AAC6B5	6	Active	Connected	No	00:50:56:aa:c6:b5	sdwan0	Yes	10.50.7.9	40524	29/04/2025										sdwan1	No	10.50.8.1	33584	16:51:47			<input type="checkbox"/>	vGW-11: 8000005056AA9EA5	1	Active	Connected	No	00:50:56:aa:9e:a5	sdwan0	Yes	10.50.1.1	45014	29/04/2025	Moscow, Leningrad Avenue, 39A c2		<input type="checkbox"/>	vGW-12: 8000005056AAD2B1	2	Active	Connected	No	00:50:56:aa:d2:b1	sdwan0	Yes	10.50.2.1	56938	29/04/2025	Moscow, Leningrad Avenue, 39A c2	
<input type="checkbox"/>	Name	Order	Status	Connection	Bloc...	MAC	Interfa...	Pr...	IP	Port	Created	Location																																																																																																																																																											
								se...	address																																																																																																																																																														
<input type="checkbox"/>	vCPE-3: 8000005056AAC4FD	3	Active	Connected	No	00:50:56:aa:c4:fd	sdwan0	Yes	10.50.5.9	34946	29/04/2025	Moscow, Leningrad Avenue, 39A c2																																																																																																																																																											
<input type="checkbox"/>	vCPE-4: 8000005056AA35FF	5	Active	Connected	No	00:50:56:aa:35:ff	sdwan1	No	10.50.6.1	52378	29/04/2025																																																																																																																																																												
							sdwan0	Yes	10.50.6.1	56942	16:50:31																																																																																																																																																												
<input type="checkbox"/>	vCPE-51: 8000005056AAB512	4	Active	Connected	No	00:50:56:aa:b5:12	sdwan0	Yes	10.50.7.8	39176	29/04/2025																																																																																																																																																												
							sdwan1	No	10.50.8.1	45890	16:48:32																																																																																																																																																												
<input type="checkbox"/>	vCPE-52: 8000005056AAC6B5	6	Active	Connected	No	00:50:56:aa:c6:b5	sdwan0	Yes	10.50.7.9	40524	29/04/2025																																																																																																																																																												
							sdwan1	No	10.50.8.1	33584	16:51:47																																																																																																																																																												
<input type="checkbox"/>	vGW-11: 8000005056AA9EA5	1	Active	Connected	No	00:50:56:aa:9e:a5	sdwan0	Yes	10.50.1.1	45014	29/04/2025	Moscow, Leningrad Avenue, 39A c2																																																																																																																																																											
<input type="checkbox"/>	vGW-12: 8000005056AAD2B1	2	Active	Connected	No	00:50:56:aa:d2:b1	sdwan0	Yes	10.50.2.1	56938	29/04/2025	Moscow, Leningrad Avenue, 39A c2																																																																																																																																																											

4.14.6. Проверить построение GENEVE туннелей между CPE.

Перейти в раздел **Links** и проверить построенные GENEVE туннели между SD-WAN шлюзами и CPE.

От всех CPE созданы линки до каждого шлюза с обоих интерфейсов sdwan в двух направлениях.

Infrastructure

Switches

Topology

Segments

P2P services

P2M services

M2M services

IP multicast services

L3 VPN services

TAP services

Service interfaces

Constraints

Traffic filters

OpenFlow port groups

Links

Links

Set default utilization

Discovered links

Active links

Source	NAT/Disjoint src	Source IP/port	Destination	NAT/Disjoint dst	Destination
vCPE-4: 8000005056AA35FF : 4800	10.50.5.10:4800	N	vGW-11: 8000005056AA9EA5 : 4800	10.50.1.11:4800	N
vCPE-4: 8000005056AA35FF : 4801	10.50.6.16:4801	N	vGW-11: 8000005056AA9EA5 : 4800	10.50.1.11:4800	N
vCPE-4: 8000005056AA35FF : 4800	10.50.5.10:4800	N	vGW-12: 8000005056AAD2B1 : 4800	10.50.2.12:4800	N
vCPE-4: 8000005056AA35FF : 4801	10.50.6.16:4801	N	vGW-12: 8000005056AAD2B1 : 4800	10.50.2.12:4800	N
vGW-11: 8000005056AA9EA5 : 4800	10.50.1.11:4800	N	vCPE-4: 8000005056AA35FF : 4800	10.50.5.10:4800	N
vGW-11: 8000005056AA9EA5 : 4800	10.50.1.11:4800	N	vCPE-4: 8000005056AA35FF : 4801	10.50.6.16:4801	N
vGW-11: 8000005056AA9EA5 : 4800	10.50.1.11:4800	N	vCPE-51: 8000005056AAB512 : 4800	10.50.7.8:4800	N
vGW-11: 8000005056AA9FA5 : 4800	10.50.1.11:4800	N	vCPE-51: 8000005056AAB512 : 4801	10.50.8.17:4801	N

5. Управление трафиком

5.1. Настройка транспортного сервиса L2 M2M

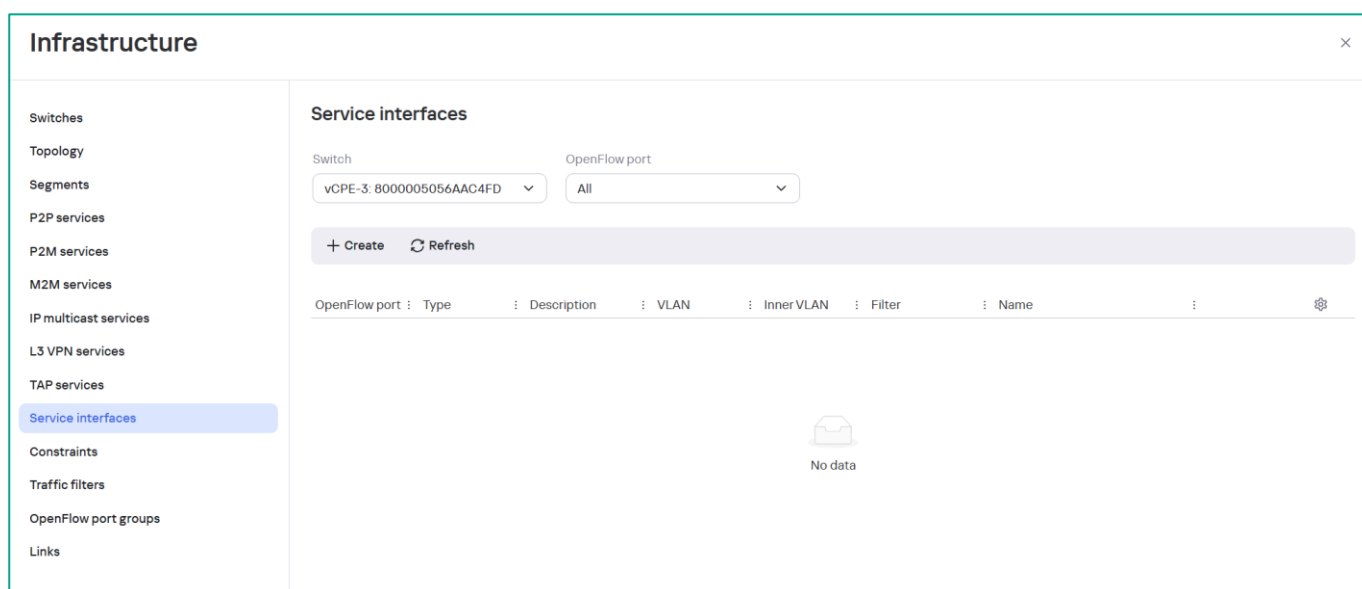
Топология Hub-and-Spoke является наиболее распространенной при построении сетей SD-WAN. По умолчанию CPE автоматически строят линки до устройств с ролью шлюз.

Для обеспечения связности поверх построенных линков необходимо создать транспортный сервис. В рамках PoC используется сервис L2 типа Multipoint-to-Multipoint (E-LAN в классификации MEF).

M2M – это транспортный сервис, в рамках которого трафик передается между несколькими сервисными интерфейсами без иерархии.

5.1.1. Создать сервисные интерфейсы.

Перейти в меню **Infrastructure** → **SD-WAN Cluster** → **Configuration menu** → **Service Interfaces**.



Выбрать устройство CPE, затем нажать **+ Create**.

Задать:

- **OpenFlow port: 2 (ovs-lan)**. Данный порт ovs связан с интерфейсом overlay CPE.
- **Type: Access** (на интерфейсе будут приниматься как тегированные, так и нетегированные кадры).

Нажать **Create**.

Повторить для всех шлюзов и устройств CPE.

5.1.2. Создать транспортный сервис L2 типа M2M.

Перейти в меню **Infrastructure** → **SD-WAN Cluster** → **Configuration menu** → **M2M Services** и нажать **+ Create**.

Задать имя сервиса и нажать **Next**.

New M2M service

Name

L2 M2M

Constraint

Threshold

Balancing mode ⓘ

Per-flow

MAC learn mode

Learn and flood

MAC age (sec)

300

MAC table overload

Flood

MAC table size

100

Description

Cancel

Back

Next

В секции **Service endpoints** нажать **+ Add** и добавить сервисные интерфейсы, созданные в п. 0.

Задать параметры service endpoints:

- **Switch:** поочередно выбрать все CPE и шлюзы (в PoC транспортный сервис M2M настраивается для всех устройств).
- **Service interface: Port 2 Access.**
- **QoS: Unlimited-QoS.**

Нажать **Next**.

New M2M service

Service endpoints

+ Add

Switch	Service interface	QoS rule	Inbound filter	Backup switch	Backup service interface
vCPE-3: 8000005056AAC4FD	Port 2, Access	Unlimited-QoS	—	—	—
vCPE-4: 8000005056AA35FF	Port 2, Access	Unlimited-QoS	—	—	—
vCPE-51: 8000005056AAB5...	Port 2, Access	Unlimited-QoS	—	—	—
vCPE-52: 8000005056AAC6...	Port 2, Access	Unlimited-QoS	—	—	—
vGW-11: 8000005056AA9E...	Port 2, Access	Unlimited-QoS	—	—	—
vGW-12: 8000005056AAD2...	Port 2, Access	Unlimited-QoS	—	—	—

Cancel

Back

Next

Оставить значения по умолчанию и нажать **Create** для создания транспортного сервиса.

New M2M service

Port groups

+ Add

Cancel

Back

Create

Транспортный сервис M2M создан.

Сервис работает и находится в состоянии **UP**.

Infrastructure

Switches
Topology
Segments
P2P services
P2M services
M2M services
IP multicast services
L3 VPN services
TAP services
Service interfaces
Constraints
Traffic filters
OpenFlow port groups
Links

M2M services

+ Create

Search...

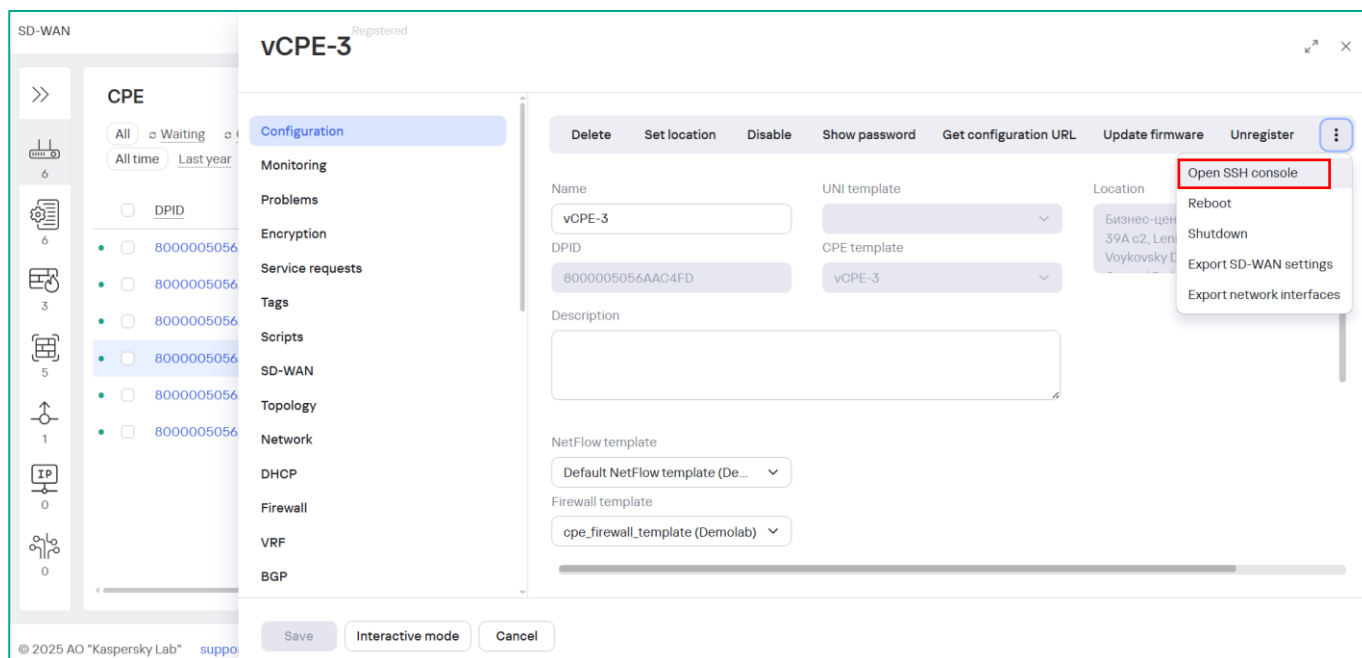
All Up Down Degraded

Name	MAC age (sec)	MAC learn mode	MAC table size	MAC table overload	Endpoints	Status	Description
L2 M2M	300	Learn and flood	100	Flood	St://vCPE-3: 8000005056AAC4FD/p:2 St://vCPE-4: 8000005056AA35FF/p:2 St://vCPE-51: 8000005056AAB512/p:2 St://vCPE-52: 8000005056AAC6B5/p:2 St://vGW-11: 8000005056AA9EA5/p:2 St://vGW-12: 8000005056AAD2B1/p:2	Up	Management

6. Проверка работы протоколов BGP и VRRP на CPE

6.1.1. Проверить работу BGP на vCPE-3.

Перейти в меню **SD-WAN** → **CPE**, выбрать устройство CPE и нажать **Open SSH Console**, после чего в браузере откроется SSH сессия к CPE, также возможно подключиться к устройству CPE в отдельной сессии SSH.



Note: Для просмотра пароля CPE требуется выбрать в меню SD-WAN → CPE нужное устройство CPE, затем нажать **Show password**. Пользователь по умолчанию: **root**.

Для BGP используется FRRouting. Перейти в shell FRR:

```
vttysh
```

Выполнить команды:

```
show ip route
```

```
show ip bgp sum
```

```
show run
```


В таблице маршрутизации есть маршруты, полученные по BGP от CPE.

Установлены сессии BGP до шлюзов.

```
8000005056AAC4FD# show ip bgp summary

IPv4 Unicast Summary (VRF default):
BGP router identifier 172.16.1.3, local AS number 65500 vrf-id 0
BGP table version 8
RIB entries 13, using 2496 bytes of memory
Peers 2, using 1449 KiB of memory

Neighbor      V      AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd  PfxSnt  Desc
172.16.1.11    4      65500    225     219      0     0     0 00:35:50        6          1 N/A
172.16.1.12    4      65500    225     219      0     0     0 00:35:50        6          1 N/A

Total number of neighbors 2
8000005056AAC4FD#
```

6.1.2. Проверить работу BGP на vGW-11.

Подключиться к SD-WAN шлюзу по SSH.

Выполнить команду:

ip r

```
-----
CPEOS knaas-cpe_2.24.09.release.28.amd64, 1730242530
-----

root@8000005056AA9EA5:~# ip r
default via 10.1.4.1 dev eth0 proto static src 10.1.4.11 metric 1
10.0.1.0/24 nhid 91 via 10.1.3.13 dev eth1 proto bgp metric 20
10.1.1.0/24 nhid 91 via 10.1.3.13 dev eth1 proto bgp metric 20
10.1.3.0/24 dev eth1 proto kernel scope link src 10.1.3.11
10.1.4.0/24 dev eth0 proto static scope link metric 100
10.11.13.0/24 dev br-nfvmgmt proto kernel scope link src 10.11.13.73
10.20.3.0/24 nhid 106 via 172.16.1.3 dev overlay proto bgp metric 20
10.20.4.0/24 nhid 108 via 172.16.1.4 dev overlay proto bgp metric 20
10.20.5.0/24 nhid 112 proto bgp metric 20
        nexthop via 172.16.1.52 dev overlay weight 1
        nexthop via 172.16.1.51 dev overlay weight 1
172.16.1.0/24 dev overlay proto kernel scope link src 172.16.1.11
root@8000005056AA9EA5:~#
```

В таблице маршрутизации есть маршруты, полученные по BGP от CPE.

6.1.3. Проверить связность между wst3, wst4, wst5, srv1 и orc1.

Note: wst3, wst4 и wst5 получают динамические адреса по DHCP. Требуется повторно запросить IPv4 адреса с рабочих станций после настройки CPE.

Подключится к хосту wst3 через SSH.

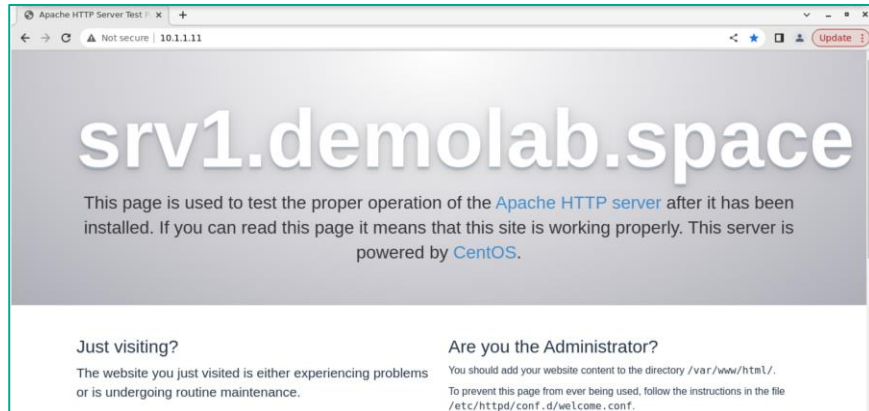
Запустить команду ping поочередно до IP-адресов хостов wst4, wst5, srv1 и orc1.

```
[root@wst3 ~]# ping 10.20.4.171
PING 10.20.4.171 (10.20.4.171) 56(84) bytes of data.
64 bytes from 10.20.4.171: icmp_seq=1 ttl=62 time=6.97 ms
64 bytes from 10.20.4.171: icmp_seq=2 ttl=62 time=2.67 ms
^C
--- 10.20.4.171 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.675/4.825/6.975/2.150 ms
[root@wst3 ~]# ping 10.20.5.200
PING 10.20.5.200 (10.20.5.200) 56(84) bytes of data.
64 bytes from 10.20.5.200: icmp_seq=1 ttl=62 time=8.28 ms
64 bytes from 10.20.5.200: icmp_seq=2 ttl=62 time=2.89 ms
^C
--- 10.20.5.200 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.897/5.592/8.288/2.696 ms
[root@wst3 ~]# ping 10.1.1.11
PING 10.1.1.11 (10.1.1.11) 56(84) bytes of data.
64 bytes from 10.1.1.11: icmp_seq=1 ttl=61 time=3.49 ms
```

ICMP ping проходит успешно.

Повторить для хостов wst4 и wst5.

6.1.4. 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.

6.1.5. Проверить работу VRRP на vCPE-51 и vCPE-52.

Подключится к vCPE-51 и проверить, что vIP (10.20.5.1) назначен на интерфейс eth2:

```
ip --br a | grep eth2
```

```
-----
CPEOS knaas-cpe_2.24.09.release.28.amd64, 1730242530
-----
root@8000005056AAB512:~# ip -br a | grep eth2
eth2                UP                10.20.5.2/24 10.20.5.1/24 fe80::250:56ff:feaa:dd49/64
root@8000005056AAB512:~#
```

Подключится к wst5 и проверить сетевую связность до хоста org1 или внешних ресурсов:

```
ping 10.0.1.11
```

```
ping 8.8.8.8
```

```
[root@wst5 ~]# ping 10.0.1.11
PING 10.0.1.11 (10.0.1.11) 56(84) bytes of data.
64 bytes from 10.0.1.11: icmp_seq=1 ttl=61 time=4.08 ms
64 bytes from 10.0.1.11: icmp_seq=2 ttl=61 time=2.13 ms
^C
--- 10.0.1.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.136/3.112/4.088/0.976 ms
[root@wst5 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=17.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=13.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 13.762/15.698/17.635/1.940 ms
```

Отключить **lan** интерфейс (**eth2**) на vCPE-51:

```
ip link set dev eth2 down
```

Подключится к vCPE-52.

Проверить, что VRRP назначил виртуальный IP-адрес на **lan** интерфейс (**eth2**) данного CPE:

```
ip --br a | grep eth2
```

```
-----
CPEOS knaas-cpe_2.24.09.release.28.amd64, 1730242530
-----
root@8000005056AAC6B5:~# ip --br a | grep eth2
eth2                UP                10.20.5.3/24 10.20.5.1/24 fe80::250:56ff:feaa:f104/64
root@8000005056AAC6B5:~#
```

Подключится к wst5 и проверить сетевую связность до хоста ocs1 или внешних ресурсов.

```
ping 10.0.1.11
```

```
ping 8.8.8.8
```

```
[root@wst5 ~]# ping 10.0.1.11
PING 10.0.1.11 (10.0.1.11) 56(84) bytes of data.
64 bytes from 10.0.1.11: icmp_seq=1 ttl=61 time=4.08 ms
64 bytes from 10.0.1.11: icmp_seq=2 ttl=61 time=2.13 ms
^C
--- 10.0.1.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.136/3.112/4.088/0.976 ms
[root@wst5 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=17.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=13.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 13.762/15.698/17.635/1.940 ms
```

Вернуть настройки после завершения теста.

Требуется включить обратно интерфейс **lan(eth2)** на vCPE-51.

Подключиться к vCPE-51 через веб консоль (т.к. интерфейс lan отключен) и выполнить:

```
ip link set dev eth2 up
```

Проверить, что виртуальный IP-адрес вернулся на **lan** интерфейс (**eth2**) данного CPE (vCPE-51 перейдет в статус MASTER через промежуток времени, который определяется по формуле **3 x Advertise interval + skew_time (256 - Priority) / 256**)). Пример расчёта: $5\text{ s} + (256 - 101) / 256 = 0.605$

```
ip --br a | grep eth2
```

```
root@8000005056AAB512:~# ip --br a | grep eth2
eth2                UP                10.20.5.2/24 10.20.5.1/24 fe80::250:56ff:feaa:dd49/64
root@8000005056AAB512:~#
```

7. Обновление компонентов системы управления Kaspersky SD-WAN

7.1.1. Подготовить хост оркестратора для обновления SD-WAN.

Загрузить архив **knaas-installer.<release_name>.amd64_russia_en-US_ru-RU.tar.gz** с новой версией контейнеров и плейбуками установки компонентов системы управления Kaspersky SD-WAN в домашний каталог пользователя **sdwan** на хост **orc1**.

При обновлении используется файл **/home/sdwan/poc_aio.yml** с переменными для обновления, подготовленный в п. 3.2.6.

7.1.2. Запустить процесс 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 развёрнутой версией контейнер изменён не будет.

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

Задать параметр согласия с EULA:

```
export KNAAS_EULA_AGREED="true"
```

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

```
cd knaas-installer.<release_name>.cis.amd64_en-US_ru-RU/
```

Затем запустить плейбук установки, указав в нём путь к файлу с паролем vault. При запуске плейбука будет запрошен пароль sudo:

Note: Необходимо проверить пути до файла с параметрами установки и файла с паролем vault и изменить при необходимости!

```
ansible-playbook -i inventory/generic -e "@/home/sdwan/poc_aio.yml" -e "@inventory/external/images.yml" -K --vault-password-file \${HOME}/passwords/vault_password.txt knaas/knaas-install.yml
```

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

7.1.3. Очистить историю команд.

```
history -c && history -w
```

Приложение А. 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 -F INPUT ACCEPT
iptables -F FORWARD ACCEPT
iptables -F 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

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

```
-----  
  
R13  
-----  
  
!  
  
#Очистить iptables:  
iptables -F INPUT ACCEPT  
iptables -F FORWARD ACCEPT  
iptables -F 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

Note: При изменении IP плана из пункта 2.4 использовать новый IP-адрес хоста ors1 и публичный IP-адрес (заменить 10.0.1.11 и 10.50.1.14).

```
-----  
  
R14  
  
-----  
  
#Очистить iptables:  
  
iptables -F INPUT ACCEPT  
iptables -F FORWARD ACCEPT  
iptables -F 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
iptables -t nat -A PREROUTING -p tcp --dport 10051 -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 -F INPUT ACCEPT

iptables -F FORWARD ACCEPT

iptables -F 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 -- 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 -F INPUT ACCEPT

iptables -F FORWARD ACCEPT

iptables -F 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 -- 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

Приложение Б. Программа и методика испытаний

Note: Все проверки должны выполняться последовательно.

N	Название проверки	Пункт PoC	Методика проверки	Ожидаемый результат	Фактический результат, комментарии
Базовая настройка оркестратора					
1	Авторизация в веб-интерфейсе оркестратора.	3.3.1	<ol style="list-style-type: none"> 1. Открыть URL веб-интерфейса оркестратора в браузере. 2. Ввести учетные данные администратора системы и нажать Login. 	Авторизация проходит без ошибок, открывается раздел Dashboard.	
2	Смена пароля пользователя.	3.3.2	<ol style="list-style-type: none"> 1. В веб-интерфейсе оркестратора перейти в меню Users. 2. Выбрать пользователя Administrator. 3. Нажать Management → Change password, ввести новый пароль и нажать Save. 	Пароль пользователя admin успешно изменен.	
3	Проверка созданного домена.	4.1.1	<ol style="list-style-type: none"> 1. В веб-интерфейсе оркестратора перейти в меню Infrastructure. 2. В секции Resources выбрать Domain. 	Добавленный домен отображается в списке ресурсов.	
4	Проверка созданного центра обработки данных.	4.1.2	<ol style="list-style-type: none"> 1. В веб-интерфейсе оркестратора перейти в меню Infrastructure. 2. В секции Resources выбрать Data center. 	Добавленный центр обработки данных отображается в списке ресурсов.	
5	Подключение к системе мониторинга Zabbix.	4.1.3	<ol style="list-style-type: none"> 1. В веб-интерфейсе оркестратора перейти в меню System → Monitoring. 2. Нажать кнопку Test connection. 	Подключение успешно настроено, успешно проходит тест соединения.	

N	Название проверки	Пункт PoC	Методика проверки	Ожидаемый результат	Фактический результат, комментарии
6	Проверка настроек Zabbix Proxy.	4.1.4	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Infrastructure → System resources. Проверить настройки Zabbix proxy. 	Настроенные параметры Zabbix proxy отображаются в интерфейсе оркестратора.	
7	Проверка созданного пула IP-адресов для сети управления.	4.1.5	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Infrastructure → IPAM. Проверить пул сети управления, созданный в ходе выполнения PoC. 	Добавленный пул IP-адресов отображается в списке подсетей.	
8	Проверка настроек дескриптора PNF контроллера.	4.1.7-4.1.9	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Catalog. В секции Physical network functions найти добавленный дескриптор PNF контроллера. Проверить соответствие параметров во вкладках с настройками, сделанными в ходе выполнения PoC. 	Дескриптор PNF контроллера успешно добавлен в оркестратор и настроен.	
9	Проверка шаблона сервиса SD-WAN.	4.3	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Catalog. В секции Templates найти созданный шаблон сервиса SD-WAN. Проверить соответствие параметров во вкладках с настройками, сделанными в ходе выполнения PoC. 	Шаблон сервиса SD-WAN создан и добавлен в оркестратор.	
10	Создание Tenant.	4.4.1	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Tenants. Просмотреть список тенантов. 	Созданный тенант успешно отображается в секции Tenants .	
11	Добавление пользователя в tenant.	4.4.2	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Tenants. Выбрать, созданный в ходе выполнения PoC, тенант. Проверить добавленных пользователей в секции Users тенанта. 	Пользователь успешно добавлен в tenant и отображается в секции Users тенанта.	

N	Название проверки	Пункт PoC	Методика проверки	Ожидаемый результат	Фактический результат, комментарии
12	Проверка развернутого сервиса SD-WAN.	4.4.1-4.4.7	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → SD-WAN instances. Найти развернутый в ходе выполнения PoC сервис SD-WAN. 	Развертывание сервиса SD-WAN проведено успешно: в веб-интерфейсе оркестратора для развернутого сервиса отображается индикатор зеленого цвета.	
13	Проверка добавленного сертификата CA для устройств CPE.	4.7	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → Certificates. Просмотреть загруженные сертификаты. 	Добавленный CA сертификат отображается в веб-интерфейсе оркестратора.	
Работа с устройствами CPE и SD-WAN шлюзами					
14	Проверка шаблонов SD-WAN шлюзов.	4.6	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → CPE templates. Найти шаблоны SD-WAN шлюзов. 	1. Шаблоны SD-WAN шлюзов отображаются в оркестраторе с настройками, соответствующими PoC.	
15	Проверка шаблонов устройств CPE.	4.13	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → CPE templates. Найти шаблоны устройств CPE. 	1. Шаблоны устройств CPE отображаются в оркестраторе с настройками, соответствующими PoC.	
16	Проверка новых зон межсетевого экрана.	4.5.1, 4.12.1	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → Firewall zones. Найти настроенные зоны. 	1. Добавленные зоны отображаются в оркестраторе.	
17	Проверка шаблонов межсетевого экрана.	4.5, 4.12	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → Firewall templates. Найти шаблоны межсетевого экрана. 	1. Шаблоны межсетевого экрана отображаются в списке шаблонов с настройками, соответствующими PoC.	

N	Название проверки	Пункт PoC	Методика проверки	Ожидаемый результат	Фактический результат, комментарии
18	Проверка подключения SD-WAN шлюзов.	4.9.1-4.9.4	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → CPE. Проверить статус SD-WAN шлюзов. 	<ol style="list-style-type: none"> SD-WAN шлюзы успешно добавлены в оркестратор и находятся в статусе Registered. 	
19	Проверка транспортного сервиса управления.	4.10	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Infrastructure → SD-WAN Cluster → Configuration menu → P2M services. В отобразившемся меню найти сервис SD-WAN managementTunnel. 	<ol style="list-style-type: none"> Сервис SD-WAN managementTunnel находится в статусе UP. 	
20	Проверка подключения устройств CPE.	4.14.1-4.14.3	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → CPE. Проверить статус устройств CPE. 	<ol style="list-style-type: none"> Устройства CPE успешно добавлены в оркестратор и находятся в статусе Registered. 	
21	Доступ к CLI консоли CPE из web-интерфейса оркестратора.	4.10.3	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → CPE. Выбрать vcPE-3. В меню Configuration нажать Open SSH console для запуска веб-консоли к CPE. Повторить для остальных устройств CPE и SD-WAN шлюзов. 	<ol style="list-style-type: none"> CLI консоль CPE успешно открывается из web-интерфейса оркестратора. 	
22	Проверка работы подсистемы мониторинга.	4.9.7	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню SD-WAN → CPE. Выбрать vcPE-3. Перейти на вкладку Monitoring и поочередно выбрать в селекторе данные для отображения. Повторить для остальных устройств CPE и SD-WAN шлюзов. 	<ol style="list-style-type: none"> Подсистема мониторинга работает, в web-интерфейсе оркестратора успешно отображается статистика для всех устройств CPE. 	

N	Название проверки	Пункт PoC	Методика проверки	Ожидаемый результат	Фактический результат, комментарии
23	Проверка автоматического создания линков между шлюзами и CPE.	4.9.5, 4.14.6	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Infrastructure → SD-WAN Cluster → Configuration menu → Links. Просмотреть отобразившейся список построенных линков. 	<ol style="list-style-type: none"> GENEVE туннели успешно построены в обе стороны между всеми интерфейсами SD-WAN шлюзов и устройств CPE. 	
Работа с транспортными сервисами					
24	Проверка созданных сервисных интерфейсов.	0	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Infrastructure → SD-WAN Cluster → Configuration menu → Service Interfaces. Выбрать устройство vCPE-3 и порт 2 (ovs-lan) для отображения списка сервисных интерфейсов CPE. Найти созданный интерфейс типа access. Повторить для остальных устройств CPE и шлюзов 	<ol style="list-style-type: none"> Сервисные интерфейсы для всех устройств CPE и SD-WAN шлюзов успешно созданы. 	
25	Проверка M2M транспортного сервиса.	5.1.2	<ol style="list-style-type: none"> В веб-интерфейсе оркестратора перейти в меню Infrastructure → SD-WAN Cluster → Configuration menu → M2M services. В отобразившемся меню найти M2M транспортный сервис. 	<ol style="list-style-type: none"> M2M транспортный сервис успешно создан и находится в статусе UP. 	

kaspersky

kaspersky

<https://kaspersky.ru/>
<https://securelist.ru>

© 2025 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.